Risk Management: Faculty of Business and Law

This thesis is submitted in partial fulfillment of the requirements for a doctorate degree within the Faculty of Business and Law at the University of Portsmouth

Humanitarian Aid and Development Sector Resilience Finding Solutions to Complex Problems

Submitted by: Michael Blyth

Student No: UP840253

Word Count: 54,910

Signed: 

Dated: 13th September 2021

ABSTRACT

The research employs a sequential mixed methods research strategy to explore organizational resilience within the humanitarian aid and development sector. The research builds on existing literature focused on sectoral resilience, while also encompassing out-of-sector literature focused on resilience, business continuity, security risk management, and emergency and crisis management. The research methodology includes three tools of data gathering: 1) an online survey, 2) semi-structured interviews, and 3) a competency framework focus group. The research examines the sector as a multi-billion-dollar enterprise which represents millions of organizations with hundreds of millions of employees and volunteers operating worldwide (Boris, 2013) which is, by its very nature, is drawn towards danger. The research examines the role of the sector within responding to complex global health emergencies, natural disasters and deteriorating security conditions (Dilley et all, 2005), and the imperative for individuals to deploy to—or work in—increasingly fragile and dynamic environments. The research places the competing demands of supporting beneficiaries in high-risk environments with the increasing duty of care expectations from employees, families, donors and governments (Kemp and Merkelbach, 2011), and considers the need for high-reliability organizations (La Porte, 1996) which can work effectively within high-risk conditions. The research explores the requirement for a security culture (Wenger, 2017), the growing need to professionalize security within the sector, the importance of recognized standards, the value of knowledge production (Gibbons et al, 2002), and the role forum groups and associations play in consolidating and articulating best practice. The research highlights the absence of a consistent approach to organizational resilience and offers action-based outcomes in the form of a Hybrid Model of Security and Resilience which addresses four key areas: 1) the hierarchy of security, 2) competency accelerants, 3) professional convergence, and 4) the need to both implement and evidence effective resilience measures.

Keywords

Resilience; security; business continuity; emergency; crisis; disaster; threat; risk; disruption; incident; reliability; standards; knowledge production; NGO; humanitarian aid and development.

Table of Contents

Acknowledgments

The author would like to thank the following for their professional guidance in the preparation of this thesis: My two supervisors, Dr. Risto Talas and Dr. Emre Cinar whose advice, enthusiasm and insights have been invaluable. My thanks also to my wife Kristen, whose patience and motivation was a driving force for my studies.

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Full Name
AED	Academy for Educational Development
ALARP	As Low As Practically Possible
ANSO	Afghanistan NGO Safety Office
APP	Associate Protection Professional
ASIS	American Society for Industrial Security
AU	African Union
BINGO	Baluchistan INGO Consortium
BSI	British Standards Institute
CoE	Council of Europe
CHCF	Core Humanitarian Competencies Framework
COSO	Committee of Sponsoring Organizations for the Treadway Commission
CPP	Certified Protection Professional
DFID	Department for International Development
DRC	Danish Refugee Council
DSN	Dutch Security Network
ECHO	European Commission Humanitarian Aid
EISF	European Interagency Security Forum (now GISF)
FHA	Foreign Humanitarian Assistance
GISF	Global Interagency Security Forum
HAD	Humanitarian Aid and Development
HEAT	Hostile Environment Awareness Training
ICT	Information Communications and Technology
ILM	Institute of Leadership Management
INSSA	International NGO Safety and Security Association
INSO	International NGO Safety Organization
IRD	International Relief and Development
ISO	International Standards Organization
JICA	Japanese International Cooperation Agency
MOSS	Minimum Operating Security Standards
NATO	North Atlantic Treaty Organization
NGO	Non-Governmental Organization
NGO-SPAS	NGO Security Preparedness and Support Project
NCCI	NGO Coordination Committee in Iraq

NRC	Norwegian Refugee Council
OSAC	Overseas Security Advisory Council
OSCE	Organization for Security and Co-operation in Europe
OFDA	Office of U.S. Foreign Disaster Assistance
PLSO	Partner Liaison Security Operations
PSP	Physical Security Professional
SSAFE	Safe and Secure Approaches in Field Environments
SAG	Security Advisory Group
SFP	Security Focal Point
SMOM	Security Management Operations Manual
SOP	Standard Operating Practice
SPM	Security Management Policy
TWG	Training Working Group
UN	United Nations
UNDP	United Nations Development Program
UNDSS	United Nations Department of Safety and Security
UNHCR	United Nations Refugee Agency
UNICEF	United Nations Children's Fund
UNSMS	United Nations Security Management System
USAID	United States Agency for International Development

CHAPTER 1

INTRODUCTION

Background

In the first two decades of the 21st century the humanitarian aid and development community has seen significant changes to the risks it faces, as well as to the levels of accountability it is held to, by both donors and its own employees. The sector operates in high-risk, dynamic, and remote environments that face heightened threats, both human and natural in origin (Maren, 1997). While other companies typically avoid or withdraw from such environments as conditions worsen, organizations within the humanitarian aid and development community actively head towards the danger. Research by Kovacs and Spens (2011) suggest that about three percent of disasters can be attributed to natural causes, and that more relate to political crises, and wars. Research by Smet, Schreurs and Leysen (2015) also indicate that disasters are not only growing in frequency but are also presenting more complex operating environments that seem to distress humanity to a considerably higher degree than in the past. The USAID **U.S Agency for International Development Risk Appetite Statement** (USAID, 2018) defines the importance of Enterprise Risk Management (ERM) and the need to address programmatic, fiduciary, reputational, legal, security, human-capital and information-technology risks. Risk management, notably within non-permissive environments, requires effective resilience strategies for organizations to perform effectively, protecting not only people, but also the business interests of those supporting beneficiaries in either conflict, disaster struck or otherwise high-risk and uncertain environments.

As a result of escalating natural disasters and human conflict there are increasing levels of aid operations working in high-risk and uncertain environments. Logically, this requires a commensurate level of resilience to manage elevations in risk and uncertainty. This process must not only meet the needs of security risk management, but it must also critically address all other forms of vulnerability that are highly disruptive, or which could threaten the very survivability of those organizations delivering assistance. Where resilience is weak or absent, the implications to the organization, its staff, and to the beneficiaries of assistance can be significant. Resilience at the organization, as well as at the

wider sector level, is critical to meet the increasing demands for support in uncertain and hostile environments (Beal, 2014).

The sector addresses vulnerabilities through three key groups: 1) the security practitioner, who assumes security risk management responsibilities with little to no experience or formal security credentials; 2) the security professional, who enters the sector with preexisting technical knowledge and crises-tested experience; and 3) the risk professional, who owns non-security-related aspects of the risk portfolio, including addressing public relations, legal, financial, and operational needs. These distinctions are important when considering how the security and wider resilience approach is structured, how individuals begin or evolve their careers within the field of security risk management, and how education and the concept of knowledge and experience convergence supports the professionalization of both security risk management and organizational resilience.

While the community has historically benefited from the concept of "acceptance" (Childs, 2013) as a mechanism to off-set humanmade threats by leveraging relationships with local stakeholders to gain support and protection, increasingly organizations are being subjected to direct targeting by criminals, communities, governments and terrorist groups. In addition, donors are becoming less tolerant where funds are mismanaged, or where ethical violations occur. Furthermore, employees are increasingly taking organizations to task when duty of care failures arise. Exacerbating these risks is a concurrent intensification of both the frequency and complexity of natural disasters and humanmade crises which increasingly drive beneficiary needs in hostile and complex environments.

The sector's ability to view and address resilience holistically, and across cultural divides, is crucial. What resilience means to the myriad of risk owners is often compartmentalized within departmental functions, operating areas or programs, rather than offering an integrated and mutually-supportive approach. A crisis response, when triggered, often resonates throughout the entire organization, and the level of integration defines the strength of the organization's resistance to risk, and how positive and successful incremental adjustments or transformative changes are when seeking to manage or recover from a crisis. The social phenomena which shape the meaning of resilience is also problematic, as the understanding of the concept of resilience is continually being introduced, and revised, by social actors within organizations and the community at large. This results in a constant process of *construction* and *reconstruction* within the emergent reality of risk (Becker, 1982), influencing both

the security community and their organization's perspective of risk. The diversity of sector specializations and operating practices, geographic micro-communities, the existence of sub-cultures within organizations themselves, as well as the influence of varying forms of funding, all contribute to the challenge of establishing a consistent understanding and approach to resilience. To address this, the meaning of resilience must be agreed upon within a community of resilience practitioners, codified through standards, articulated throughout the community at all levels, and then operationalized through training.

The donor funding source naturally influences the geographic placement of organizational decision-making with the gravity of business relationships drawing leadership decision-making to where the contracting agencies are located. However, this is rarely where the work is conducted as programs more often operate far from the point of a contract award and so are distanced from executive leadership decision-making. The implementation of work is also increasingly conducted by local staff, rather than those who design the solution, are awarded the contract, and who define the initial resilience strategies. As such, the strategic planners and decision-makers are frequently far removed from the risks that will be encountered. This naturally presents a challenge, as exposure, experience and the resultant perception of risk differs dramatically within an organization. In addition, tolerances of risk can also vary markedly, with those distanced from threats becoming hyper-sensitive to risk, compared to those in constant proximity to danger who are often desensitized to danger. In the Global Interagency Security Forum (GISF) study **Risk Thresholds in Humanitarian Assistance** (Kingston and Behn, 2010, p3) the forum states that a: "risk threshold is defined by a particular organization, according to the nature of its work and the specific context" and that (p.4): "evidence suggests that international and national aid workers with a security remit can feel disconnected from programme assessments conducted by senior management, which are based on cumulative risk, resources and institutional factors". The idea of 'risk', whether to people, operations, assets, business or finance, is highly subjective, and this ambiguity complicates the process of developing consistent and credible resilience strategies across a diverse and global sector.

Maslow (1942) describes security as a: "feeling of safety; rare feelings of threat or danger", while Fischer and Green (2004, p21) state that security: "implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear or

disturbance or inquiry." Security, whether viewed as the physical protection of people and assets, or the prevention of any form of risk presented against the organization and its interests, is central to the concept of organizational resilience. Talas (2010, p17) also states that: "an individual who is surrounded by threats but has taken steps to reduce the threats may feel secure" in relation to port security. The same is true of the humanitarian aid and development sector in that it needs to take appropriate steps to address identified risks which harm people, or which disrupt organizational business interests.

The complexity of defining what constitutes resilience complicates the establishment of a consistent sector-wide strategy. Organizations not only have to manage how risk is perceived and what tolerance levels are acceptable, they must also seek to create a consistent understanding and accompanying language within diverse sub-cultures. This is made problematic within a diverse sector which competes for funding, where individualism can undermine collaboration, and where individual and organizational constructs of perceived reality can derail the development of a 'guiding truth' on what risk is, and how to appropriately address it. This thesis proposes that organizational resilience measures in the sector do not presently reflect the severity of interrelated vulnerabilities which harms not only people, but also damages the wider interests of humanitarian aid and development organizations. The shortfall in both research and practice spans both organizational resilience, as well as specifically the field of security risk management which is frequently the root cause of a crisis situation (Allen et al., 2013).

Research aims

The aim of this research is an action research-based outcome, providing practical value to both risk owners and organizations in shaping their approach to security risk management, and more broadly, organizational resilience. The research is also designed to support the sector to identify effective and scalable mechanisms by which to build a consistent and appropriate approach to resilience, incorporating defined management structures, consistent standards and practices, and appropriate educational resources which reflect varying organizational sizes and natures, risk tolerance levels, operating environments, and funding sources. To accomplish a scalable solution this thesis will address the placement of risk practitioners within an organization hierarchy, how standards are practices are

codified in document systems, how risk owners gain knowledge and experience to enable effective decision-making, and how external resources augment internal capacity.

The research aims are influenced by substantial literature which states that the growing rate of natural disasters, coupled with a rise in social instability, intra-state conflict, the hostile government targeting of organizations within the sector, and trans-national terrorism is drawing the sector increasingly into fragile conflict and post-conflict environments. The **ACA Report** (2014) emphasized the major surge in global humanitarian crises, with a rise in beneficiary assistance requirements increasing from 81 million people requiring support in December 2013, to over 100 million in 2014. The report called out the effects on ongoing insecurity as a contributing factor to the complexities of supporting communities in need, citing Syria, South Sudan, and the Central African Republic as conflict zones, coupled with natural disasters in the Philippines, as the cause of major population displacements, famine, and social instability.

Resilience is a concept which has widely differing meanings at the individual, organizational and sectoral level. This ambiguity negatively shapes communities of practice (Wenger, 2017) in terms of learning, meaning and identity. Resilience is also a polysemic concept, facing the challenge of having no agreed-upon meaning (Normandin and Therrien, 2016). The absence of a universal understanding of organizational resilience (MacAskill and Guthrie, 2014) and the growing need for a consistent application of resiliency practice (Manyena, 2006) presents a significant challenge in establishing the professional standards and the accompanying community of practice needed to effectively govern complex risks.

Significant research has been conducted in the field of risk and resilience with studies spanning a broad cross-section of thematic areas, including detailed research on societal resilience by USAID (2012), DFID (2014) and the United Nations (2005). Supply chain resilience is also extensively studied, with research conducted by Kovacs and Spens (2011), Christopher and Peck (2004), Oloruntoba and Kovacs (2015) and Tabaklar et al (2015). Research is also widely available on enterprise risk management (Moeller, 2011) and high-reliability organizations (La Porte, 1996), with disaster risk management being addressed in detail by De Smet (2017), Below (2009), MacAskill and Guthrie (2014), and Matyas and Pelling (2014). At the operational level risk management is explored by USAID in the **Operational security – General Information addendum to ADS Chapter 303** (2006), and within the **USAID**

Risk Appetite Statement (2018). Fast et al (2011), Kingston and Behn (2010), Reilly and Llorente (2014), and Bickely (2017) have also been addressed operational risk management in depth. However, this thesis proposes that a significant gap exists in the study of organizational resilience at the strategic level—that is how risks which may be security or operational in nature present a secondary and potentially more impactful threat to the integrity and survivability of the organization.

The objectives of this research are, therefore, to establish the risks the sector faces, what drives change, and how the sector can professionalize resilience. This is achieved through five main objectives:

1) Define what risks exist, assess their impacts, and establish what constitutes resilience;
2) Enable the process of professional convergence for individuals operating within the security field;
3) Codify knowledge, skill and experience through recognized standards;
4) Expedite professionalization by leveraging forums, associations and commercial resources; and
5) Operationalize knowledge and skills through credible and recognized educational programs.

Outline of chapters

The thesis is laid out as follows. First, the literature review in Chapter 2 establishes the breadth of academic and grey literature relating to organizational resilience within the sector, identifying where gaps exist which undermine the ability for individuals and organizations to address risks. This chapter discusses the meaning of resilience and the risks the sector has faced, and which it might face. Chapter 3 outlines the empirical realism epistemological and social interactionism ontological approach and argues the case for a mixed-methods approach. Chapter 4 presents the results of the primary research findings on the risks the sector faces, drawn from both the semi-structured interviews as well as the survey tool. It looks at how historic and emergent threats are forming catalysts for change, examining physical security challenges and the resulting litigation and reputational implications. Chapter 5 presents the results of the primary research findings, specifically the competencies and value of security professionals and practitioners in sectoral resilience. It investigates how different career start-points influence the effectiveness of how the sector addresses security and more broadly, resilience needs. Chapter 6 examines the primary research findings on the importance of standards in codifying knowledge and experience to enable the professionalization of security within the sector. This builds

upon the literature review and offers both quantitative and qualitative data on how document systems are used to meet multi-faceted resilience challenges. Chapter 7 explores the primary research findings on how standards and practices are operationalized through education, including using the data gathered from the focus group research instrument. It looks at the need for training to address risk, the problems associated with measuring the effectiveness of risk reduction or prevention training, and the mechanisms by which knowledge and experience might be shared or grown. Chapter 8 provides an overview of the research findings. It examines the implications associated with the current ambiguity over the concept of resilience, and how *framing* helps to shape resilience strategies across functional and organizational boundaries. It looks at how the establishment of consistent and recognized standards offers a solid foundation from which resilience can be formed, how the security profession can be advanced and consolidated, and how incremental and transformative change can move the sector to a more resilient state. Chapter 9 presents the conclusion of the thesis.

CHAPTER 2

LITERATURE REVIEW

Introduction

This chapter presents a review of literature that is relevant to the topic of humanitarian aid and development resilience. It outlines the strategies used to identify relevant literature relating to organizational risk and the measures used or required to address identified shortfalls or gaps within current academic research. The objective of the literature review is to determine what risks the community faces, what resilience means are in place, and what further measures are required to appropriately manage risks to people, assets, facilities, business interests, operations, information and the reputation of organizations working within the relief and development space. The literature review looks at five core areas: 1) the risks and catalysts for change; 2) the meaning of "resilience" to the sector; 3) the structure, role and importance of the sector's security community; 4) how standards and best practice are codified within document systems; and 5) how knowledge becomes practice through training, exercising and testing.

The search parameters used to answer these questions focused both on research conducted specifically for the sector, and then extended out to include research that has transferable value. The practice of "borrowing" theories from other disciplines to advance knowledge and understanding (Tabaklar et al, 2015) was leveraged extensively to address substantive gaps in research focused on sector organizational resilience. Out-of-sector research associated with resilience, standards, communities of practice and the production of knowledge was applied to the thematic areas addressed within this thesis in order to illustrate how the application of non-sector specific concepts could quickly and effectively help organizations, and the sector at large, to professionalization resilience and security risk management strategies and constructs. Key words were placed into various search engines, including within sector forum groups such as: the Global Interagency Security Forum (GISF, previously the European Interagency Security Forum or EISF); the International NGO Safety Organization (INSO); the Armed Conflict Location and Event Data Project (ACLED); the Dutch Security Network (DSN); the International NGO Safety and Security Association (INSSA); Security Insight, Devex; the

Humanitarian Practice Network; Humanitarian Outcomes; the Security Management Initiative, ReliefWeb; and DisasterReady. Searches were also placed within various Journals, including: The Journal for Business Continuity and Emergency Management; The International Journal of Mass Emergencies and Disasters; The Crisis Response Journal; and The International Journal of Business Continuity and Risk Management. Literature from the United Nation's Department of Safety and Security (UNDSS) also contributed to the research materials, as did publications from the United States Agency for International Development (USAID), and the United Kingdom's Department for International Development (DFID) on resilience, security, crisis and business continuity. Wider use of the internet was also made to augment relevant journal articles and materials not available within the University Library subscriptions, as well as for case examples which represent high-profile or high-impact incidents which have significantly disrupted humanitarian aid and development organizations. As a result, a wide range of reports, studies, articles, publications and news reporting contributed to the research parameters.

Despite the humanitarian aid and development community being central to the resiliency needs for disaster and conflict-impacted communities and countries (Mathan and Izumi, 2015), and the obvious importance of supporting conflict or disaster impacted beneficiaries through highly resilient supply chain mechanisms which can effectively react to unpredictable or surging demands requiring a significant degree of inter-agency coordination (Kovacs and Spens, 2011), the availability of literature on how the sector itself manages its own risks—notably at the strategic level—is sparse. Indeed, while both donors and beneficiaries expect implementing partners to be "High Reliability Organizations" (La Porte, 1996) in terms of implementing the donor's objectives and meeting the beneficiaries needs within high risk and uncertain environments, little has been done to look inwards at how organizations establish internal tactical, operational and strategic resilience measures to safeguard organic needs.

Research exploring the geo-social environmental risks within which the sector operates is readily available, with extensive research being conducted by groups such as the Geneva Center for Security Policy and their **Security Management Initiative** study. Operationally focused research is also abundantly available through various forum groups, such as GISF, InterAction and Devex, on methods by which to reduce security risks at the operational or field level. However, there is a sparsity of both academic and grey literature on the area of strategic organizational resilience and business continuity.

Concepts such as the "acceptance model" do touch upon organizational resilience (Fast and O'Neil, 2010), but suggest the value of this approach is becoming less effective in managing threats from criminals, hostile governments, and terrorist groups. Some limited materials address the leveraging of the United Nations MOSS within the sector; however, at best, this suggests broad-based principles rather than substantive technical direction. The research found a preponderance of data focused on operational and tactical security risk management, meeting more physical security needs, but highlighted a significant gap in strategic organizational resilience which shapes the field of security risk management, and which addresses litigation and reputational harm.

The research found that forum groups such as GISF, INSSA and InterAction have started (over the past decade) to recognize the value of out-of-sector standards and strategies but have yet to offer substantive contributions to the evolution of strategic resilience measures. USAID in their 2018 **Safety and Security Sector Update** specifically call out EISF (now GISF) as a partner in developing risk management solutions for the implementing partner community and have also implemented the Partner Liaison Security Operations (PLSO) concept in high-risk countries to offer security risk management support to implementing partners, recognizing the increasing security challenges implementers face. However, despite the clear need for resilience at all levels, the focus of forum groups who tackle resilience remains largely hardwired to security risk management at the operational and tactical levels (Bickley, 2017). Examples include research provided by Davies and Reilly (2017) and Fairbanks (2017) for humanitarian aid agencies on security risk management which speaks to operational risk management, but which fails to protect organizations from macro-level vulnerabilities which threaten their very survivability. Conversely, strategic resiliency is acknowledged by Kingston and Behn (2010), but without the required level of granularity needed to offer an actionable outcome.

Other studies conducted by Merkelback and Daudin (2011) and Stoddard, Haver and Czwarno (2016) also begin to explore the value of ISO standards, looking at ISO 31000 standards for risk assessments and business impact analysis, as opposed to focusing purely on operational security risk management. However, despite a brief foray into the ISO standards the current literature does not explore the wider strategies offered by other ISO standards in terms of ISO 22301 standards for business continuity, the emerging ISO 22316 organizational resiliency standard, ISO 22320 standards for emergency management, ISO 34001 standards for security and resiliency, ISO 18788 standards for the

management systems for private security operations, and ISO 27001 standards for information, communications and disaster recovery. Nor has the sector assessed the value of the pending ISO 31030 standard on travel risk management, anticipated for release in 2021, or the BSI 17091 standard which addresses crisis management. Tangential studies, including those by Kemp and Merkelbach (2011) and Guttry, Frulli, Greppi and Macchi (2018) underpin the increasing vulnerabilities from litigation risks, and so escape the gravity of a more typical security risk management approach, but again only to a limited degree.

As a result of the identified limitations in current research focused on strategic risks: that is, risks which impact the wider interests and very survivability of the organization itself (as opposed to tactical risks occurring more often at the point of crisis), tangential areas of research drawn from corporate resilience, disaster risk management, and supply chain management have been included into this thesis—reflecting a "borrowing" from more established disciplines.

Facing dynamic and complex challenges

This section addresses the driving force behind the need to develop more resilient standards and practices within the sector (Kingston and Behn, 2010), balanced against the need for organizations in the sector to proactively operate within what is commonly considered fluid and high to extreme-risk environments (Stoddard, Haver and Czwarno, 2016). It is this need that defines the level of complexity, inclusiveness and resourcing required for the development—and sustainment—of organizational resilience strategies. It is risk, from a negative perspective of causing harm to people or assets, or disruptions to activities, information, financial solvency, litigation vulnerability and reputational worth which must be addressed (USAID, 2006). From the positive perspective, risk can also be the catalyst to enable growth and success with uncertain and challenging environments (DFID, 2014). As such, effective resilience offers a mechanism to address the negative implications of risk, while capitalizing on the positive opportunities which risk may offer.

Increasing disasters and worsening security conditions

The sector operates in high-risk, dynamic, and remote environments that face heightened and escalating humanmade threats and natural disasters. While other sectors or industries typically avoid or withdraw

from such environments, sectoral organizations and their staff are—by virtue of their mission—drawn towards risk. This requirement to operate under challenging conditions is increasing, with Smet, Schreurs and Leysen (2015, p.3) noting that: "since the second half of the century the disaster landscape has experienced important changes. Disasters are not only increasingly in quantity, they are also qualitatively different and seem to distress humanity to a considerably higher degree than in the past". Jackson and Zyck (2016, p.24) also note that: "in 2015 more than 80 percent of UN humanitarian funding was directed at conflict response". The evidence points to an escalation in the tempo and impacts of global crisis events (Garrett, 2015). Indeed, predications are grave, suggesting that disasters will increase fivefold over the next 40 years, making disaster relief an imperative (Kovacs and Spens, 2007). DFID within the **Operational Plan 2011-2016: Conflict, Humanitarian and Security Department** (2014, p.4) report also state that: "The world is currently facing unprecedented levels of humanitarian need. Mega disasters… have shown that despite best efforts, international humanitarian assistance could be quicker and more effective". Merkelbach and Daudin (2011, p.47) also comment that: "the hallmarks of future humanitarian crises will be greater uncertainty, complexity and rapidity. Future humanitarian crises will be particularly prone to synchronous, simultaneous and sequential events that will intensify the effects of any crisis and complicate the response". Burkle, Martone and Greenough (2014, p.1) also support this concern, noting that: "The scale and cadence of crises that demand international humanitarian response is increasing".

Responding to mega-catastrophes and mega-trends

If these predictions are accurate, with mega-catastrophes and mega-trends occurring with greater frequency in the future, then the sector will be drawn, willingly or unwillingly, into increasingly complex and dangerous situations. These challenges must concurrently contend with increases in humanmade conflict that exacerbate the challenges the community faces when delivering aid and relief operations, or when supporting development initiatives. Faced with the need to work in dynamic environments with elevated security challenges, coupled with changing employee, donor and legal pressures, organizations will be forced to establish a scalable and evidentially professional approach to resilience. The approach may be similar to the **United States Foreign Humanitarian Assistance** (FHA) model, which addresses scalable resilience measures for groups working across the spectrum of permissive, uncertain, or hostile operating environments (Beal, 2014). Frequently, especially in

conflict- or disaster-affected environments, organizations face unique security challenges where both they and their beneficiaries must contend with "out-of-the-box" crisis events that outmatch their knowledge, experience and resources (Smet, Schreurs and Leysen, 2015). The complex, often unforeseen, and frequently high-impact challenges will require the sector to blend a formalized program of standards and practices with the nimbleness and flexibility required to adjust to emergent or changing risk conditions. Burkle, Martone and Greenough (2014, p.2) explore the ability for the humanitarian system is able to operate within: "extraordinary scenarios that are beyond their current capabilities". This system requires the inclusion of a layered approach to meet both the locational (coalface) threats, as well as higher level disruptions that go beyond the point of crisis to potentially harm the wider interests of the organization.

Transnational terrorism and hostile governments

Exacerbating the risks associated with the trend of growing global disasters is the increase in transnational terrorism (Wainwright, 2017), coupled with growing social instability (Annawitt, 2010; Ammour, 2012). Coupled together, these challenges make the risk landscape increasingly more complex and dynamic for organizations who either head towards disaster-affected regions to support impacted or displaced communities, or who support conflict and post-conflict environments struggling with fragile rule of law, internal security, or human rights challenges. The sector arguably then, more than most, requires resilience as a pillar for how it is structured and operates; not only to support the beneficiaries of disaster or conflict, but also to protect its own people and business interests.

The sector is also increasingly being directly targeted by hostile governments, criminal and terrorist groups. This exacerbates existing challenges, while reinforcing the need for mature, consistent, evidenced, and resourced resilience measures. Fairbanks (2017, p.1) notes that: "during the first nine months of 2016 open sources reported 487 aid staff killed, kidnapped, injured or assaulted… that is 60% more than for the same period in 2015". **Table 1** highlights the escalation in risks between the period of 2008 and 2018. Whether a kidnapping, an active shooter or armed aggressor attack, a mass casualty incident, civil disorder, a pandemic or epidemic, or a catastrophic earthquake or flood, research shows that the risks are more complex than ever.

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Number of incidents	165	155	130	152	170	265	192	149	163	158	228
Total aid worker victims	278	295	250	311	277	475	332	289	295	313	408
Total killed	127	108	73	86	71	160	123	111	108	139	131
Total injured	91	94	84	127	115	179	88	109	99	102	146
Total kidnapped	60	93	93	98	91	136	121	69	88	72	131
International victims	51	74	41	29	49	60	32	29	43	28	29
National victims	227	221	209	282	228	415	300	260	252	285	379
UN staff	65	102	44	91	57	106	66	43	71	48	69
International NGO staff	158	128	149	135	97	142	152	173	159	98	183
LNGO and RCS staff	44	47	47	77	93	167	74	49	48	115	138
ICRC staff	6	17	10	5	3	20	23	6	11	42	13

Table 1. Aid Worker Security Database (2020)

UN: United Nations — LNGO and NRCS: International non-governmental organization or National Red Cross / Red Crescent Society
ICRC: International Committee of the Red Cross — IFRC: International Federation of Red Cross / Red Crescent Societies

Stoddard, Haver and Czwarno (2016, p.5) state that: "INGOs seem to be taking on greater risks than ever before", suggesting that the frequency and severity of security incidents, and subsequently risks, will only increase over time. The cascading effects from a security incident often exacerbate the disruptive impacts to the organization and confuse risk control measures. The secondary and tertiary risk implications originating from the initial incident are also often more impactful than the root cause incident in terms of causing deep and lasting harm. These can also quickly deplete capacity and resources, while overwhelming ill-defined and unpracticed resistance measures (Maren, 1997).

Changing donor expectations

By design, the sector focuses on the beneficiary, with a natural inclination to accept unusual levels of risk as a by-product of the "mission". Donors have historically provided a generous degree of latitude for implementing partners, with little involvement in how they manage risk. In part, this was historically due to the concept of "acceptance" (Fast and O'Neil, 2010) which predicates that local actors will protect those providing aid. However, research data suggests that this strategy has seen erosion over the past two decades (Metcalfe, Martin and Pantuliano, 2011), with studies indicating that

the sector is exposed to escalating risks from criminals, hostile governments, and terrorist groups (Stoddard, Harmer and Czwarno, 2017). While acceptance still offers some value, there is a growing debate over its failure to address increasingly complicated out-of-community threats. This paradigm shift occurs at the same time as employees are expecting more in terms of duty of care, and as donors require organizations to be more effective custodians of funding, program success, and their reputational interests (Brabant, 2001). The ECHO-sponsored **Report on Security of Humanitarian Personnel** (2004, p.7) states that: "Donors have played a key part in the evolution of thinking and practice in security management by funding a range of research, training and information management initiatives". This indicates a growing appreciation for the challenges the sector faces, coupled with increasing expectations for demonstrable duty of care and organizational professionalism. This is certainly true of the larger implementing partners who effectively operate as multi-billion-dollar corporations, and who are now expected to meet the same standards as their commercial counterparts.

As funding levels increase, the need for demonstrable professionalism commensurately increases. Jayawickrama (2011, p.2) notes that: "World Vision International now has an annual global budget exceeding $2 billion… this challenges INGOs to become more professional, well managed organizations". Such funding moves organizations from being perceived as "humanitarians" to being considered as "corporations". This then leads donors to move from expecting, to demanding, sophisticated resiliency practices. This, coupled with tighter discretionary budgets and higher levels of accountability represents a double-edged sword as donors are more likely to fund resilience measures, but will be less tolerant of failures to implement effective risk-control strategies (Stoddard, Haver and Czwarno, 2016). Case examples include the suspension and subsequent demise of the Academy for Educational Development (AED) in 2011 over several fraud incidents, as well as the significant financial impacts on International Relief and Development (IRD) in 2015 for financial misconduct. As security incidents occur with greater frequency, tolerance levels by the donor community will be lower where negligence or ethical misconduct is presumed or discovered.

Crisis case studies highlight tangible risks

The **Independent Panel on the Safety and Security of UN personnel in Iraq** (2003, p.3) report found that the bomb attack against the United Nations, which resulted in 22 killed and 150 injured in Iraq,

occurred due to: “the failure of UN management and staff to comply with standard security regulations and directives” and that: “the current security management system is dysfunctional”. Case examples where organizations are affected by a perceived—or actual—failure to protect staff can be found in the increasing number of lawsuits against the sector, including the Norwegian Refugee Council 2012 Dadaab refugee camp kidnappings, and the 2011 Samaritan’s Purse Darfur kidnapping. The Oslo court found: “the Norwegian Refugee Council guilty of gross negligence for its handling of the kidnappings of Steve Dennis and three other staff members” (Guttry et al. 2018, p.15).

Bickley (2017, p.8) observes that: “the duty of care benchmark has risen significantly over the past decade, and what once was considered good enough would certainly not be considered adequate today”. Research substantiates this statement, showing that reputational harm often results in the greatest impact, with Guttry et al. (2018, p.23) noting that: “for international organizations, reputation plays an important role particularly in terms of legitimacy and credibility. When strong allegations of misconduct or failure to meet high duty of care standards are directed towards international organizations their legitimacy and credibility is put under risk, undermining the organization’s effectiveness”.

As a result, the concept of “action and evidence” is becoming increasingly important as organizations are required to not only take the appropriate measures to protect people (action), but also to prove that the appropriate steps were taken (evidence) through alignment or compliance with recognized standards, comprehensive document systems, credible training, and appropriate resourcing. These expectations are becoming more pronounced, with increasing litigation forcing the security community, as well as organizational executives and boards, to critically examine whether reasonable measures, evidenced through documentation and record keeping, have been taken to address foreseeable risks. This emerging requirement is noted by Kemp and Merkelbach (2011, p.4) who state that: “safety and security are not only an ethical and moral concern, but a legal obligation”, and that donor involvement in defining security risk management expectations is also increasing: “some major donors now exercise some scrutiny of programs and projects when it comes to security” (p.11).

Studies focusing on the beneficiaries of aid within disaster and conflict or post-conflict environments speak in depth to resilience strategies which have a direct bearing on the implementing partner community, and these same principles apply to the humanitarian aid and development sector. Research

such as the DFID **Promoting innovation and evidence-based approaches to building resilience and responding to humanitarian crises** (2012); the **Hyogo framework for Action 2005-2015**: **Building the Resilience of Nations and Communities to Disaster** (2005); the DFID **Operational Plan 2011-2016 Conflict, Humanitarian and Security Department** (2014); the **Geneva Center for Security Policy** (2015), and the USAID **Building Resilience to Recurrent Crisis** (2012) provide a wealth of research on the need for resilience within disaster and conflict-affected communities and nations. Many of these same principles are applicable to the need to develop resilience within the sector. With a wealth of research on the value of resilience, it is an inescapable fact that donors have—or will eventually—draw parallels on the importance for the sector to have appropriate measures in place to effectively address risks or respond in a timely and professional manner to a disruptive incident.

Measuring risk and its implications

As the sector is increasingly forced to focus on resilience as an integrated part of how activities are planned and conducted, the need to effectively measure complex risks and their implications will also become more important. An effective understanding of risks and their impact will shape informed decision-making and resource allocation. Tracking security incidents can, however, be problematic, although efforts are being made by various groups such as Aid Worker Security, Devex, INSSO, ACLED and Humanitarian Outcomes to monitor violence against the sector, providing the data necessary to guide organizational policy makers and the security community. Guttry, Frulli, Greppo and Macchi (2018, p.11) posit that, between 1997 and 2017, a total of 2,344 incidents were reported against humanitarian workers. Of the 4,370 victims, 699 were international employees and the remainder were national staff with: 1,671 killed, 1,494 injured and 1,205 being kidnapped. Kravitz and O'Molloy (2014) also remark that in 2013 there were 460 aid workers involved in violent attacks, of which 155 were killed, with shootings and kidnapping being the most common form of risk. However, this data is likely the tip of the iceberg, as many incidents involving national staff are likely to go unreported.

Stoddard, Haver and Czwarno (2016) in **Figure 1** explore the different risks the sector faces, addressing not only security and safety vulnerabilities, but also fiduciary, legal and compliance, information, reputational and operational risks, with the research acknowledging the cascading implications of how one risk may trigger others.

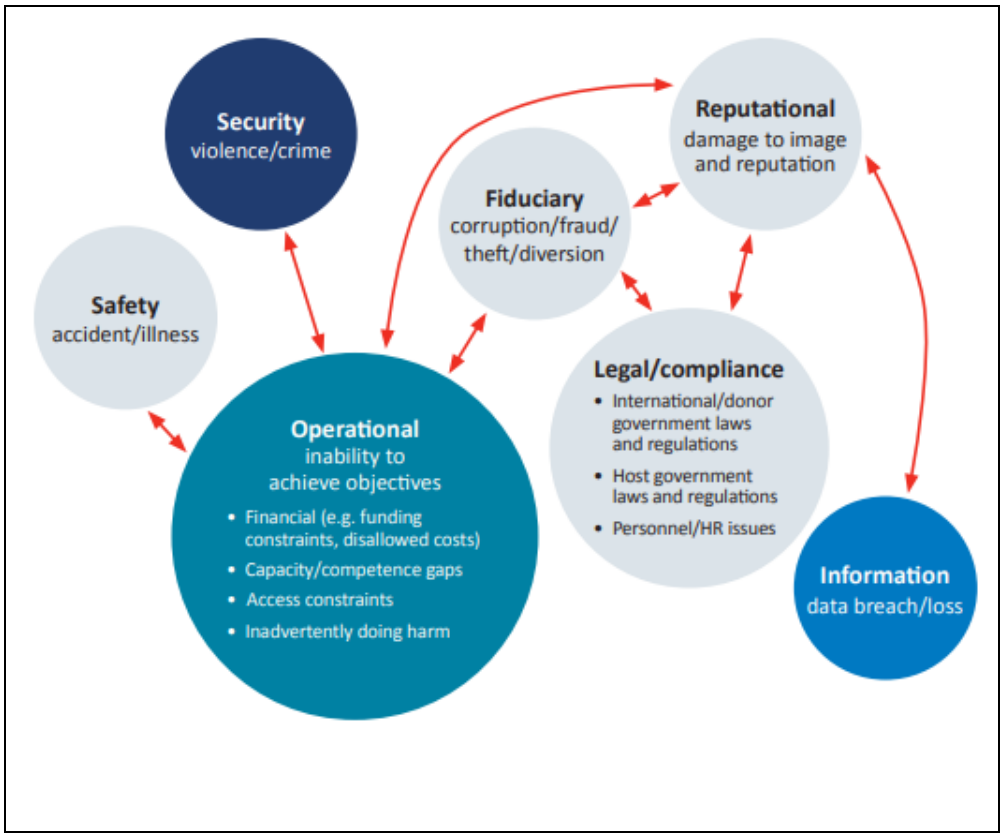


Figure 1. Stoddard, Haver and Czwarno 2016 Risk Categories (p.9)

The findings suggest that organizations are becoming less rather than more tolerant to risks. Given the rising tempo of natural disasters, increasing social instabilities, and elevated targeting by governments, criminals and terrorists, this underpins the need for the sector to develop and formalize a resilience strategy. In order to accomplish any form of standardization, decision-makers need to establish a common understanding and taxonomy of what risks are present, their implications, what tolerance levels are universally acceptable, and what standards and practices are necessary to bring risks to tolerable levels. As a start-point, the perception of what risk "means" and the associated implications within a diverse community will be the driving force for how resilience will then be approached.

Defining resilience

This section of the literature review discusses in further depth what is meant by the term "resilience". It provides context for complex and often interrelated risks and the resultant impacts the sector faces. The term *resilience*, derived from the Latin word *resilio* (to jump back), can be traced to the study of natural history (Bacon, 1625); however, more recently, the term has become associated with enabling disaster-affected communities (Alexander, 2013) to survive or to "bounce back" from highly disruptive events. The Community and Resilience Institute's **Definitions of Community Resilience: An Analysis** report (2013) seeks to define what resilience means, enabling a common vernacular across sectors. Donors have historically sponsored detailed studies into community resilience and the **Hyogo Framework for Action 2005-2015** (2005) looks at how resilience builds flexibility and survivability within nations and communities, including a predictive 10-year review of resilience needs and strategies which includes the need for a more systematic approach to address risk, better knowledge management and education, and more effective preparedness measures. The International Organization for Standardization (ISO) defines resilience as: "the ability of an organization to absorb and adapt to a changing environment" (ISO 22316), and: "adaptive capacity of an organization in a complex and changing environment" (ISO 22300). The Business Continuity Institute (BCI) addresses resilience and business continuity as separate—but intrinsically related—areas, stating that resilience: "enables organizations to get to where they want to go (strategy) and do so in the manner they desire (reputation, preservation of value)", while business continuity: "is one of the key management disciplines that is essential for building and improving organizational resilience". However, despite resilience being as important to implementing partner community operations as to their beneficiaries working and living within the same operating environment, research shows surprising levels of ambiguity over its meaning and application.

The concept of resilience has expanded beyond the fields of engineering, ecological science and psychology, and is increasingly being applied to the areas of disaster risk management, logistics and supply chain management; and critically to safety and security (Duijnhoven and Neef, 2014). Resilience is a ubiquitous term that incorporates methods to control risk (resistance), as well as how to address the effects of a crisis. Resilience addresses all areas of vulnerability, including security risk management which often focuses at the tactical and operational level. It also addresses strategic needs,

including: business interests, financial solvency, asset and information loss, operational disruptions, litigation risks and reputational hazards. While security may often be the trigger for a crisis, it is often the secondary effects at the strategic level that cause the greatest harm to the organization.

Efforts have been made within the international security community to formalize the concept of resilience as it relates to the wider approach to risk management and business continuity. The International Organization for Standardization (ISO) within its 22316: 2016(E) standards for organizational resiliency states that: "Organizational resilience is the ability of an organization to respond and adapt to change. Resilience enables organizations to anticipate and respond to threats and opportunities" (2016, p.15). The British Standards Institute (BSI) within its 17091:2018 (2018, p.9) standard for crisis management, also state that business continuity management is the: "holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might have, and which provides a framework for building organizational resilience with the capacity of an effective responses that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities". These definitions and the accompanying standards offered by recognized centers of professional knowledge offer not only a consistent understanding of what resilience means, but also a process by which organizations can design and implement scalable and tailorable resiliency strategies.

For a sector which heads towards danger, rather than away from it, resilience is not to be presented as the opposite of vulnerability (Timmermann, 1981). Indeed, the sector may arguably be more vulnerable to certain risks than others, given its propensity to operate in uncertain, if not openly hostile, environments. Given the experience gained, often over decades, through stress-testing management structures and operating practices, this exposure would logically make the sector inherently more resistant to risk than its commercial counterparts, despite being more likely to face danger. The value of effective resilience, then, is in the ability to effectively prepare for and then respond to predictable threats. To be effective, resilience is shaped by standards, implemented through practice, and operationalized through education and resourcing. This requires some level of consistency within the sector, with Timmermann (1981, p.21) stating: "a strategy promoting resilience would therefore seek to protect and strengthen the qualities or elements of resilience". Merkelbach and Daudin (2011, p.49) also suggest that: "for organizations working in volatile hazardous environments the notion of

uncertainty is essential", highlighting the need to both acknowledge and address the potential for disruptive events, but that: "building resilience helps organizations to cope with uncertainty and reduce vulnerabilities". As such, risk and uncertainty should not be considered the challenge; rather, establishing flexible and scalable resilience measures across management structures, document systems, practices, education and resourcing should be the goal.

Agreement as to what constitutes appropriate resilience varies markedly within the sector, especially in the absence of universally agreed upon standards. Duijnhoven and Neef (2014, p.425) suggest that: "resilience, security, risks, threats, vulnerabilities, etc. are all social constructions that obtain their meaning in interpretive negotiations and processes of framing". Resilience is therefore concerned with both abstract concepts such as moral or legal obligations (which fall under the arena of "duty of care" to address the physical and psychological welfare of people), as well as the more nebulous, but highly impactful risks resulting from reputational harm. The root cause of many crisis events facing the sector involves the threat of assaults, kidnappings, civil disorder, serious injuries, earthquakes, floods, storms and murder. These can trigger the more incorporeal risks of reputational harm, operational disruption, or the potential for costly litigation. Both the tangible and intangible risks are viewed through the lens of personal experience, with the interpretation of resilience shaping leadership decision-making, and ultimately organizational and sectoral resilience strategies.

The beneficiaries of aid have, for decades, been the subject of detailed studies to address resilience needs. Studies such as the **Hyogo Framework for Action 2005-2015**[1] (2005), the USAID **Building Resilience to Recurrent Crisis: USAID Policy and Program Guidance** (2012) report, and various reports from the Harvard Humanitarian Initiative provide the broad basis for what resilience means, and what universally applied mechanisms can be used to prevent, or address, disruptive incidents. The UNDSS **Saving Lives Together: A Framework for Improving Security Arrangements Among IGOs, NGOs and the UN in the Field** (2006) led by InterAction and United Nations Children's Fund (UNICEF) also recognized the need for the sector to be resilient; including developing standards and operationalizing these through training. The concept of resilience outside of the sector is also not new, with Horne and Orr (1988, p.31) stating that it is: "a fundamental quality of individuals, groups and

[1] The report offered a 'look forward' over ten coming years from a start point of 2005.

organizations, and systems as a whole to respond productively to significant change that disrupts the expected pattern of events without engaging in an extended period of regressive behaviour". This provides deep and broad set of resources from which the sector can form its own understanding of resilience.

The interpretation of resilience is also shaped by terminology. Reactive terms such as "withstand" "bounce back" and "recovery" lean towards the resistance model—that is, preventing risks. Conversely, proactive terms such as "continuity of operations" or "adaptiveness" will support the concept of incremental adjustments or transformation change—that is, responding to and managing predicted or occurring risks (Matyas and Pelling, 2014). While this language is abundant within the field of disaster risk management, it is not consistently found within available literature on sector resilience strategies. Research indicates that, despite rich data on resilience being available within the fields of disaster risk management, business, operations, manufacturing, information, logistics, communications and technology, and other governmental or commercial pursuits, there is a surprising vacuum of literature addressing strategic resilience within the humanitarian aid and development sector.

The security community

This section looks at the security community, the importance of risk forum groups, and the changes to the perceived value of security risk management and organizational resilience within the sector. Schneiker states that: "since about the end of the 1990s humanitarian NGOs have established more and more institutionalized security forms" (2016, p.53). These forums have sought to develop a framework for security risk management, and to act as a platform from which to share best practice and experience on broader areas of risk. Forum groups such as the InterAction Security Advisory Group (SAG), the GISF, and the International NGO Security Organization (INSO), offer the mechanism for organizations and professionals to collaborate and share critical knowledge and experience for the betterment of individuals and their organizations. Forums also act as the link to other agencies, such as the United Nations and donors, acting as the voice piece for the sector on critical needs. In so doing, such forums support the interests of the wider humanitarian aid and development community in understanding and managing risk, or in effectively responding to crisis situations. USAID are also now directly investing

into the risk management forum building business through the Partner Liaison Security Operations (PLSO) initiative, providing a mechanism by which implementing partners can gather security information, share resilience best practices, and draw from centralized security risk management advisory support, templates and training resources.

The establishment of a security culture contributes to the formation of a defined body of similarly minded professionals who seek to address consistent risks, needs, and limitations. This evolving "culture" reflects not only the common goals of the sector and the needs found within different activities, operating areas, and communities, but also brings together of a subset community which blends transitioning second-career security professionals drawn from the police, military and intelligence services with non-security practitioners coming from the academic and civilian fields. **Figure 2** shows that historically the value of military and police experience—when applied to security risk management—was seen in that: "The police and armed forces churn out individuals with intensive training in the practice of security and protection, and have a wealth of hands-on experience that is scarcely available elsewhere" (Briggs and Edwards, 2006, p.78).

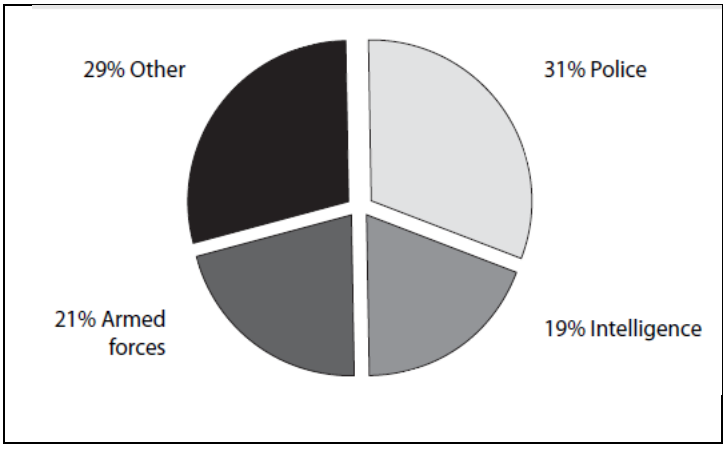


Figure 2. Briggs and Edwards Primary Career Fields for Security Professionals (2006, p.78)

Increasingly, security practitioners are also being drawn from more academically-orientated fields, or from those who migrate from a technical area—such as program management, business, or logistics and operations, the emergency services, or disaster relief—within the sector, who then assume a security responsibility based on *learned* rather than *trained and experienced* knowledge. Both within and outside of the sector, especially at the more strategic level, there is a growing realization that security includes a strategic component which does not necessarily depend on a formal security background (Briggs and Edwards, 2006). Regardless of the background of the individual, those leading on security risk management form a unique community whose focus is to enable safe, secure and productive

operations in dynamic and uncertain environments. In this role they must bring the level of sophistication needed to evaluate, define and articulate resilience needs and strategies. Their selection and placement within decision-making circles must not only reflect appropriate (and critically proven) experience and qualifications to withstand scrutiny following a crisis, but also must reflect their ability to be an *enabler* and positive influence as a champion of resilience.

When considering the evolving culture of security within the sector it is important first to define what is meant by a "culture". Garrett (2017, p.46) defines culture as: "the totality of socially transmitted behavior patterns, arts, beliefs, institutions, and all other products of human work and thought". The ability of the security community to develop, transmit and grow behaviors, beliefs, institutions and products around both security risk management as well as the more strategic areas of organizational resilience requires clear direction. Like any profession, standards and practices around resilience must be developed, sanctioned, and then applied. Without established standards, then other disciplines should be leveraged to advance knowledge and practice (Tabaklar et al, 2015).

Sector resilience is shaped both by how organizations perceive and manage risk, and how security professionals guide their organizations in building and sustaining resilience measures. To understand the effect the security community has upon organizational resilience it is important to understand that individuals themselves are influenced by ontological considerations relating to the nature of the social entities they service (Wenger and Lave, 1991), while also representing a subset community of practice within the wider field of security risk management. And, where individuals are involved in strategic resilience, then they also reflect the field of business continuity management, influencing financial, cyber, legal, public relations, operational and business fields.

Arguably, more than most societal groupings, the sector forms unique socially focused entities that are naturally in a constant state of flux as they meet the needs of donors and beneficiaries, while working within diverse, complex and fluid environments. This is especially notable where organizations function within uncertain operating environments, which results in varying degrees of *constructionism* where organizations are deeply influenced and changed by the social actors whom they assist or interact with. Constructionism is also influenced by the security professional or practitioner, who shapes organizational understanding and the subsequent approach to risk management. For organizations that have matured into well-established entities with a defined appreciation of resilience, objectivism can

also occur, where organizations consolidate and take on a personality of their own, irrespective of the individuals who inhabit them, or who are designated to lead resilience measures. These two influences shape the security subculture which works within the construct of the larger organizational culture, and even more diverse sectoral culture. The influence of constructivism and objectivism also has an effect upon the selection process for security professionals, and it influences how organizations shape and control the individuals selected to serve their security risk management, or business resilience, needs. This is complicated, in that the security community includes a wide range of roles, qualifications and experiences, ranging from a Global Security Director down to a non-security professional assuming part-time responsibility of risk management as a Security Focal Point (Brabant, 2001). Cost also plays a role in the selection process, with less experienced individuals being appointed where budgets are tight, or where the value of seasoned professionals is not understood, valued, or defined.

A culture of security

Effective organizational resilience absorbs the shocks of a crisis event (Manyena, 2006), bringing a degree of control to the outcome, and ensures the survivability of an activity or entity. Security professionals are often designated to take either a technical or leadership role in preparing organizations for absorbing this shock, and make a direct contribution to how effective, or ineffective, that shock absorber is. Security professionals are often required to enact decision-making quickly and with little opportunity for assistance or approval, and so must have be afforded a high degree of discretion during a crisis (La Porte, 1996). In turn, the maturity of the organization influences the effectiveness of the security community in being both *heard* and *felt* within their team. The security community may face the challenge of contested budgets and limited resources, may wrestle to secure equity of ownership within the management of organizational risk, might be unable to rely on leadership support, and sometimes may find that they lack the legitimacy to be taken seriously—all the while being held accountable for literal life and death resilience standards and practices. The security community, therefore, both influences, and is influenced by, the social entity they support; and this has a tangible impact on how resilience is developed and sustained within the sector. Organizations must develop a culture of security vertically through all levels of leadership, and horizontally spanning all technical areas, cultures and geographies, in order for security risk management to be truly accepted.

Behn and Kingston (2010, p.3) make the observation that: "in recent years organizations have also drawn on findings in the field of risk management, acknowledging that "risk" encompasses not only direct threats to staff and operations in insecure environments, but also threats to an organizations broader remit, such as loss of reputation, issues or liability etc.". This suggests that risk owners need to work more collaboratively—as a hybrid community managing a diverse risk portfolio—to identify where one risk creates or influences another, and how the impacts of an event can ripple across functional boundaries. Uniformity concerning the understanding of risk, and the standards and practices which govern effective resilience, is therefore important across functions, management levels and geographies. Bickley (2017, p.11) states that: "where organizations have no embedded security culture, the culture in each location is dependent on individuals in that location; meaning multiple different security and safety approaches across the organization". While Bickley specifically looks at the field of security risk management, this also is true for the diverse suite of risks within the wider remit of resilience, as commented on within the 2004 ECHO report which recommends the development of an organizational culture on security management, and the integration of security into administrative and program management processes and decision-making.

Professionalization of the sector

Based on the work of Peter Haas (1992, p.3), we can say that an epistemic community represents: "a network of professionals with recognized expertise and competence in a particular domain and authoritative claim to policy-relevant knowledge within that domain". The Australian Professional Standards Council, in their paper, **21 Years of Regulatory Innovation through Professional Standards** (2015, p.5) also explores the meaning of professions, indicating that the term "professional" is subjective and may denote an individual: "deriving income from a particular task may make you an "expert" or "good at your job". These definitions are certainly true of the security community, which nonetheless faces the challenge that there is no performance expectations nor formal career or learning pathways to determine when an individual is deemed either *competent* or an *expert* either within the field of security risk management or organizational resilience. This is even more pronounced where individuals cannot point to a first career which includes security, resilience or crisis management as a verifiable foundation for experiential learning and underlaying (proven) competency.

Agreement of what constitutes professionalism within the sector is either weak or (often) absent, despite the efforts of several forum groups to establish a common understanding—or agreement—of what defines effective security risk management. INSSA have sought to develop competency-based qualifications for security[2], and GISF have published various studies and papers on security management. However, these efforts remain isolated concepts which have yet to be developed into a comprehensive, and accepted, set of standards across the community. The sector also faces the risk that the vocal few may—in the vacuum—establish standards and practices which are sub-optimal, or which may be driven by self-interest, rather than being formed as a result of unbiased research and actual sector needs. Schneiker (2015, p.89) observes that: "significant differences in the approach to NGO security exists among American, European, and Southern NGOs. These differences result in poor information sharing and cooperation both at the headquarters level and in the field, creating fragmented and incoherent responses across the international humanitarian community". Despite the lack of structure and agreement, the need for professionalism in the sector is being driven by the growing demand by beneficiaries and donors for support within disaster-struck, conflict and post-conflict environments, combined with the: "greater attention to security concerns affecting humanitarian workers" (Jackson and Zyck, 2016, p.12). This reinforces the need for the professionalism of security in terms of standards and competency frameworks, and the development or a multi-faceted approach to resilience.

The subjective perception of risk, coupled with how transnational organizations address layered resilience needs at both the organizational and local levels, influences the establishment and maturation of both security risk management and organizational resilience strategies. This layering approach across strategic, operational and tactical levels—simplistically split between the headquarters and field—creates a security community whose members must collaborate in order to effectively address global, national and local risks within diverse operating environments, and within wildly different cultures. Research by Jackson and Zyck (2016, p.12) highlight that the bulk of professionalism is occurring at the international level, despite local management teams facing the majority of the risks: "these developments remain focused upon and embedded within international humanitarian entities rather than among national and local organizations that are so often present at the front lines". This

[2] Entering into a pilot agreement with the United Nations in 2020 to test their security management qualification.

weighting of investment at the headquarters level effort distorts the ability of organizations to most effectively address the fundamental interconnectedness of resiliency between the place where standards are developed, and the place where they are most often employed.

The security professional and practitioner belong to an evolving community which, through individual relationships and professional forums, share knowledge, experience and the validation of their individual and collective beliefs. The security profession should have an intense *elan*, bringing spirit and vigor to their role, as well as strongly held expectations for themselves (and others) regards the value of a strong professional performance (La Porte, 1996). This brings shape, substance and direction to perceptions, standards and practices. Schneiker (2016, p.8) remarks that: "formed at the end of the 1990s, the epistemic community of humanitarian security experts has helped the humanitarian NGOs to establish internal and inter-organizational security management policies, structures and procedures". However, the complex portfolio of risks, the lack of definition on standards, ambiguity as to what constitutes best practice, ill-defined or poorly constructed roles, and the absence of an agreed competency framework which defines educational needs all result in ambiguity over who belongs in the community, and what constitutes a professional. Schneiker (2016, p.11) goes on to say: "it has not been explained yet why we can think of security professionals as an epistemic community, who precisely are members of this epistemic community and how exactly such a community fosters NGO security cooperation". This raises the question of the identity, function, and positioning of security within the sector.

The diversity of professional backgrounds and experiences among those performing a security role naturally results in multidisciplinary interpretations of resilience (MacAskill and Guthrie, 2014), and this potentially weakens the focus and overall approach of resilience efforts. While diversity is often a positive contributor to growth and change within a profession, there is a risk of maladaptation doing more harm than good as unqualified—or inexperienced—individuals seek to guide or implement change, rather than draw from—and build upon—a reservoir of established and proven standards, best practices, and experience. The application of resilience is further complicated by differing constructions of reality that influence the mandate and definition of what constitutes "professionalism" or "best practice". As such, the sector struggles to agree with what best practice means, and how to construct and operationalize it. This illustrates the need to develop universally agreed-upon

professional standards by which to framework where the security community sits, and what individuals are expected to accomplish. This also requires individuals to reflect upon their role, and how that role operates within the broader resilience framework. Polanyi (2009, p.55) suggests that: "tactic knowing achieves comprehension by indwelling[3], and that all knowledge consists of or is rooted in such acts of comprehension". It is through reflection and the resultant sharing of knowledge and experience that professionalization of security can be accomplished.

The influence of donors on the security profession

Donor needs drive the security profession, not only from a funding perspective, but also from expectations of role and performance. Kemp and Merkelbach (2011, p.3) state that: "some of the major donors had become sensitive to the need to finance security and contributed to the overall professionalism of IAO security management". Donor interest, and indeed demands, are increasingly starting at the business capture point where risk management strategies must be articulated within proposals, including up to full security plans with the technical proposal and a separate security budget section. This, then, requires the security community to become familiar with the fields of business, operations, and finance in order to shape resilience from the outset. It also requires professionals to be competent in developing technical narratives for proposals, and in also calculating security costs for proposal budgets.

The escalation of direct and indirect targeting risks has also raised the importance of the security community. Behn and Kingston (2010, p.4) posit that: "the emphasis decision-makers now give to security concerns is reflected in the marked increase in full-time security positions within NGOs, as well as deeper responsibility for security within the program management line". Schneiker (2016, p.9) also observe that security is: "an enabler for humanitarian programmes". This weight of responsibility requires the sector to have a clear understanding of what standards to expect, or demand, from its security professionals. Professionals also need to bring a wide range of talents to the role to best support their functional peers.

[3] 'The theory of tacit knowing (holds that) dwelling in our body clearly enables us to attend from it to things outside.

The security community and career transitioning

Individuals within the security field typically originate from outside of the sector, and this requires reorientation of learnt skills, professional experiences, and behaviors in order to fit into the unique humanitarian culture. The manner in which professional transitioning occurs is critical to the success of the individual, while also impacting the available pool of professionals from which the sector can draw. The manner in which individuals lead on security risk management, and contribute to wider organizational resilience, is driven by a combination of taught knowledge as well as experiential development. Polanyi (2009, p.34) explores the concept of the tacit dimension of learning, stating that understanding is developed through: "the proximal, which includes the particulars, and the distal, which is their comprehensive meaning". This has important relevance for the transitioning professional as proximal knowing may be gained within the primary career field, such as risk and crisis management on the battlefield, or when policing a challenging community. Conversely, the distal application of this knowledge within a humanitarian setting will be colored by the nuances of the organizational mission, the donor influence, program specific goals, the beneficiary community, differences in support and resources, and the risks resulting from direct and indirect targeting. This is not to say that primary career technical competency is not of value; rather, that the lens through which this knowledge and experience is applied must go through a transition to have meaning within the sector. Polanyi (2009) also touches upon this process in terms of "emergence", discussing knowledge in action which forms new comprehension as the application of existing technical knowledge and skill evolves against changing conditions. As such, for the individual entering the sector, a conscious effort is required to reorient knowledge and experience to a much different culture and operating environment. This adjustment of comprehension must be intellectual, practical, and behavioral to be effective.

The **ECHO Report on Security of Humanitarian Personnel** (2004, p.30) observes that: "Where security officers have a military or police background, they can become isolated within the organization due to the "us and them" relationship humanitarians tend to have with the military". Brabant (2001) also questions whether individuals require a military or police background, noting that this knowledge and experience does not directly translate into the sector. Thacker (2017) also explores the changing background and makeup of the new security professional, suggesting that the security profession has evolved in recent years, and that academic prowess is potentially now more important than hard

security skills and crisis proven experience. If the sector seeks to continue to draw from the military or police community then a supported cultural shift of social perceptions, behaviors and practices is required. Barnett (2000, p.258) explores the different human dimensions, noting the importance of epistemological (knowing), praxis (action), and ontological (self-identify) elements. These three components shape not only the process of successful transition, but also the continuum of learning (Eraut, 1994) for those within the security community (regardless of their backgrounds) as they service multiple stated and implied functions.

The challenge individuals face when transitioning is unlike that found in many professions, which offer—or demand—a formal learning pathway, and which provide defined and accepted professional standards and practices. Security risk management in the sector has (to date) no such structure. Comprehension is developed at the individual level, without frameworks or guidance from a formally recognized body of experts, or from a community of likeminded and similarly experienced professionals. This is inherently dangerous for both the individual, as well as the employer, as the margin for error within the field of security is small (certainly in high-risk environments) and any misstep can have dramatic consequences in terms of risks to life, safety, and the psychological well-being of people. Errors can also result in asset or sensitive information loss, operational disruption, litigation, financial losses, or reputational harm for the organization. As such, the option of "learning by doing" is inherently problematic. Points of accelerated or directed learning exist within primary career fields for leadership development under high-stress conditions, as well as when working within the sector where crisis-forced learning results in a rapid stress-tested upskilling. Formalized training also offers opportunities for compressed learning outcomes against defined best practices. However, the former presents a risk to the individuals and those they support, while the latter is undermined by the absence of an established competency framework and supporting resources.

The use of standards to codify knowledge and best practice

Within this section we will consider standards and practices within two main levels: 1) the strategic level where the organizational approach is defined, and where crossing-cutting practices are established, and 2) at the operational and tactical levels which are typically at the point of project implementation, and which deal with how standards are then implemented through practice. Standards

and practices codify resiliency strategies, enabling consistent best practices to be applied against organizational risks. Standards define risk attitudes and thresholds, allowing knowledge and skills to be both transferable and measurable. Standards also evidence the steps taken by an organization to protect people, operations, assets, information, and business interests. As such, standards, and how they are enacted through practice, ensure appropriate duty of care is taken to protect people, as well as to concurrently protect the interests of the organization as a business entity.

The application of standards is found not only within the need to professionalize the security community (Brabant, 2001), but also within the phases of preparing for and preventing risks, responding to and managing incidents, and then transitioning and recovering from disruptions. The bulk of current literature is focused on security risk management at the operational and tactical levels—or in terms of the application of security at the point of program implementation. Even then Brabant (2001, p.6) suggests that: "Few agencies have a safety and security policy", and this leads to a lack of direction in adopting security strategies to consistently and effectively control risks. The lack of direction also affects resilience more broadly, as security is but part of the resiliency solution, with Merkelbach and Daudin (2011, p.4) positing that: "Safety and security management are increasingly seen as one element of an organization's overall risk management, which also includes financial, reputational and legal risks". Research by GISF and InterAction provides a comprehensive review of security risk management; however, rarely does available research "look up" at the higher-level organizational resilience needs. Nor does available research discuss the potential leveraging of standards (outside of ISO 31000 for risk assessments) and associated disciplines to help frame the approach to security risk management, and how it resides within the wider resilience framework. Rather, the bulk of current research presents a very practical approach to managing tactical or operational risks.

Favorable order and favorable disorder

When seeking to build standards and consequently practices within the sector, the debate as to whether resilience is a spontaneous or deliberate process can be a debilitating factor. Some argue that resilience measures in complex environments are wholly reliant on leadership experience, and that documented systems quickly become irrelevant and overwhelmed by events for which it is impossible to plan a

response (Faraj and Xiao, 2006). Others argue that resistance measures and predefined incremental adjustments can be predicted, and that core risks and cascading effects can be predetermined, with codified measures to aid with a more coordinated response (Buth, 2010). Coping cascade strategies and the need for adaptation during a complex crisis are well-documented within the field of disaster risk management (Pelling, 2011), but such strategies are poorly defined as they relate to organizational resilience in the sector. Two opposing camps represent those who propose value in frameworks and system to address known risks, opposed by those who feel that any framework is constraining and will fail under duress. For resilience to be established both camps must come to a common understanding of where the balance between order and chaos should lie.

Standards and evidencing duty of care

The allegation of negligence following a security incident and the resultant legal implications are increasingly forcing change with the humanitarian aid and development community. Klamp and Associates (2019, p.2) explore potential lawsuits against humanitarian NGOs for tort claims (negligence), focusing on where the organization has: 1) a legal duty of care to confirm to a certain standard, 2) failed to meet appropriate standards, or 3) caused a staff member to be injured as a result the failure of a standard or act. Guttry, Frulli, Greppi and Macchi 2018, pp. vii-viii) also state that: "duty of care constitutes a non-waivable duty on the part of organizations to mitigate or otherwise address foreseeable risks that may harm or injure its personnel and their eligible family members". Duty of care addresses incidents of injury, death or kidnapping in the sector during the performance of work, and Guttry et al (2018, p.5) go onto say the liability exists where a violation is proved by: "demonstrating the lack of measures adopted by the sending organization to secure and guarantee the safety of personnel working on the ground". These measures may include effective management structures, documented standards and practices, the provision of awareness and competency programs, and the allocation of budgets, support and resources to enable effective security risk management to be implemented. Should any of these risk control measures fail then the organization may face a resultant crisis which reaches beyond the impacts of the incident itself, presenting a threat to the organization's ability to function—or even continue—as a business. Guttry et al (2018, p.376) also recommend meeting both the practical needs encapsulated within the field of security risk management, while also addressing the needs of developing incident management plans to: "address the four stages of

emergency management: Preparation, Mitigation, Response and Recovery". This includes the various levels of escalation, as well as the need to activate the crisis response at the headquarters or strategic level. This pertinent point, albeit lightly touched upon, is largely absent from other available research which tends to focus on dealing with the localized response at the point of the emergency, rather than defining how an integrated response to a crisis is achieved by bringing the field and headquarters teams together to be mutually supportive during a crisis; addressing tactical, operational and strategic needs concurrently. As such, by isolating resilience to a particular area or event, rather than treating the cascading tangible and intangible impacts themselves, organizational resilience is weakened, and the effects of the incident can (and likely will) become more pronounced.

InterAction MOSS standards

While the requirement for security standards is broadly accepted, no agreed-upon standards for security risk management have yet been developed. Klamp and Associates (2019, p.4) note that: "InterAction is requiring that all of its 168 members adopt and conform to its 'Minimum Operating security Standards' in the year 2008", and that: "any organizations that falls substantially behind these standards risks being considered unreasonable, imprudent or unsafe by a court of law". The MOSS concept developed by InterAction in 2008 is sound, offering a good first step towards developing agreed-upon standards for resilience within the sector. However, the "borrowed" standard lacks substance, seeking to address a complex topic in only seven pages. Nor were the necessary resources made available to operationalize these standards, either in the form of documented templates, training or direction on how to take a principle to the point of action. As such, InterAction mandated significant change, but failed to provide the tools by which change could be accomplished; in so doing, InterAction placed organizations at significant reputational and litigation risk. To date, there are no universally-agreed-upon standards relating to security or resilience, and this presents risks—not only at the individual level, but it also creates a vacuum for the interpretation of what is a "reasonable measure" of protection. In addition, the research identified that the Interaction version of MOSS is universally dismissed within the sector.

Donors and resilience standards

The USAID **2012 Building Resilience to Recurrent Crisis: USAID Policy and Program Guidance report** (2012) identified the need to support recipients of aid that have experienced repeated disasters, where pre-defined resilience strategies can be developed. The implementing partner community also faces similar risks and would benefit from also developing appropriate strategies by drawing from lessons learned from their commercial peers, as well as beneficiary counterparts. DFID's **Operational Plan 2011-2016 Conflict, Humanitarian and Security Department** (updated 2014, p.4) paper also notes that: "the world is currently facing unprecedented levels of humanitarian need. Mega disasters such as the floods in Pakistan (2010) and Haiti earthquake (2010) Typhoon Haiyan in 2013, and the ongoing crises in Syria and Iraq, have shown that despite best efforts, international humanitarian assistance could be quicker and more effective". The paper explores improving international humanitarian system preparedness within high-risk environments to allow expedited responses to a rapid onset disaster—with obvious inference to the need to enhance resilience within the implementing partner community. The **Hyogo Framework for Action 2005-2015: Building the Resilience of Nations and Communities to Disasters** (2005, p.1) similarly notes that: "There is now international acknowledgement that efforts to reduce disaster risks must be systematically integrated into policies, plans and programmes". The ECHO (2004, p.1) report also specifically explores the need for security policies and guidelines, noting that: "Donors have played a key part in the evolution of thinking and practice in security and practice in security management by funding a range of research, training and information management initiatives". Outside of the donor community, other research echoes the need for resilience, with Bickley (2017, p.20) discussing the need to develop a security risk management framework through the establishment of a global security policy, stating that: "establishing a global security policy will help demonstrate your organization's commitment to the security of its staff". However, despite the evident need expressed across multiple disciplines of research to formalize resiliency strategies as mega crises escalate, the sector has yet to design its own standards, nor has it leveraged out-of-sector resources which could be modified to meet its needs. And, where a focus does exist, it is invariably at the tactical rather than strategic level.

Expanding the risk management focus and ISO standards

Merkelbach and Daudin (2011, p.5) expand beyond the focus on programmatic security risk management, offering recommendations for risk management practices to include: "explicit focus on organizational and operational resilience or business continuity", offering a rare focus on how implementing organizations manage their strategic risks. Stoddard, Haver and Czwarno (2016) also look at the standardization of a risk management framework, including the application of Enterprise Risk Management, the International Organization for Standardization (ISO), and the US-based Committee of Sponsoring Organizations of the Treadway Commission (COSO)—however, only with reference to the 31000 ISO risk management approach, rather than including the wider portfolio of existing resilience and emergency management standards.

The research suggests that a blend of "favorable order" through codified standards and stabilizing practices, and "favorable disorder" through effective leadership (Normandin and Therrien, 2016) potentially offers a solution. The production of new knowledge and the resulting requirement to establish accompanying standards, resources and training often results in: "putting the existing institutional structures and procedures under strain, which require new and radical transformations" (Gibbons et al., 2002, p.140). This is true as donors, forum groups and individual organizations seeking to develop new standards, evolve resiliency strategies, transform organizational structures, and implement the resulting practices—often with limited budgets and overstretched resources.

Duijnhoven and Neef (2014, p.427) suggest alignment of resilience measures to counter specific identified threats, with: "another type of resilience enhancement approach are those that are threat orientated… floods, earthquakes… terrorist acts…", and to match these threats to specific owners of risk: "specific societal groups can also be the focal point of resilience enhancement". This approach resonates with how ISO standards approaches resilience: with ISO 31000 addressing risk assessments, ISO 22316 addressing organizational resilience needs, ISO 22301 meeting the needs of business continuity, and ISO 22320 meeting the needs of emergency management. This internationally recognized approach, developed by a professional body, allows resilience measures to be crafted against identified threats. It shapes how standards might be developed effectively and credibly to support both the sector, as well as its heterogeneous security community, to better control all forms of

potential risk. ISO standards also offer sufficient flexibility to meet the size, shape and needs of different organizations within the sector, and so are scalable and non-prescriptive.

Kemp and Merkelbach (2010, p.2) state that the: "humanitarian enterprise is no longer a matter of well-intended philanthropy or charity but must be considered a global multi-billion dollar "business". Indeed, the IAO community strives to be a distinct professional enterprise with objective professional standards for the overall humanitarian aid community, organizations and with professional staff". The principles of ISO call for leadership commitment, stakeholder engagement, standards to be formed and then articulated, the need for knowledge to be operationalized through practice, the application of appropriate support and resources, training and exercising to confirm knowledge, skills and practice, and a performance-monitoring process to ensure systems remain fit for purpose. COSO also supports the standardization of Enterprise Risk Management, which incorporates a frame-working approach to crafting and sustaining organizational resilience (Protiviti and DeLoach, 2014).

Brief references to the ISO standards are made within the limited literature focused on the humanitarian aid and development sector's approach to organizational resilience, including research by GISF which states: "In line with the ISO 31000, Risk Management – Principles and guidelines, we argue that risk assessments should consider both external (context-related) and internal (capacity, resources) factors, in order to integrate risk attitudes and thresholds at the operational and the organizational levels" (Behn and Kingston, 2010, p.3). Merkelbach and Daudin (2011, p.12) also reflect upon the value of ISO 31000 standards for risk management, suggesting that this standard: "proposes a logical and systematic framework and accompanying vocabulary to address this complex issue (risk) in an integrated enterprise-wise management system". However, neither discusses how other ISO standards might be used by the sector to build security or broader resilience standards, both of which are critical.

The operationalization of knowledge and skills

Within this section we will consider the operationalization of resiliency measures within different learner groups through training, exercising and testing. This section will explore the knowledge and skills required for security professionals and practitioners at the point of program delivery, as well as higher level security professionals and other risk portfolio owners who shape and implement organizational standards and practices.

Research indicates that donors recognize the importance of developing a culture of awareness and internal capacity through knowledge and skill transference within disaster-affected communities, with the **Hyogo Framework** (2006, p.6) specifically calling for: "knowledge, innovation and education to build a culture of safety and resilience at all levels". Given a sector focus of working in challenging environments, that same logic of sharing knowledge through learning applies equally to the beneficiaries as it does to those organizations supporting a beleaguered community. The success of resilience is built upon both the human dimension of understanding, as well as the effective application of concepts and practice. Field et al (2012, p.56) observes that: "robustness over time would increase if learning were a central pillar of adaption effects, including learning focused on addressing current vulnerabilities and enhancing current risk management". GISF studies, including the **Joint NGO Safety and Security Training** (2009) and the **How to Create Effective Security Training for NGOs** (2014) substantiate the premise that training is central to resilience needs within the sector. Outside of the sector, this is also articulated within White et al and the Australian Professional Standards Council (2015, p.6) which states that professionalization relies upon ensuring: "the continuing competence of members". Work by Polanyi (2009) also explores the concept of hierarchies of human performance, with skills and experiences being built as stratified layers to culminate in a complex outcome, supporting the need to grow knowledge and skills to advance personal, professional and sector goals.

While acknowledging the need for training is a critical first step, the funding of learning and exercising activities will determine whether a good idea is then transformed into an actual outcome. The ECHO (2004, p.4) report indicates that: "Most major donors are willing to fund security measures and training", while noting that implementors cite a lack of funding as a rationale for failing to train staff. The USAID PLSO concept offers varying types of free workshops and training to implementing partners—however, only for a limited number of operating environments, and principally only for USAID funded activities. Bickley (2017, p.46) also notes the cost of financing training and security, stating that: "Many NGOs understand the importance of security training; in practice, however cost and availability remain significant barriers to organizations actually implementing and sustaining security training". However, the matter of funding limitations is unclear, with Kingston (2010, p.7) countering this perspective, offering that: "Whilst donors are increasingly aware of the need for consistent funding for security measures and skills training, there has been no concurrent move by NGOs to capitalise on this awareness, primarily due to poor communication between donors and

humanitarian agencies, or between NGO SFPs at HQ level and security managers at country or project level". As such, it is clear that training is deemed important when addressing both beneficiary as well as implementing partner resilience needs, and that donors have an interest—and potentially a willingness—to invest in training.

Research indicated that training in security risk management—as well as the wider risk portfolio—is clearly needed to protect people, as well as the wider interests of the organization. However, the benefits of security-focused training extend beyond tactical or operational risk management, offering protection to organizations from high-impact and long-term strategic risks. Despite the known risks facing organizations that fail to appropriately train against predictable threats, the sector has yet to clearly define its own training needs through a competency framework. Nor has it developed the standards to which training would be aligned. Stoddard, Haver and Czwarno (2016, p.17) state that unlike fiduciary risk management: "the same is not true for security risk, and many understood their national NGO partners to be exposed to high levels of security, risk, often without sufficient support, training, and discussion". Kravitz and O'Molloy (2014, p.6) also posit that: "In many cases, simple training can go a long way to avoiding serious injury or death". Training can also reduce the reputational and liability risks, as experienced by both the Norwegian Refugee Council and Samaritans Purse for allegations of negligence following incidents of kidnapping. Training is also acknowledged as an important part of evidencing approach duty of care efforts, with Klamp and Associates (2019, p.5) offering that: "there are several ways that a US NGO can lessen the chances that it will be held legally responsible if a US NGO staff member is injured overseas", including providing information on the potential risks so as to ensure that staff then are appropriately "informed" before accepting the risk.

Developing awareness and competency

The provision of effective knowledge and the sharing of relevant experience is the cornerstone of an effective risk owner who can apply knowledge and experience to the unique belief systems, standards and practices of the sector, who is attuned to strategic, operational and tactical risks, who understands the complex impacts of a crisis, and who can form solutions that address the complex interplay of risk. The sector has increasingly become aware of the need to develop leadership awareness and competency

levels (Jayawickrama, 2011), however this has been more focused on disaster risk management than on organizational resilience and security risk management. Critically, the effective security professional needs both professional development within their technical field but must also be able to speak the language of other risk portfolio owners in order to communicate across functional or geographic boundaries. They must also be able to impart knowledge and skills through training and exercising to build competency within those they support. However, research indicates that the availability of appropriate training, at all levels, is insufficient to meet the full and complex needs of the sector, and that no defined body is in place to shape the learning goals, establish agreed training standards, or implement the provision of critical knowledge and skills.

Learner populations

The term "risk practitioner" is used in this paper to discuss those who manage resilience both within and outside of a security remit. Risk practitioners range from the Chief Executive Officer leading the organizational resilience strategy or a crisis response, through to functional roles within Human Resources, IT, Finance, Operations, Legal, Contracts, and Communications. Each has a role in supporting resilience goals which may be triggered by a security incident, or which might address non-security related vulnerabilities. Within the field of security also exists the "practitioner", typically an individual assigned to manage aspects of security, but with little to no formal knowledge and experience within the field of security. Conversely, the security "professional" brings more measurable technical and experiential capacity, has measurable credibility, but is typically grown from outside of the sector.

Studies by both GISF (2009) and Bickley (2017) touch upon the requirement to develop security risk management knowledge and skills within Security Focal Points (security practitioners at the field level) and program managers (risk owners), while also acknowledging the requirement to provide senior-level training and exercising on crisis management (operational and strategic risk owners). Any individual involved in resilience is, to a greater or lesser degree, grown through the influence of who they are, and where they are, on their personal and professional learning journeys (Engestrom, 2001). The influence of transitional learning as individuals exit one career and enter another (typically from a military or police background for the security professional), and the application of transdisciplinary

knowledge (Gibbons et al, 2002), has a strong influence on the way in which resilience is shaped, prioritized, and then articulated through standards, practices and ultimately training. The influence of the continuum of learning (Eraut, 1994) upon those leading organizational resilience as either a risk portfolio practitioner or security professional also either enhances or hampers the sector's ability to evolve and strengthen resilience, as individuals mature and evolve along their own individual learning journeys.

Proximal and distal learning

Security practitioners and professionals, as well as those managing other aspects of the risk portfolio, also need to balance technical knowledge with direct experience. Brabant (2001, p.9) notes that: "There is now broad consensus among agencies that the priority is not awareness, but management training. Underlying this is an admission, sometimes unspoken and even unrecognized, that "field experience" provides fertile ground, but does not automatically and by itself mean "full competence". While experiential learning clearly offers opportunities to situate the production of new knowledge in a context-rich environment (Gibbons et al., 2002), this also potentially limits knowledge growth, as experiences can often be repeated with diminishing returns on learning outcomes. While tacit knowledge is invaluable, being able to evidence a credible source of knowledge—certainly where litigation and reputational risks exist—can be critical. In addition, where risk is concerned, individuals who learn "by doing" can inadvertently place people and organizations in harm's way. As organizations define their training needs, it is important to understand that: "everyone's perspective on the world is influenced by and mediated through contextualized (socio-cultural) systems of meaning. Such cognitive frames provide our experiences in reality with meaning" (Duijnhoven and Neef, 2014, p.425). This presents a challenge, as there is no single truth to map the training needs within both the security community and those managing other facets of risk. Rather, there is a collection of individuals applying their own individual truths inconsistently, and without agreed and potentially appropriate controls. While this is arguably inescapable, more established professions do exert appropriate controls by constructing professional peer-reviewed standards, as well as more defined learning pathways through a universally agreed upon competency framework. The knowledge shared should be credible and should be recognized by awarding bodies as representative of proven best practices, creating a consistency of standards within the sector.

Learning models: opportunity driven, incremental and directed

There are three mechanism by which individuals or groups can advance: 1) opportunity-based, 2) by repetitive action while in role, and 3) through directed learning programs. Directed learning offers opportunities for individuals to rapidly expand their knowledge and skill base, rather than being forced to wait for random experiential learning opportunities to occur, or where they are exposed to low value repetitive role-based learning. Gibbons et al (2002, p.140) recognized that: "knowledge is dynamic. New concepts, methods and instrumentation are being continuously created leading to new capabilities and know how", while Eraut (1994, p.208) notes that: "capability can be said to provide a basis for developing future competence, including the possession of the knowledge and skills deemed necessary for future professional work".

Directed learning offers a defined and progressive learning pathway with compressed areas of competency development, without necessarily compromising the contextual application of knowledge. While there is currently a diverse range of training available to meet individual safety and security awareness needs, there is an absence of third-party certified leadership training on resilience[4]—including specifically on security risk management and organizational resilience. This gap undermines a top-down approach to the production of knowledge and the resultant strategies, standards and processes this learning then triggers. The ECHO (2004, p.2) report discusses the weaknesses of accessing training, indicating that: "staff competence is the most significant weak point in current security management" and that barriers include "the ability to source, and access, appropriate training resources". This gap spans all aspects of the community, from the executive leaders who develop the resilience strategies and define organizational standards and practices, senior functional risk owners managing their portion of the risk portfolio, the security professionals and practitioners who sit at the nexus of many of the risk issues, to program leaders managing program delivery—and often at the point of crisis. The shortfalls in training also impact the individual, whether an international or host nation staff member. As a result, gaps in knowledge and experience production weaken the legitimacy of the security community as it cannot evidence the origin and legitimacy of its own best practices.

[4] Withstanding INSSA's Regional Security Manager and Security Focal Point program.

The effectiveness of first authoring and then operationalizing resilience measures lays with the security and wider risk portfolio community, whether these are experts within the sector, professional forums and institutions, centers of learning and excellence, or commercial companies who develop learning products for financial gain. Academic institutions also play a critical role in developing higher level competencies, meeting the needs of more experienced or senior professionals in their individual learning journeys, as well as validating—through research—organizational and sector level strategies and standards (Scott et al, 2004). It is from these sources that the security and broader resilience community is shaped and provided the mechanism to evolve.

CHAPTER 3

RESEARCH METHODS

Introduction

This chapter outlines the empirical research methods used in the preparation of this thesis. It provides insights into the design and implementation of three research instruments used as part of a sequential mixed methods approach; including an initial online survey of 77 participants (from a pool of 100 candidates), semi-structured interviews of 32 participants (from a pool of 50 candidates) which built on the results of the survey, and a focus group of 10 participants (from a pool of 15 candidates) focusing specifically on sector resilience competency frameworks, which ran concurrent to the semi-structured interviews. It explores the rationale behind the selection of the research participants for the initial survey and the subsequent semi-structured interviews and focus group, and how each group was approached to ensure that a solid foundation of both qualitative and quantitative data was gathered relating to organizational resilience at the strategic level. It also looks at how the initial survey then influenced the subsequent selection of research participants, and how the semi-structured interview and competency framework group questions and engagement strategy was structured. Case examples were also used to highlight real-life examples of where resilience failed, and the resultant impacts upon the sector.

This chapter also addresses researcher reflexivity and key ethical considerations – critical in that the researcher is a professional within the field of organizational resilience, and as such research integrity, validity, and objectivity (Drake and Heath, 2011) was of paramount importance.

Theoretical framework

The focus of the research is problem-based: "**the humanitarian aid and development community operate within increasingly high-risk environments and must be resilient in order to effectively protect both people and organizational interests**". The objective of the research is to contribute to

the body of academic knowledge, while concurrently offering action-based outcomes to benefit both organizations and security professionals.

The theoretical framework leverages Wenger's social theory of learning (2017) coupled with La Porte's theory of high reliability organizations (1996), both of which are applied to the context of resilience in that ultimately high-reliability organizations are defined by both the individual and collective negotiated meaning of what constitutes resilience, how practice results from the joint enterprise of a community to share perspectives and define accountabilities, how a community of practitioners define social configurations in which enterprises are defined as "worth pursuing", and how learning changes who we are within the community.

Research design

The goal of the research was to explore the concept (Bryman, 2001) that organizations operating within the humanitarian aid and development community are faced with increasingly complex and dynamic risks, coupled with the influence of diminishing employee and donor tolerances for risk. Combined, these require a highly sophisticated approach to organizational resilience. The scarcity of research data on humanitarian aid and development sector resilience illustrated a significant gap within both academic and grey literature focused on "organizational" or "strategic" resilience for those implementing work on behalf of donors, or as funded by charitable contributions. This highlighted the need for research focused on specific-to-sector resilience, through which meaningful action-based outcomes might address both current and future sector risks.

Research question

Recalling the statement of the research goals addressed within the introduction, the problem the research sought to address was to assess the complex, interrelated and fluid threats the sector faces against the mechanisms required to appropriately counteract the resultant risks. The research question asked: "**what risks does the sector face, what is driving change, and how can the sector professionalize its resiliency strategy**". The research question was broken into component five parts, each of which is addressed as a define point within the thesis:

1) What risks exist, what are their impacts, and what constitutes resilience?
2) What enables the process of professional convergence?
3) How can knowledge, skill and experience be codified through standards?
4) How can external resources expedite professionalization?
5) How can knowledge and skills be operationalized through learning?

Epistemological and ontological considerations

The research design considered Gibbons et al concept of knowledge production (2002), applying the goal of Mode One which seeks to contribute: "ideologically or theoretically to academic fields of knowledge", as well as Mode Two which seeks: "to make a significant contribution to practice and practitioner knowledge" (Drake and Heath, 2011, p.72). The research design was intended to lean more towards Mode 2, in that action-based outcomes might bring practical value to those leading on resilience within the sector. However, it also sought to concurrently bring academic value, simultaneously contributing to the body of academic knowledge.

Work by Bryman (2016) supported the identification of suitable research methodologies, including the options to employ a cross-sectional research design, experiential design, longitudinal design, the use of case studies and examples, and the option for comparative design. These were explored to determine the strengths, weaknesses, and potential applications within the thesis research strategy. Practical issues influenced the choice of the research methodology and the instruments used, including researcher experience, time and the bandwidth constraints, availability limitations of participants, and sensitivities over the research content. As such, a two-step approach was adopted: 1) The use of an online survey to lay the foundations of knowledge through the gathering of largely quantitative data, with a limited level of qualitative inputs by participants, and 2) using survey data and experience to shape the subsequent semi-structured interviews and competency framework focus group. All instruments were also used to identify case examples to illustrate sector specific crises.

The semi-structured interviews were designed to gather a rich source of qualitative data for the thesis on several areas of focus (the key questions) which had been addressed from a largely quantitative standpoint within the initial online survey, while the focus group looked specifically at competency frameworks for sectoral resilience. A detailed literature review also supported these two steps,

exploring the available academic and grey literature surrounding resilience within the sector, or where data was absent, non-sector-specific literature which addressed resilience of comparative value on the theory of organizational resilience. Case examples were also included where the sector has suffered from crisis incidents; these were garnered from both the literature reviews, open media sources, and as an output of the semi-structured interviews.

Given that this research was implemented by a research practitioner with an insider's vantage point, the inductive theory (Bryman, 2019) was used, with observations and findings driving resulting theories and concepts found within the Discussion Chapter of this thesis.

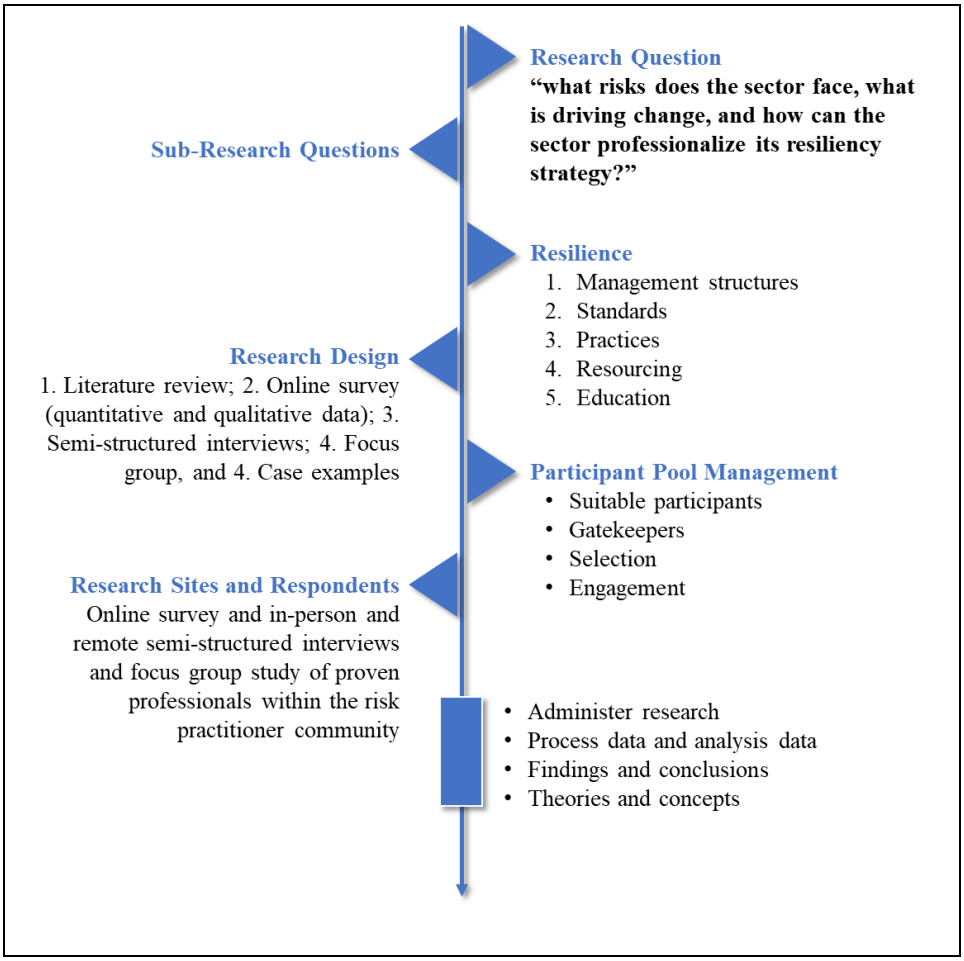


Figure 3: Research Strategy

The empirical realism methodology was employed (Bryman, 2001), as the research sought to define reality through observation and experience, with this observation reflecting the personal and professional opinions of the research participants. The research accounted for subjectivity surrounding what "risk" means at the individual, group, and organizational levels, coupled with the complex implications of different forms of risk, with opinion gained through observable phenomena and events. This provided tangible examples of the importance of resilience and how risk controls can be applied within complex and fluid

environments. Critically, it also demonstrated, through case examples, the serious implications where risk controls and resilience strategies are not in place, or where they failed.

The ontological approach of social interactionism (Blumer, 1986) was used, in that participant observations might originate from personal deep-seated beliefs, and that their knowledge is only gained through personal experience. This influence, if substantiated through research, might expose key impediments to evolving resilience practices within the sector, as standards must be shaped by a collective body of knowledge and belief to form a profession, rather than the disaggregated beliefs and practices of individuals. Given the understanding of risk is highly subjective and the participant pool was not a homogenous group, the principles outlined by David de Vaus within his **Surveys in Social Research** (2014) were applied in that the analysis of the data gathered requires creativity and imagination from the researcher to gain an accurate understanding of the meaning of the data gathered. As such, the survey and subsequent interviews and focus group sought to explore how out-of-sector traditions and cultures might be viewed as "unworthy" (whether consciously or unconsciously) of consideration, and how a coming together of experience and opinion might contribute to agreed-upon standards and practices within a diverse population of security professionals, practitioners, and other risk owners.

Research methods

The research method sought to separate what was known to be true, from what is believed to be true. This is important, given the high levels of subjectivity surrounding what "risk" and "resilience" means to both the research participants and the researcher, and how a broad range of resiliency measures might then be effectively applied across a diverse and dynamic sector. An exploratory sequential mixed methods approach (SAGE publications, 2019) was adopted, moving from an online survey methodology in order to explore and analyze largely quantitative data, before using the results to then shape the qualitative semi-structured interview and focus group research approach, as well as which participants to include within each group. All three research instruments drew upon the concept of social interactionism (Becker, 1982) in that the knowledge gained from survey responses and subsequent interviewee dialogue was based largely on personal experience.

As explored by Drake and Heath (2011), having privileged access to senior and highly experienced research participants influenced the methodology used for the online survey, semi-structured interviews and focus group, impacting how experts across a broad range of organizations were approached. Bryman's (2016, p.29) "messiness of social research" was also identified as an important influence on the applied research methodologies when seeking to design a replicable system which draws personal insights from a unique pool of highly seasoned and well-placed participants. From the outset, it was accepted that social phenomena and their meanings are being continually introduced and revised by social actors within the security community; and that the operating environment also shapes the risks which individuals and organizations must continually manage. The implications these shifting risks have upon people, operations, assets, facilities, information, business interests and organizational reputations, both past and present, were also key considerations. It was recognized that those engaged in the study did not form a homogenous group, but rather brought different attributes to the research in terms of career paths, education, qualifications, risk and crisis related experiences, sector or industry influences, and cultural and social dynamics.

Research participants

The online survey included a wide cross-section of sectors and industries, while the semi-structured interviews and focus group included only humanitarian participants. **Figure 4** shows the breakdown of military, police and civilian participants across all three research instruments. The high representation of government primary career start-points summarized under "Government Services", compared to those coming from a civilian career start-point reflects the overall propensity for security professionals to come from a foundational security background (this combines military, police and intelligence into a single category[5]). This is later supported in the thesis by commercial research on organizational recruitment sources for security professionals. However, the civilian representation is still comparatively high, illustrating the increasing movement of civilians with no formal grounding into the security community.

[5] The chart shows greater than the 77 survey participants as some have a mixed career field which results in a double counting effect – such as a military professional also having a second career as a police officer before starting a third career.

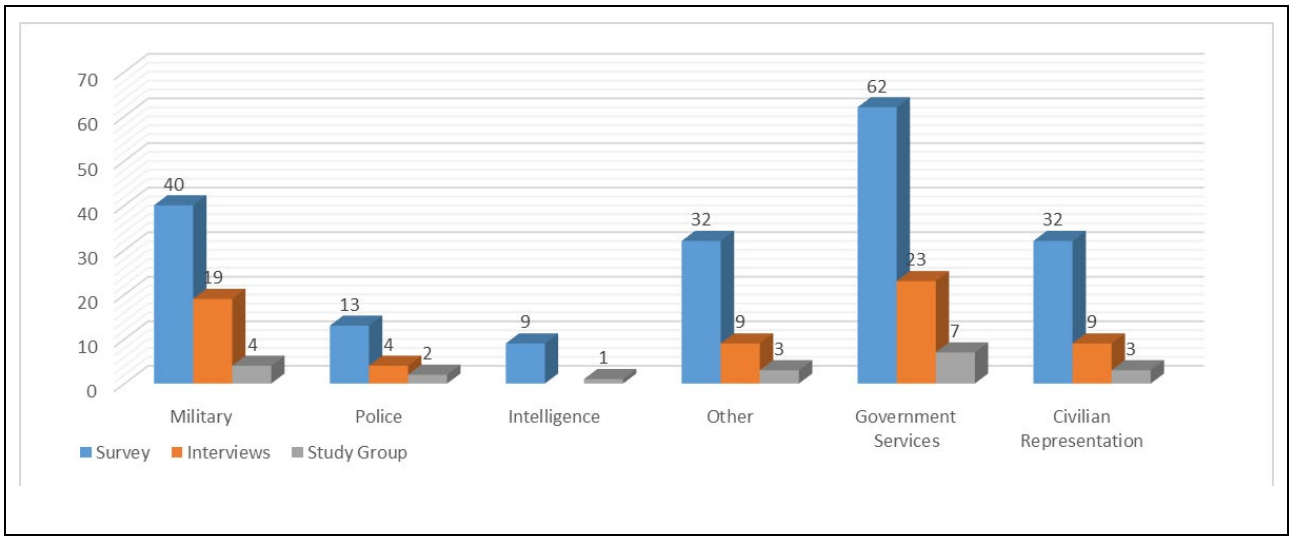


Figure 4. Summary of Research Participants

Figure 5 illustrates the goal of the study to be inclusive of women and members of the LGBTQIA community within the research. This is important, as currently there is an under-representation of women and members of the LGBTQIA community within the security community at large, while there is a strong proportional representation of women and the LGBTQIA community within the humanitarian aid and development sector workforce given the positive influence of civil rights groups, coupled with the greater levels of sensitivity over inclusivity.

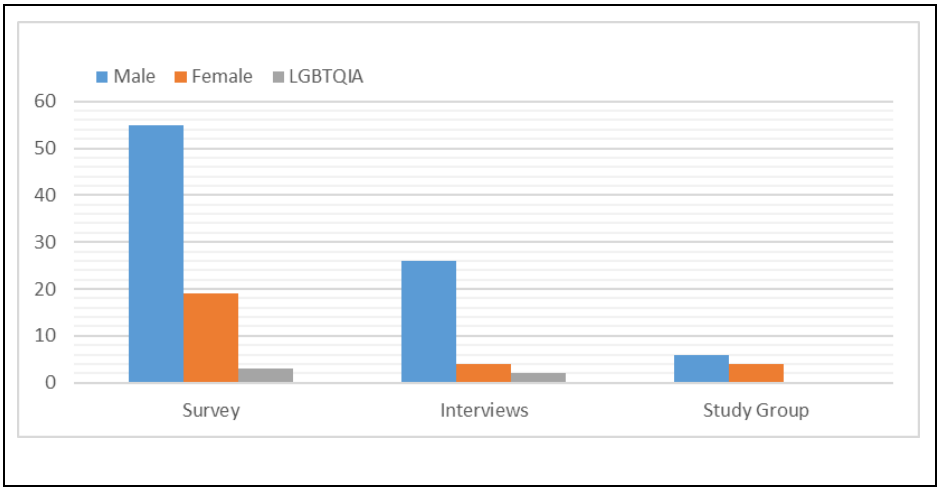


Figure 5. Participant Gender and Self-Identification data

Participants across all three data gathering instruments were selected based on: 1). experience, with at least 5 years professional experience within the field of security, 2), international exposure, with all having experience in multiple high-to-extreme risk environments, and 3) seniority, with all holding a

management or leadership position. The research pool represented a group of highly seasoned professionals who brought personal insights across the tactical, operational, and strategic spectrums. Within the semi-structure interview pool and competency framework focus group the current geographic responsibilities of participants were mapped to enable an analysis of the complex interplay of risk factors participant organizations face, including: 1) the criminal, social disorder and terrorist security risks, 2) natural hazards and disasters, 3) cultural, legal and social factors, and 4) infrastructure vulnerability and reliability. **Figure 6** shows the current geographic coverage of the semi-structured interview participant group.

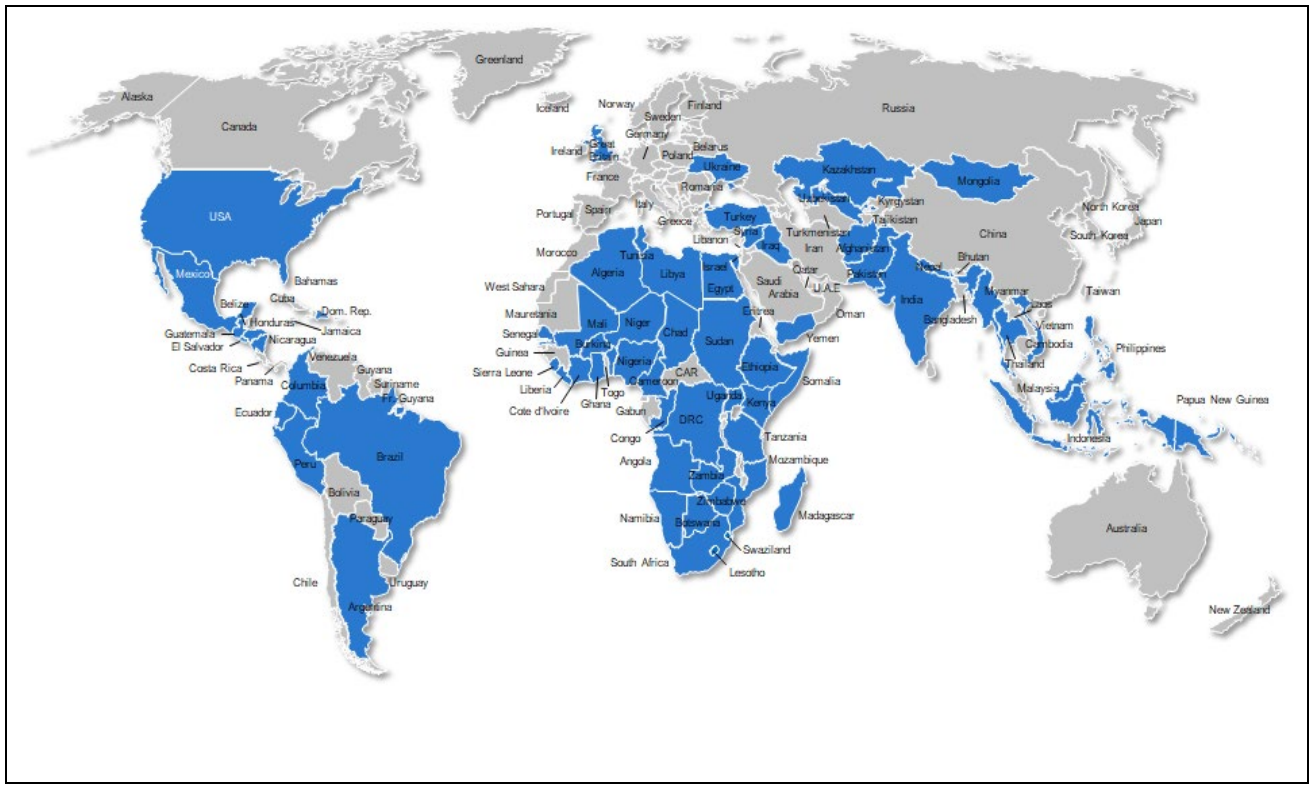


Figure 6. Participant Geographic Responsibilities

Literature review

A literature review was conducted at two key milestone points in the research, with ongoing literature reviews being conducted over the course of the research. The milestones were: 1) prior to the survey tool being released, and 2) prior to the semi-structured interviews and focus group being conducted. Both academic and grey literature was sought to establish a baseline of understanding of how resilience

was perceived, and how it is implemented within the sector. Forum groups, such as GISF[6], yielded significant studies at the operational and tactical levels focused on security risk management. Limited studies and papers were also produced by InterAction on the MOSS standards (a derivative of the United Nations Minimum Operating Security Standards, 2009); Devex[7], INSO[8], INSSA[9] and similar groups who release articles and interest stories related to sector-specific security concerns and crisis case studies. Limited literature also exists on resilience in terms of legal risks through Kemp and Merkelbach (2011), and Brooks (2018). Significant studies have also been conducted on the risks the sector faces through studies by Hoelscher, Miklain and Nygard in their paper **Understanding Violent Attacks against Humanitarian Aid Workers** (2015), by Behn and Kingston (2010), Bradant (2012), and by the Humanitarian Outcomes group paper **Behind the attacks: A look at the perpetrators of violence against aid workers** (2017). Significant research has also been conducted by the United Nations, USAID, World Bank Group, DFID, ECHO and other institutions and agencies on community, climate and food and security resilience—all of which have a direct bearing on the humanitarian aid and development sector risk and resilience. Kovacs, Spens, Tabaklar and Oloruntoba have also provided extensive research on supply chain resilience within the sector and the importance of "borrowing" knowledge from more established disciplines. However, a significant gap in academic literature exists on "organizational resilience" within the humanitarian aid and development sector, with limited studies (whether academic or grey) addressing how the strategic interests of implementing partners are protected within an increasingly dynamic and hostile world.

[6] GISF was formally EISF and provides a fusion point for NGOs globally on security related matters, including for the production of studies, working groups and training resources.
[7] Devex provides the sector platform for sharing concepts and best practice on a range of issues within the sector, including regarding security and professional development.
[8] INSO offers the sector a fusion point for sectoral security risk management information and best practice.
[9] INSSA offers the sector a competency framework and management qualifications for the professional advancement of security professionals and practitioners.

The online survey tool

The design of the online survey was informed by the initial literature review and reflected methodology outlined by Creswell and Guetterman (2019, p385). It was determined that a mixed-methods approach would be used for the survey, collecting statistical data as the main focus of the instrument, but with the ability to access basic participant observations through a combination of closed and open-ended questions. All respondents held risk management leadership roles.

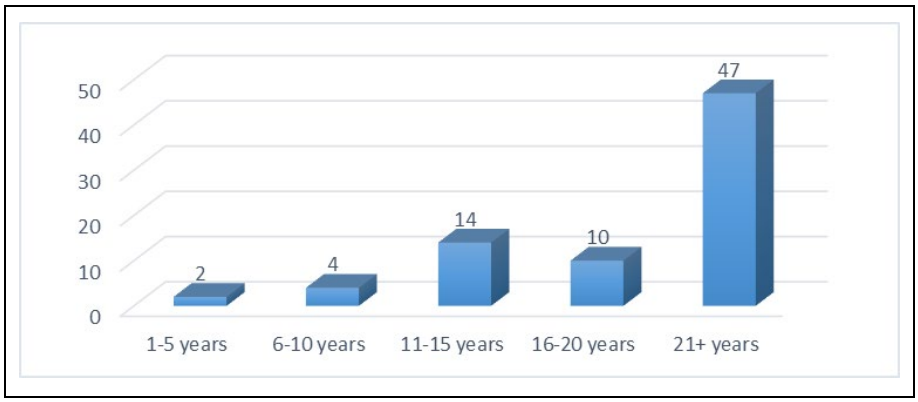


Figure 7. Survey Group Years of Professional Experience

The survey is a tool used to collect consistent data to understand, and then define, the beliefs or experiences of a defined population—in this case the humanitarian aid and development security community (Robson, 2011). Surveys employ questionnaires focused on thematic areas of interest, allowing for statistical data to be gathered from a sample population. A Likert scale was used (Bryman, 2001) to score observations. The thesis drew upon a survey population of 77 participants from an original pool of 100, which included a broad cross-section of both humanitarian aid and development sector representatives, as well as diverse cross-section of commercial security professionals to offer a comparison of how the sector operates against their commercial peers. The majority of participants brought over 10 years of professional experience, as shown in **Figure 7.** Many participants had operated in both the humanitarian and commercial spaces. The online survey questions are found in **Appendix 1.**

The literature review highlighted a heavy focus of grey literature on operational and tactical security risk management, with a noticeable absence of both academic and grey literature on organizational resilience and business continuity management within the sector. This gap in research then shaped the structure of the survey questions. Specific lines of questioning addressed how resilient organizations are, the degree with which recognized standards are applied, how document systems

are valued or used to codify standards and practices, how resilience is integrated by organizations, and the perceived importance of training and exercising.

The process of identifying and engaging the diverse pool of participants was enabled through direct access to both peer and client security professionals (with a heavier focus on security risk management professionals). The process started with identifying 50 humanitarian organizations representing various sub-set communities, such as faith-based groups, philanthropic organizations, charities, and human rights groups (Brech and Potrafke, 2014). These formed the humanitarian participant group. A group of 50 commercially orientated organizations was also selected to enable a comparative analysis, with a heavy representation from the extractive industry, as well as the commercial risk consulting and security sector. These commercial groups were then augmented by other sectors, such as construction, IT, and hospitality. Each survey participant was directly engaged with the choice to respond to an anonymous online survey questionnaire, with data collection occurring over approximately eight weeks.

While the survey was straightforward and yielded good results from a large proportion of the research group, it was found that by including both commercial and humanitarian aid and development sector participants, some findings were weighted, potentially distorting some aspects of the data gathered. In addition, while the quantitative data was comprehensive, the qualitative data was limited in that the majority of respondents offered little to no narrative against their responses. As a result, the qualitative data lacked the granularity required to draw sufficient context from the data gathered. In addition, the survey failed to include useful areas of study, including how professionals were supported during their transition from a primary career into humanitarian security, their perception of the value of a military or police background, and how forum groups contribute to sector resilience strategies. These shortfalls then refined how the second phase of data gathering was structured.

Semi-structured interviews

The lessons learnt from the survey phase offered useful insights which shaped the semi-structured interview approach, in terms of: 1) who would be invited to participate within the semi-structured interviews, 2) what questions would be used within the interview process, 3) how much flexibility would be used when interviewing participants, and 4) how would data be analyzed following the

interviews. It was determined that while commercial security representation was useful during the survey phase to enable a comparative analysis, that only participants from the humanitarian aid and development community would be used for the interviews as the inclusion of too broad a ranging participant group would dilute and potentially confuse the findings. The interview questions (**Appendix 2**) followed the same themes used for the survey, but expanded some on specific points:

1) Are organizations in the sector appropriately resilient to risks?
2) Are there recognized standards and practices organizations work towards?
3) What is the value of qualifications and certifications to individuals within the field of security?
4) Is there value in codifying standards and practices through the use of document systems?
5) Is resilience effectively integrated into organizational structures and practices?
6) Is the concept of "acceptance" still valid in terms of reducing risks?
7) The perceived value of training, exercising and testing within the management of risk.

From this foundation, additional questions where then added to the semi-structured interviews during the process of exploring ideas with participants, including:

1) What risks most significantly impact organizational resilience and business continuity?
2) Are any supporting frameworks or resources in place to assist with career transitioning?
3) What advantages or disadvantages to primary career fields are offered?
4) What forum groups and "communities" exist which help with forming resilience strategies?

A potential research pool of 50 candidates was identified from a wide cross-section of "for profit" and "not-for-profit" organizations, of which 32 participated. In addition to senior security risk management professionals, the interviewee pool also included legal specialists to draw out legal opinion on the importance of resilience, as well as the legal ramifications of risk. Several of the participants were also published authors in the field of humanitarian security. **Table 2** defines the semi-structured interview group in terms of their position within an organization, as well as their technical areas of responsibility:

Group	Participant Level and Focus	No
A	**Global Security Directors:** Leading organizations in global security risk management. Advising the executive leadership team on strategic to tactical risk measures. Acting as a senior technical advisor to high-impact and fast-burn crisis situations.	21
B	**Regional Security Managers:** Responsible at a multi-country or national level for security risk management. Leading the local response to emergency situations. Acting as a technical advisor to the Crisis Management Leadership Team and the Global Security Director.	6
C	**Legal Experts:** Supporting organizations within the humanitarian aid and development sector with legal action as a result of security-related incidents.	1
D	**Risk Leaders:** Responsible for security risk management as a component of their wider duties – where organizations have no defined Security or Risk Department.	4

Table 2. Semi-Structured Interview Participant Roles and Responsibilities

The average professional experience of participants was over 10 years, noting many had spent at least 15 years within the military or police before joining the humanitarian aid and development community. The gender breakout was 4 women, 26 men and 2 members of the LGBTQIA community. Interviewees represented the following in terms of their primary foundational careers:

1) Military backgrounds: 19.
2) Police backgrounds: 4.
3) Non-conventional backgrounds[10]: 9.

Once data was gathered, the results were coded (Bryman, 2001, p.186) into an excel Coding Schedule, ensuring that participants were assigned a number and pseudonym to protect their identify. The results were captured into the following core thematic areas:

1) The risks the community faces.
2) The reputational concerns the community must manage.

[10] Backgrounds without a formal security basis.

3) The meaning of "resilience" within the security community, as well as their organizations.
4) Why resilience is needed within the sector.
5) What catalysts have driven organizations / the community to adjust their resilience strategies.
6) The value and importance of education to organizational resilience and business continuity.
7) How are professionals recruited, and what transitionary structures aid them in their new role?
8) How are security professionals and practitioners positioned within their organization?
9) How standards are perceived, and applied, to organizational resilience.
10) Does "acceptance" still have a place within the risk management framework?
11) What forum groups exist, and what value do they bring?
12) The influence of external stakeholders—donors, communities and governments?

The semi-structured interviews sought to explore whether humanitarian security professionals and practitioners, as well as those owning other aspects of the risk portfolio, have the bandwidth, organizational support, codified standards and practices, and effective positioning to be heard within their organization. It was deemed that these factors would enable individuals to be better positioned to address areas of super-complexity (Barnett, 2000) within not only a rapidly evolving risk environment, but also in how individuals evolve professionally and academically.

Both interviewer and interviewee bias were a consideration in terms of developing the semi-structured interview questions, and how these questions were then presented to the participants. Open-ended questions were used (Bryman, 2001, p.142), allowing respondents to answer on their own terms, and to explore areas outside of the original intent of the research. The coding strategy encountered the challenge of discrete dimensions (Bryman, 2001, p.188) where conceptual and empirical overlaps occurred. This was found where standards of training were concurrently addressed in terms of standards within document systems. In addition, mutually exclusive categories were also a consideration to ensure that clear boundaries were set where thematic areas might pull answers in to one or more categories. An example was organizational risk, with a sub-category of reputational risk.

Competency framework focus group

The survey and semi-structured interviews highlighted two critical areas associated with resilience: 1) the development of standards by a body of recognized experts, and 2) the operationalization of these

standards through training. To establish how standards could be mapped to education and operationalized through training a focus group was formed to explore the concept of "competency frameworks". Members collaborated and shared ideas and experiences on the specific topic of competency frameworks and their values, before contributing observations via a simple questionnaire. The Delphi method was adopted, using a two-step process to present a question, and expand upon the resulting commentary. This focus group (Bryman 2001, p335) was comprised of 6 male and 4 female participants, of whom 7 came from a government services background, with 3 coming from a civilian primary career field.

Participants attended two remote webinar sessions where questions were presented to the group, and as a group they explored ideas and experiences. These were not taped to ensure privacy, allowing participants to discuss potentially sensitive case studies and/or controversial experiences. The researcher acted as a moderator to present questions on key areas of interest, after which the participants had an open forum to explore their ideas and challenge each other through discussion. Where a point was unclear, the researcher presented clarifying questions, or confirmed key points raised to reduce any potential ambiguity. At the end of the second moderated session, participants were then sent a questionnaire seeking their opinion on the value of establishing a competency framework against which the security community could be educated (see **Appendix 3**). The resulting narrative was then applied to the research. The decision to not record the focus group sessions potentially led to a loss of some data as the narrative was hand-written during discussions, however the approach enabled an open sharing environment where sensitive topics were explored in depth. On reflection, participants could have been offered the opportunity to strike any controversial remarks made from a taped transcription to better mine observations made during the focus group sessions, while protecting their interests.

Research reflexivity

The research approach included reflexivity throughout in terms of why the approach was used, and how potential ethical considerations were effectively addressed so that participants and the researcher were not unintentionally compromised in what is a sensitive and potentially highly contentious area of study. This is especially pronounced as any negative comments, or case studies, offered by participants could compromise their employment status, or the well-being of their employer.

The concept of "researcher identity" and conducting research within the researcher's own practice area (Drake and Heath, 2011) underpinned the relationship between the research methodology and the researcher's practice-based experience. When designing the research approach, the researcher was forced to candidly reflect on the strong and embedded values and beliefs which result from a personal experiential and academic learning and development journey (Vygotsky, 1980), and the influence this has upon the research design, strategy and the associated methodology employed. Engestrom's "Activity Theory" (Drake and Heath, 2011, p.61) also shaped the research in terms of how both the researcher and research participants are influenced by who they are, and where they are. This was especially relevant as it shaped the research questions, as well as how the participant's personal context shaped their responses.

Ethical issues

Ethical considerations included virtue ethics, deontological ethics, and consequentialist ethics (Drake and Heath, 2011, p.49), shaping how participants were selected and engaged, and how their contributions were applied to the thesis. As a researcher practitioner virtue ethics was applied in terms of personal integrity. As a professional within the field of security, deontological ethics were reflected in my moral duty to both the research goals, and to the professionals supporting the study. As a business owner consequentialist ethics also played a key role in the implications to the reputation of both the participants, and my personal business interests. Collectively, these supported a robust approach to how ethics guided the research.

The ethical controls used sought to reflect the unique risks associated with some of the more probing (intrusive) questions relating to organizational resiliency. Where case examples where discussed, these also presented the potential to compromise (legally and reputationally) both the interviewee as well as the organization they have in the past, or do currently, represent. The ethical standards and guidelines provided by Portsmouth University were also used as a foundation for the ethical approach used, with further levels of risk control being applied by disregarding any data which might be damaging to a participant or to their employer (current or previous). This included explicit consent from participants, the researcher applying professional judgment when utilizing potentially sensitive comments, and robust data protection of the survey data and interviews.

CHAPTER 4

RISK, RESILIENCE AND CATALYSTS FOR CHANGE

Introduction

This chapter presents the findings of the primary research into the sector's perception of risk and examines what has motivated organizations to change their approach to resilience and business continuity over the past 15 years. These findings constitute the foundation upon which standards and practices are defined, establish the importance of the security community within the sector, and shape how competency frameworks and the community of security professionals might be developed. The chapter discusses why security risk management is important, what it seeks to achieve, and what catalysts motivate current and future change.

Risk means different things to different people. It impacts people, operations, assets, information and business, along with the reputation of individuals, activities, locations and organizations. Risk tolerances are also dynamic (Kingston and Behn 2010), being influenced by individual, group and sectoral knowledge, experience, culture, and resourcing. The quality of risk data varies greatly (Guha-Sapir and Below, 2002) and the perception of risk is also influenced by external factors such as the physical environment, government regulatory requirements, donor and government expectations, and societal expectations. Risk tolerances also function at the organizational, activity and individual level, with significant variations directly impacting how risks are addressed, and the resulting level of investment (time, commitment and money) made into organizational resilience. Tolerances are also subject to hypersensitivity at one end of the spectrum, and risk fatigue at the other. Where a crisis occurs, external influences, such as litigation (Ross and Sidebottom, 2017), negative media exposure and community perception (or outrage), as well as donor and government demands, can also drive change. The increasing importance of "Duty of Care" is also a motivating factor (Merkelbach, 2017), as both employees and donors expect more from the sector and its members. Resilience also has many definitions (CARRI, 2013), whether relating to psychology (Windle, 2010), community resistance against disruptive incidents (CoBRA, 2012; Haase, Ertan and Comfort, 2017), for natural disasters (Dilley et al, 2005), terrorism (EuroPol, 2017) or for international standards for organizational

resilience (ISO 22316). The lack of a consistent understanding and accompanying vernacular makes defining risks and establishing corresponding measures to reduce the probability and impacts of a crisis highly challenging.

Where formal research into the risks faced by the sector is conducted—whether externally driven or resulting from an internally-identified need (Egeland and Harmer, 2011)—then the willingness of executive leadership teams to accept the findings and associated recommendations determines how resilient organizations become, and how much importance is placed on security (Khorany, 2017). Some findings may drive change which is painful and costly, while other changes may go against the ethos of the organizational decision makers—certainly until a "new normal" takes root.

The purpose of this chapter is to explore strategic, operational, and tactical level risks, the difference between the headquarters and field approaches to risk and resilience, and how donor or government perceptions, employee expectations and the operating environment is encouraging, or forcing, change.

The risks the sector faces

This section looks at the varied risks the sector faces, not only from a security standpoint, but also risks to the wider business interests of humanitarian aid and development organizations. It is against these multi-faceted and evolving risks the sector faces now, and in the future, that resilience measures are aligned to ensure that risks can be effectively and preemptively identified, mitigated, controlled, or managed.

The research findings from both the literature reviews and the semi-structured interviews suggest that there are three categories of risks: 1) strategic risks, which impact the wider interests of the organization beyond the immediate effects of an incident; 2) operational risks, which impact a defined activity or outcome, and 3) tactical risks, which impact specific and isolated points of vulnerability (people, places, assets). These risk levels then influence four thematic areas of risk, including: 1) people, whether physically or psychologically; 2) assets, in terms of facilities, materials and information; 3) operations, in terms of activities and outputs; and 4) business, in terms of opportunity, finance, contracts, litigation, and reputation. Other factors also shape the perception of risk, such as societal influences (nationality, culture, race, religion), and the physical environment (geography, health,

infrastructure, humanmade threats and natural hazards). Tom[11], a seasoned risk consultant and published author who has held multiple senior positions within major humanitarian organizations, also suggested that donors are forcing organizations into areas with known terrorist problems in an effort to combat insurgency and transnational terrorist threats:

> "You see more funding for international development coming through stability operations, trying to either mollify or give new opportunities to people in areas likely to be impacted by transnational terrorism, to try to put a downward pressure on the ability of these groups to recruit locally. That's where the money is, and so I see more and more NGOs getting drawn into that".

This then further elevates the risk to the sector as organizations are both inherently at risk from hostile actors, but then face additional risk as they directly support foreign government efforts to undermine the activities of these violent groups. These interlocking factors, as illustrated in **Figure 8**, highlight the complexity associated with effectively evaluating risk. This complexity demands both a sophisticated and nuanced understanding within the security profession of how risks are layered and resonate collectively.

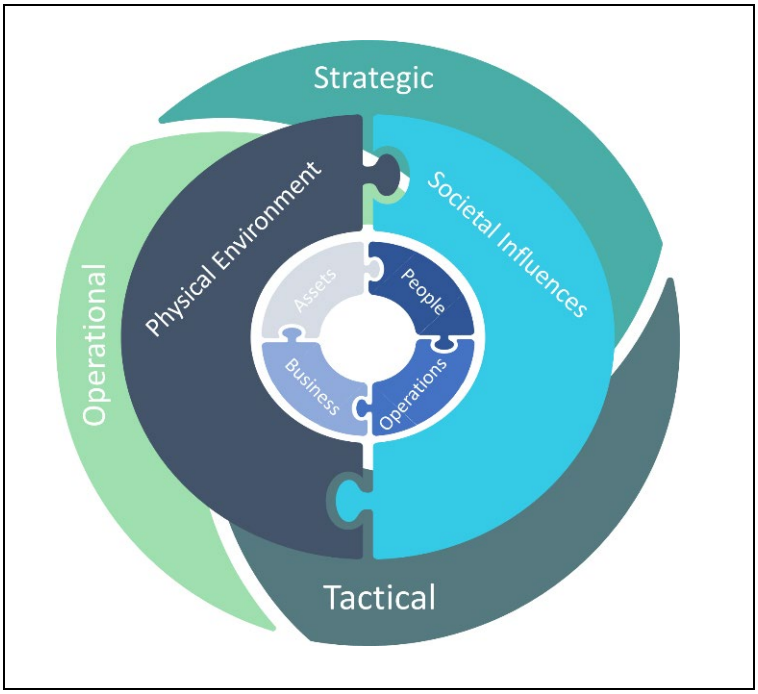


Figure 8. Blyth Layering Risk Considerations (2020)

Many of the those interviewed commented on the escalating nature of specific risks which have a direct impact on organizations in terms of how they now think and operate. The rise of domestic and transnational terrorism, exacerbated as prominent threat actors focus increasingly on both western interests and specific humanitarian aid and development activities (gender, human

[11] Real names are not used for any interviewee or focus group quotations.

rights, education and health initiatives) has elevated some groups into a higher-risk category. Anna, a senior regional risk advisor for a major development group, commented on these increasing and evolving risks, and how they have required humanitarians to rethink how they operate within environments where this risk had not been historically present:

> "There is an increasing risk certainly in the areas of terrorism and being targeted. NGOs now are being increasingly targeted in areas that they used to not be. They are facing more risks".

The maturation of risk perceptions by both the security community and their organizations has led to the realization that security risks are, in themselves, often not the primary disrupter of deeper and more long-lasting organizational interests. Rather, security incidents will trigger a crisis if risk and incident response management measures are ineffective. Security professionals are also coming to realize that another factor that must be included in their resilience strategy is the nature of the work they perform, whether it is associated with youth programs which bring unique *locus parentis* legal obligations and intense media exposure, or where grant funding activities might expose organizations to anti-terrorism financing vulnerabilities or aggressive government scrutiny. Debbie, a Global Director of Security for a major humanitarian organization, noted that physical risks are well understood and easy to plan for, but that reputational risks are often the greatest cause of harm, being influenced by the profile of the organization and the nature of their programmatic activities:

> "It depends also on the profile of the organization. Of course, the physical one is quite obvious in the field in areas in which NGOs are working, but the reputational risk has a huge impact on the operation, on the operation of donors and on activities".

Camila, the risk focal point for a major development organization, also stated that reputation was the greatest risk, speaking to the rapidly growing need to meet, and demonstrate, duty of care obligations for people (including full-time employees, consultants, fellows, interns, volunteers, and event participants), and how a perceived or actual failure to protect people could lead to litigation, as well as harming donor funding opportunities:

> "I think the greater risk is to reputation, whether that is an individual having an issue and then turning around and accusing the organization, or in terms of reputation with donors. And, if

> they're not doing a good job with duty of care, then they are less likely to be competitive and to get more funding".

While humanitarian organizations as a collective face many of the same risks—crime, social disorder, terrorism, disease, vehicle or industrial accidents or natural disasters—some organizations also face unique forms of risk specific to the nature of their work. This then requires those within the security community to be a generalist to manage common vulnerabilities, while also concurrently being a specialist in order to master the unique sub-set of threats associated with their specific organization or activities. Alex, the Global Security Director for a major humanitarian organization, posited the need to specialize as a risk practitioner:

> "One of the things that would impact us massively would be sexual exploitation of children, child-safeguarding issues, obviously huge from a reputational risk".

The security community also needs to balance realism with how they present risks and the associated impacts to executive leaders. While security-related threats are on the increase, risks are not equally distributed and a one-size fits all approach is not realistic; nor is it accepted at the leadership level. Consequently, segments of the community might be exposed to greater or lesser risks, based on: 1) the geographic focus, 2) whether they operate in urban or rural areas, and 3) the types of programs they implement. Gavin, a respected academic and author of security and resilience, noted that, while threats are increasing, the security community needs to analyze what this means to individual organizations:

> "The rising rate of violence against aid workers is not a global phenomenon, but only a serious issue in the handful of active conflict environments. Without those, you see the number of violent incidents stable or falling in other places, as organizations have gotten better at managing their security".

It is also important for the sector to realize that they are not necessarily unique, and that other sectors or industries face many of the same risks. This allows the security community and their organizations to leverage experiences learned by those outside of the community, and so borrow from more established disciplines. It also provides deeper resources from which the community can draw in terms of standards, best practices, and training resources. Historically, the sector has felt that it was sufficiently different that out-of-sector knowledge and resources were of little to no value; however,

this has proven not to be true and, increasingly, the security community and risk portfolio owners draw upon commercial knowledge and resources to build both organizational resilience as well as personal capacity. Indeed, such an attitude is self-defeating and limits the capacity for the sector to rapidly and effectively evolve the field of security—and more broadly the resilience—profession. Andy, the Global Security Director for a major development organization, noted the importance difference of risk tolerance within the sector, positing that:

> "I don't think they (humanitarian organizations) face unique risks. I think they face more—they are more willing to face those risks than other organizations".

The acceptance of risk as part of the social make-up of humanitarians draws the sector into risky operating environments and dangerous situations, amplifying the need for the sector to be resilient. If beneficiaries face political instability, armed conflict, a natural disaster, or a serious disease outbreak, then invariably humanitarian support is required by governments and beneficiary communities, exposing the implementing partner to many of the same risks. Andy used COVID-19 and post-conflict environments as an example, stating that:

> "So, when there is a pandemic, they are (humanitarians) the first people in there. When there is a call for aid to develop, they are the first people in, even though it is a post-conflict scenario".

With the sector's acceptance of danger being inextricably linked to the nature of their work, the importance of understanding the probability and impacts of a risk is critical for effective resilience measures to be established and maintained. In the absence of clearly defined standards and practices against which a common sector-wide understanding can be established, then perception becomes highly personalized and so is debilitated by subjectivity. This variance of perception spans from the individual through to the executive leadership team. The sector is also homogeneous only at the macro level, with significant differences at the lower levels in terms of for-profit and not-for-profit groupings, and subsets of the community focusing on the thematic areas of development, relief and aid. Further delineations then exist in terms of the various areas of work, ranging from micro-financing, education, health, agriculture and governance to civil rights and a plethora of other technical areas. This, then, places the concept of resilience within a melting pot of factors, resulting in highly variable perceptions of what constitutes risk, and how risk is effectively managed. Alice, the Global Head of Security for a

major humanitarian organization, stated that risk was not typically understood and so the reaction to vulnerability typically only comes after a crisis has occurred:

> "Ignorance is probably the key risk, that they don't know physically what's going on, that they are not aware of a problem until it becomes a problem".

This lack of understanding is exacerbated by the dynamic nature of risks, how quickly emergent risks have grown within the sector, and how rapidly the risks can mutate within each operating environment. This is also compounded by the need for some organizations to operate alongside, or in some instances, even cooperate directly with the actors who present a direct or indirect threat. As such, humanitarians walk the tightrope of living with, working with, and, in some instances, even directly supporting groups who may present a physical, reputational, or legal threat. Betsy, the Global Director of Security for a major humanitarian organization, noted that this growth in the risk portfolio and the need to maintain neutrality, especially when being funded by governments hostile to threat actor interests, was a challenge:

> "The risk portfolio, if you like, has broadened, because you are not only strictly considering staff safety or security. You are considering risk in a much broader context in terms of how they (humanitarians) operate with different armed actors, how they don't compromise neutrality and impartiality".

Over the past 15 years humanitarians have been forced to recognize the need for bringing security risk management into broader decision-making and operational practices. This process was not transformative; rather, it has been incrementally adopted across the sector over a period of some 15 years. Professionals noted that the evolution within their organization was often associated with a crisis incident impacting their organization, or a peer group, which acted as the catalyst for change. Participants noted that disruption (a crisis) forces change, but that acceptance of the need for resilience within organizations is still slow, and often is not welcomed. April, the Global Security Director for a major development organization, noted that security was initially perceived as a negative influence in terms of how the organization would operate being a disabler, rather than an enabler:

> "When I first risk strategies didn't exist but we had incidences which caused my organization to establish an actual security office. It was difficult at first to introduce it. There was a lot of

> hesitancy. NGOs felt that security people were going to tell them where they could and couldn't go, what they could and couldn't do, but as we've introduced it more senior leadership accepted it, promoted it, supports it completely".

While security is increasingly being included into management decision-making cycles, those interviewed noted that their expertise and opinion is not always included during the critical inception phase of work. This then places security on its back foot, having to insert itself into a pre-formed approach with neither a platform to effectively gain buy-in, nor the necessary funding. Fred, a senior risk advisor within the sector, stressed this as a concern for many, articulating the implications this has for both the individuals as well as the organizations they support:

> "The security approach to a new market entry seems to be something which is retrofitted, once all of the money is on the table. So then security is scrabbling around, looking for bits and pieces of cash, it doesn't make sense to me".

Both real and perceptional risks define how resilience measures are prioritized. It is by understanding the implications of direct and indirect threats (and how risks may quickly cascade from a localized security incident to an organizational crisis) that organizations can decide what standards and practices to adopt, and what resources to apply. It is this understanding which also defines which individual is best suited for a particular role, and how they are then positioned and resourced, which then ultimately shapes the security profession and the culture of resilience.

What resilience means to the sector

This section looks at what resilience means to the sector. Research data supports the perception that risks from criminals, social disorder, hostile governments, and terrorist threats are on the increase. Alongside this, epidemics and pandemics, medical incidents, and various forms of natural disaster also present a challenge to those working in remote areas with weak rule of law, or limited health and emergency services. It is within these complex, dynamic, and high-morbidity environments that beneficiaries exist, and it is where humanitarian assistance is often most needed. With risks being well-documented over the past several decades it would be logical to assume that humanitarian aid and

development organizations would take the necessary steps to identify and address predictable risks, and thus be more resilient to them.

Figure 9 is drawn from a pool of 77 survey participants when asked to respond to the statement: "***Are organizations highly resilient to human-made and natural threats"***. Of the 77 participants only 27% felt organizations were highly resilient, while the majority either held a neutral or negative opinion.

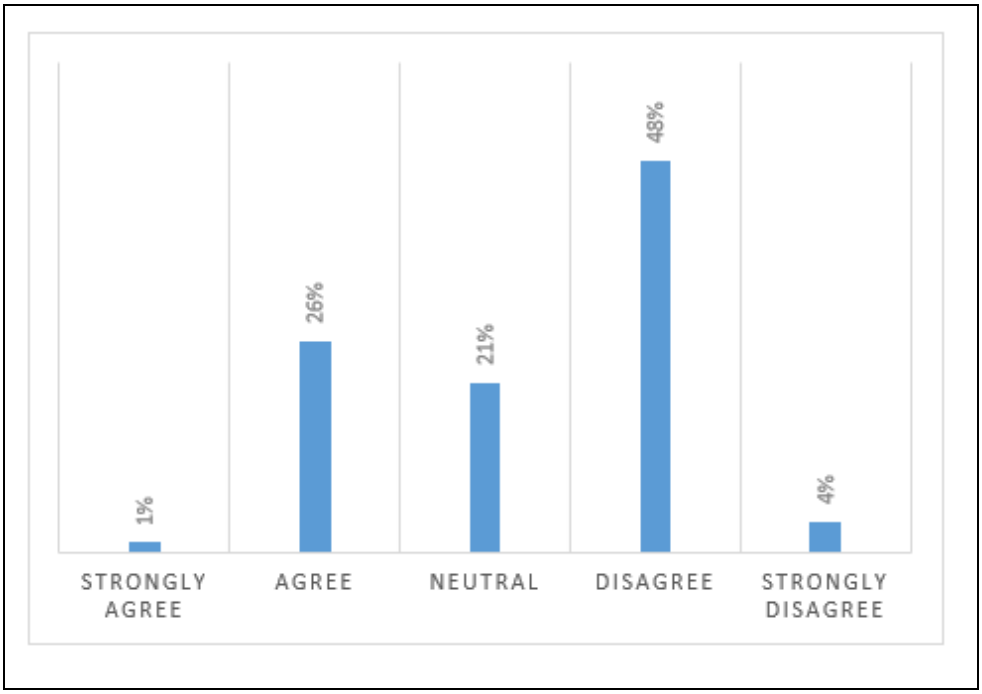


Figure 9. Are Organizations are Highly Resilient to Humanmade and Natural Threats

The survey results reflect an awareness within the security community that risks are known, but that the sector has yet to take the necessary steps to effectively manage them.

The concept of resilience has grown over the past decade as humanitarian aid and development organizations have increasingly come into the direct line of fire, both literally (in terms of physical risks), but also figuratively (in terms of litigation and reputational harm). This emerging inclusion of not only security risk management, but broader resilience, is being applied incrementally across the sector, but is taking time to be incorporated into the mindset and behaviors of leadership teams. Isolated examples of transformative change are found (typically) within organizations that have been directly impacted by a catastrophic crisis. As such, those who have experienced the pain of a crisis firsthand are more likely to invest in resilience strategies to avoid the pain again. Conversely, those who have not experienced a highly disruptive incident often struggle to understand how damaging a crisis can

be. This reactive approach to resilience, coupled with the disagreements over what risk means, impedes the ability for the community to prioritize the management of complex interrelated risks. It is from this platform that the professionalization of security risk management, and more broadly, organizational resilience and business continuity management, is built. Debbie noted the lack of agreement on what resilience means within the security community and sector at large:

> "I think resilience is a very new concept in that sense. You could call it continuity of operations—business continuity, but resilience goes further."

Organizations are also increasingly realizing that security risk management is inextricably linked to their ability to effectively deliver services to beneficiaries and satisfy donor expectations. As the availability and implications of statistical data and anecdotal incidents grows, the implication of mismanaged risk practices and their disruptive effects becomes more tangible with Alice positing that:

> "They realize also that if they don't keep themselves safe or they don't follow security practices, that they can't actually do their job. So we look at it as we're helping to enable them to do their job, because if they stop, then those beneficiaries don't get the assistance that they're there to help with".

If effective resilience practices are not in place, then the ability for organizations to effectively respond to a beneficiary crisis is also consequently weakened. Resilience can be broken into three distinct phases: 1) the *preparedness and prevention phase*, which identifies, evaluates and controls risks; 2) the *response and management phase*, which meets the immediate and longer-term reaction to a disruptive event; and 3) the *transition and recovery phase*, where organizations return back to normal, or alternatively move to a new normal.

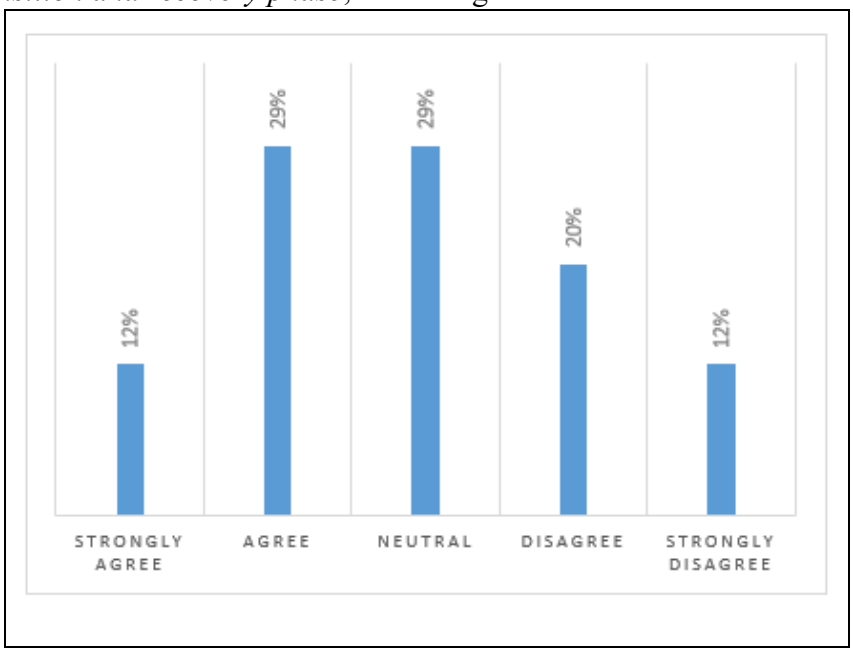


Figure 10. Is the Response to a Crisis is Integrated Effectively with Governmental, Community, Peer and Other Stakeholders

Figure 10 is drawn from a pool of 77 survey participants when asked if: "***The response to a crisis is integrated effectively with governmental, community, peer and other stakeholders"***. Of the survey pool, only 41% felt that crisis response was effectively integrated with relevant stakeholders. Given the heightened risks the sector faces, and the reliance that organizations have on external technical support and physical resources during a crisis, this level of stakeholder engagement reflects a serious vulnerability to organizations within every phase of resilience.

Participants within the interview group articulated that the establishment of functioning resilience measures takes time, appropriate resourcing, and leadership focus. The need to fully embrace and embed the concept of resilience at all levels, and then apply it in practice, ultimately defines the effectiveness of the organization's ability to understand and address known, as well as emergent, risks. Debbie posited that:

> "It takes several years to actually implement [resilience], embed it and indoctrinate it and actually implement the plan and be able to actually measure the impact of your resiliency plan".

Participants agreed that the organizational understanding of what resilience means is growing. It was also felt within the interview pool that the remit of security has expanded to encompass more than just physical security risk management. Betsy noted the increasing relevance of enterprise risk management to the NGO community—rather than being relevant only to commercial companies—positing that:

> "It is an emerging approach. Typically, risk is managed through contingency or mitigation, and depending on how well defined your risks were, there would be some kind of mitigation to offset those so that your residual risk was well mapped. The issue with that with the broad-based threat risk approaches is it doesn't allow you to look on the enterprise level, and I think the enterprise level of risk is really interesting at the moment for NGOs, because it also includes opportunity risk and all the other risks".

Betsy went on to add that, despite the relevance and growing interest in broader resilience strategies, the sector had yet to fully embrace strategic organizational resilience:

> "We are really struggling. Other organizations are ahead of that (risk management), but they tend to be thinking very much threat-based risk management and resilience versus big, enterprise risk management".

Conversely, while many participants felt that incorporating resilience consistently within the sector still had some distance to go, many have seen considerable change over recent years, with Alex offering that:

> "It is better today than it has ever been, in my experience. I would say that's only come in play in the last 18 months, a year. The organization has a dedicated risk team, which sits outside of your global safety and security. Are we resilient enough? Absolutely not. Are we getting better and learning as we go? Yes. That's why we brought in experts to lead the process through".

Participants also recognized that expertise in resilience was broad ranging, with organizations leveraging both internal and external expertise to meet the diverse portfolio of technical proficiencies required. This also underpinned the need for individuals to work to an agreed competency standard, enabling those within the profession to extend their technical knowledge and experiences outside of the field of security risk management. Erik, a legal expert within the humanitarian sector, remarked on the need to expand the risk or security professional's remit, positing that:

> "Very rarely is the organization going to have all that kind of expertise in house. It is so specialized and takes people a long time to become that expert, so they need to be reaching out (to external professionals)".

Participants also recognized the need for resilience to be embraced at every level, spanning the levels of organization, project, site and individual. Clarity is required to ensure the framework of resilience is pragmatic, reasonable, and effective, that it is understood and is mutually supportive, and that it can be successfully implemented, leveraged and sustained. Charlie, a Global Security Director for a medium sized humanitarian organization, remarked on the need for a framework of expectations, the need for accountability, and the requirement for performance metrics, positing that:

> "The weakest component in any of that is human behavior. If you have a look at the country officers, they usually have great SOPs in place. They maybe haven't documented them or have done the due diligence from a compliance perspective. But they have things in place. I would say where the weakness in there comes in is the accountability, so where there's noncompliance to it, the accountability framework is lacking".

The importance of establishing a common vernacular and a consistent approach to resilience from the headquarters through to the field level was stressed as critical by the majority of those interviewed. Participants commented on the need for the headquarters team to better understand the tactical needs of the field team, and, conversely, for the field team to appreciate the strategic interests of the organization. At the mid-point is the area of operational risk management, the connective tissue between both groups. Gavin stressed the importance of both levels working more proactively together to ensure a more effective resilience strategy, stating that:

> "Shared risk assessments and mitigation measures should be planned by international organizations with their national organization partners".

Participants also identified a heavier investment into security risk management at the field level (where the majority of incidents occur), rather than at the headquarters level (where the lion's share of resilience and business continuity management resides, and where standards and practices for resilience are typically established). While this is understandable, as the practical needs at the point-of-crisis may be more obvious, participants noted that ultimately the governing standards for security

risk management, and, at the higher level, organizational resilience, are developed not in the field, but rather at the headquarters level. Where governing standards are developed locally the result is inconsistency across the organization. David, the risk focal point for a mid-sized humanitarian organization, stressed the need for the headquarters to take the lead on—and to resource—the establishment of organizational resilience standards, positing that:

> "At the headquarters level, in my experience, we are not (effectively addressing resilience), and this is across the board, not just in the headquarters level. We are not providing enough resources and we are not putting enough focus on risk mitigation".

The interview findings indicated the importance of establishing an integrated system between the headquarters and field management team, as well as the need to bridge the division between functional areas. Camila identified this as a major failing within many organizations, citing a disjointed and at times conflicting approach to organizational resiliency:

> "A lot of organizations will have plans specific to core functions. For example, there will be an HR policy or a communications policy or plan. There will be in some cases a business continuity policy, but they are independent of each other, and there isn't really an overarching plan in a lot of cases that link those different functions up in the event of a crisis, or in terms of mitigating risk. In some cases, they are not consistent, so one may be employing a strategy that isn't really consistent with another core department's plan".

The competency levels within the hierarchy of security practitioners and professionals were also cited by many interview participants as a both varied, and a point of vulnerability. Generally, strategic level competencies are found at the headquarters level where standards and practices are defined, before flowing down to those implementing security practices or outcomes at the field level. As a result, higher levels of competency and accompanying qualifications reside at a point often most distant from where the majority of security incidents occur. Conversely, at the field level, where the greatest physical security needs exist, the majority of practitioners are neither formally trained nor qualified as security professionals. This was largely attributed to Security Focal Points assuming security responsibilities as a secondary role, rather than security being managed by full-time security professionals. David commented on this gap in competency, stating that:

> "I definitely believe there are gaps in the field because of limited expertise in security and risk in many of our field offices. We tend to bring in program staff and they are great and wonderful at running programs, but the security infrastructure is often not fully funded. I have struggled with being able to get accurate security reports, plans and information from many of our field offices, because of the fact that they just don't have the expertise in order to be able to generate such things".

The understanding of what resilience means is therefore impacted by the level of competency within the security community at large, and at every level. If professionals reside where standards are defined, but where a firsthand understanding of granular level risks is limited, this may then distort the organizational perception of risk, and thus how risks are addressed. If those facing the risks at the coalface lack knowledge and experience, or the platform to effectively assess and articulate the risks to policy makers, then their ability to communicate the needs and so shape the approach is diminished.

Resilience standards and practices are codified within document systems, reflecting the collective body of knowledge of both the practitioner and the professional. The documentation of resilience standards and practices enables knowledge and experience to be shared; these transcend personalities, cultures, experiences, geographies, time, resourcing, and training opportunities. Codification of standards and practices also enables individuals to leverage the collective competencies of those within the security sector. Concurrently, organizations are then provided a proven shortcut to ensure that their approach is built on "best practice", enabling them to better protect people, operations, assets, and their wider business interests.

Figure 11 is drawn from a pool of 77 survey participants when asked to respond to the statement: "***Do documents typically address ALL FORMS of risk effectively"***. While the sector widely recognizes the need for resilience, data suggests that codifying critical knowledge has not yet occurred, with only 23% of survey participants stating that resilience had been effectively documented.

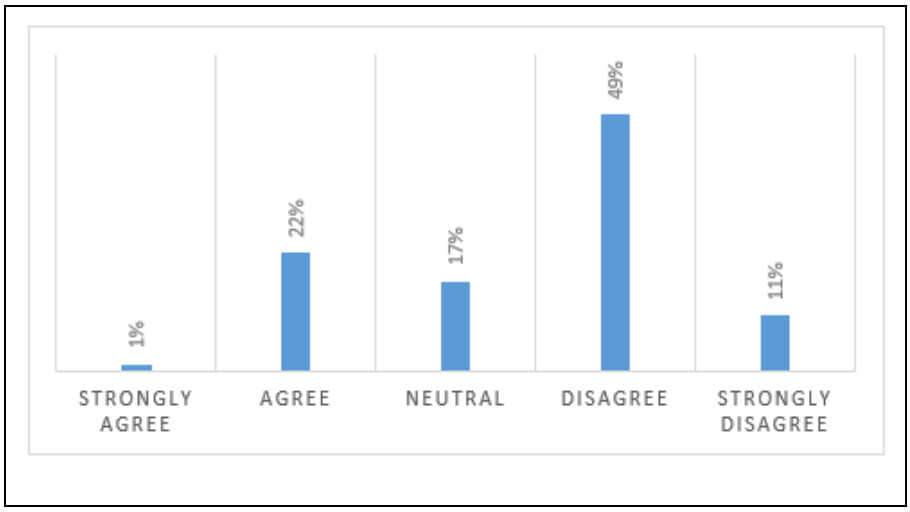


Figure 1. Do Documents Typically Address ALL FORMS of Risk Effectively

Adam, the Global Director of Security for a major humanitarian organization, commented on the growing need for resilience to be consistently approached and captured in documents, positing that:

> "So, we now have documentation in place where documentation didn't exist previously. I would say that has the last five years, especially in terms of standards, guidance and just learning and applying that learning to practice. So, we are always as an organization looking for best practice to benchmark against, and so ISO standards provide perhaps the best practice out there".

The cost of codifying effective resilience strategies and supportive measures was identified as a limiting factor, both financially, as well as in terms of effort. While many noted that the desire to invest in security was generally low and was often being driven through necessity rather than desire, some noted that larger humanitarian organizations were effectively mega-corporations with billions of dollars of funding per year. The ability to fund security and resilience was easier for those with larger budgets, while smaller NGOs often struggle to allocate limited funds to security, with Camila positing that:

> "I think there are gaps. There's always room for improvement, and some organizations do a much better job than others, and some organizations face major resource constraints. Maybe

> they are smaller and do not have the funds to do some of the things that larger organizations do".

Those with funds can not only hire in-house security or resilience experts (Security Departments), they can also contract specialists across a wide range of technical fields. This ability to resource resilience then shapes how organizations perceive and value security and enterprise risk management. Andy noted that internal funding disparities were also a factor, with the headquarters team leveraging experts in various areas, while at the field level—where most physical security or safety incidents occur—there is often insufficient funding to appropriately resource security needs:

> "We have contracted a global leader in security and risk management to give us an overall risk management picture that includes political security and operational risk. We have also contracted a health professional to give us an overall health and pandemic risk coverage, but at the local level they are employing operational people and giving them security hats, rather than employing security professionals to handle the risk management".

The internal competition for funding remains a constant disrupter to the resourcing and inclusion of effective resilience measures. Brad, the head of training and development for a major humanitarian organization, noted that the leadership team often acknowledged the importance of resourcing security and broader resilience needs, but cited funding as a major limiting factor for many organizations:

> "Security is on the radar, but it is not the number-one thing on their radar. They (executive leadership) know it is organizational crippling if we have a major event in the field. We know that organizations need to be able to bounce back. We know that we need to be as resilient as we possibly can be, but there are other competing priorities that go against security all the time. The biggest one of them is funding. We are still seeing the amount of money that's being given to security in organizations that I've been working for is less than 5% of the overall organization's budget, yet we want to work in these high-risk environments".

The meaning and importance of resilience is determined by those who assess what risks exists, articulate their significance, and who define how they can be addressed. Whether risks are addressed through decision-making processes, risk management practices, document systems, resourcing or training, it is ultimately down to the individual practitioner or professional to drive and sustain change.

Historically, many humanitarian aid and development organizations felt that they were exempt from the standards and practices—and specifically duty of care requirements—applied to commercial companies due to the nature of their work, with many believing that "doing good deeds" meant "we are exempt from scrutiny". Society has now changed and the sector's latitude in paying lip service to address security risks, or meet ethical standards, has either diminished or has disappeared completely. Consequently, the sector must meet the same standards as their commercial peers in these areas, if not exceed them. Alex commented on how the sector is increasingly recognizing the need to behave like commercial companies, requiring a significant readjustment to how organizations perceive themselves.

> "Although we are in an unregulated sector per se, the Charity Commission obviously do look at us very hard. We still have to submit books. We still have to manage ourselves appropriately".

Donors are increasingly aware of programmatic security risks and their impact on organizational resilience. This has the dual effect of both empowering and forcing organizations to embrace resilience standards and practices. This change in the donor mindset on one side allows organizations to seek increasing levels of security funding for their activities or to push back on donors where the risks are too great, while conversely it also requires them to articulate their security approach within competitive proposals. Humanitarians are then held accountable for implementing an effective security risk management program as donors believe that the failure of an implementing partner is a failure of their program. As such, the expectations of donors are changing, requiring organizations to show how they address security risks, and how they continue or recover from business disruptions. The influence of donors was stressed by Andy who stated that:

> "I would say the donor has pushed that, because we work on donor money we have responsibility to that. USAID and DFID have a different approach, while the Japanese (JICA) have a completely different approach because they are so new to this exposure they don't fully understand the risks involved".

As donors better understand the risks that implementers face and the ramifications of a weak resilience strategy, the level of involvement between donors and humanitarian organizations will likely continue to grow as the increasing levels and complexity of risks lead to a growing realization that security risk management must be included throughout the lifecycle of a programmatic activity.

Figure 12 from the survey pool of 77 participants when asked to respond to the statement: ***"Is risk management included in business planning from the outset"***. While data suggests that resilience measures overall are not yet at an appropriate level, 43% of participants did note that security was being included into business planning from the outset.

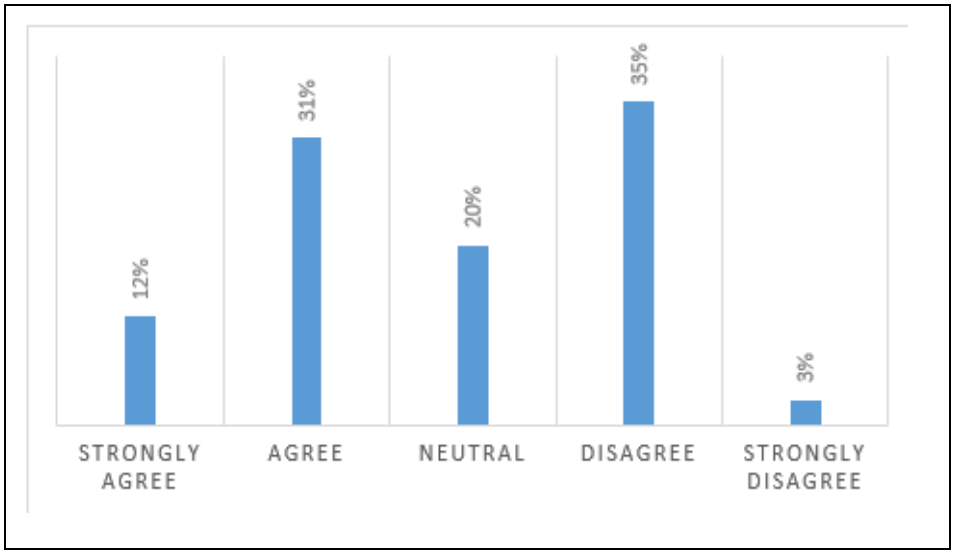


Figure 12. Is Risk Management Included in Business Planning from the Outset

This allows security to better shape the organizational approach at the inception phase, and to carve out the required budget and management focus at the point where work is won and started. The interview results likely reflect a higher inclusion of the security profession for high to extreme-risk operating environments, with security being less involved in medium- to low-risk project environments. The basis of how organizational risks are addressed rests on the perception of risk. Perception then drives how internal and external forces motivate the security profession and those they support to effect change. The concept of risk is both highly complex and fluid, and it is subjective. Without a defined basis of understanding, the ability for security professionals, practitioners, risk owners and organizations to bring about structured and consistent change is difficult to impossible.

CHAPTER 5

SECURITY PROFESSIONALS, PRACTITIONERS AND FORUM GROUPS

Introduction

This chapter presents the results of the primary research into the diverse backgrounds of the security community. It demonstrates how a competency framework can define individual, role and organizational expectations, the importance and influence of the security professional and practitioner within their respective organizations, and how forums and associations might support the advancement of security as a profession. The research started with the fundamental question of what constitutes a security professional, recognizing the three stages of an individual's professional journey: 1) where they came from, 2) where they are now, and 3) what their destination is. This chapter also looks at the areas of knowledge, skill, experience, and attitude which collectively define an individual's suitability and competency within the hierarchy of security.

Those operating within the field of security begin life as something else, coming from such fields as the military, police, intelligence services, disaster response, project management, or from an academic background. Individuals invariably draw from their foundational careers as the basis of knowledge and practice. Rarely does an individual enter the field without some level of prior professional or academic experience. Despite the need for a defined community of security professionals and practitioners, the sector lacks a consistent framework of what is required from those performing a security function, as well as a mechanism for individuals to transition into, and develop within, the field of humanitarian security risk management. This presents a challenge to both the security professional performing security as a primary function, as well as the security practitioner who may perform security as an ancillary role. Concurrently, the situation exposes those who employ the security professional and practitioner to avoidable risks where gaps and shortfalls exist.

Understanding the influence of different career start-points, what is needed to support effective career transitioning, and then mapping the available or necessary mechanisms for further professional

development is useful to both the security professional and security practitioner, as well as their employer. Despite the widely accepted importance of security within an increasingly dynamic and dangerous world (Harmer, 2018), little research exists on what constitutes a humanitarian security professional (Khorney, 2017). And, as the risks to the sector increase, the importance of the those leading on security risk management proportionally grows.

The purpose of this part of the research, therefore, was to establish how an epistemic community of humanitarian security experts (at various levels) can be initially established, and then be provided with opportunities for continued advancement. In doing so, this might: "bring about institutional change within security governance within the humanitarian NGO community" (Schneiker, 2015, p.75). This chapter explores the different career start-points, how professionals and practitioners are perceived, how convergence of career fields occurs, the importance of defining competency frameworks (Rutter, 2011), the importance of the security professional and practitioner as the voice and engine for institutional change, and the value associations and forums offer to the humanitarian security profession.

Career starting points and mechanisms for transition

Given that security professionals will almost always hold at least one position before assuming a security role (92% of the survey pool participants had more than 11 years of security experience), the need to assess the value and application of a primary career field is important to both the organization employing those performing a security role, as well as for the individual seeking to make a successful transition between career fields. **Figure 13** shows that the majority of professionals have a career start-point within the "uniformed services" (a military or paramilitary background), with 66% of the 77 survey participants coming from a military, police or an intelligence agency background. Similarly, from the semi-structured interview pool, 73% also originated from the government sector. The results point strongly that the recruitment pool (currently) favours those coming into the sector with a formal security background, rather than professionals being "grown" into the role of a security professional from an unrelated field.

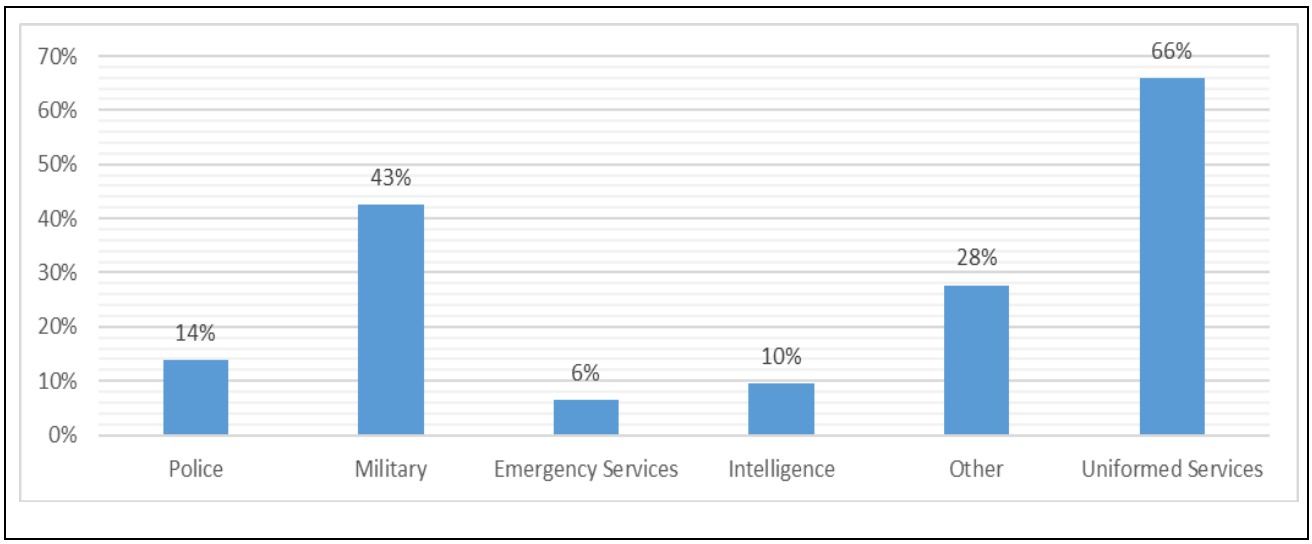


Figure 2. Survey Pool Primary Career Fields

The data resulting from the survey, semi-structured interviews and competency framework focus group suggest that formal research focused on primary career field transferable competencies could be highly beneficial to the sector. Such research might determine transferable knowledge, skills and experiences and, critically, might expose areas which bring little to no transferable value.

While the propensity for professionals to come from the government sector is not necessarily reflective across the entire humanitarian space, research indicates that the primary career field from which organizations currently recruit security professionals is associated with a military or para-military background. As such, the rationale behind the favouring of military or police experience warrants investigation. Despite this weighting, the primary research data indicated that the majority of those within the security community felt that a government sector background was not necessarily a mandatory requirement, and that other areas of technical knowledge, skill and experience were of equal or greater importance. Charlie stated that increasingly members of the security community with a strong academic background were being seen within the field, suggesting that a driver for change was the need for the sector to be more sophisticated to address increasingly complex and interrelated risks:

> "We have got a growing market of academic professionals due to the knuckle-dragging ex-police officer, ex-military who was not refined, who was not able to address an executive team or board. The pendulum swung to the other end, where we have gone very, very academic,

> very professional but not necessarily everyone having a grounded footing in practical fieldwork".

Each primary career field offers different benefits, whether a purely security background or a sophisticated level of academic acumen. Almost without exception, all interviewees commented on the importance of understanding the strengths and weaknesses of any career start-point and how transferable competencies might then empower the transitioning individual and benefit the employing organization. The need to ultimately achieve a balance—fundamentally the *convergence* of disparate technical knowledge and experiences drawn from different career fields—was cited as paramount in achieving the optimization of a security professional's fitness for role.

While many interviewees commented that those coming from a uniformed services background brought readily transferable security related knowledge and experience, interviewees also cited that often these individuals were not a good "personality fit" for the sector, and that their ability to articulate nuanced concepts was not as effective as those coming from a civilian or academic background. Conversely, interviewees also noted that those entering from a civilian or academic field lacked the technical knowledge and pressure-tested experience needed to effectively manage fast-burn and high-impact crisis situations, but conversely fared better than their government counterparts in articulating complex ideas verbally and in writing. As such, the findings suggest that the sector must aid transitioning government professionals in terms of better understanding the nuanced cultural needs of the sector, as well as how their skills and experiences could be better applied. Or, conversely, the sector must provide the framework, resources and support needed to enable those with no security grounding to achieve the technical and experience competencies required of a security role. Brad highlighted this gap and the implications to the sector, noting that:

> "There is no transitional bridge that has been helped for the security professional to come in, to transition from the previous life into the current life. It is people learning by making lots of mistakes. People learn by having to adapt to a culture that's totally different than the one where they're coming for".

The individual's professional versatility, capacity to learn, willingness to consciously change, and innate ability to view risk through a multi-dimensional lens is, potentially, as important as what they have learnt or experienced within any primary career field. These human characteristics play a large

part in shaping the convergence of technical competency and contextual application—that is, the coming together of leadership and management skills, the blending of vocational and academic knowledge, the application of standards and practices through action, and the ability to articulate complex problems and solutions. Successfully combined, this enables the successful transition, transformation and continued growth of both government and civilian professionals. Alex commented on the importance of the individual's personality in terms of successfully transitioning into the field of security risk management:

> "It is all about the personality. It is all about the individual. Some people have made the transition very effectively, others not so".

Many of those interviewed stressed the importance of attitude as the basis of a successful transition from a primary career field into a role within humanitarian security. No interviewee suggested that the technical skills learnt within a military or police career fields were not useful. Rather, they expressed the belief that the focus of a successful transition relied upon the capacity for the individual to integrate themselves into an entirely new, and often very difficult, culture. Dustin, a senior expert within a humanitarian forum group, supported this view, noting that for some the transition was easy and painless, while for many others the ability to understand and embrace the unique culture of the humanitarian sector was difficult to impossible. Interestingly, Dustin also voiced concern that even if the individual was not ultimately embraced within the sector, ex-military professionals could still undermine the profession as external trainers, negatively influencing security standards and practices through training:

> "Some get it. Some make the transition brilliantly. Others will never understand, and then they go and become trainers, and they train the rest of them, which is quite terrifying".

The ability, certainly for those professionals who bring decades of experience within a single field, to transition from a very distinct vocation into another can be challenging, as institutionalized attitudes within a regimented career field can lead to cogitative inflexibility. The humanitarian space is, by its very nature, largely dynamic and collaborative. Humanitarian aid and development organizations, unlike their commercial peers, are engineered to support beneficiaries through engagement, discussion and persuasion. Arguably, the uniformed services are more typically associated with a rigid

hierarchical structure that conforms to entrenched practices and an autocratic leadership style, rather than through democratic decision-making processes. Alex noted that:

> "We are moving away from an authoritative structure to a very consultative structure. The loudest voice is not always the right voice".

The stereotype that all military professionals are autocratic by character, through either nature or nurture, also has flaws. It represents a simplistic view of the military profession being a blunt instrument in comparison to the "softer" culture more typically found within the humanitarian sector. Within the arms of each military service are different cultures, and within each culture are sub-cultures with diverse personalities, remits, and experiences. However, the perception of inflexibility was articulated by the majority of those interviewed (noting that the majority were themselves ex-military professionals), with Francis, the country head of security for a major development organization and retired from the military, positing that:

> "Military and the police practitioners are very set in their ways. It is very difficult to try to change their approach, change their thought processes. There is an old term, often used, called "knuckle draggers". They are still the old gunslingers. They still want to be the guys that are running in front with the body armor. Whereas the new generation, the academics who are coming in are a lot more pliable to situations, and they can better adapt".

This challenge is compounded by an absence of supporting mechanisms to assist a smooth transition and cultural realignment between professions, allowing government professionals to reorient their philosophical approach and apply their substantial security knowledge, skills and experiences appropriately. The absence of an effective transitional pathway is exacerbated by the need to ensure a humanitarian "personality fit" which can be (at times) unforgiving. This challenge was reinforced by Alex (an ex-military professional) who posited that:

> "There is not any course, that I am aware of, on how to take someone from that career mindset (military) to this career mindset (humanitarian), and there is definitely a need for it. But if ex-military or ex-police believe that they can do this transition course (if one existed) and they would then immediately work in charity, they are kidding themselves, because it still is very personality driven".

Conversely, those entering from a non-purest security career field are also faced with their own set of unique challenges. With an increase in professionals entering with little to no security foundation to draw upon, the need to first access and secondly contextualize knowledge within dynamic and at times life-threatening situations, can be highly problematic. Many of those interviewed suggested that academic competency and strong management (verses military leadership) skills are of increasing importance. However, interviewees also voiced the concern that a balance is required, noting that, in high-risk environments, security experience was more important that academic excellence. Edith suggested situational awareness and the ability to make decisions under duress as an important part of the security role, positing that:

> "If you are put onto the ground as a security operator, people expect you to know first aid, how to drive, how to behave under fire. If you only ever come from the academic side that is quite hard to learn without the pre-military side, whether it be part time, full time or learning from courses".

While life-threatening incidents are not a daily occurrence for most, when they do occur members of the security community may be called upon to offer advice or to make time-sensitive and high-pressure decisions with little to no external direction which, if wrong, could result in harm to people (themselves or others), and potentially could result in catastrophic damage to the wider interests of their organization (legal, financial and reputational). The ability to make autonomous decisions during a crisis underpin La Porte's (1996) principles of high reliability organizations and the requirement for rapid autonomous decision-making capabilities. This is especially true of crises, which may occur with little to no warning, and where time-sensitive decision-making is paramount (i.e., during armed attacks, coups, riots, the early phase of a kidnapping, explosive attacks, earthquakes, tsunamis, or an arrest where an immediate risk-to-life is present). Where risks can be more effectively predicted, or where the organization has time to mobilize expertise or to ruminate on a course of action, then the importance of a strong background within security is perhaps less important (i.e., seasonal storms, an upcoming volatile election, or where risks may evolve over time, such as growing social instability or the spread of a serious infectious disease). Charlie commented on the importance for members of the security community to be stress-tested during crisis situations, a trait more commonly found within military, police or emergency service practitioners:

> "The fact that they (ex-military) are not giving emotional responses or advice and the leadership team is getting factual, thought-through information on which to base their decision-making allows them to make better decisions regarding the crisis response".

The challenge, then, is how do those not coming from a strong security foundation firstly develop the required technical knowledge in security risk management, and secondly have the opportunity to apply this knowledge to a simulated crisis situation without exposing the practitioner—and those they serve—to unacceptable levels of risk. Perhaps a bigger question is at what point does "professionalism" occur, not only for the practitioner entering into a new field (security), but for the professional transitioning into a new culture (the humanitarian aid and development sector). While no interviewee suggested that an academic or other civilian starting point should preclude entry into the field of humanitarian security, the ability to base decisions upon recognized training and duress-tested experiences was identified by the majority of interview participants as important. Conversely, many government professionals also recognized a serious academic shortfall within their peer group when assuming more senior positions. The majority of those interviewed stated that the more senior the role, the more important it was to have either strong academic skills or strategic vocational competencies, with noting that:

> "The problem with coming from the purely security role is you do not know how to convey this information in the academic way by writing reports, using spreadsheets… the way it can be read at the higher level".

Brad also reflected that the optimal solution within the security field is a blending of practical first-hand experiences with the attributes which come from academic excellence, underpinning Gibbons et al's (20020) concept of hybrid communities, stating that:

> "The practitioner has that (first-hand security and crisis management) experience, but may not have the academic piece, you have to have a hybrid (practitioner) that has both".

Cultural bias and changing perceptions

This section looks at how individuals must overcome cultural preconceptions, whether transitioning between roles from within the sector, or were seeking to enter the sector from another career field. The

sector has its own unique culture, language, social habits, belief systems and values. Where individuals already in the sector change roles or progress, they do so with the benefit of being already within—and accepted by—their culture. However, while advantaged by understanding and being accepted by their fellow humanitarians, their challenge is to now become competent—and be deemed as credible—within a new profession. Conversely, established security professionals seeking to become part of a potentially alien culture must reorient their belief systems, attitudes, mannerisms, language, technical knowledge and experiences in order to be accepted. Their knowledge and experience must evolve through the process of "emergence" as it is adjusted to meet the demands of new conditions and different social constructs (Polanyi, 2009). And, they must concurrently overcome the perception that a significant—if not insurmountable—difference, exists between the two cultures.

Within the sector, the importance placed on different professional backgrounds can differ significantly, with the INSSA **2017 Competency Framework** (GISF website, 2020) stating that: "ex-military security professionals and seasoned aid workers do not make easy bedfellows, so security management and humanitarian principles are often perceived as incompatible". Alex, coming from the military profession, reinforces the reluctance of some organizations to recognize the potential value that ex-military professionals bring to the humanitarian security field, noting that:

> "Sometimes, there is an active refusal to take on ex-military or ex-police, or that sort of profile".

Interestingly, even those with a military background are at times reticent to recruit from their original peer group, with Alex going on to say that:

> "I have actively not recruited someone from the military because of the context that they would be working in".

Interviewees also remarked on how community perceptions differ on the importance of the individual's background, including whether they enter with established security risk management credentials, or whether knowledge and experience can be gained outside of a formalized and certified career setting. Debbie posited that the reluctance to embrace those coming from an armed forces background had seen change, with an increasing acceptance of military professionals entering the field of humanitarian security:

> "Organizations have different perceptions on do we want a military guy to come in and do our security or do we want someone who picked it up along the way? I think the attitudes are changing… people are warming up to former military people who have a strong, hard security background".

Many of those interviewed stated that cultural friction between humanitarians and transitioning government professionals had historically suggested a cultural incompatibility. It was, however, also widely recognized within both the competency framework study group and semi-structured interview participants that the sector has a responsibility to formalize role responsibilities and define the knowledge, skills and personality traits needed to effectively fulfil humanitarian sector expectations. Adam noted that:

> "When I am selecting staff to fill a security role I look for a much wider range of skills and attributes: people that are good thinkers, are tolerant and are agile in their thinking, people that are creative. We didn't always ask that of the security people in the past. There is a need much more well-rounded people, people that can communicate well, and who engage and work well with others".

While the majority of those interviewed felt government professionals required a cultural reorientation, the primary research findings highlight exceptions where government professionals have attended academic programs, or where they have worked with, or alongside, humanitarian groups while in their primary career field. In addition, with the growing number of ex-military or police professionals now within humanitarian security, an informal community now exists where transitioning professionals can leverage the experience of their peers now positioned and successful within the sector, reducing the barriers for entry. Similarly, exceptions also exist for those without a strong security foundation where they have served within an emergency services or a disaster relief role and so have been crisis stress-tested. **Table 3** reflects the primary research data of commonly perceived strengths and shortfalls within the different career start-points, while acknowledging that individuals do not always fit neatly into a particular box. The primary career start-points are disaggregated into uniformed government services (police, military and intelligence) and those coming from a non-security focused role, such as academics, business professionals, project managers, emergency responders, and teachers.

Government Sector (typically military, police and intelligence services)	
Strengths and Qualities	Gaps and Shortfalls
• Hierarchical environment • Strong leadership skills (autocratic) • Crisis stress-tested • Experiential based knowledge • A training and exercising culture • International experience • Systematic thinking • Mission and results-driven	• Autocratic leadership approach • Limited academic experience • Poor technical writing • Lack sensitivity (bullying attitude) • A confined and linear culture • Intolerant of failure – abrasive • Often more rigid and inflexible • Personal experience-based
Non-security focused primary career fields (academics, business, project management etc)	
Strengths and Qualities	Gaps and Shortfalls
• Academically focused • Strong technical writing • Strong management skills – collaborative • Tolerant of failure in others – encouraging • Adaptable and fluid • Project management-focused • People and business-driven • Analytical and evidence-based approach	• Non-hierarchical background • Not stress-tested (unproven in a crisis) • Theoretical vs practical security knowledge • Lacking an authoritative character • No formal training and exercising culture • Limited international experience • Less systematic in nature • Lack credibility in high-risk settings

Table 3. Mapping Primary Career Field Strengths and Shortfalls

Donna, the Global Director for Security for a mid-sized humanitarian organization, observed that differences also exist within the military as a sector in itself, and that these differences further extended to how militaries within different nations brought advantages and disadvantages to the humanitarian sector, positing that:

> "I think especially maybe in the American military, where individuals are very pigeonholed into one specific task, it makes them less capable to adapt to a more rounded security business, whereas I think maybe a smaller military, where individuals take on a much broader spectrum of responsibilities, are probably better at the adaption".

The research findings offer useful context to show how the security profession has evolved over the past 20 years, and how this influences the present-day security community. The 9/11 terrorist attacks revolutionized the security sector, forcing a dramatic shift within the types and weighting of security services as governments recognized, and sponsored, large-scale security services. Historically, the services which emerged during 2008 and 2009 were formally considered "mercenary" and can be traced back to Sir David Stirling's company WatchGuard International, as well as subsequent companies such as Executive Outcomes. Before 9/11, the line between a security professional and a "gun for hire" was very distinct. However, growing demands from the United States (and other nations) to leverage lawfully armed private security services blurred, and eventually eradicated, this line. The 9/11 catalyst led to a surge of support for United States and Coalition Government security requirements, but also drove humanitarians to take security more seriously. Parallel to the sector's changing perception of the security profession was the increasing recognition for the sector to include security into their higher-risk programs. This change in both risk perception and clear operational need was also influenced by increasing demands for appropriate and evidenced "duty of care" within the sector, with a realization that humanitarians were not exempt from legal or reputational harm. The 2008 **Congressional Research Service Report** (2008, p.5) stated that: "The Department of State and the military, Iraq is, in some ways, an atypical situation. There, the United States is relying heavily, apparently for the first time in an unstable environment, on private firms to supply a wide variety of security services". A further 2011 **Congressional Research Service** report went on outline the critical need for commercial security services, indicating that in December 2008 contractors made up 69% of the workforce in Afghanistan, while in March 2011 contractors made up 52% of the workforce in Iraq and Afghanistan. The economic value for the security sector also drove dramatic change within the profession at large, with the United States spending $33.9 billion from 2005 to 2010 in the Afghanistan theatre of operations, and $112 billion for the same period in Iraq. Concurrently, the size of the humanitarian aid and development sector security market also started to significantly increase.

Alice, who had managed multiple large-scale projects in Iraq shortly after Gulf War Two, commented in this divergence of security professionals based on nationality:

> "With 9/11 Iraq saw a mass surge of private security growth. The commercial work was largely met by Brits and Europeans as it required a less militaristic approach and a greater degree of consulting expertise. The US government work, largely supporting the State Department and US camp guarding contracts, drew from retired American military; initially the Special Forces and then basically from anyone who could handle a gun. While the quality of the commercial consulting expertise grew, the quality of the US government contracts professional was quickly diluted".

The divide between United States and other nation security professionals has resulted in a perception of different attitudes, technical knowledge, skills and experiences across this nationality divide. While a hybridization of security companies has occurred in the interviewing years, with companies moving from specialists to generalists and frequently bridging the European and US divide, this perception continues to favour European and British security professionals, as their United States counterparts continue to redress the imbalances caused by the Afghanistan and Iraqi conflicts. Reputational harm to the security sector has further impacted the ability for Americans to transition easily from the government to humanitarian space, with human rights violations associated with Blackwater—including the killing of 14 Iraqis by Blackwater security contractors in 2007—making the sector reticent to accept professionals with a certain security background (Guardian, 2020).

The hierarchy of professionals and competency convergence

Within this section, the hierarchy of security professionals and the concept of competency "convergence" is explored. Within most professions, the hierarchy theory dominates (Wu, 2013), where vertical and horizontal structures (seniority and specializations) exist. For security professionals, hierarchical structuring establishes the individual's seniority and placement within the diverse field of security risk management—and, at the higher level, organizational resilience and business continuity management. Hierarchical structures aid the individual in starting, and then continuing, their professional journey. The application of a competency framework establishes universally agreed goals and performance metrics under which both the individual and organization can map out technical or

skill-based knowledge, leadership or management acumen, and experiential needs. For the security community, a competency framework offers a road map to those entering, and developing within, the profession. This reflects epistemology in terms of *truth*, *belief* and *justification*. Convergence reflects a blending of multiple layers of capacity within the hierarchy of security roles, up to the point of entering into the higher field of organizational resilience.

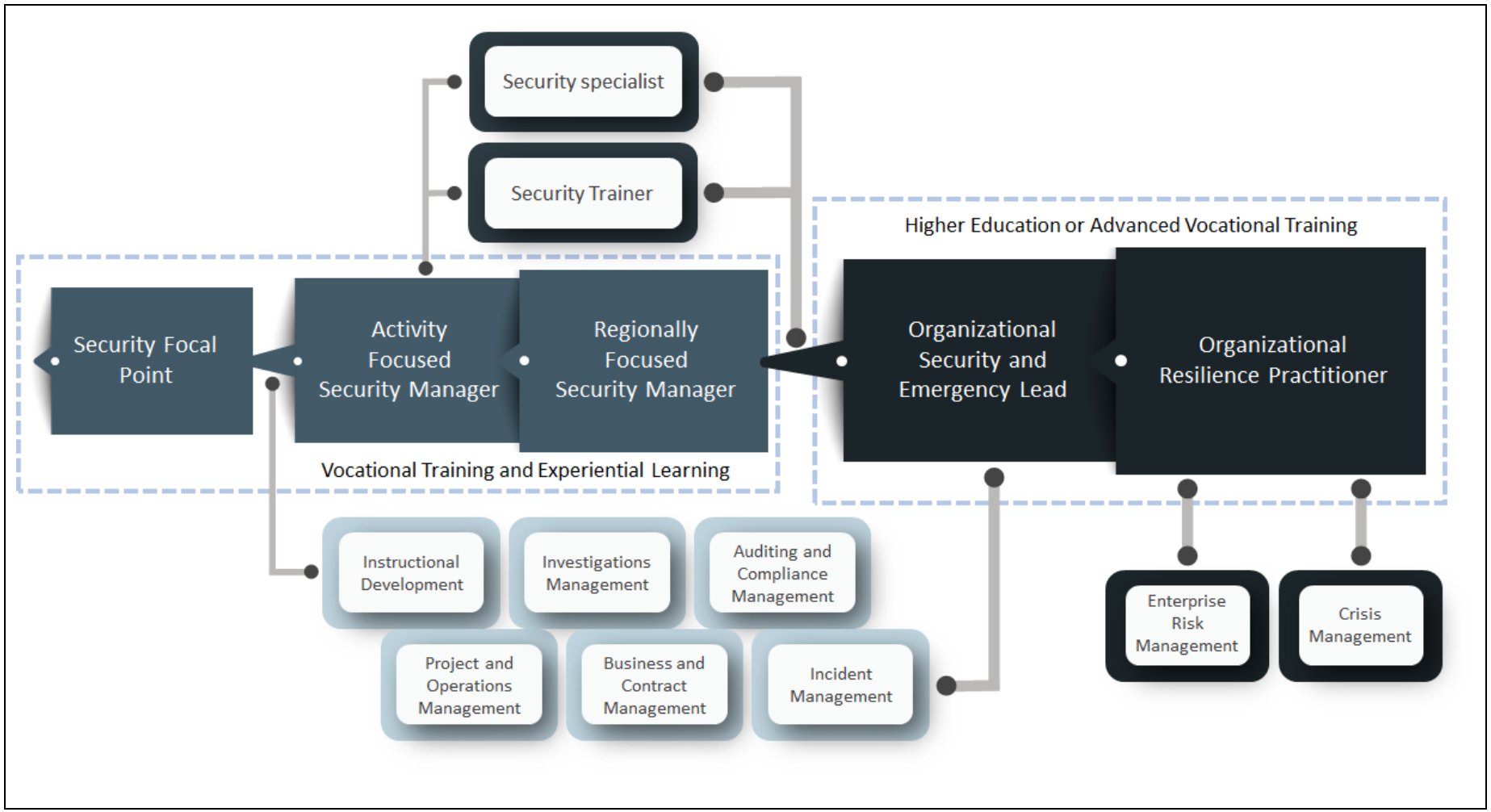


Figure 3. Blyth The Career Pathway for Security Practitioners and Professionals (2020)

Figure 14 illustrates the findings of the primary research in terms of mapping a formal career path that security (and ultimately resilience) practitioners and professionals might typically follow. The research illustrated a very clear divide between the "practitioner" role of the Security Focal Point commonly held by a non-security professional as a secondary function, compared to the subsequent specialist positions more typically performed by trained and/or certified security "professionals".

Research indicates that the ratio of non-security professionals within the sector is higher than those who have formal security expertise, as the cost of hiring security professionals to address security needs is often cost-prohibitive, with Brandie positing that.

> "The field Security Focal Points comprise the biggest group of individuals addressing security and safety, yet these individuals are often doing security as an ancillary function part time, rather than being trained and qualified in the role."

The illustrated career path also reflects branching points for the development of specific areas of expertise where a professional may grow vertically in terms of seniority, but also laterally in terms of technical skill. Professional training, and to a lesser degree simulation-based experiential learning, may support the individual in expanding their capacity out to include: auditing, investigations, instructional responsibilities, emergency and crisis management, or acting within a Family Liaison Officer's role. Ideally, the more seasoned the individual, the more extensive their technical knowledge and experience. The effectiveness of applying this hierarchical structure is dependent on defining the role requirements for each position, and to establish whether individuals are required to bring the required competencies to the role—before being appointed. Conversely, it may also define where some areas of competency can be developed in post, providing further opportunities for both the non-security professional as well as for those with existing competencies.

Convergence recognizes that individuals come from different career start-points, but ultimately must come together—or converge—to reflect the same breadth and depth of technical knowledge, as well as similar experience-based competencies. Convergence recognizes that all experience, whether academic or vocational, bring a degree of positive value to an individual's personal and professional development. **Figure 15** illustrates primary research findings of how each career field brings different strengths, which, when combined at the point of convergence, offers an optimal security solution.

Where convergence is achieved within the field of security risk management, the next step past technical and experiential competency is the leveraging of academic or strategic level vocational knowledge to move the individual into the realm of organizational resilience and business continuity management.

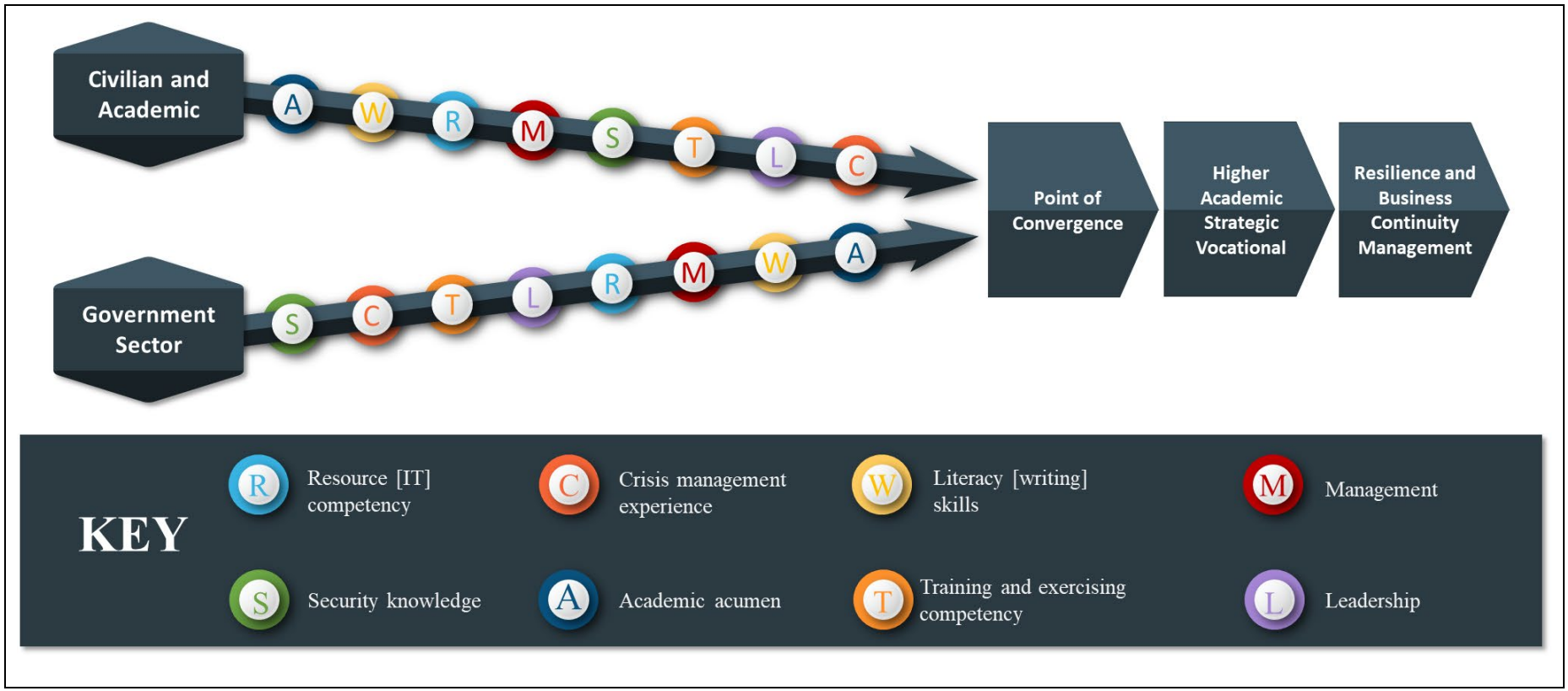


Figure 15. Blyth Competency Convergence Model (2020)

Individuals are faced three challenges related to career transitioning and role stagnation within the hierarchy of security: 1) the absence of clear transitionary support mechanisms, or defined expectations, between primary and secondary career fields, 2) ambiguity over the specific technical qualifications and experiences required across the various layers and specializations within the field of security risk management (a competency framework), and 3) an ill-defined professional road map for continued technical and experiential growth for the established and motivated professional. Research also suggests that professional development within the field of security risk management and, at the more strategic level, organizational resilience, is gained through three main areas of competency: 1) leadership and/or management acumen, 2) vocational and/or academic knowledge, and 3) effective contextual application through first-hand or observed experience.

The three areas of professional development must be viewed against the three levels of need: 1) tactical, 2) operational, and 3) strategic. The challenge, then, is to achieve the three areas of competency while contending with the three core challenges. To complicate matters further, this must be accomplished within a complex and dynamic global setting. It is also set against the background of increasing and ever-changing risks the sector faces. This suggests that the responsibilities of the practitioner and professional are also changing, evolving from a focus on physical risks, to encompassing more broad-ranging organizational resiliency responsibilities. Dustin noted that, historically, security professionals were focused on the physical security needs of the sector, rather than being part of the broader approach to organizational resilience and business continuity management, positing that:

> "They (security professionals) tended to be more around the hard security than risk management. I think more and more organizations are going down the route of enterprise risk management. We are definitely seeing more organizations who are developing a risk management position, capacity, and approach; where they address security risks, as well as finance risks and reputation risks. They (the organization) are seeing a much stronger interlink between the various risks, rather than being so finance risk focused".

The requirement then is for both the individual serving in a security role and their respective organization to recognize the strengths and weaknesses that each primary career field brings, as well as the associated competency needs within the hierarchy of security required to formalize the sector's security profession.

Figure 16 offers thematic areas drawn from the primary research data which supports the successful convergence of competencies. The findings of the primary research suggest six key areas of consideration: 1) competency expectations, 2) career transitioning, 3) leadership and management acumen, 4) vocational and academic knowledge and skills, 5) contextual application of knowledge and skills, and 6) continued professional and personal development. These areas, when effectively working together, can influence how successful the individual's entry into the humanitarian security space may be. Further, it underpins how productive their onward professional learning journey can be.

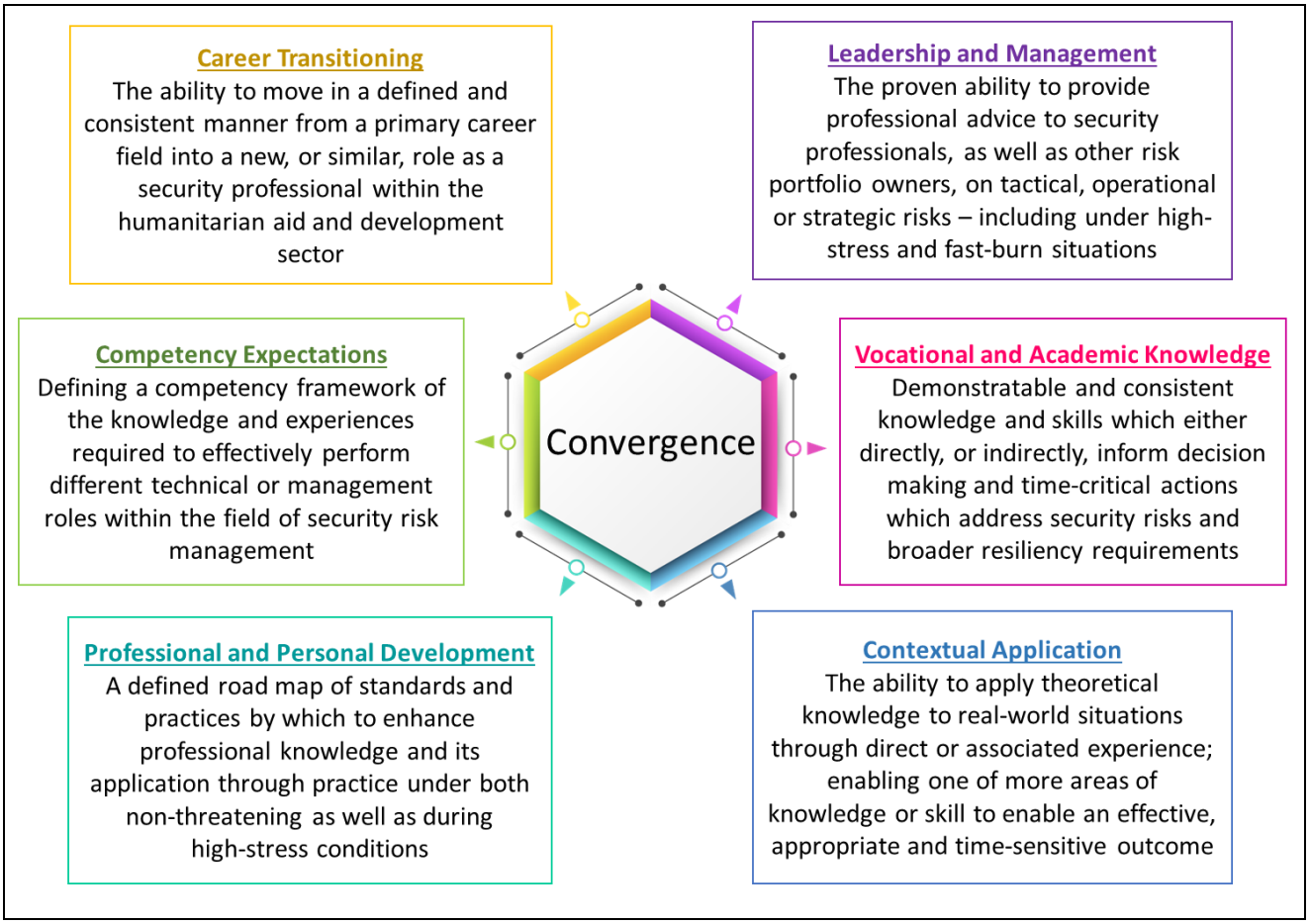


Figure 4. Blyth The Principles of the Convergence Model (2020)

While the primary research confirmed a stated need to formalize a competency framework and the different attributes primary career fields offered, the underlying findings indicated that a road map has

yet to be developed, and that the resourcing of technical and experiential competencies is largely absent within the sector, with Dustin positing that:

> "A couple of organizations are actively trying to create a supportive career path for program staff to move into security. They want to have people who come from a humanitarian background, so they are offering them training, capacity building, mentoring and opportunities for advancement as part of this supported package".

Ultimately, convergence must recognize the common strengths and shortfalls associated with each primary career field. It must recognize how risks are managed differently between the point of tactical and operational risk management (the field) and organizational resilience (the headquarters). Convergence must also recognize the competency gaps often found between the headquarters level where the seasoned security professional more frequently sits, and the field level where more junior security professionals or practitioner security focal points operate. Where security is "managed" then the difference between generalist and specialist management competency must also be recognized. Hilda reflected on these differences, stating that:

> "It seems like there's almost always this ass-covering approach at the headquarters level, where they want to have a policy that describes how they approach risk in the field. But then at the field level, how do these connect, the security for people and infrastructure at the field level, the approach seems to be so different".

Within the international context, convergence must also incorporate emotional, social and cognitive competencies, since cultural influences will shape how individuals within the security community (and, critically, their organizations) think and act. Convergence also relies on the professionals' ability to integrate themselves into the leadership structure, gaining political currency to influence cultural change from within, and to shape executive decision-making. Professionals must therefore have the sophistication and persuasiveness to alter entrenched perceptions, having the "smarts and clout" to effect change. The security community and sector at large must also recognize knowledge, experience and technology resource limitations, and must also recognize limitations for individuals to competently leverage technologies in order to effectively perform their role, and to advance in their profession[12].

[12] Noting that in less developed nations' access to IT and internet bandwidth limitations can severely hamper the ability of practitioners to access knowledge and so professionally grow in their field.

Defining competency needs

This section looks at the need to establish a universally agreed competency framework within the humanitarian security space, against which both organizations, and professionals or practitioners, can define (and agree on) expectations. A competency framework also provides the platform from which a logical and consistent approach to professionalizing the field of security risk management can be launched. The competency framework reflects the three areas of the: 1) individual, 2) job demands, and the 3) organizational environment, as illustrated within **Figure 17** (Boyatzis, 2008, p.7).

Figure 5. The Boyatzis Theory of Action and Job Performance

Competency supports three fundamental levels of organizational need: 1) strategic, 2) operational, and the 3) tactical levels. Simplistically, at the strategic level, the focus is on protecting organizational resilience and business continuity management. Operationally, the focus is on location or activity risks. At the tactical level, the focus is on protecting people or materials. This complex interplay of considerations defines the layered needs of the organization against which the security community must then define associated knowledge, skills, experience, and attitude requirements.

Organizations such as INSSA have sought to construct a competency framework for both security professionals and practitioners within the humanitarian space, offering a competency outline and accompanying testing methodology to enable individuals to achieve the professional standards which accompany job demands, as well as the organizational environment (Boyatzis, 1982). Tom stated that

INSSA's approach used a focus group to develop competency requirements in order to better address the wide-ranging beliefs of the community:

> "This process involved 35 or 40 academics, Security Directors, security field personnel, to highlight, isolate, define, what are the core competencies that any security risk management professional in the international NGO space needs in order to perform effectively. They broke these down into risk assessments and leadership and communication and training and incident management and so on. It was a very useful exercise".

The need for a competency framework to be established—ideally with widespread engagement of both those performing a security role and the end user organizations—was underpinned by Focus Group Participant No. 1 who offered that:

> "From my experience many organizations lack a consistent way to articulate safety and security needs when recruiting, managing and mentoring professional security personnel. Equally many security professionals can make poor choices in investing in skills and personal development, with the wrong kind of training or development choices for their career paths. Having guidelines and a technique for establishing different levels of security professional, and what each level should be aspiring to achieve can only promote higher levels of competency and professionalism".

While the INSSA competency framework is a significant step in paving the way to define both a hierarchy of security practice and accompanying competency requirements, it has three main flaws: 1) the research data was not published and so the logic behind the framework is unknown, 2) it has yet to be universally accepted by the community, and 3) it reflects the testing component of the process, absent the resources needed to firstly teach critical areas of knowledge. As such, it represents a partial solution to a much larger need. That said, INSSA has taken the first and critical step in forming a common understanding of competency requirements against the limitations of funding and collective community engagement, and importantly INSSA has collaborated with an established training provider to address the missing "teach" component of its solution—drawing from out-of-sector disciplines to advance knowledge and practice (Tabaklar, 2015). INSSA is also an entity staffed by volunteers, each providing their time and resources *pro bono* for the benefit of the community, and so the advancement of best practice is naturally constrained by these limitations.

Table 4 offers a basic outline of a security hierarchy drawn from the Competency Framework Focus Group primary research findings. It reflects the pathway illustrated in **Figure 15,** adding substance to the generalized expectations of each role.

Role	Description
Security Focal Point	Effective field-level tactical competency within the area of security risk management, typically focused on immediate life-safety needs. The position commonly does not have formal security training, experience or certifications, and is performed as a secondary function. The focal point offers advice and support during a local incident.
Security Manager	Effective tactical through to operational competency supporting the management of project-wide or location-specific security risks, focused on life-safety as well as broader operational risk management needs. Is commonly a dedicated full-time security professional with some level of security certification. May lead the immediate localized response to a serious incident.
Senior Security Practitioner	Effective tactical and operational security competency with a degree of strategic resilience capacity. Focused on life-safety and operational risk management, with an understanding of organizational resilience. A seasoned and often internationally experienced / certified security professional. Manages multiple projects / locations, leading on specific technical areas in a crisis.
Global Security Director	Responsible for establishing organizational security standards and practices. Oversees operational security needs across countries / activities. Cognizant of the broader organizational resilience requirements. Offers technical advice at the strategic level before, during and after a crisis. An internationally proven / certified senior security + crisis specialist. Leads on some forms of crisis.
Resilience and Business Continuity Practitioner	A fusion point for holistic resilience considerations, shaping cross-cutting resiliency strategies. Is certified in security and business resilience. Has a deep understanding of the implications of an incident and how this creates cascading risks which resonate across the organization. Provides expert advice to all functional areas during a crisis—may lead a crisis response.

Table 4. Security Profession Hierarchy - Primary Research Findings

While these roles and responsibilities are broadly accepted within the field of security risk management, there is little agreement as to which technical competencies and experience are desirable or mandatory. This lack of consensus presents challenges, both for security professionals seeking employment, and the organizations seeking to employ them. And, for the practitioner without any basis of reference, it makes progressing within the security community difficult, if not impossible.

Focus Group Participant No. 2 noted that the humanitarian aid and development sector has been reluctant to address the obvious need to develop a universally agreed competency framework. This was partially due to the complexity of meeting variances between international and national professional competency needs, as well as the absence of in-country resources required to meet demands:

> "Within the humanitarian and development sector there has been a reluctance to adopt any standardized competency framework or utilize mainstream security professional certifications as a means of assessing professional skill competencies, one core humanitarian competency framework has been developed, which is general in nature. A similar hesitation has been seen in other areas of technical competence in the sector, this may be a product of the required skill and qualification difference between international staff and national staff, along with organizations being required to provide specific skill training to national staff in many countries that do not have functional technical skill training or functional education system, for various reasons".

The complex nature of the security professional's role, especially when addressing the shifting complexities of international risks, requires the professional to be able to apply *deductive*, *inductive* and *abductive* reasoning techniques, based on a combination of both theoretical and applied reasoning. While some deductive decisions may be based on a proven hypothesis (i.e., terrorists are targeting western interests, we are a western entity and so we may be at risk), other decisions may be made inductive by making broad generalizations from specific first-hand or peer-shared information or experiences (i.e., terrorists operate in the region, peers are concerned, we are likely at risk). Alternatively, professionals may form an opinion based on incomplete data and make a "best guess" through abductive reasoning (i.e., an explosive has occurred, terrorists use bombs, the explosive was caused by terrorists). The more senior the position, complex the situation, or high-risk the environment, the more individuals must intuitively evaluate the situation based on taught, observed and experienced knowledge.

Table 5 reflects the primary research findings of the Competency Framework Study Group, illustrating competencies within both generalist as well as threat-aligned thematic areas. Deductive, inductive and abductive reasoning as well as metacognition are required when applying the framework in terms of seniority and specializations within the security hierarchy, as well as the contextual application in widely differing threat environments within which the sector and security professionals and practitioners operate.

General Competency Area	Competency Alignment to Threat Types	
• Risk and impact assessments • Predictive risk planning • Establishing and managing standards • Defining and implementing best practices • Policy, plan and protocol development • Report writing and record keeping • Technical risk advisory support • Leading internal experts and teams • Evaluating vendors and suppliers • Managing subcontracted services • Contract and financial management • Leveraging security technologies • Optimizing security equipment • Infrastructure security hardening • Travel risk management • Investigations management • Family liaison • Liaison and stakeholder management • Effective communication skills • Training, mentoring, exercising and testing • Emergency and crisis management • Auditing and performance monitoring	• Active shooter attacks • Armed aggressor attacks • Arrests and detentions • Bomb threats • Bush and forest fires • CBRN risks • Civil disorder (riots) • Coercion and intimidation • Coups • Cyber or information risks • Death threats • Earthquakes • Espionage • Facility fires • Fatality in management • Financial loss • Flooding (severe) • Fraud and corruption • Gang violence • Gender risks • Hostile media • Intellectual property loss	• Key person loss • Kidnapping and hostages • LGBTQIA targeting • Litigation • Mass casualties • Missing persons • Murder • Pandemics • Physical assaults • Political risk • Reputational risk • Road traffic accidents • Serious casualties • Sexual assaults • Severe weather • Terrorism • Terrorist financing • Tsunamis • Volcanic eruptions • Youth risks • War • Workplace violence

Table 5. Mapping Competencies Against Threat Factors and Common Tasks: Primary Research Findings

Focus Group Participant No. 5 discussed the hierarchy of security and the importance of understanding the needs of a security "practitioner" verses a security "professional":

> "For our organization it is a bit more complex, because the Security Focal Point, generally speaking, is an individual who is not a security person, but takes on (often without additional compensation) certain duties within security that tend to be more on the administrative side as they have no previous security experience… We have now taken a logistics person, provided him additional salary, and are attempting to get him properly trained. We also have a part time country security manager to look after our projects, and we have relied heavily on this person".

Collaboration within the sector, coupled with the proactive leveraging of other sources of expertise and experience, collectively strengthens a competency framework. **Figure 18** outlines how risks establish the fundamental needs of the framework against which control measures are applied. These risks and controls are then mapped against individual, community, activity, location and wider organizational needs. Outputs include the sharing of knowledge and best practices, evidence-based and consistent standards and practices, a clear road map for both the practitioner and/or professional and organizations on professional expectations, and the ability to determine what resources are required to build and sustain capacity. The sector then has to decide whether to implement transformative change where a rapid evolution of security risk management accelerates change—or, where change will be incremental and through osmosis.

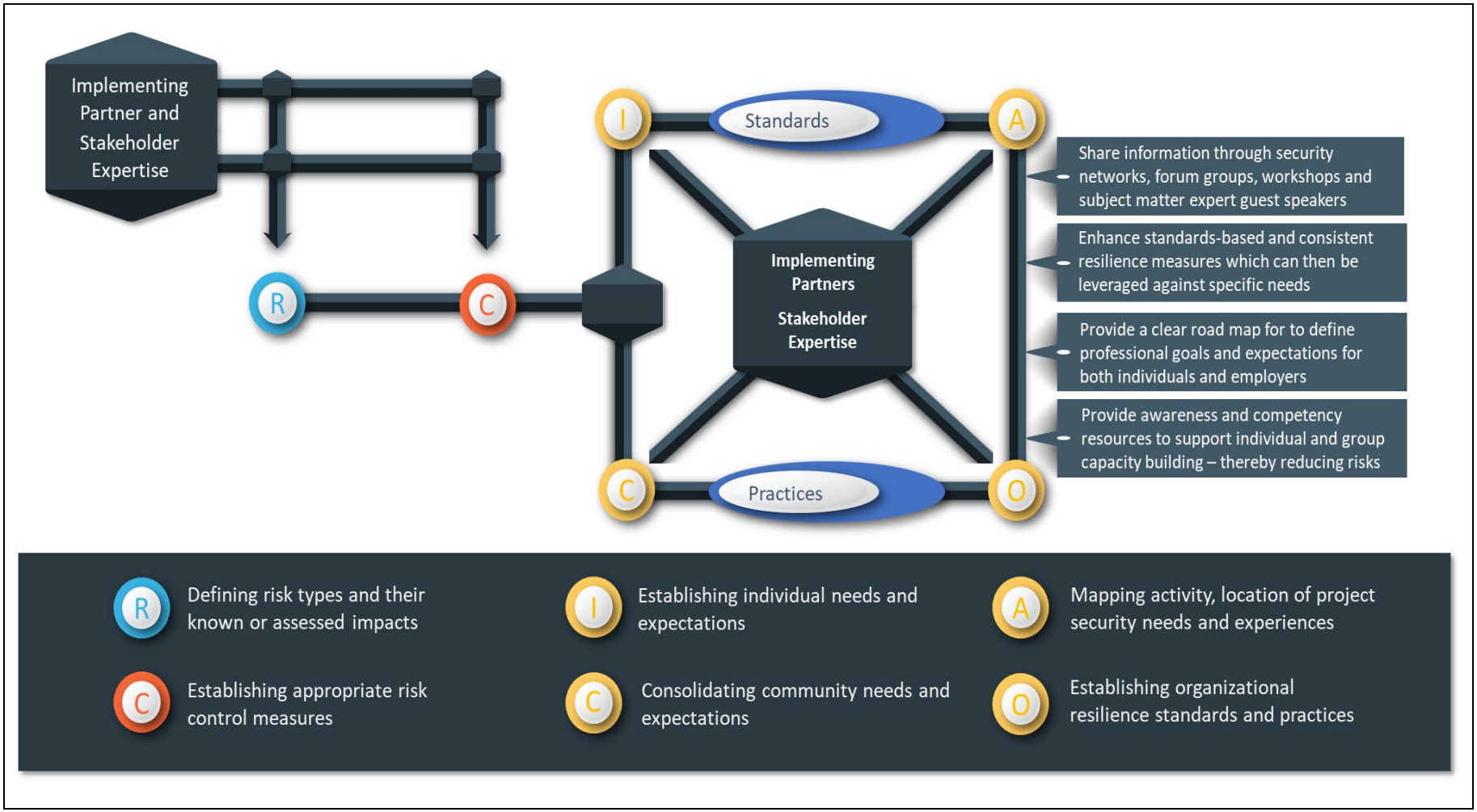


Figure 18. Blyth Competency Framework Fundamental Needs: Primary Research Findings (2020)

The value of forums and associations

This part of the research analyses the value which forums and associations bring in terms of acting as gravity points for recognized, credible and reliable knowledge, and so help shape the profession, provide educational resources and tools, and to present a mechanism for information-sharing and collaboration. Forums and associations also provide metrics by which to measure the credibility of the professional or practitioner—and, in so doing, establish consistent and widely-recognized standards and practices. These resources help the humanitarian security profession to take root and ultimately grow, benefiting both the security community and organizations within the sector. High reliability organizations also see "extraordinarily dense patterns of cooperative behavior" (La Porte, 1996) both within as well as external to the organization, underpinning the potential value of cooperation between organizations.

The European Commission's Directorate-General for Humanitarian Aid **NGO Security Collaboration Guide** (2006, p.1) state that security and safety was a significant concern, with escalating threats against organizations operating within environments where both direct targeting and indirect threats presented physical risks to personnel. The report identified the need for collaboration but stated that: "formal collaboration on security issues remains rare". The causes are poor and inconsistent funding, the lack of mechanisms to share ideas and best practice, and a fluid environment where organizations and professionals struggle to form solid and lasting structures. The guide calls out successes with the Afghanistan NGO Safety Office (ANSO) and the involvement of InterAction's SAG in forming a mechanism for information-sharing for NGOs operating within post-Taliban Afghanistan. The report also identified the NGO Coordination Committee in Iraq (NCCI) which was formed by a small group of NGOs as an ad hoc forum to share time-sensitive security information. Other groups, including the NGO Security Preparedness and Support Project (NGO-SPAS) in Somalia, the Baluchistan INGO Consortium (BINGO) and other field-based forums where organizations and the security community can share information, ideas and seek out opportunities for personal development also sporadically emerge to fill temporary needs. The guide (p.4) stated that: "Effective security management in the field takes significant time and investment. Essential components include: developing and maintaining an understanding of the context; determining the risks; building and maintaining security contacts and information sources; monitoring security incidents and trends; establishing security plans and procedures; and providing security training and inductions for staff".

While some forum groups offer a consistent level of technical knowledge, shared experiences, tools and forums of collaboration, others have proven to be less consistent or effective. Andy commented on the GISF which provides a wealth of articles, reports, studies, blogs, training alerts, mechanisms for information sharing and collaboration, and forum speaker sessions, offering:

> "They are doing a remarkable job of making (EISF now GISF) of raising awareness to NGOs in a very cost-effective way. They are pushing out a lot of awareness".

The InterAction SAG was also formed to bring seasoned practitioner professionals together to help establish standards, share ideas, and promote professionalism within the sector. However, the successful SAG concept was discontinued, resulting in a noticeable void within the United States security forum space (GISF in 2020 are moving to fill the US void). InterAction's MOSS launched in 2006 was also discussed with interviewees; however out of the 32 practitioners interviewed, only five were aware of the InterAction MOSS, and all felt it served no useful purpose. Brad also mentioned the failure of InterAction to provide guidance within the United States sector, requiring professionals and practitioners to form their own associations through networking, rather than through a formal and structured mechanism, stating that:

> "You get an international body in Europe, and an international body here on the US side (InterAction), which has been broken on the US side for years now. It has now totally disintegrated. The only body or group of professionals that work together is those friends that you have made in the field and those people that are your buddies today. So it is the informal networks which are being formed".

While other forums such as DisasterReady and INSSA offer varying levels of useful direction and information for the United States humanitarian security professional and practitioner community, their remit is either limited, or is provided on a part-time *pro bono* basis. The resources provided by commercial sector associations and United States government agencies were also discussed by interview participants, with Andy suggesting that some effective resources are offered by commercial associations which support individuals with their career transitioning and professional development:

> "I think over the past two, three years, especially in the UK industry, there has been a massive development in this [supporting career transitions]. It has been spearheaded by the Security Institute and ASIS, they have been really instrumental in meeting this need".

USAID has in recent years realized the need to support their implementing partners in managing security risks, and thus established the Partner Liaison Security Operations (PLSO) program. Grace, a senior risk advisor involved in the PLSO program, commented on the PLSO concept in Nigeria (similar projects exist in Kenya, Haiti, Ethiopia and South Sudan) through commercially contracted companies. These vehicles act as a security focus point within a national humanitarian setting formed to support the sharing or ideas and experiences, provide training resources and tools, and assist with the formation of a community of risk practitioners at the country level, with Grace stating that:

> "The PLSO concept is fantastic. It provides much needed resources to the Implementing Partner community (humanitarian aid and development sector) through USAID funding, and also provides the platform from which organizations can share ideas, best practices and experiences to enhance security risk management, and better manage local crisis situations".

Forums and associations then play an important role in acting as a point for knowledge and experience consolidation, evaluation, processing, and dissemination to support the professionalization of the security sector.

CHAPTER 6

STANDARDS AND EFFECTIVE RESILIENCE

Introduction

This chapter presents the findings of the primary research into the importance of standards in defining and articulating organizational resilience strategies. Standards form a level of quality or attainment, establishing an accepted norm or a model for comparative evaluation. Standards are expected within any organization, regardless of its size, worth, longevity or nature. They define the degree of consistent professionalism expected from managers and staff, as well as the broader performance goals of the organization.

Standards at the most fundamental level reflect a commitment to meet duty-of-care obligations. Operationally, they protect against disruption and optimize performance. At the strategic level, standards protect against business extinction events resulting from litigation or reputational harm, demonstrating to both internal and external stakeholders the organization's maturity and professionalism. Standards are developed by a body of recognized professionals as the accepted norm and a measure against which organizations should hold themselves accountable, and against which others will measure them. With the absence of a formed security community or a recognized and effective membership body that can effectively pool ideas, consolidate concepts, document outcomes, and articulate the value of resilience, then the sector must rely upon out-of-sector standards against which it can work.

Organizations are by nature objective-based, whether they deliver emergency relief, build hospitals, educate children, address gang violence, support farming initiatives, or build governments. As such, resilience is effectively an overarching objective which supports all organizational goals. Protiviti and DeLoach (2015, p.2) stated that: "An organization is designed to accomplish objectives. It is presumed that the organization's leaders can articulate its objectives, develop strategies to achieve those objectives, identify the risks to achieving those objectives and then mitigate those risks in delivering the strategy". Whether standards are designed by humanitarians for humanitarians, or whether the sector takes advantage of out-of-sector standards, the need for standards remain.

The fiscal value of the sector, coupled with growing employee, donor, charitable contributor and government expectations, is requiring the sector to quickly meet recognizable and measurable levels of professionalism, with Alex positing that:

> "We work for what is primarily an unregulated sector, but we need something that is going to bring us online. I can move from one organization to the next, and this organization's perception of a policy and a procedure and an SOP is significantly different from that. There is no alignment".

This chapter looks at the importance of standards, what steps have been taken by humanitarian membership bodies and forums to leverage the UN MOSS, the applicability of ISO and other out-of-sector standards, and the value of codifying standards and practices through document systems.

Leveraging international standards

This section looks at professions as hierarchical social institutions that possess a body of knowledge which is consistently applied. Professions reflect *behaviors*, *knowledge* and *skills* developed through intensive academic or vocational programs, and which are then applied in action. They adhere to codified standards and practices which define agreed-upon performance metrics. For the security profession, members form a disciplined group of individuals who possess special knowledge and skills, and who are recognized and trusted as experts within their domain. As the sector matures, its approach to security risk management and organizational resilience forms an urgent need to establish a recognized security profession. This is becoming increasingly important as the remit of security grows, through a combination of internal and external demands.

Most professionals within the security sector recognize that marginal differences exist between how the humanitarian sector and their government or commercial peers address security risk management needs, with Adam stating that:

> "NGOs are not really that different from any other organization, so we need to look at what are the practices and the standards that other organizations are looking at".

This opens the door for the sector to leverage the extensive array of existing international resilience standards already in use by commercial companies. However, while many security risks and their associated impacts are common, regardless of whether they effect a humanitarian organization or a

commercial company, interviewees also recognized that the sector is comprised of a diverse range of nationalities, cultures and risk environments. This presents a significant challenge in coming to a common understanding of what constitutes "best practice" across highly disparate cultures and geographies, with Alex positing that:

> "You have a massive sector, a huge bunch of different nationalities that have a different approach, and a different understanding of what best practice is. We need something that is going to bring us online. Currently I can move from one organization to the next and this organization's perception of resilience is significantly different from the next. There is no alignment."

The establishment of sector-recognized standards provides a framework not only for professionals transiting from one career or position to another, but also for organizations to measure the effectiveness of their individual resilience strategy against a peer benchmark. Alice emphasized the need to be able to benchmark against a consistent standard in order to measure the organizational effectiveness in managing increasingly complex risks, stating that:

> "We need to have a standard. We need to have a benchmark to run to".

The need for both achievable and appropriate standards also extend beyond the practical need to reduce physical risks to people, assets, operations and information. Litigation risks have also dramatically increased against organizations who had historically being immune to legal action. Erik posited that the application of sensible, scalable and achievable standards would better insulate against litigation risks:

> "From the legal side, the overarching standard is reasonableness. So if everyone within a particular industry space is relying on the MOSS standard or an ISO standard, then yes, you should be relying on it. If it is a standard that's maybe the gold standard but not every day best practices, then you have to figure out what's reasonable for your organization?".

Figure 19 is drawn from a pool of 77 survey participants who were asked to respond to the statement: ***"Do organizations see value in seeking to be aligned with, or certified to, recognized standards"***, and reflects the acknowledged importance for the sector to align itself with recognized standards relating to risk, security and organizational resilience. Of the participants surveyed, 72% indicated that their organizations saw value in being aligned to, or certified by, recognized standards.

Despite data from all three research pools acknowledging the importance of standards, the application of this strategy in reality falls far short of the mark. Primary research indicates that the challenge is a lack of understanding of what standards exist, which standards are appropriate, and how these standards might be applied. Indeed, the majority of participants were unaware of the full extent of the ISO and BSI standards relating to risk, business impact analysis, resilience, business continuity management, emergency and crisis management, and security management. The majority were also unaware of the InterAction's version of the UN MOSS, and how this might be applied to reducing risk. As such, while both security professionals and their respective organizations largely recognize the value of standards, only a few understand what system they might draw on, with fewer still meeting the criteria of achieving any form of consistency in managing risks.

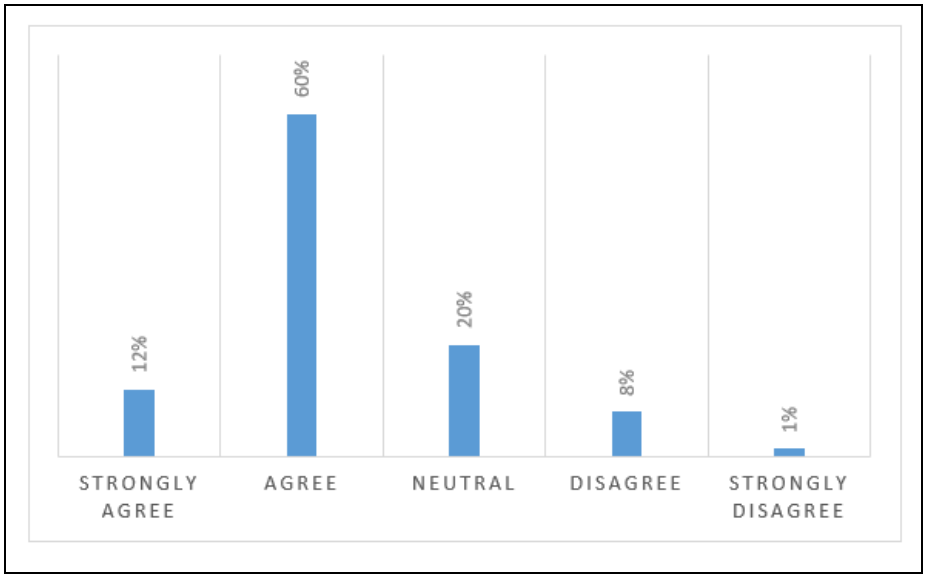


Figure 19. Do Organizations See Value in Seeking to be Aligned, or Certified to, Recognized Standards

MOSS standards

The humanitarian aid and development community has historically sought to establish sectoral security standards by leveraging work already developed by the UN and peer agencies. In 2006, InterAction launched its own 7-page version of the MOSS[13]. However, this "standards lite" approach was not well-received within the sector. Participants stated that the InterAction standards lacked depth, were not appropriately resourced, and forced outcomes which were either unachievable, or which placed an

[13] The United Nations MOSS reflect a significantly more comprehensive set of directions and guidance (thousands of pages) and includes comprehensive training programs to operationalize standards and practices.

organization at litigation risk if they failed to live up to the espoused standards. The majority of those interviewed indicated that they had not heard of the InterAction version of MOSS, with more (but not all) being familiar with the foundational UN MOSS system. While the objective of InterAction's MOSS variant was worthy, neither the application of UN's standards, nor the subsequent dissemination by InterAction, succeeded in achieving the desired outcome. Bill commented on the inception of InterAction's MOSS and the goals it had originally set for itself, stating that:

> "It is useful to understand that the InterAction version of MOSS came out probably about 10 years ago at a moment in time where it was obvious to the security practitioners within the humanitarian sector that standards such as MOSS would go a long way to do two things. One would be to enable and empower and organization to increase safety and security for its staff and therefore its program, and secondly, to also provide some sort of measurable benchmark for donors to feel comfort about giving funding to an organization".

Tom offered an insider's view of the challenges InterAction faced when developing the MOSS, acknowledging that the standards failed to meet the known requirements facing the sector, but that fear of litigation resulted in a good idea being diluted to the point of irrelevancy:

> "It was a painful process. They are general, so general you could drive a truck through some of the holes in the standards. But that was a result of lawyers. You have to understand at the time you had various NGO lawyers weighing in and they couldn't agree with each other. They watered it down so much, because as one of them said: "clearly you don't want to give information to the plaintiffs, right?".

InterAction as a forum has a longstanding history within the community, including the establishment of a highly successful SAG which, in the early years of its establishment, did much to offer security value to the community at large. Resultingly, InterAction was well-placed to establish standards in collaboration with leading security professionals within the sector. Fay, head of country security risk management for a major humanitarian organization, commented on the value and placement of InterAction as a trustee of intellectual excellence, but reflected that its success as a standard setting organization was not commensurate with its otherwise strong standing within the sector:

> "I know InterAction. They are an advocate organization, and they deal with certain issues of NGOs across the globe. We had a critical situation in which InterAction got also involved, and

> probably they get involved once there is something really substantial, something very serious at the government level, at the policy level. But I have never heard of their MOSS standards".

Interestingly, the majority of those interviewed were not aware of the InterAction interpretation of MOSS, with only 5 of the 32 participants interviewed being award of these standards. Erik stated that:

> "I am not (aware of the InterAction MOSS standards). When you mention now, I don't know if you saw my frown, so coming out of a security background, not military, private security, that duty of care is drummed into us, but this is the first time I've heard of the MOSS standard".

To contextualize the value of InterAction's MOSS it is useful to compare what was produced in 2006 against the extensive resources developed by the UN and other publicly available standards. The UN's MOSS and supportive materials are publicly available, allowing any professional or forum to access resources which can be quickly tailored to framework sector specific standards. The rich depth of publicly available technical data also offers professionals the ability to benchmark against multiple documents and thousands of pages of useful content, such as: the **United Nations Security Policy Manual** (2017), the **United Nations Security Policy Manual** (2017), the **UNICEF's Standard Operating Procedures for Crisis Management and Emergency Operations** (2000), and the **UNDP Standard Operating Procedure for Immediate Crisis Response** (2018). While the United Nations' MOSS reflected a macro-level organization with significant funding, it is arguable that InterAction's 7 pages of content failed to reflect the depth and breadth of materials required to tackle the complexity of establishing sector-wide security standards, with Anna positing that:

> "The reality is if you were to be MOSS compliant, it is financially prohibitive for most NGOs whether they are for profit or nonprofit. I would say both international development and humanitarian sector groups cannot afford to put in the full MOSS standards".

Alex also neatly summarized the difference between how the UN and the Interaction variant, stating that while the MOSS works for the UN, its application within the sector was not successful:

> "The UN employ MOSS particularly well. I would say we don't".

While the intent of the InterAction MOSS was inarguably sound, the research findings suggest that a multi-billion-dollar sector operating in high-risk environments with predictable risks should be able to achieve a better outcome. InterAction's MOSS was of little practical value, and once drafted (2006) it was never updated, with Brad positing that:

> "We totally ignore it as an organization [InterAction MOSS]. It is so basic that we are so far ahead of what those standards are. When I looked at those standards it was automatically noticeable to me that it was not designed for an organization that operates in high-risk environments. Our minimum standards are triple-fold what that is".

Interestingly, Brad went on to compare InterAction's MOSS with the existing ISO standards, stating that:

> "ISO standards have huge value in my opinion. It is an extremely useful strategy that all organizations strive to implement".

This comment, supported by a strong sector belief in the need for standards, coupled with the growing awareness of ISO, BSI, ASIS and other standards, suggests that in the absence of sector-generated standards that out-of-sector disciplines should be leveraged to address the current standards gap. The application of the security risk management principles found within the **Sphere Project: Humanitarian Charter and Minimum Standards in Humanitarian Response** (2011) was also cited by participants as being of limited value. Few participants were aware of the handbook, and those who were indicated that any security and resilience value was lost within hundreds of pages addressing other areas of interest.

The International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) addresses a wide range of thematic areas within the fields of risk management, security, resilience, business continuity management, emergency and crisis management. ISO was established in 1946 and represents 164 national standards bodies. Through these members, it brings together experts to share knowledge and develop consensus-based international standards. Of direct relevance to the humanitarian aid and development sector are the following ISO standards:

- ISO 31000: Risk management.
- ISO 22317: Business impact analysis.
- ISO 22301: Business continuity management.
- ISO 27001: Information security management (and 27031 for ICT business continuity).
- ISO 22320: Emergency management.
- ISO 34001: Security and resiliency.

- ISO 22316: Organizational resiliency.
- ISO 18788: Management systems for private security operations.

Other standards, including the Business Standards Company (BSI) 17091 standards for crisis management also offer additional resources which the sector can easily access. The National Fire Protection Association (NFPA) also offers publicly available standards on continuity, emergency and crisis management (NFPA 1600). Governments also release publicly available security, business continuity and crisis management standards which can be modified to meet the sector's needs, such as the United Kingdom's **Government Functional Standards GovS007: Security** which provides security guidance across organizational boundaries (2020). While research suggests that ISO 31000 for risk management was more widely recognized—with GISF exploring this standard within multiple articles for its members—the community at large has yet to fully explore how these other standards can be adopted to address the multifaceted needs of sector resilience. Where interviewees were cognizant of ISO standards, the response was generally positive (with limited reservations), with Adam positing that:

> "So we are always (as an organization) looking for best practice to benchmark against, and so ISO standards provide perhaps the best practice out there".

While the underlaying findings from the research is that organizations are often slow to adopt new standards—often being forced to do so by painful experience—when the ISO standards are adopted, they are almost invariably deemed of value. Andy indicated that crisis events can drive the need to adopt recognized standards, positing that:

> "The Norwegian Refugee Council, where they sent somebody to north Kenya, and the legalities resulting from the kidnapping of one of their staff members led to a big change and the understanding where ISO standards can fit in to reduce their exposure to litigation, but also to ensure that the duty of care is being provided".

Figure 20 is drawn from a pool of 77 survey participants when asked to respond: "***Do organizations fully understand and are compliant with ISO standards associated with Enterprise Risk Management, Business Continuity Management Systems, and ICT DR resiliency; or use comparable standards****"*. The results suggest that despite the relevance of ISO standards, only 13% of survey participant organizations utilized ISO standards to address their resilience needs, with 59% indicating that ISO standards where specifically not used. When the same survey pool was asked do: "***Organizations see value in seeking to be aligned with, or certified to, recognized standards****",* the

results indicated that despite ISO standards not being broadly adopted, the majority of organizations— some 72%— actively saw value in being aligned to some form of recognized standards, as shown in **Figure 21**.

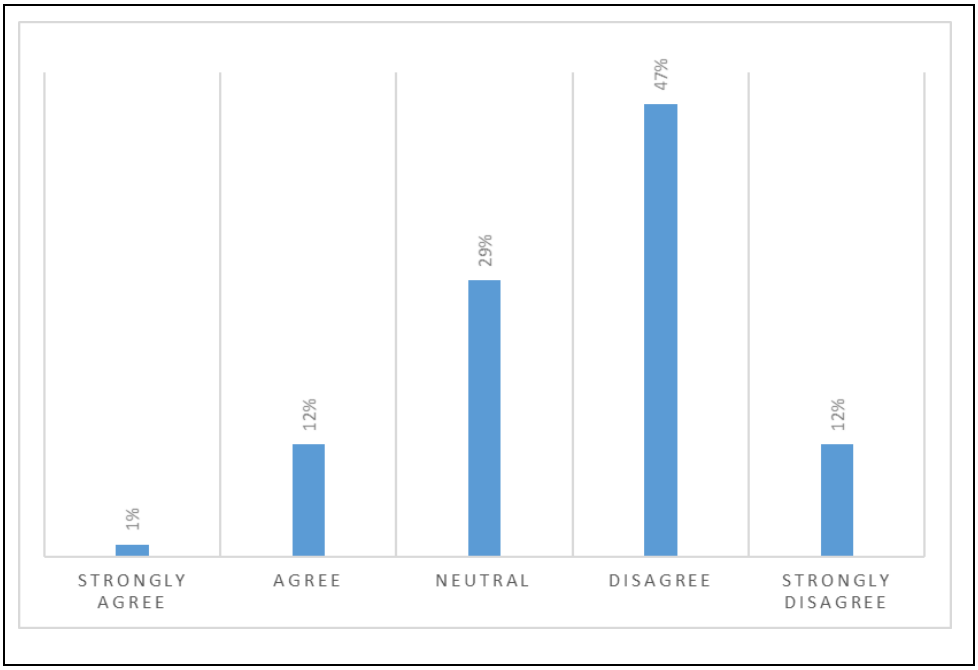


Figure 20. Do Organizations Fully Understand and are Compliant with ISO Standards Associated with Enterprise Risk Management, Business Continuity Management Systems, and ICT DR Resiliency; or use Comparable Standards

The challenge identified by participants was the overarching need to raise awareness of what standards are available, what value they bring, and how they can be applied. This is set within the context of a diverse sector which requires significant flexibility as standards are being applied by macro-level organizations with tens of thousands of employees working in dozens of countries, down to the micro-level NGO, with only a small number of employees operating within a specific geography.

The value of the ISO standard is its scalability, being applied from small and local to monolithic and global organizations. However, the current perception is that ISO standards have been developed for rich commercial companies who have significantly more funding and resources than the typical NGO.

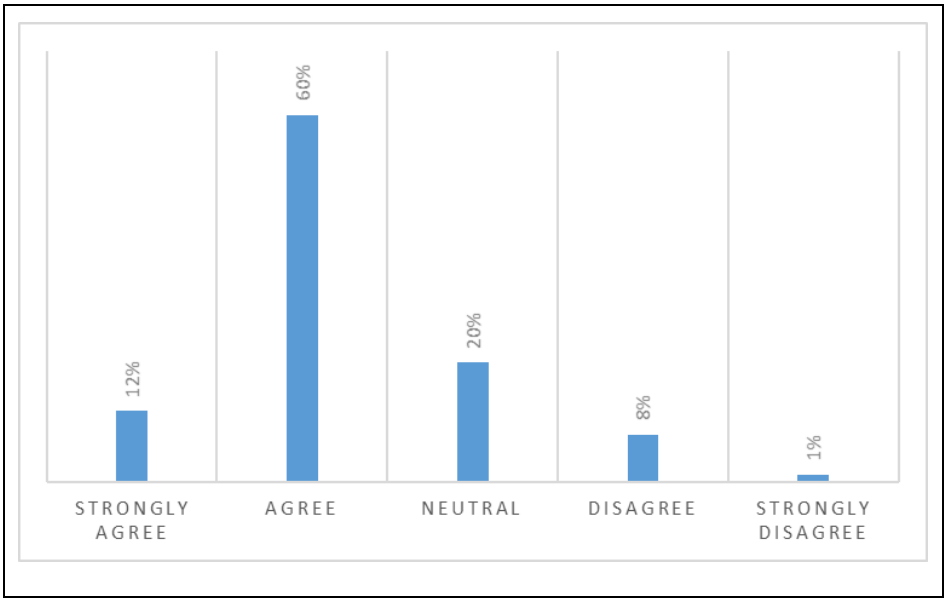


Figure 61. Do Organizations See Value in Seeking to be Aligned with, or Certified to, Recognized Standards

Concern was also raised over how rigidly ISO standards should be applied, with Caren, the Global Director of Security for a major development organization, stating that:

> "I think those ISO standards are so rigid that they don't have an application in the humanitarian sector, or in smaller organizations that don't have the overhead cost, availability, staffing and so forth to do all the documentation and all of the other requirements that ISO might have. ISO standards are great guidelines, and major corporations with significant resources often have the ability to build protocols that can meet or exceed those standards".

Adam also echoed the lack of awareness within the sector of ISO standards, reinforcing the belief that ISO standards were more aligned to the commercial sector than toward humanitarians:

> "I suspect they are not as aware of global standards or ISO-type standards as maybe some of the corporate sector is".

The need, then, is to raise awareness not only on what standards exist, but how they can be applied to meet the needs of a diverse sector. This also involves an understanding of the difference between "compliance" and "alignment". Compliance requires a costly and time-consuming audit for organizations to be officially certified to ISO standards; while alignment involves using ISO standards as a framework to build resilience systems which reflect ISO best practices, but do not involve a costly

audit and certification. Professionals with more familiarity with ISO standards recognized they could be applied in a scalable and highly tailorable fashion, and voiced confusion over why the sector had not sought out and leveraged these standards, with Betsy stating that:

> "I have no idea why we do not embrace and build systems off ISO standards".

All interviewees saw the value of developing consistency within the sector's security community. ISO standards can support professionals' careers as individuals enter the sector, are advanced within their organization, or as they move from one employer to another. It was also recognized that organizations needed to extract from any standard the elements which meet their specific needs, using ISO standards as a framework and resource for establishing personalized resilience standards, with Anna positing that:

> "I think it is the way that organizations should go (ISO standards). It sets a standard that's accepted across the board for organizations that they can all meet, so again, standardizing it so that people move from one organization to the next and it is always going to be the same. It is something that a lot of organizations should do, because especially in our sector there is a lot of movement".

Interviewees also recognized that standards establish accountability, which would accelerate the sector's need to formalize a universally agreed approach to resilience. The importance of the standards' origin appeared unimportant to those interviewed, with Bill offering that:

> "Increasingly organizations are being held to a more universal standard of risk management, which would come from the ISO standards, which is broadly applicable, regardless of whether it is corporate or humanitarian. Standards are critical".

Bill went on to say that the sector could no longer use perceived sector uniqueness as a reason to ignore externally designed standards, offering that:

> "I think in the humanitarian sector, there is a lesser understanding of the ISO standard, because for some humanitarian practitioners, they believe themselves so sufficiently unique and different that anything that is perceived as mainstream security industry would be not relevant. That, I find, is shortsighted".

While ISO standards are flexible and could be easily adopted across a diverse community—in a scalable and flexible fashion—the cost of accessing the ISO standards was cited as a challenge, with Dustin positing that:

> "The problem with those standards is they're bloody expensive, and you can't get hold of them to look at them and go, is this something we are interested in or not? Trying to persuade an NGO to spend $90 or $110 on a standard just so you can have a look at it and see what it's like doesn't happen, unfortunately".

This interviewee's viewpoint raises the question of how important security risk management is to the sector—the perceived value and the willingness for organizations to invest—and at what size of funding does it make sense for an organization to invest several hundred, or even many thousands, of dollars to build a standards-based resilience system?

Member-based organizational standards

The growth of member-based organizations potentially offers the security community a platform to share information and ideas, while concurrently offering a source of credible certification programs. These organizations increasingly provide a library of published standards and practices which are operationalized through accompanying educational resources. Various associations exist, including the American Society for Industrial Security (ASIS), the Security Institute (SI), Skills for Security (S4S), the Institute for Leadership Management (ILM), and City and Guilds. Some, like ASIS, are largely focused on the United States market, while others, including the Security Institute, Skills for Security, the ILM, and City and Guilds (while global) have a heavier weighting in the United Kingdom and Europe.

With the United States representing the largest portion of the global security market, it would be reasonable to assume that it leads the way on international security standards. ASIS was formed in 1955 to principally support the United States security sector, but is increasingly seen as a global player in the area of standards and accreditation, with Chapters being formed in many countries. Acting as a not-for-profit organization, the ASIS remit is to disseminate information and educational materials to enhance security knowledge, practice and performance. ASIS provides standards on topics such as **Business Continuity and Crisis Management** (2005); **Information and Asset Protection** (2007); and **Physical Asset Protection Standard and Facilities Physical Security Measures** (2012), and also offers a range of management courses, such as the Associate Protection Professional (APP), the Certified Protection Professional (CPP), and the Physical Security Professional (PSP). Beyond standards and educational programs, ASIS also offers useful information through the Security Management Magazine, as well as conferences, special interest groups and workshops.

While ASIS is undoubtedly a well-established and highly credible organization, it has yet to identify the humanitarian aid and development sector as a distinct market. Rather, ASIS focuses on more traditional security areas. The ASIS **Security Industry Career Pathway Guide: Practitioners and Suppliers** (2018) outlines the hierarchy of security and competency framework requirements for the commercial security professional, addressing the concepts of job responsibilities, education and credentials, and specialized knowledge and competencies. However, unlike the commercial sector, the humanitarian space has a higher proportion of "practitioners" than "professionals" which the guide fails to address. The majority of interviewees were not aware of ASIS as a useful mechanism for either developing standards, accessing educational resources, or sharing ideas and experiences. Of the survey pool, only 8% of humanitarian survey participants leveraged ASIS for professional standards, compared to 17% of their commercial and government peers, with Debbie positing that:

> "I think also you have these ASIS CPP, which I feel has its place. This is just another up-and-coming standard, but I think it is of value".

Organizations such as the Security Institute represents the largest body of United Kingdom security professionals, offering a platform for professionals to collaborate, as well as mechanisms for professional development. However, unlike ASIS, the Security Institute was more recently formed (2000) and does not provide published standards and guidelines. As such, its value to the sector in developing standards is limited, lacking formal tools which professionals can readily leverage. The Institute of Leadership Management is a certifying educational body for leaders and managers around the world. While not exclusively a security platform, it addresses security risk management and organizational resilience within some of its educational resources. Despite the ILM not being focused on security, 16% of humanitarian participants indicated that they had leveraged the educational programs the body provides on security and resilience. Skills for Security is a focused awards body and provides both professionals and practitioners, at all levels, a recognized educational resource specifically for security. Of the survey pool, 14% of humanitarians and 18% of commercial and government professionals had leveraged this awarding body.

The need for member body organizations to define standards for their own community is recognized within the sector, providing a benchmark against which practices are aligned, and a metric against which both professionals and organizations can measure performance effectiveness. Member body organizations have an advantage in that the members themselves develop the standard, rather than an external body which may lack a critical awareness of sectoral nuances. As such, if standards are to be

developed by an existing membership body, then organic expertise should be augmented by sector-specific contributions to ensure that any nuances are incorporated.

The importance of documented systems

This section looks at the steps required to establish standards, including consolidating knowledge, skill and experience into documents. Without the establishment of documented best practices, significant levels of subjectivity exist both across the sector, as well as down to the organizational and ultimately the individual level. This creates an uneven resilience landscape where personality, ego, education, resourcing, and environmental influences can easily warp and undermine the security profession's ability to replicate effective risk control measures. The absence of standards also hampers both the professional's ability to articulate and validate what must be done and why, making justifying appropriate levels of professionalism problematic. For executive leaders who know they need security but who lack the technical knowledge to identify good professionals from bad, there is no benchmark against which informed decisions can be made. Hilda, the Global Security Director for a large humanitarian organization, noted the connection between standards and document systems, stating that:

> "I do think that having some sort of standard you could point to and say that this is the foundation of your own policies and procedures would be extremely useful".

The lack of specific-to-sector standards does not diminish the need for the humanitarian aid and development community to have its own unique constructs of resilience, regardless of whether the community leverages existing standards designed originally for the commercial sector. These constructs must also reflect the vertical nature of security, from the tactical to strategic. They must also meet the horizontal needs, crossing the range of different geographies, cultures and activities. While some components of a business continuity management system may be singular in that they address an overarching need or a defined aspect of risk, others are repetitive, as risks are addressed across current and future activities or locations. Resultingly, organizations need to establish a document system which addresses strategic, operational, and tactical level requirements at the headquarters and field levels, but which also recognize that components will act as templates which are only finalized as they are applied to a specific activity or geography. Given the complexity of addressing sector resilience there is a requirement to design document systems which work collaboratively to address the phases of prepare and prevent, respond and manage, and transition and recover; and to do this vertically and horizontally.

Figure 22 is drawn from a pool of 77 survey participants who responded to: ***"Do organizations have an overarching document bringing together all organizational risk and resiliency needs"***. Of the participant group, only 33% felt that some form of cohesive document existed to link all resilience-related documents together. This suggests that organizational resilience is often fractured and operates in silos, rather than being addressed as an organizational strategy. Betsy indicated that the importance of documenting resilience strategies was a relatively new concept for many, and that most organizations were still only now starting to see the value of document systems:

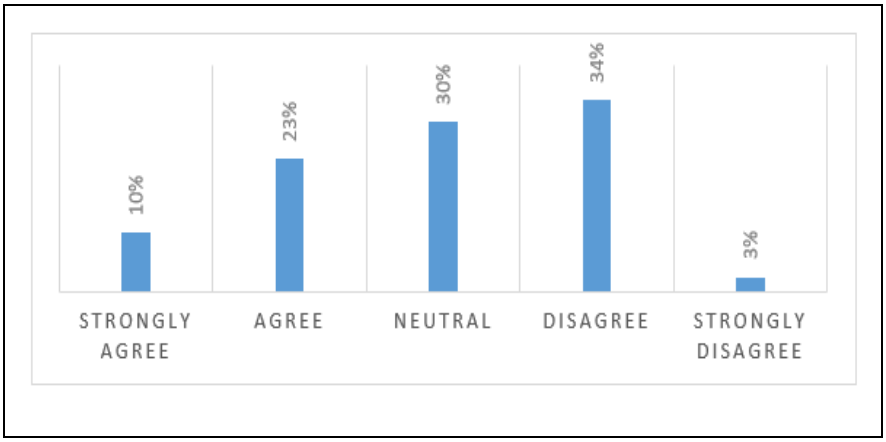


Figure 7. Do Organizations have an Overarching Document Bringing Together all Organizational Risk and Resiliency Needs

> "The first organization I joined had nothing, no policy, no practice - nothing. So you work from the ground up, but as I said, now I think it's more nuanced, and the soft skills are equally as important as the hard skills".

Camila supported this sentiment, stressing that security professionals see documented standards and practices as a priority in order to establish a consistent framework of best practice, but that organizational resistance often exists:

> "I was really pushing for priorities, the first place that I and other people in my position probably push is just to get the policies and procedures in place. Develop this, really have the buy in and get everyone on the same page. And then from that, the next push is always to try to get the training for senior management, so that it's not just a static document. We are going through it on a regular basis, and everyone understands their roles, and in particular the executives have that capacity and have had that training to know what to do".

Despite either overt resistance or lack of organizational appetite to embrace documented resilience strategies, the majority of professionals indicated that their organizations recognized that documented standards enable better knowledge-led decision making.

Figure 23 is drawn from a pool of 77 survey participants who responded to the statement: "***Do documents effectively address the need to establish context for knowledge-led decision-making"***. Fifty-two percent of participants felt that existing documents effectively provided context to enable knowledge decision-making, with only 25% feeling that documented standards brought little to no value.

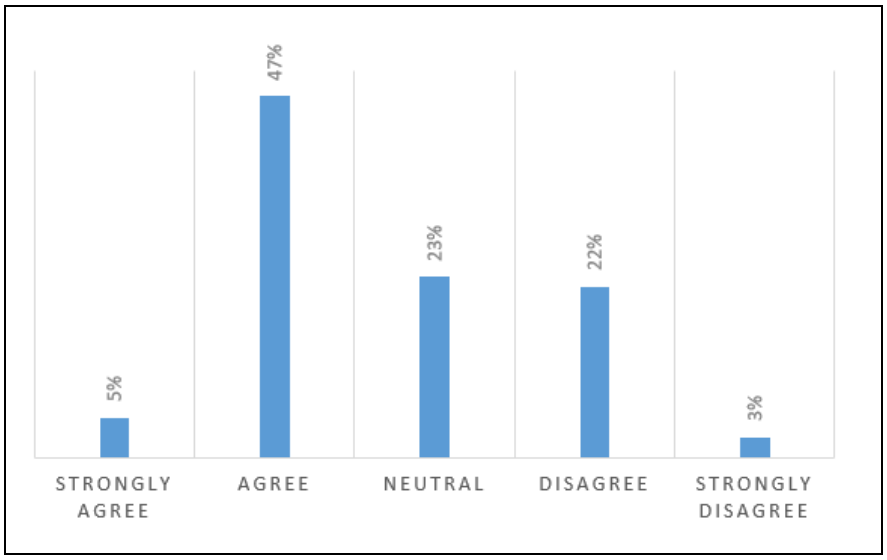


Figure 23. Do Documents Effectively Address the need to Establish Context for Knowledge-led Decision-making

To be effective in building or operating an integrated resilience strategy, the security profession needs to be able to differentiate—and then articulate this to others—between the field of security risk management and the more holistic remit of organizational resilience. Professionals must expand beyond the more obvious security topics such as kidnap and ransom, riots, assaults, murder, explosive attacks, and active shooter incidents, and include resilience requirements such as media management and crisis communications, family liaison, stakeholder management, political risks, fraud and corruption, investigations management, natural disasters and health and safety crises. Anna reflected on this layering of document systems, positing that:

> "I think at the HQ level, it is much more systematic so they have written procedures, but those don't necessarily trickle down to the field".

Document systems not only capture best practice in order to control risks or respond to a crisis, they also form the framework for the hierarchy of security professionals and practitioners. **Figure 24** is drawn from a pool of 77 survey participants who responded to: ***"Are organizational management structures and roles and responsibilities clearly defined in documents"***. Of the survey group, 69% of participants indicated that roles and responsibilities relating to security, risk, resilience or crisis management are clearly defined within document systems, enabling security risk management to be codified and articulated formally across the organization.

This is important, as it validates the role, placement and importance of the security professional. This also holds both the professional and other managers accountable to resilience requirements. With both the security professional and practitioner seeking to address the increasingly complex and impactful security challenges the sector is facing, the formalization of their role is critical for their success. Denise emphasized the importance of recognizing the role of security, stating that security professionals and practitioners led on security risk management within high to extreme-risk environments:

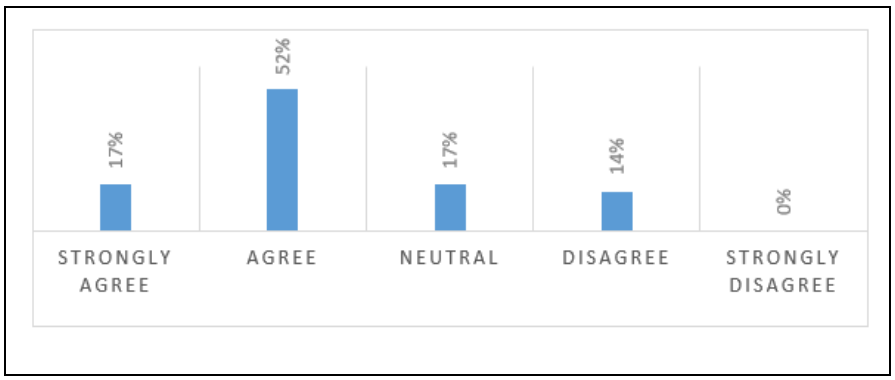


Figure 24. Are Organizational Management Structures and Roles and Responsibilities Clearly Defined in Documents

> "People are operating in pretty tough places. Their programs have very specific deliverables, and sometimes it means you have to work in places where there is tons of political and social unrest. There's crime, there's conflict".

Despite the obvious need for effective resilience measures to be developed, many organizational leaders remain indifferent to funding or supporting the establishment of best practices within document systems. This not only hampers the development and implementation of standards and best practice, it also places organizations at liability and reputational risk, with Anna positing that:

> "It is not systematic. It is not written down. It is not codified, which down the line can have issues because if there's nothing to prove that they did it. There are policies or procedures in place, that's where they'll lose out, if there was any form of litigation".

The counterargument to codifying standards and best practice is the complexity of the risks faced, and the diversity of the environments in which organizations operate, with Dustin stating that:

> "One of my concerns is often when security risk management becomes too procedural, and it becomes a checklist exercise rather than one that's useful. And people are actually empowered to make decisions, with security part of the decision-making process. Some places, they (managers) abdicate responsible to the security person. Some people see it as security is too procedural, it inhibits the country manager from making decisions".

The balance, then, lies in defining the difference between a policy, plan, guide, procedure or template, and the extent to which professionals can act independently of standards and decision-making approval processes.

The security profession recognizes the importance of not only developing standards to form best practices, but also in using document systems as a "binding agent" which enables leaders not only to understand their own remit within the field of resilience, but as importantly to understand the role of their peer risk practitioners (HR, Legal, Finance, Business, IT etc.). It also defines how, as a collective, they must work together.

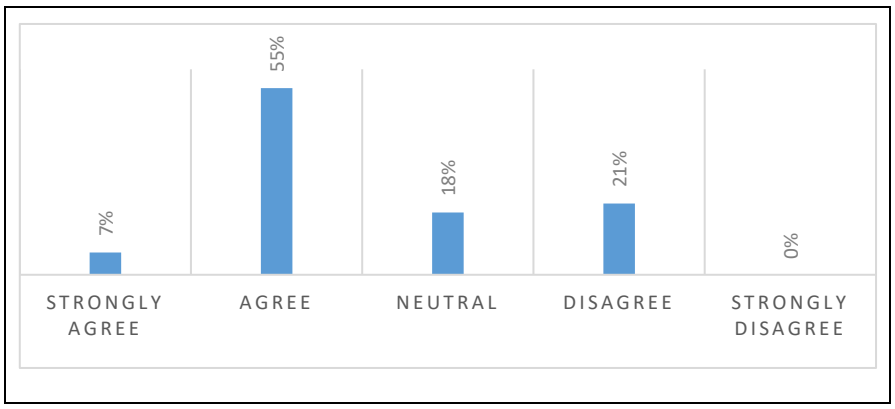


Figure 25. Do Organizational Documents Typically Bring Together Stakeholder Needs, Functions and Activities

Figure 25 is drawn from a pool of 77 survey participants responding to: "***Do organizational documents typically bring together stakeholder needs, functions and activities***". Of the participants, 62% of recognized the value of document systems in linking risk owners together to ensure a more holistic approach to organizational resilience. This is important as the effects of transitory leaders and security professionals must be countered through a bridging mechanism in order to minimize the disruptive influence of personalities, behaviors,

promotions, terminations, and transitions. Document systems then become the approved road map which defines how risk is managed, how disruptive incidents are controlled, and which ultimately define the expectations of the organization.

CHAPTER 7

OPERATIONALIZING KNOWLEDGE AND SKILLS

Introduction

This chapter examines the importance of codifying knowledge and skills through the production and application of knowledge. Training is where the "rubber meets the road" for organizational resilience, with effective decision-making involving the application of technical knowledge against the backcloth of experience, and then applied to the unique conditions of a particular situation. Training enables effective favorable disorder (Normandin and Therrien, 2016), allowing flexibility of action within new or complex risk conditions. While standards and practices define resilience objectives, education operationalizes them. The production of knowledge then forms the cornerstone of organizational resilience and how it is applied. Wenger (2017) observed that people are social beings, and this is true of the security community in terms of how standards are developed, and how knowledge is applied. Ethnography also plays a role as subset cultures exist within the sector, presenting different belief systems which influence how knowledge is both formed and delivered.

Standards drive the security community's competency framework, setting out the technical needs and performance goals of the sector. Camburn (2011, p.1) states that: "Within any recognized profession there exists a core set of values, knowledge and skills that bring coherence and connection to the professional workforce". The production of knowledge, based on recognized standards which are transferred through document systems, allow individuals to enter the security community, and then importantly to continue to progress within it. At the individual level, where people are responsible for controlling their own security risks, the process of knowledge retention and transfer is equally important. This chapter explores the various learner groups, including: 1) the executive leadership team responsible for resilience and crisis management, 2) the security professional and practitioner as the nexus of physical risk management, 3) other risk owners who play a role in resilience and crisis management, and 4) the individual who must address personal risks and localized emergency response requirements.

The professionalization of the individual—and at the higher level the security community—may be transformative, incremental or opportunistic, with accelerators for development being drawn from vocational or academic resources. Learning never stops, forming a continuum of learning (Eraut, 1994)

as individuals continue to grow vertically in terms of seniority and influence, as well as laterally in terms of technical skill and geographic experience. Those performing a security role must also by nature be reflective, so as to effectively apply knowledge in the context of dynamic and evolving security risks (Schon, 1983). While many studies have been conducted on professionalization and the development of competency frameworks, little research exists to address the learning needs of the humanitarian security community. Gosling, Marturano, and Dennison (2003) explore the importance of consolidating information in order to provide organizational direction, offering a framework to establish clearly defined performance objectives. This and other studies, whether specifically focused on the humanitarian security profession, drawn from the commercial security sector, or not focused on security but with tangential relevance, can be leveraged by the sector to establish professional standards, and then train against these in a focused and credible manner.

The mechanisms for learning

Adults learn through three domains: 1) the *cognitive,* which include lectures, brainstorms, and discussions; 2) the *affective,* which addresses value clarification exercises, nominal group processes and consensus-seeking activities (emotion); and 3) the *behavioral,* which includes roleplays, simulations, and teach-backs (NHI, 2020). The delivery of knowledge is then imparted through visual, auditory, and kinesthetic means. The importance of tacit versus codified knowledge is also important, as seasoned professionals instinctively make decisions based on a career's worth of experience, without necessarily having to consciously analyze the "why" of how they reached a decision. Conversely, practitioners are arguably more reliant on learned knowledge, requiring a conscious act to reach a same solution.

Initial studies by Ebbinghaus in 1880 on memory retention coined the "Forgetting Curve" have been replicated by Murre and Dros in their study **Replication and Analysis of Ebbinghaus Forgetting Curve** (2014). These studies indicate that certain styles of learning have associated retention patterns, with studies ranging from 3 days to 120 days. While research has produced uneven results, all uniformly agree that people forget, and that significant memory fade occurs over a period of 100+ days. Resultingly, unless knowledge is consistently applied through action and in a manner that resonates through perceived or proven value to the learner, then it is unlikely to be retained. Consequently, critical knowledge is quickly lost. **Figure 26** shows the NTL Institutes **Applied Behavioral Science Learning Pyramid**. This form of metric is also discussed by Chi, Bassock, Lewis, Reimann and Glaser (1989,

p.13) where they state that retention rates are typically: reading 10%; seeing 20%; hearing 30%; seeing and hearing 50%; collaboration 70%, and through doing 80%.

Charlie also reflected on the importance of immersive learning—the *see*, *hear* and *do* approach—for the leadership team, noting that high-stress simulations illustrated critical knowledge gaps within time-sensitive decision making:

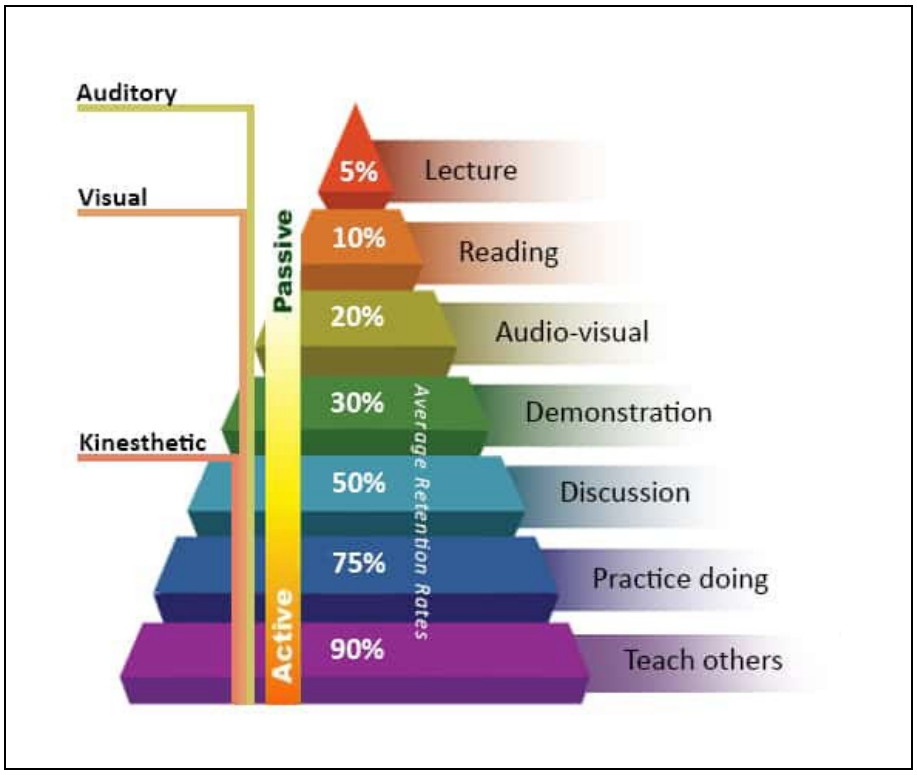


Figure 26. NTL Institute - Applied Behavioral Science Learning Pyramid

> "Every time I do the training with our executive team, they are absolutely overwhelmed by the size of what's got to be considered, and the difficulty around making decisions".

Narli's (2010) study of constructivist learning underpins the value of "active learning"—the process through which learners carry out learning on their own, and where they are required to proactively think about their learning experience and what it means. Immersive and often highly interactive learning, through Hostile Environment Awareness Training (HEAT) at the individual level, or through emergency or crisis management exercising at the leadership level, provides the environment where learners are required to apply knowledge and skills on their own, or within a group. It offers the framework where the individual must actively think about how their knowledge addresses real-world threats. The traditional teaching approach, where leaners are passive information receivers, creates an environment where learning is not optimally received and retained, and where the opportunity to apply knowledge to a real problem is either limited or absent. Narli (2010, p.37) goes on to say that: "some educational psychologists say that students from different parts of the world learn better when they gain experience together and tackle problems which require authenticity and simulation". This is supported by Craik and Lockhart's (1972) concept on the level of processing which states that familiar and meaningful stimuli is better retained than less meaningful stimuli. This process not only accelerates knowledge growth, but

at the same time amplifies its relevance to the participant. It also significantly reduces knowledge and skill fade. The value of instruction—and the return of investment to the employer—is therefore extended past the typical point where refresher training is required. Authentic and simulation-based knowledge is also more likely to be applied effectively and in context when the individual is faced with danger, and where fear of making the wrong decision may undermine timely action, increasing the potential for harm. Camila supported the view that individuals working together to resolve realistic problems within a HEAT course was beneficial in developing competency at the personal level, stating that:

> "From a duty of care, wanting the staff to be fully prepared, I think they should receive some sort of in-person and immersive training".

Erik, supported the need for the see, hear and do approach, but indicated that the level of investment and the degree of professional delivery was inconsistent across the sector, stating that:

> "Some organizations are extremely sophisticated and put a lot of time and effort into HEAT. I see others that either because they're naive or they don't feel like they have the resources have actually put very little effort into it".

The Competency Framework Focus Group explored the risk of knowledge and skill fade, including for leaders and individuals. Specifically, the requirement for HEAT refresher training was explored, noting that for those organizations with sufficient organizational mass and funds to run their own training the requirement to continue the learning journey was clearly evident, with refresher training occurring between 3-5 years—as shown in **Table 6**. The focus group noted that funding and logistics created challenges not only for running the initial training, but also in conducting refresher training. As

Organization	Certification Validity
Care International	5 years
United Nations	Open
World Bank Group	3 years
Danish Refugee Council	3 years
Norwegian Refugee Council	3 years
International Monetary Fund	3 years
World Vision	5 years

Table 6. HEAT Refresher Training Cycle: Primary Research Findings

a result, organizations such as the World Bank Group and the International Monetary Fund are now looking at videogame solutions to meet refresher training needs.

The FCO, DFID, USAID, the State Department, DTRA and other government agencies also provide deployed diplomatic and military staff with HEAT course variants, also known as Survival Evasion Resistance and Escape (SERE) training, both online and in-person. However, the training either reflects the warfighting role of the military or the significant resources commonly provided to embassy staff, rather than reflecting the unarmed and resource constrained reality of the humanitarian aid and development community. The ability to gain and retain knowledge, and then to effectively transfer or apply knowledge is different (Semb and Ellis, 1994), and effective learning requires not only the ability to gain and retain knowledge, but also to apply this against the context of different, and often high-stress, situations.

The need for training and exercising

With a recognized need for humanitarians to operate within challenging and remote environments with increased criminal, terrorist and hostile government targeting, the need for awareness and competency at all levels is increasing. Exacerbating the complex range of risks the sector faces is the need to contend with anti-NGO legislation which further compounds security risks. Over the past 15 years, 11 African countries have adopted legislation which constrains NGOs to a narrow democratic space to prevent challenges to oppressive regimes (Musila, 2020). As such, training must address all forms of risk, whether this is the obvious physical threat from a criminal or terrorist, in dealing with a serious disease outbreak or a natural disaster, or in attending to the more nebulous challenges which are associated with political risk or reputational harm. Risks then become interwoven, and the associated training solution must meet all forms of harm that the individual or their organization might face.

Figure 27 reflects the findings from a survey pool of 77 seasoned professionals when asked to respond to the statement: "***Do organizations place great importance in raising the knowledge and skill of executive leadership on resiliency and continuity management"***. Of the pool, only 45% felt that importance was placed in raising the capacity for executive leaders to understand and effectively address resilience. The absence of top-level support directly impacts the prioritization of resilience within both the organization, and more widely the sector, in defining the level of capacity-building investment. Without executive commitment, business development teams will remove training costs in

order to win bids as security is invariably the first item on a proposal team's chopping block to financially win a business opportunity.

Stephen noted that budgets were a key factor in how training was resourced, stating that where the security community could not articulate the need effectively then budgets were unnecessarily tight:

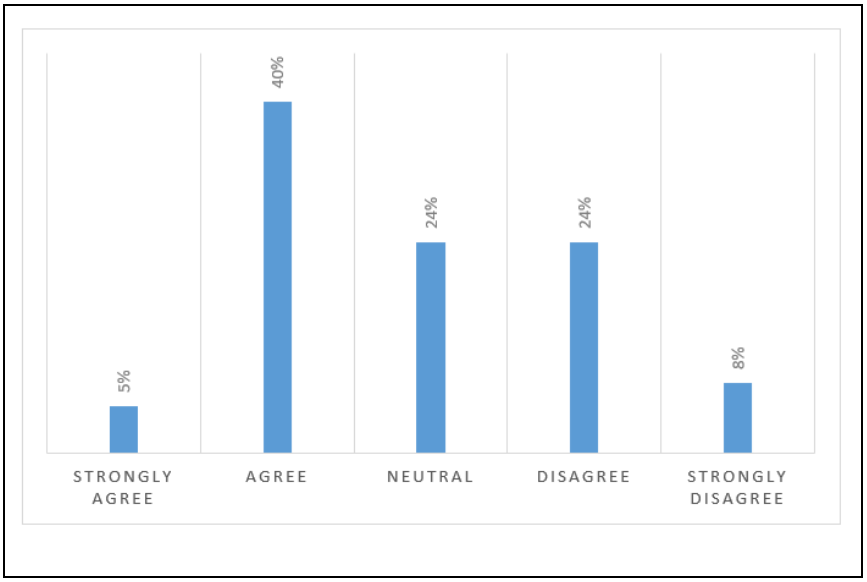


Figure 27. Do Organizations Place Great Importance in Raising the Knowledge and Skill of Executive Leadership on Resilience and Continuity Management

> "They (the security community) lack the ability to make sure that the funding is available for training for some reason. I think the money is actually there from the donors, so something's not working".

Amber highlighted the need for leadership training in order to remove ambiguity over accountability requirements, as well as a mechanism for enhancing organizational effectiveness, stating that:

> "Number one would be leadership training, training specific to what they are tasked to do. So everybody that works for us has a different role in some sense".

Interviews also recognized this need to raise awareness and competency at all levels, coupled with the need to address the limitations of field security practitioners who are most commonly at the point of crisis, and who are typically disadvantaged in that they lack foundational security knowledge and experience, with Andy offering:

> "I think there is a gap. From experience looking at our people in the field they don't have that training, they don't have the knowledge. So if we could develop something that could train them and make sure that they are understanding that role they we are going to strengthen the core resilience, because they are at the front line".

This need to address resilience at the lowest level where those leading security are most typically practitioners, rather than professionals, is the foundation for the success or failure of preventing or reducing risk at the point of occurrence. However, while grass roots capacity often aggravates the cause for most crises, it can be argued that a capacity gap within those who define or shape resilience standards is arguably the cause for resilience not working in the first place. Capacity at all levels was cited as a problem by interviewees, with Charlie offering that:

> "There is a lack in the foundation of learning. So if you consider that security risk is a part of the enterprise risk management, I don't feel that everyone has a full understanding of the enterprise risk and the linkages between the different risk components within an organization".

Figure 28 represents 77 seasoned security professional's opinion when asked to respond to: "***Do organizations place great importance on building the knowledge, skill and confidence of the broader staff population in risk management at a personal level"***. Of the survey participants, only 43% felt that organizations saw value in addressing individual safety and security risks through training. This result is complicated as the humanitarian population is broadly split between three main groups: 1) headquarters staff, who are typically office-bound, 2) international traveler or long-term international embedded staff, and 3) host nation staff who reside and work in their home country. The last category of staff represents the largest portion of the humanitarian community, and those who typically face the most persistent levels of personal risk—and yet receive the least amount of training. What drives the focus on developing knowledge and skill principally within international staff are the litigation and reputational risks occurring where an individual travelling or working internationally is harmed through a security incident.

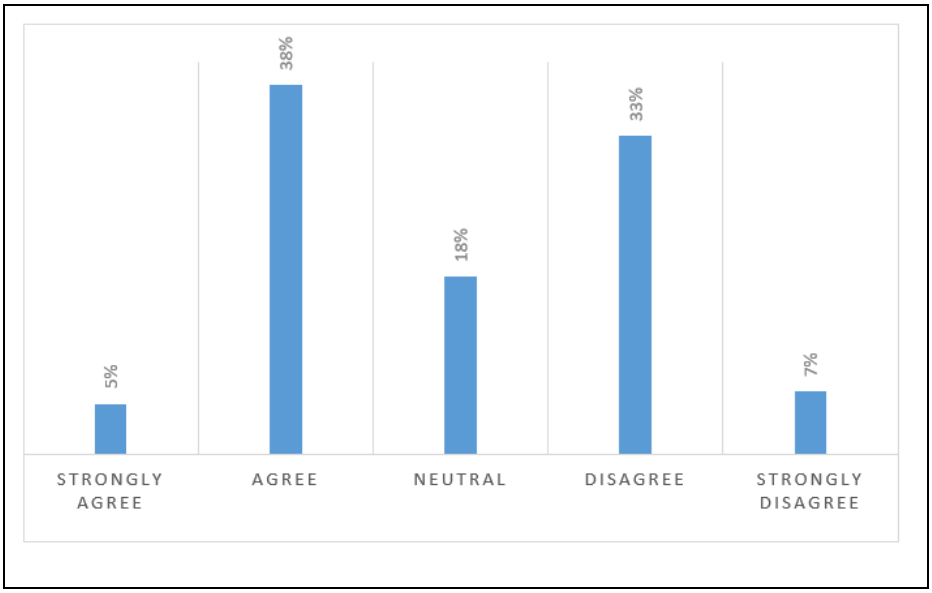


Figure 8. Do Organizations Place Great Importance on Building the Knowledge, Skill and Confidence of the Broader Staff Population in Risk Management at a Personal Level

Over the past decade, the importance of HEAT has grown in prominence as international staff increasingly demand immersive training before deploying to high-risk, remote and unfamiliar environments. Host nation staff are similarly demanding some form of HEAT as they recognize they face prolonged exposure to many of the same risks. Currently only the largest NGOs run in-house courses (i.e., Care International, World Vision, the Danish Refugee Council, and the Norwegian Refugee Council). The World Bank Group and the International Monetary Fund also run comparable SSAFE programs. The majority of organizations, however, leverage commercial providers to meet their HEAT needs, as the cost effectiveness of internalizing authentic and simulation-based training can be both cost and resource prohibitive. This again raises the need for humanitarians to leverage existing—and appropriate—commercial resources in order to build and deliver immersive awareness building programs, with the growing need to invest into immersive training being reinforced by Andy who stated that:

> "I think situational awareness is a big word at the moment, that and duty of care. Situational awareness goes into training so developing trainings like online trainings and going into the physical training side is now being implemented across the board. You have to do some sort of awareness training. At a medium risk, you'll have to do a more advanced training. When you go into the hostile and high-risk areas, you're having to do a physical Hostile Environment Awareness Training".

The availability of recognized training

Where organizations see value in training and are willing to commit time, funds and resources (or are willing to approach their donors for funding), the next challenge is identifying which resources best support organizational requirements. The interview pool offered mixed responses regarding whether sector-specific training was needed, or whether commercial training met capacity-building needs. Adam indicated that, while appropriate training was widely available, not much had been developed to meet the explicit needs of the sector:

> "There are courses out there, absolutely. There aren't so many tailored to humanitarian security, but my experience is that humanitarian security isn't completely unique, either, so I think people in the sector are learning from other courses that are available".

Figure 29 reflects the opinion of 77 seasoned security professionals who responded to the statement: ***"Do organizations see value in key representatives for risk and business continuity management having qualifications or certifications in associated and recognized educational programs"***. Of the participants, 67% stated that their organizations felt that the security community should have recognized vocational or academic educational credentials, while only 12% were actively dismissive or opposed to the value of recognized learning.

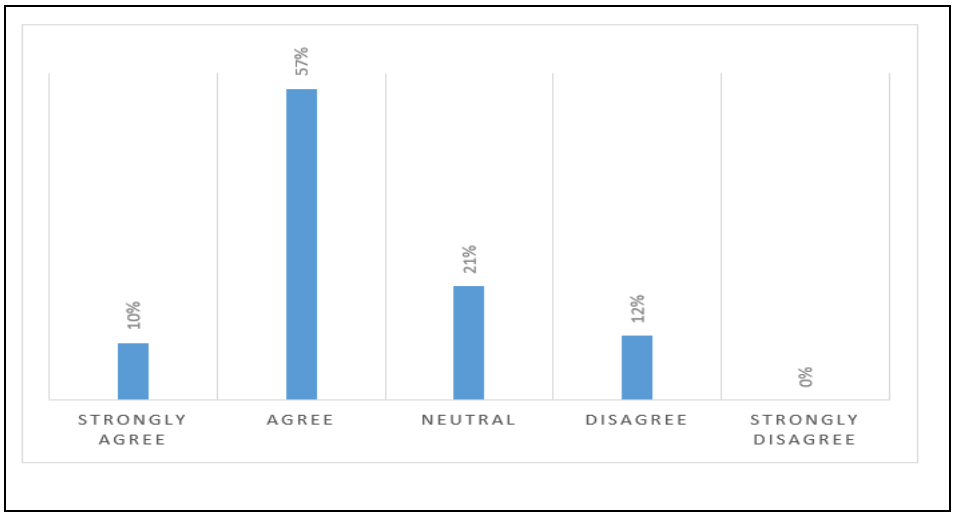


Figure 29. Do Organizations see Value in Key Representatives for Risk and Business Continuity Management having Qualifications or Certifications in Associated and Recognized Educational Programs

This offers fertile ground for the security community to grow organizational investment into standards-based learning. The primary research findings show a disparity between a willingness to invest in the security community, compared to an interest in upskilling executive leadership in the field of resilience. While any investment is useful, organizations will only truly understand—and therefore embrace—the importance of resilience if executive leaders have an appropriate level of awareness themselves of its value, prioritization, and application.

Hilda voiced the need for some form of recognition within training programs to lend credibility to the knowledge gained, and what this represented to both the individual and their organization:

> "I do think certification are useful it really allows you to feel that there's a common understanding of what it is that you were trained on. Certification gives it more specificity".

The increasing willingness of humanitarians to step away from sector-focused training and draw on more established disciplines significantly expands the resources the community can potentially draw on. However, this requires a continued culture shift as the sector increasingly recognizes the value of—and makes use of—commercial educational resources. Where the value of out-of-sector resources is recognized, then associations and forums should assist the sector in aligning standards and the designing

a competency framework. Absent a universally-agreed-upon approach, it becomes difficult for the professional to align a security "need" to the appropriate resilience "solution". Similarly, absent any formally recognized standards against which resources can be efficiently measured, the sector will struggle to measure quality in a consistent and evidenced fashion. Consequently, professionals must sift through innumerable training resources which may be poorly designed or inappropriately presented. The instructor or content may be a poor cultural fit—or, at the extreme end of the spectrum, might go against the sector's ethos and operating practices. Conversely, if a competency framework and associated standards were formally aligned, then professionals can more easily navigate the breadth of available resources to quickly identify and engage appropriate knowledge production tools. Alex stressed the need to look outside of the sector for educational resources, indicating that non-sector resources could meet the need:

> "If people are looking for NGO-specific risk training or risk leadership or risk management for leaders, they're probably not going to find it as effectively as they could if they went somewhere like ILM or they went and found a big bank and their risk managers are going to go and do specific courses".

For this to be effective, sector associations and forums need to be impartial in their approach, removing personal bias or self-interest when defining or articulating competency requirements to their members. It is here that security professionals—aided by recognized bodies—must consolidate knowledge and help shape both sectoral standards and the associated training strategies. Historically, the disconnect between the commercial sector and the humanitarian space has undermined the ability to impartially evaluate commercial resources, with InterAction refusing to engage with commercial providers on behalf of their members. Conversely, GISF and INSSA have recognized their role as a training broker, impartially presenting training resources to the community. This supports the needs of the security profession, as interviewees felt that recognized training programs, whether commercially derived or designed in-sector, would be useful for their entry and development within the security community. In addition, most felt that some form of standards recognition would be useful, with Alice offering that:

> "Training should absolutely have regulation. It should be done in a university-style library where you can pick what you would see as useful. Or the company would pick what is useful as forward learning, something that you must complete within the first two years of probation".

The need for some level of formal recognition involves developing multiple learner groups concurrently, including: 1) executive leaders within resilience and crisis management, 2) the security community in all aspects of risk management, 3) programmatic leaders in leading or support security and emergency management, 4) specialist risk owners, and 5) raising the ability for individuals to assume self-help measures. At all levels, whether building leadership or individual competency, some form of recognition is useful, with Andy stating that:

> "So for Hostile Environment Awareness Training I don't see a standard in the sector. I don't see anybody who is saying, we are conforming to the Security Institute or ASIS".

Consequently, the sector needs to define what constitutes professional content and an appropriate delivery mechanism in order to determine how training credibly supports recognized resilience standards and practices.

Transformative verses incremental change

In order for the sector to meet multi-faceted and evolving risks, there is a need to adopt either "transformative" or "incremental" change. Transformation provides a focused accelerant to professionalizing the security community, while also rapidly enhancing resilience measures. The ability to accelerate the individual's learning journey offers an opportunity for individuals and organizations to expedite professional development goals, while concurrently addressing complex and varied organizational risks. David stressed the need to quickly grow organizational capacity to address security challenges, especially at the point of risk, stating that:

> "We really need to be able to grow our expertise at that level, at the security focal point level. The way that I think will provide the greatest impact in improving the security in our organization is to find in all of our programs someone interested and motivated to address security enough that they can at least create awareness of potential risks and challenges in all of our programs".

Figure 30 visualizes the participant observations on how those managing security responsibilities must bring certain capacities to meet the complex needs of their organization. Those managing security risks require commensurate levels of technical knowledge, skill, and experience from which they can select and apply appropriate risk controls. This must then be supplemented with time-sensitive or current knowledge that reflects unique "point-in-time" considerations against which a contextualized decision is made. Further, the professional must look past security risk management to encompass the

implications of the risks to business, legal and reputational harm, being able to concurrently look through the lens of their functional peers. The level at which the professional contributes to resilience measures is then defined by their seniority or specialization. Ideally, transformative change would occur as the security professional enters the sector—or, as the practitioner assumes the secondary role of security while already working within the sector. This transformation would accelerate the process of conversion, convergence, and emergence, supporting professional and behavioral change within a compressed timeframe.

Figure 30. Blyth Managing Risks Through an Integrated Approach: Primary Research Findings (2020)

Figure 31 represents observations from the interview group in terms of the four pillars which form an effective security practitioner or professional: 1) knowledge, 2) skills, 3) experience, and 4) attitude. This model has three learning opportunities—*knowledge*, *skill* and *experience*. However, formal learning does not necessarily address the fourth and equally important component, attitude.

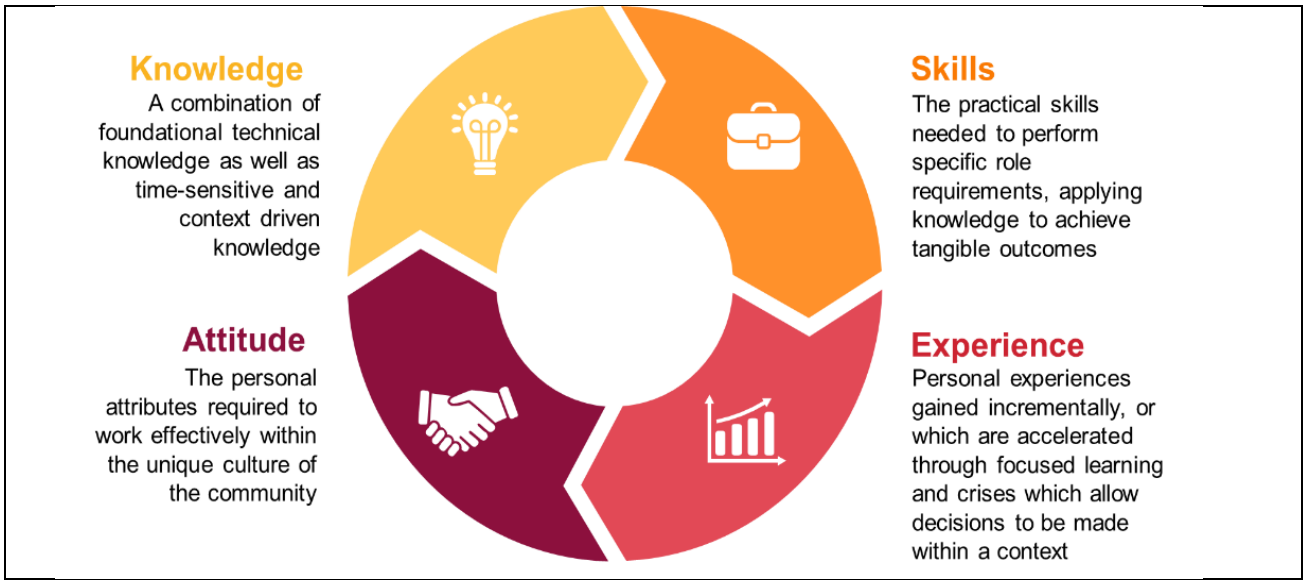


Figure 31. Blyth The Four Pillars of the Security Practitioner or Professional: Primary Research Findings (2019)

Incremental adjustment, while still beneficial, extends the process, exposes people and their organizations to a prolonged period of risk, and can require an unnecessary expenditure of cost and effort. Incremental adjustments are often exhausting, costly, risky, and can often fail to achieve an optimal or measurable outcome. This is especially challenging as incremental change requires a continued investment in the individual who, just at the point of becoming truly effective, may then leave the organization taking their value with them. Training and exercising can, to an extent, alter behavior; however, ultimately the recruitment process needs to weed out personality types who are not the right fit for the sector or an organization. Edith commented on this fourth softer area of competency, and the need for the right attitude to be effective within the security field:

> "The military and police person comes in with a certain attitude, certain behaviors and certain cultures, which can enhance an operation in some ways. But if they don't understand how the mission, mandate and values of an organization, it can disable, not enable, by the word 'no' where they should be saying, 'yes, but this is how we do it'".

The sparsity of transitionary and transdisciplinary learning resources to aid transformative change hinders the speed and effectiveness of professional development or behavioral change. Bill noted that, within the sector, little exists to support either a defined career path or the technical upskilling for security professionals:

> "As far as training is concerned for anyone transitioning into the humanitarian security sector there are actually very few courses available. As the safety and security profession as an industry has evolved there has been increased access to academia, various degrees or certifications, or some form of recognition. They have got the resources needed to support you".

The findings from the interview pool indicated that the high-level vocational resources which directly met sectoral needs were either limited or completely absent, but that tactical training—typically with a focus on individual security awareness—was more prevalent. The absence of high-level resources undermines career advancement for all risk portfolio decision-makers, and inhibits their ability to effectively assess and express organizational resilience needs. Brad offered that the ability for security management teams to map a learning journey and accompanying career path for their security management subordinates was a real challenge. This presents a significant limitation, as security professionals at every level struggle to advance their knowledge, and thereby fail to bring evidenced value to their employer. Concurrently, organizations also have limited options by which to address the growing level of sophistication associated with resilience, with Brad positing:

> "There is a massive gap. I manage several security professionals and every year when we do their performance appraisal you need to identify what can you do in order to develop them in their career. There are so few places you can send security professionals for development. If you look hard and long enough, you'll find it, but it's never really driven towards my sector of security professionals. It's very much focused on the civilian sector, not so much in the aid sector".

This challenge arguably has the greatest significance for the security practitioner who has little to no foundational knowledge upon which to build. It is unreasonable to appoint a manager absent any formal guiding standards or training, and then to expect a professional outcome. Within the field of security this also exposes people to a very real physical risk, while presenting significant vulnerabilities to the organization. Brandie noted that the most vulnerable point was in the field where most practitioners of security operate, but where the lowest level of competency resides:

> "The weakest aspect is the Security Focal Points because they have a set of procedures and responsibilities but it's integrating them into the organizational systems and how proactive they are really varies. This is because it is a secondary responsibility, and some of them are not interested, and some of them just are a bit lazy due to lack of interest".

Convergence recognizes that opportunities to gain knowledge and experience may be opportunity-driven or may be accessed through structured mechanisms for learning. The coming together of the security professional and practitioner learning journeys therefore may be incremental, or they may be accelerated through circumstance or a conscious act. To escape stagnation, both the security community and their employer must recognize the value of creating opportunities to develop focused knowledge, and to then test these newfound competencies through action. Where a crisis occurs then the individual will draw from three resources, and organizations are obliged to ensure that these are commensurate with the challenges faced:

1) Their reservoir of technical (tacit) knowledge within the area of security risk management.
2) Their experience in terms of the contextual application of knowledge against a problem.
3) Applying effective leadership based on managing same or similar challenges before.

Opportunity-driven growth is a dangerous "hit or miss" approach, where any competency gaps place people, the organization, and the donor at risk. A structured learning journey which is aligned to a defined career path and competency expectations enables both the security community and their employers to develop—and then measure—defined standards and performance outcomes. Erik noted that absent recognized training programs, professional development progress was slow, and major risks were not being properly addressed:

> "People are just clunking along with the same old skills, making pretty major mistakes in the new space that the organization may or may not even realize is happening".

Figure 32 visualizes how structured learning offers plannable opportunities for growth. *Incremental* growth is gained over a protracted period and results in a prolonged exposure to risk, whereas *opportunity*-driven growth is sporadic, uncertain and may never result in the required proficiency outcome. Neither incremental nor opportunity-driven learning necessarily offers recognizable or measurable value, and incremental or opportunity-driven growth can result in repetitive learning, offering diminishing value to the richness and relevancy of the individual's development.

Figure 9. Blyth Structured, Opportunity and Incremental Driven Learning (2018)

At the point of knowledge or experience saturation, the individual has effectively reached a level where there is no discernible opportunity for meaningful growth. The individual then has a choice to either stagnate in role, or to proactively seek out other mechanisms for transformative change. Both opportunity-driven or purposely structured opportunities both to learn, and critically to put knowledge into practice, provide a mechanism for the security professional to mature as well as demonstrate credibility. Conscious acts of developing capacity can be considered "formal accelerators", providing structured opportunities to develop planned, rapid, and transformative growth. At the opposite end of the spectrum, individuals may be forced to wait for a crisis to occur to access knowledge or experience development opportunities. These might be classified as "opportunity-driven accelerators". Or, where minor incidents and problems aggregate over time, then the individual may move slowly through "incremental accelerators" either by observing or doing, which often extends the learning journey considerably in short discrete bounds.

Formal Accelerators	
Advantages: A structured learning pathway will ultimately deliver all knowledge requirements. Simulations can then be used to expose the learner to likely threat scenarios, through engineered high-stress conditions. Unplanned events then offer an opportunity to apply knowledge against a real need. Further knowledge and its application will be supplemented through incremental learning.	*Disadvantages*: Structured learning pathways are typically expensive and can detract from the individual's ability to perform their role while attending training. While simulations are useful, they do not replace real-life experience and only partially prepare the individual for the stress of a real crisis event. The spectrum of technical needs is broad, so selectivity is required from the expansive portfolio of knowledge and skill areas.
Opportunity-Driven Accelerators	
Advantages: Real-life training is the greatest accelerant to learning. People learn and retain more from doing something which has immediate value. The lessons learned from a crisis which has direct meaning to the individual will resonate more deeply, and be remembered longer, than any simulation. Dealing with a real crisis offers the greatest credibility to the individual.	*Disadvantages*: Opportunity-driven growth is sporadic, unreliable and rarely fulfils the depth and breadth of competency requirements. Individuals are wholly reliant on bad things happening in order to learn, acting as the "expert" while simultaneously being a "student". Learning is limited while doing and is gained through reflection. This elevates risks to unreasonable levels, slows learning, and results in competency gaps.
Incremental Accelerators	
Advantages: Incremental growth provides a measured learning experience where knowledge may be reinforced through repetitive action. Knowledge can be gained through the observation of others, or through some level of mentoring, thereby reducing the risks associated with failure. The financial costs and disruptions associated with learner absence are low.	*Disadvantages*: Incremental growth is painfully slow and rarely moves the individual to the point of fully mastering all competency areas. Gaps in knowledge and experience expose organizations to prolonged risk until gaps are closed. Some areas of competency may be addressed repetitively, reducing the value of learning as knowledge of skill saturation occurs, and as existing knowledge is reinforced past the point of having value.

Table 7. The Advantages and Disadvantages of Structured, Opportunity Drive and Incremental Learning: Primary Research Findings

In some operating environments, opportunity-driven accelerators may be significant and frequent, while in others they may be limited or rare. Consequently, those operating in high-risk environments will invariably progress faster than those working in more benign settings. **Table 7** offers reflects the observations of the interview pool in the comparative advantages and disadvantages of each learning approach. David stated that individuals are ultimately responsible for finding mechanisms through which professional development could occur, regardless of the availability of educational resources or the support of their employer:

> "I definitely think that my transfer to this role is basically self-taught. I did not receive many resources in terms of where to start or what to do. I was selected for this role primarily because of my enthusiasm and my reliability for this sort of thing, and I have spent a lot of time and have been supported on certain self-study initiatives".

Where knowledge and experience is gained through "doing" then this requires organizations to be willing to allow the individual to experiment during a high-stress and high-impact crisis. While experience-based learning may be highly transformative, it also can add significant (potentially catastrophic) risk exposure to the organization. Past behaviour often defines future success, and so, absent a comparable crisis experience, individuals are at an immediate disadvantage. Retroactive learning also undermines learning by doing, especially under high-stress conditions, as the learner often lacks the specific information or resources during such events to enable learning. Rather, learning occurs as they reflect on the experience after the fact, for good or bad. The convergence model suggests that those coming from a military career typically bring crisis management experience with them, with the in-sector development of experience-based knowledge presenting a greater challenge for those who do not start out from a career with a security focus. Fay commented on the challenges of developing crisis experience where individuals come from a non-military primary career:

> "So the crisis-experienced military guys have an advantage over the guy who has academic qualifications. They already have the practical experience in managing a crisis. But for an academic person to go and get used to this thing, it's a bit tough".

Interviewees suggested that three legs of capacity exist for the security profession: 1) experience, through experiment, trial and test, 2) exposure, through observation or directed learning, and 3) reflection, in terms of how knowledge is applied to resolve problems. Learning pathways also determine

how leadership or management acumen is applied, and how this in turn influences the way knowledge is applied within different environments.

Academic and vocational competency within the security community

As resilience and the associated value of education becomes more widely accepted, organizations are increasingly recognizing the importance of credible professional development. **Figure 33** is taken from the survey of 77 seasoned security professionals who were asked to respond to this statement: "***Do organizations place great importance on designating, educating and supporting departmental representatives on risk and resiliency management"***. The results show that 40% felt that their organizations support the development of knowledge useful for those managing resilience needs, with 60% either having a neutral or negative opinion.

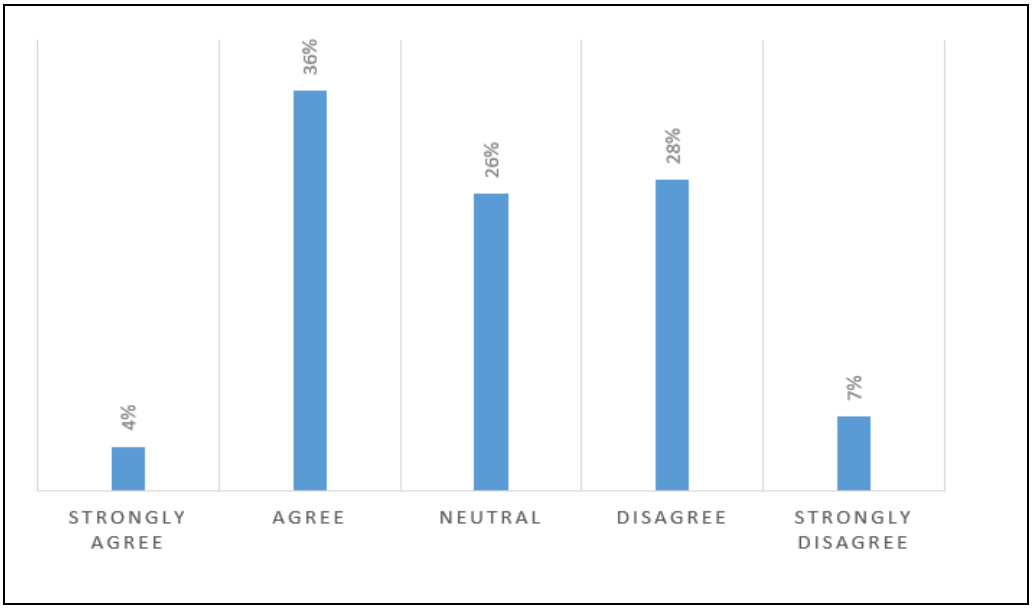


Figure 33. Do Organizations Place Great Importance on Designating, Educating and Supporting Departmental Representatives on Risk and Resiliency Management

For transformative change to occur, it is the responsibility of the organization not only to recognize the value of learning, but also to support—and critically demand—appropriate levels of competency. Given the importance of educational resources as both accelerators for professional development as well as metrics to gauge the value of knowledge, the ability to access vocational and/or academic resources forms an integral part in the process of professionalization.

Figure 34 is drawn from a pool of 77 survey participants and shows the importance of academic studies for seasoned security professionals. The results indicate a relatively high proportion of senior

security professionals had attained either a Master's degree (26%), an MBA (7%) or a Doctorate (3%). A similar percentage also held some form of higher vocational certification. This suggests that, increasingly, individuals are recognizing a gap within professional competency that can only be filled through academic learning, with vocational learning not being the priority. The disparity between bachelor's degrees within the survey pool and those holding a Master's degree is likely reflective of seasoned professionals seeking academic advancement later in their careers where their experience allows them to potentially bypass the lower degree.

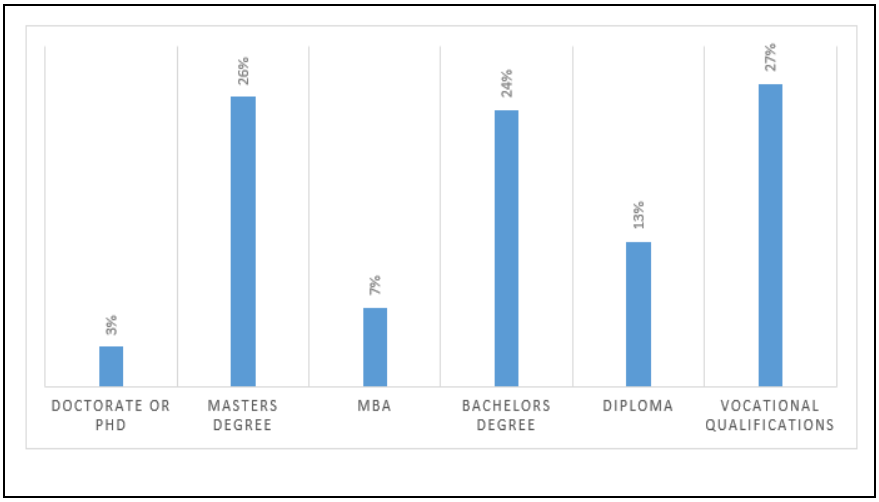


Figure 34. Survey Pool Academic Standing

ASIS, as the lead security institution in the United States, and increasingly a recognized global player for professional development, also conducted a study on the academic standing of commercial security professionals and industry suppliers. The study findings, presented in the ***Security Industry Career Pathway Guide: Practitioners and Suppliers*** (2018, p.28), noted that over 36% of security professionals held a Master's degree, compared to 26% of their peers within the humanitarian sector (**Figure 35**).

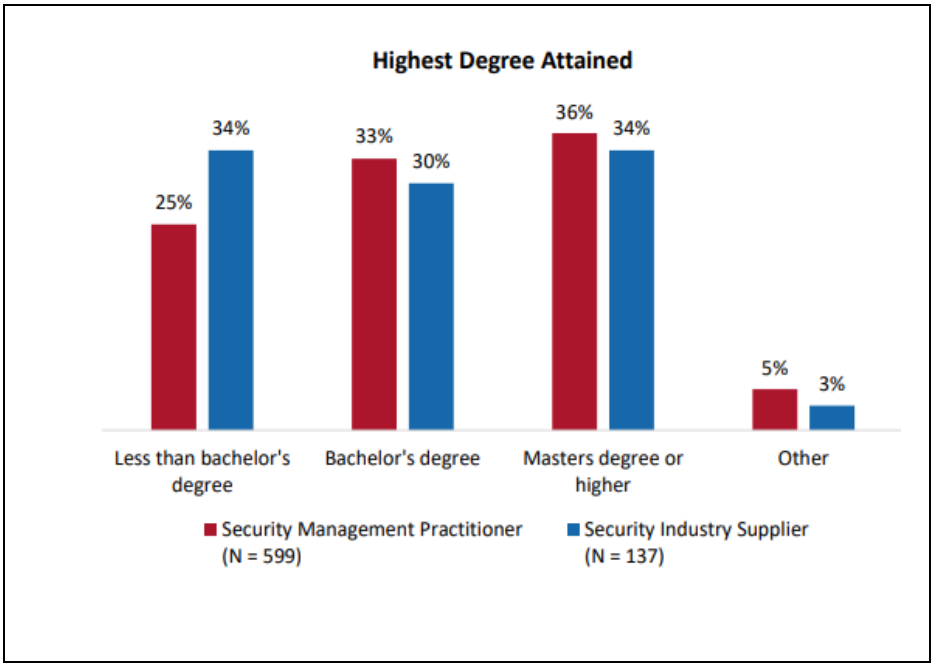


Figure 35. ASIS Security Professionals Academic Standing

This suggests that not only is there a propensity for security professionals to increasingly engage in academic studies across the security sector at large, but that the commercial sector is embracing professional development more than their humanitarian peers. It is suggested that higher pay, active promotion, and the support of professional development within for-profit companies are likely the motivators for commercial security professionals to actively seek out academic (and vocational) advancement. Erik highlighted the need to self-motivate in the absence of a structured and supported learning pathway, and the value of leveraging non-traditional training resources:

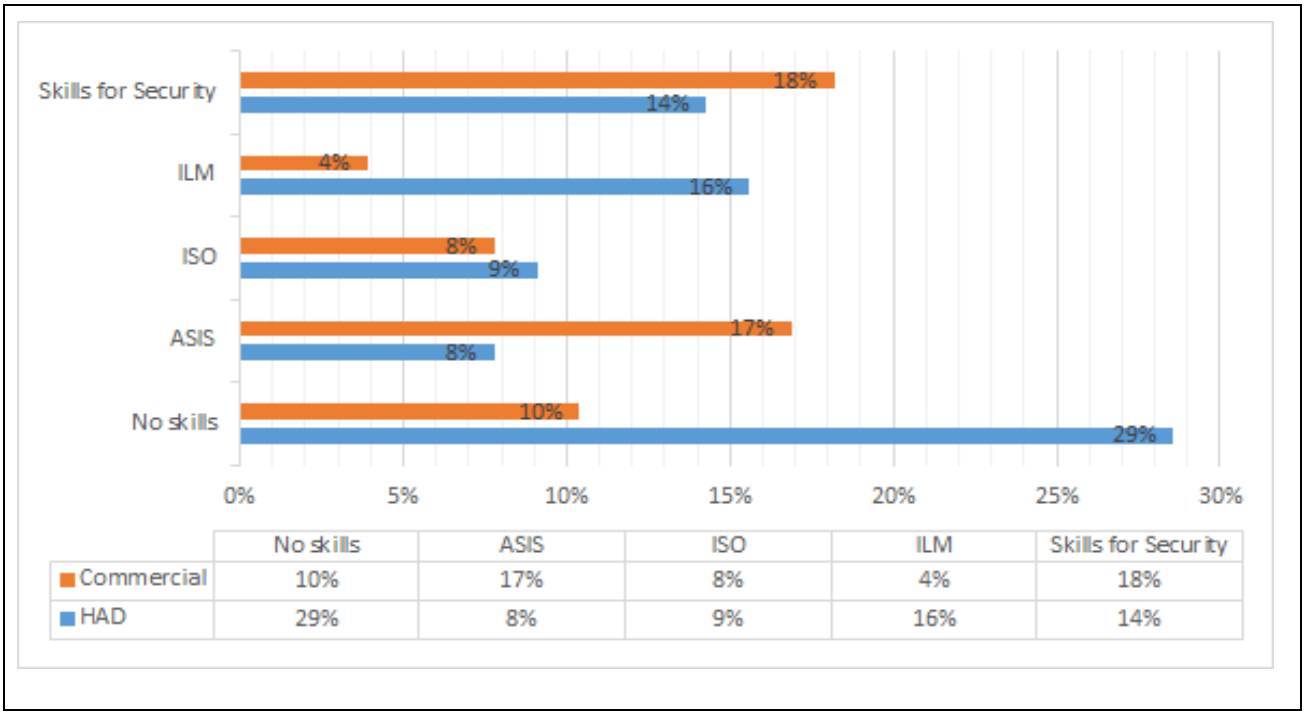
> "I think that'd be a twofold approach (to professional development). One is the individual themselves, to succeed, they need to be a learner. They need to understand, I'm in a new sphere, I'm on a learning curve. I need to be reading professional publications, talking to people, going to seminars, realizing that here there's a lot that I need to learn".

The ASIS study (2018, p.30) also produced data on the type of degree security professionals most typically focused on. A reasonable assumption would be that professionals would select degrees which were aligned in some way with their career field, thus advancing academic and technical knowledge concurrently. However, as shown in **Figure 36** at the bachelor's level 24% of the participant pool focused on business administration, 11% focused on political science, while only 37% focused on criminal justice or law enforcement. While professionals did not necessarily leverage academic learning to meet the technical needs of their careers, the majority (over 71%) saw it as important for their career advancement in terms of both professional development and promotional advancement.

Bachelor's or associate's course of study	1. Criminal justice (27%) 2. Business administration and management (24%) 3. Political Science (11%) 4. Law enforcement and correction (10%) 5. Economics (6%)
Masters degree or higher course of study	1. Management (14%) 2. Administration (9%) 3. Criminal justice (8%) 4. Law (4%) 5. Security technologies (4%)
% indicating background area of study important in qualifying for current position	Executive (73%) Management (81%) Professional (71%)

Figure 36. ASIS Security Professional's Academic Focus (p.30)

Figure 37 illustrates the differences between the humanitarian sector and their commercial peers in terms of who leveraged standards-based bodies for their professional development. Of the 77 survey participants, a higher proportion of the humanitarian security professionals similarly failed to take advantage of vocational learning opportunities than their commercial peers. This speaks to the sector again not fully embracing readily available out-of-sector resources. The limitations associated with organizationally-funded learning opportunities, a lack of awareness of what vocational resources exist and their value, combined with the lower wages and the more nomadic role of a humanitarian security professional—in terms of higher frequencies of international travel limiting access and focus on learning—may be contributing factors to the lower uptake in vocational education.



	No skills	ASIS	ISO	ILM	Skills for Security
Commercial	10%	17%	8%	4%	18%
HAD	29%	8%	9%	16%	14%

Figure 37. Utilization of Awarding Bodies by Security Professionals

Camila cited funding as a major problem with implementing training programs, suggesting that despite higher levels of risk than the commercial counterparts, organizations within the sector were less willing to fund knowledge building strategies:

> "Everyone in my position will tell you that it's an annual battle around the budget in terms of what can be included, not only for training for staff within the organization or on just basic security matters, but also for continuing to build the capacity of your risk managers or the department".

The findings from the primary research, supported by similar research conducted by ASIS, show that security professionals across all sectors and industries see value in academic studies as a mechanism for professional advancement as individuals progress within their careers. Vocational learning opportunities, while arguably less costly in terms of time and course fees—and more directly relevant to job performance—are however surprisingly less attractive to the humanitarian security professional.

The value of the competency framework

Where documented standards codify resilience strategies, then training operationalizes these into practice. The alignment between risks and associated solutions will invariably require some level of accompanying training, with competency frameworks providing the structure which connects standards to action. As yet, no universally-agreed-upon professional competency framework exists for the security community, with Stephen expressing the feelings of the majority of interviewed participants, stating that no structure or support is in place to support the security professional in understanding and meeting professional goals:

> "I think it's quite personality driven, and from my own experience, I would say that the NGO world is under so much pressure that there is not very much ability to say we'll put Stephen on a training program. We'll make sure we develop him. Now, you get onboard the galley, and then you're tied to the oar and we start rowing. That's it, and if you have the strength to put your head above the water and suck in some fresh air, please do, but you have to produce".

The application of a competency framework spans all sectors and industries, being used in military leadership development (Horey et al., 2004), for the health care profession (Harding et al., 2012) and within the humanitarian sector (Rutter, 2011; Camburn, 2013; and Narayanan, 2016). No publicly available studies exist on security professional competency requirements within the sector, aside from the output of the INSSA study which presently focuses at the local, national and regional levels, rather than addressing higher resiliency needs at the organizational level. A competency framework offers a model that broadly defines the blueprint for "excellent" performance. At the macro level, the framework will consist of a number of competencies which can be generically applied to a broad number of roles. At the granular level organizations, down to departments, it can add greater specificity to the professional requirements of a group or an individual's role. Each competency is defined in a way that makes it relevant to the organization, sector, and activity. Frameworks use language that are clear

enough to ensure that everyone has a common understanding of what "excellent" job behavior or performance outcomes look like. This common understanding then becomes the benchmark against which the performance of an individual, team, project, activity or even the entire organization can be measured. Where an organization neglects to define an expected behavior or standard of performance, then the judgement of good, bad, average, or excellent will be highly subjective. As such, a well-crafted competency framework provides a common language that can be used for the review, evaluation, and development of resilience strategies. It can also be used as part of the organization's recruitment process when selecting professionals to fulfill critical functions, with Focus Group Participant No. 4 stating that:

> "The competency framework will assist the development, recruitment and implementation stages of a project. Will provide managers and recruiters with an overview and specific knowledge of what to look for in security practitioner's performance".

Camila also noted that rarely was a defined training plan in place that formalized learning outcomes, or which supported the operationalization of security document systems:

> "Very rarely in my experience is there an actual training plan where staff are not only receiving the security plan but they're receiving ongoing training, or even training at least at the beginning when the plan is being rolled out".

The security community's competency framework needs to be mapped against the range of primary functions within the hierarchy of roles, as well as any secondary functions an individual might perform. It must reflect the technical knowledge and practical skills needed to accomplish these outcomes, and it must concurrently take into account leadership decision-making parameters, the influence and implications of predicted or occurring risks, and the consequences of making the wrong decision which might harm people, or which could disrupt organizational interests. The importance of vocational versus academic knowledge will also invariably change as the individual progresses along their career path. Vocation-based competencies will support tactical or operationally focused responsibilities, while academia might strengthen areas of strategic competency. Focus Group Participant No. 6 stated that:

> "The competency framework also provides a blueprint for shaping and delineating the security risk management component of the overall organizational structure. It gives an insight into the roles and levels of engagement security risk management professionals can fulfill to promote business continuity".

Professionals acknowledged the need for education to address both vertical and lateral knowledge production needs. Vertical competency addresses seniority in role and the associated leadership or management acumen, while lateral competency spans technical knowledge and geographies. Within this model, a Security Focal Point would represent a low vertical and narrow lateral standing. Conversely, the organizational lead on security and/or resilience would be a key decision-maker and reflect a high vertical and broader lateral positioning in the model. Using this as the premise for professional advancement, the higher the position the greater the breadth and depth in competencies, and potentially, geographic experience. Exceptions exist of course where a professional becomes a specialist in their field, such as for kidnap and ransom negotiations, or as an investigator or trainer. However, these roles are limited within the sector, and inherently have a lower seniority ceiling. **Figure 38** illustrates findings from the interview pool and competency framework focus group on how both individuals may move upwards along a promotional pathway, while also moving laterally to gain geographic and technical competency.

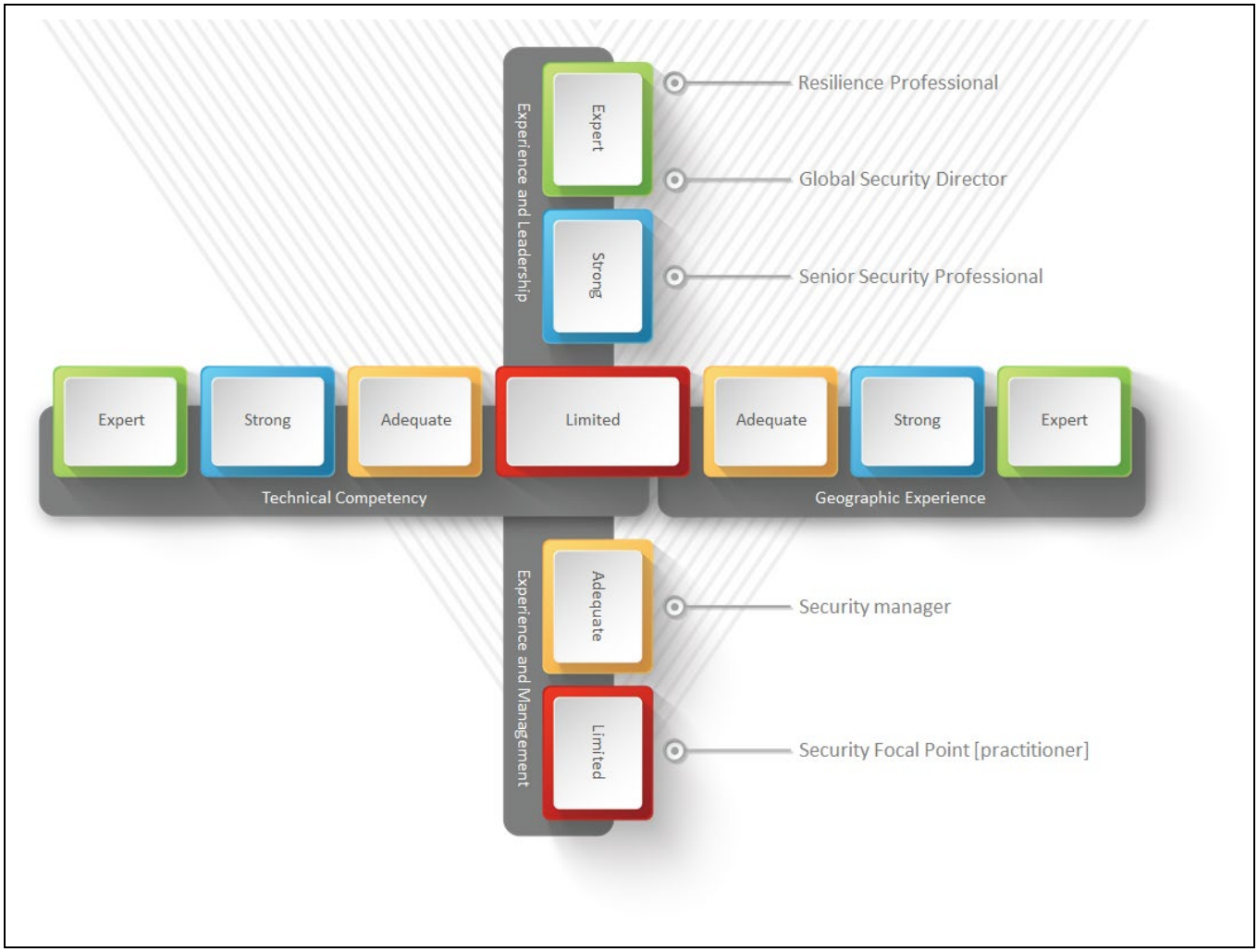


Figure 38. Blyth Vertical and Lateral Professional Development Model (2020)

The competency framework is supportive of, and critical to, transformative change. This change may be gained through one of two mechanisms: either a modification to an existing career where the individual seeks a similar role, but with a broader or higher range of technical knowledge and skills, or where the role is within a different sector and so adaptation is required to apply knowledge and experience within a different setting. This reflects the military professional bringing security expertise from the armed services security field, and then converting knowledge and experience to match the needs of the humanitarian security remit. Secondly, the individual may select an entirely new role, evolving beyond their existing scope of knowledge and experience. This reflects the civilian or academic changing professions and bringing tangential knowledge and experience to a new technical field. Charlie commented on the lack of consistency within the sector for developing the individual, regardless of background:

> "I think one of the problems around that is that the development of security professionals by the organizations is not always done in the same way that it's done within another organization, and security personnel may not be given the opportunities to develop personally or professionally or to attend conferences".

If the agreed-upon metrics by which to measure professionalism within the security community are based on the three areas of *leadership*, *knowledge* and *experience*, then the start-point for each individual will be determined initially by what they bring with them from a primary career field (transferable competencies), and secondly, it will be defined by those areas of competency which must be enhanced to achieve any required standards. The concept of convergence suggests that some foundational careers offer more opportunities to develop measurable knowledge, experience, and leadership competencies than others. These careers bring embedded tacit knowledge to the second career, a fact that employing organizations need to recognize when selecting—and then advancing— those performing a security role. Regardless of the natural talent or the inherent potential of the individual, organizations must recognize that some career start-points offer fewer opportunities to build these competencies than others, and so rapid and consciously structured upskilling may be required where gaps exist. In addition, simulations and other exercises become increasingly important where the effects of a poor decision place people at risk, or can cause irreparable harm to the organization.

The interviewees identified the need for a competency framework to be established to assist with the transition of individuals from their primary career field into a humanitarian aid and development sector security role. Tom reinforced the need for individuals to professionalize themselves in absence of an external body or system to support or validate their professional credentials:

> "The more that we aspire to being professional, the better off everybody will be and the greater the likelihood is that when the situation on the ground grows more complex and more insecure, we will still have the ability to manage the risk and access vulnerable populations. That's the working theory there".

CHAPTER 8

DISCUSSION

The chapter begins with an overview of the research findings, linking the results to the literature review, the online survey, the semi-structured interviews, and the focus group. The discussion then presents the findings against how resilience is defined and framed, how standards and ultimately the security profession plays a role in addressing risks, how change can be affected, and the value of forums and awarding bodies. The chapter concludes by offering the research implications, before presenting four *sensitizing concepts* (Bryman, 2001 p.270) which make up a research-based "*Hybrid Model of Security and Resilience*" model. The discussion ends by offering recommendations as an action-based outcome to address the vulnerabilities identified within the thesis.

Overview of research findings

The findings of the thesis build upon and adapt theories explored in La Porte's research on high reliability organizations (1996), as well as Wenger's work on communities of practice (2017), and propose several conceptual frameworks constructed by the researcher to explain narrow ideas and the relationship between areas of the study and the potential solution required to build resilience within the humanitarian aid and development sector. The conceptual framework also adapts aspects of Polanyi's research on tacit learning (2009), Gibbons et al studies on the production of knowledge (2002), and Eraut's theories on developing professional knowledge (2002). The conceptual framework encourages further research on the development of concepts and theories that would be useful to both security / risk professionals and their organizations, as well as to further academic studies.

The research sought to expand the sector's focus beyond the area of security risk management at the tactical and operational levels, and to develop more inclusive organizational resilience measures at the strategic level. It was concluded from the literature review, as well as the primary research findings, that the ability of the sector to effectively address the increasing levels of complex threats requires the professionalization of resilience standards, practices, and educational resources. The growing expectations—and outright demands—of employees, their families, donors, and governments, coupled with escalating beneficiary needs in high-risk areas, requires a more sophisticated understanding of how security risks and the cascading impacts to business, operations, and reputation is viewed and addressed. At the core of the solution sits the security community: those who identify, evaluate, articulate, and

ultimately address security risks. Where a crisis occurs, it is the security community who often manages the incident consequences, as well as the cascading effects to wider organizational interests.

Nonprofit Action (2020) estimates there are over 10 million non-governmental organizations operating worldwide, with hundreds of millions of employees and volunteers, and billions of dollars of funding annually. A sector of this size, with a rich history of working in remote and challenged environments with quantifiable threats, is duty-bound to manage resilience with the same level of professionalism as they would their program goals. The sector can no longer avoid its duty of care obligations, nor can it present itself as a poor custodian of donor funds. As the size of the sector grows fiscally, as well as in terms of geographic and human-reach, the importance of an evidenced approach to safeguarding both people and business interests will commensurately increase. Alex underpinned the changing nature of the sector and the need to reflect commercial best practice, positing that:

> "There are billions and billions of dollars going through the sector. We are a *business* and understand that we should be structured against a business model, with business processes in place. We will become a regulated sector".

Defining resilience

The term "resilience" is fraught with contextually driven meanings and subjectivity, and it is influenced by personal constructs of reality. It is also complicated, as it seeks to address strategic, operational and tactical requirements across different cultures, structures and functions, meeting the needs of diverse and fluid operating environments and organizational cultures. Resilience presents an "organizing principle" around which organizations and the wider sector constructs the approach to protecting people, facilities, assets, information, business interests and organizational reputation.

The findings illustrate the absence of an agreed meaning of what resilience means, as well as an appropriate body of knowledge focused on sector focused organizational resilience—whether found within academic or grey literature—illustrating the gap between known risks and an appropriate level of professionalism within the security and wider risk owner community. Both academic and professional studies are widely available on associated areas of risk, resilience, disaster, crisis, supply chain and business continuity, addressing risks to commercial, government and community vulnerabilities. However, little has been done to address the growing needs for a sector focused resilience strategy to protect the implementing partner community. This gap in knowledge should bring the interrelated implication of risks together—rather than treating them as siloed problems—allowing the sector to

coherently understand what vulnerabilities exist, how they affect each other, and how to address them holistically.

Framing resilience strategies

The sector's current approach to understanding, articulating, and resisting complex risks is poorly defined, undeveloped and inconsistently applied. Standards are not codified, communities of practice are disjointed, and defined learning pathways are difficult to construct or consistently apply. The ECHO (2004, p.41) report states that: "Policies are important. If there is no overall organizational policy to provide a framework for the development of plans then even when some kind of planning process does take place this can lead to inconsistent and inappropriate planning". Combined, these challenges make it difficult, if not impossible, for the sector to control risks and appropriately meet the rising expectations of employees and donors. In turn this undermines the sector's ability to effectively —and safely—meet increasing beneficiary needs.

The findings indicate that resilience crosses all boundaries, moving vertically and touching multiple internal cultures from the tactical grassroots to the strategic leadership level. It also moves horizontally across functions, activities, and geographies. Behn and Kingston (2010, p.3) state that organizations need to: "harmonise a professional humanitarian security apparatus with programme and organizational systems and imperatives". Where gaps exist, resilience must form the instrument which binds together experiences, perceptions, tolerances, beliefs, and practices. As such, the development of a resilience strategy requires effective *framing* in terms of the *intent* of resilience from a scope and objective standpoint, and both structured and recognized guidance is required for those who shape, direct, and evaluate risk management across the complex spectrum of vulnerabilities. To be effective, decision-makers and influencers need to understand how resilience operates within stages, or across time. They must also understand the influence of *environment* which presents the context of how risk is managed at all levels, and across all geographies and cultures. Collectively, this requires an inclusive approach across all functions, organizational cultures and geographies, with a recognition of the importance of placing individuals in a position to be heard, and so effectively influence the organizational strategy (Duijnhoven and Neef, 2014).

Establishing consistent standards

The research identified that, while significant investment has been placed in addressing the resilience needs of the beneficiary community, little has been done to assess how those meeting beneficiary needs can—or should—be more resilient to physical risks, and critically, how organizations exert control over the damaging effects of legal and reputational harm. The sector lacks codified and universally recognized standards without which knowledge, skills and practice can take root. The security community, while filled with highly competent individuals, is not yet a "profession" in that it lacks a recognized body of knowledge, defined educational goals and credible resources, and displays wildly different strategies, practices, and beliefs.

The sector has sought to establish its own standards but has failed. It now needs to both recognize and leverage existing international standards, upon which it can build its own resilience strategy. Coupled with this is the need to develop a competency framework around which individuals can establish the knowledge, skills and experiences needed to effectively, and confidentially, perform their roles. This supports the individual, their employing organization, and more broadly, the entire sector in addressing complex risks. Consequently, resilience will have a framework upon which the organizations can establish effective and scalable measures to transform their approach to meet the multifaceted threats faced. The sector will also then be in a position to more effectively measure success against consistence performance metrics.

The security profession

Van Maanen (1988) said the study of culture is intrinsically connected with ethnographic research and the diversity of occupational groups. This is true of those who address risk within the sector—with security forming occupational cultures within an ill-defined hierarchy of part-time practitioners and qualified professionals—and outside of the field of security, other risk portfolio owners. Schien (1985, p.6) also explored the concept of culture as: "the deeper level of basic assumptions and beliefs that members of an organization share". The resilience community is complex, reflecting: 1) a wide range of cultural orientations driven by location and activities, 2) differing "know how" in terms of the level of seniority, environmental influences and varying technical roles, and 3) beliefs in terms of what is "known", rather than what is "believed". The challenge, then, is to unify those leading on resilience through transformative change to replace what is "believed" with what is universally "known".

Creating a common understanding—or truth—of organizational resilience within the sector will result in two outcomes: 1) it will form the basis of both understanding risks and prioritizing resilience measures, and 2) it will provide the framework to enable the codification and subsequent professionalization of resilience. Research over the past 10 years calls for defined standards to address complex threats (Bickley, 2017), and there is a growing awareness of training shortfalls which presently hinders the elevation of knowledge within the security community (Kingston, 2009). Where standards define resilience goals, education operationalizes them. Both are inextricably linked, and if the sector is to establish the foundations upon which resilience can be built, implemented, and sustained, then standards need to be connected to education. Absent effective and demonstrable resilience measures which integrate standards and operationalize these through education, the sector will increasingly face disruptive situations, with organizations struggling to effectively manage crises.

Resistance seeks to avoid or minimize risks, or to negate or reduce their effects. It includes interventions, controls, and the establishment of capacity by which to identify and manage risk before—or as—it occurs. Investment in controlling risks before a crisis often defines how well, or badly, an organization responds. Yet, despite its importance, the sector has yet to define a consistent and measured approach to resistance. As stated by Beal (2015, p.275): "the first phase, mitigation, is arguably the most important phase. At the same time, it is typically the most under-utilized phase". Resistance is commonly associated with security risk management at the tactical and operational levels. However, in order to effectively shape resistance, the sector must effectively map, understand, and address all forms of risk.

Incremental and transformative change

The concept of incremental adjustment accepts that a risk may, or will, occur. As a result, systems must be designed to return the organization back to its pre-crisis condition—either to the pre-event status quo, or to a new state which is close to the previous operating condition (Matyas and Pelling, 2014). According to Normandin and Therrien (2016), resilience seeks to concurrently create order and stability (negentropy), while currently recognizing that crisis by its very nature creates disorder and change (entropy). The application of resilience strategies to meet both immediate and longer-term needs enable organizations to respond to disruptive events, restoring or moving the organization to a place of stability or safety. Proactive incremental adjustments offer an opportunity for *adaptation*, where effective resiliency systems establish *triggers* to pre-emptively adjust behaviors before a crisis occurs, thus circumventing some (or all) of the negative impacts. If the sector establishes systems that enable

proactive adaptation, or timely and painless incremental adjustments accommodating crisis-driven change and chaos, then they can more readily operate within uncertain environments. And, they will do this with the knowledge that resistance prevents much of the risk, but that system flexibility allows for effective adaptations to the turbulence invariably created by disruptive events. Resilience then creates "high-reliability" organizations which can function with confidence within an increasingly challenging world (La Porte, 1996).

Transformation reflects large-scale shocks to a system that require deeper-rooted changes and the movement to a new and improved state of affairs (Matyas and Pelling, 2014). Transformation frequently requires significant structural change, or major adjustments to practice, and it comes with high transactional costs. While organizations should have the capacity to undergo transformation and survive, such evolutions must reflect a defined, measured and driving need, and they cannot be implemented frequently for fear of becoming a destabilizing influence. As such, transformation should only occur once. To enable this transformation must be mapped against clearly defined expectations encapsulated in recognized standards. While transformation may be electively implemented to meet new strategic threats, more frequently it is forced, with transformation occurring where an organization has weathered a crisis poorly and has sustained significant damage. Ideally, effective and proactive resilience protects organizations against the need to implement forced transformation, allowing change to occur before a crisis as a positive and proactive decision, rather than as a negative, reactive measure.

The importance of education

Whether professionalization occurs through a process of transformative or incremental change, it requires standards as the cornerstone of goal setting and performance metrics. It also requires a recognized body of professionals to define what these standards are, what they mean, their value, and how they should be implemented. Professionals also walk their organizations through the process of transformation, either quickly and painlessly where expert competency exists, or slowly and dangerously where competency levels are weak or absent. Where a profession does not exist, then the risk of change through an oligarchy exists, rather than through a wider and more measured process of consensus. This undermines the credibility of standards, while also diluting the effectiveness of implementation, and ultimately, sustainment.

The absence of recognized educational goals, curriculums, and resources against which a professional can lead resilience strategies further weakens the sector's ability to self-govern the professionalization

of security risk management and resilience. This gap means that professionals are not validated against technical or experiential metrics, and so cannot be measured in terms of professional excellence. The consequence is the application of often indistinct and opinion-based nomenclature which confuses the understanding of what risk means, its consequences, and the associated value of resilience. Currently pluralist theories of truth (Wright, 1992) vary extensively across the various domains of resilience, as well as across global operating environments. To address this vulnerability, interpretations of what resilience means across coalitions of like-minded people and professional associations should ideally shape how technical knowledge, experience, methodologies, and goals are codified and trained against.

If the security profession is to work together as a body of experts aligning a competency framework to defined standards, then the profession must firstly be professionalized. This "chicken-and-egg" scenario must overcome the absence of legitimate standards which are operationalized through recognized training. This conundrum can be overcome if the sector adopts existing, and credible, resilience strategies, and concurrently takes advantage of the wealth of existing vocational and academic resources which exists both within, but critically also outside of, the sector. The benefits of vocational and academic knowledge must also be defined, offering knowledge, skill, experience, and behavioral accelerators so that individuals are not forced to develop only through incremental or opportunity-driven learning constructs.

CS Lewis (1993) stated that: "experience: that most brutal of teachers. But you learn, my God do you learn…" and the value of experiential—or situated—learning cannot be underrated, as security professionals manage fast-burn and high-impact crisis situations which can involve life and death decisions, often under highly stressful and emotive conditions. Experiential learning, alongside taught technical knowledge, sets the security professional apart from the security practitioner. The sector must recognize the attributes of those coming from a primary career with a strong and credible security foundation, as well as those who come from a civilian career with little to no security experience or formal credentials. To assist both groups in transitioning effectively from a primary career, and then growing within the sector, a competency framework is needed against which all can work to. It must also form accelerators for professional development to move the security community, with focus and purpose, along a life-long learning journey. The production of knowledge must be systematic and results-orientated (Kirkpatrick, 2016), encompassing: 1) the degree of relevance to the learning, 2) the level of knowledge, skill, attitude, and confidence attainment, 3) the extent of behavioural change required, and 4) the targeted results achieved. Where knowledge is perishable, or where individual or

leadership knowledge requires stress inoculators to make sense of the learning and ensure knowledge retention, then immersive knowledge production is required.

Forums and awarding bodies

The challenge of utilizing existing standards and applying these to the sector requires recognition of the value that different standards, whether ISO, ASIS, BSI, or COSO, bring to the sector. These standards also apply to education, with recognized awarding bodies such as ASIS, the ILM, INSSA, or Skills for Security offering not only relevant training and exercising resources, but credible ones. Ultimately, where a standard is defined, this must be accompanied by appropriate educational resources. This process can be achieved by forming a collective of seasoned professionals to conduct focused research, whose findings and recommendations can then be presented to the sector at large. This should be inclusive of acknowledged in-sector experts, professional awarding bodies such as GISF, the Security Management Institute, ASIS, or INSSA, and out-of-sector experts in the field of resilience and educational design. Donors must also be included, as they ultimately fund resilience strategies, and so must be key contributors, and advocates, of the resulting strategy. If the approach is focused and inclusive, then it is more likely to lead to a transmogrifying outcome. As the strategy is increasingly adopted across the sector it will also become the norm and so gather momentum, forcing change as organizations are required to benchmark their approach against those of their more professional and advanced peers.

Research implications and recommendations

There is little doubt that security professionals, as well as those assuming a security role as a non-professional, recognize the need to develop a more robust resilience strategy for their organizations, and that there is an absence of recognized standards currently governing the sector. However, this recognition is not always found within the executive leadership team who enable or drive resilience strategies. Whether resilience results from an internal recognition of need, or is forced by external factors, it is increasingly becoming an inescapable requirement as organizations seek to operate in remote and challenged environments. A failure to address resilience presents a “time bomb” for organizations as guided by luck, rather than by design and judgement, they seek to navigate the minefield of security risks—and more critically, seek to reduce reputation and litigation harm which comes from a mismanaged crisis.

The research findings from the inductive research approach generated the four concepts shown in **Figure 39** which form a *Hybrid Resilience and Security Model*. This model is designed to aid the sector in tackling the complex problem of developing a consistent and standards-based approach to resilience.

The four concepts within the model are interlinked, supporting security professionals in effectively transitioning from primary career fields into the humanitarian security community, while allowing organizations to better identify and recruit candidates into security positions. It enables both security practitioners and professionals to grow within the field by recognizing opportunities for knowledge and skill growth and culminates with a diverse range of experiences and knowledge coming together at a point of competency convergence.

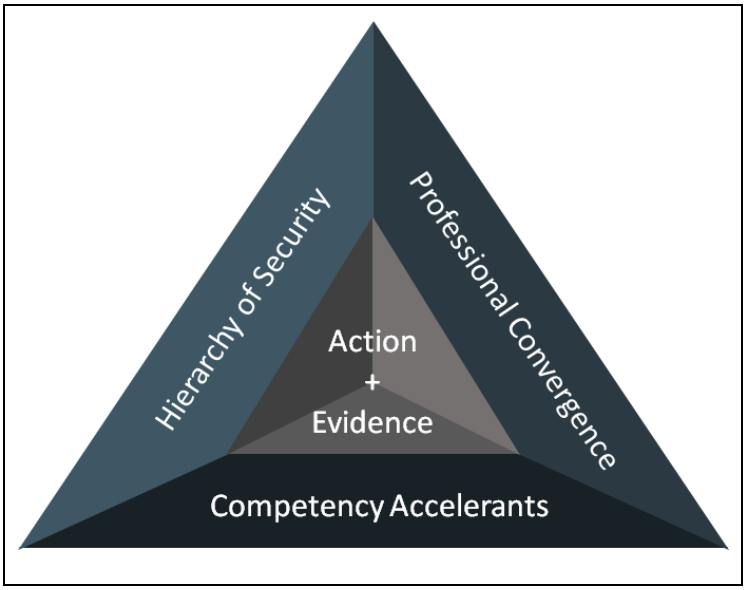


Figure 39. Blyth The Hybrid Model of Security and Resilience (2020)

The "Hierarchy of Security" concept

The first concept within the model is the "hierarchy of security" concept which reflects both vertical and horizonal knowledge, skill, experience and attitude requirements. A semi-formal structure[14] enables both employing organizations and the security community to define the positioning of an individual vertically in terms of management placement, and horizontally in terms of specialization and geographic placement. The hierarchy of security establishes the common requirements for each role, and so shapes the structure of the security profession. It also provides both an entry point and promotional road map not only for the individual, but also for the organization.

[14] Allowing for differing organizational sizes, complexity and unique knowledge and skill needs.

The "Competency Accelerant" concept

The second concept in the model is "competency acceleration", which recognize multiple mechanisms through which knowledge and experience can be artificially developed. This model includes formal accelerators to knowledge and experience through planned and structured transformative growth. It also recognizes opportunity driven development may occur through chance and circumstance, and that learning may occur piecemeal and incrementally over time.

The "Professional Convergence" concept

The third concept within the model is "professional convergence", where individuals from markedly different backgrounds eventually converge—whether through planning or by circumstance—from different technical and experiential learning journeys to a point where critical areas of competency are achieved, producing a well-rounded professional. Convergences recognizes multiple points of attained excellence where individuals reach points within the "Hierarchy of Security" through one or more "Accelerants" of knowledge and experience production.

The concept of "Action and Evidence"

The "action and evidence" concept posits that not only are effective resilience measures required, but they must also be provable under hostile scrutiny. This integrated approach requires practitioners, professionals, and organizations to be effective in not only identifying, assessing, and managing risks, or responding to, managing, and recovering from crisis situations—these measures must also be codified within document systems, training materials and records.

The next steps

A focused effort is required across the sector—with meaningful donor engagement and support—in order to address the absence of a defined strategy which might unify the sector's approach to resilience, while also offering the mechanism for the professionalization of the security community. There are 10 key interlocking actions which might strengthen the professionalization of the security community, and more broadly resilience, in order to address the increasingly complex and escalating risks the sector faces. These include:

1) Focused research should be conducted on organizational resilience and business continuity management, addressing the existing gaps in academic and grey literature. Detailed studies would provide the data required for the sector and professionals within it to make informed decisions, while articulating the needs and benefits of resilience to donors.
2) A taxonomy of resilience is required to enable the security community to communicate fluently across functional boundaries. This will develop a body of knowledge and a universal understanding of what resilience means, and how threats and vulnerabilities can be addressed.
3) Commitment is required by the executive leadership team to recognize, engage in, resource, and promote resilience strategies. This support must flow-down to encourage—or require—all leaders to be part of a community of risk practitioners, enabling resilience to be incorporated into every facet of planning, budgeting, and activity.
4) Donor participation is required to define risks and their impacts, explore the meaning and value of resilience, define minimum standards, and evaluate the benefits of resilience strategies to the donor, the beneficiary, and to the implementing partner community.
5) Established disciplines should be leveraged to enable the emergent field of humanitarian aid and development resilience to advance in knowledge, structure, standards, and practice.
6) Forums and associations should lead focus groups—including commercial and government experts—to investigate, evaluate, and articulate applicable standards and educational resources, and to support individuals transitioning into, and developing within, the security community.
7) The sector should establish a universally applicable Competency Framework reflective of scalable resilience standards, and the hierarchy of security positions. The framework should define required knowledge, skills and competencies to enable career transitioning as well as life-long learning journeys.
8) The security community, with support and direction from forums and associations, should map, evaluate, and leverage vocational education at every level in order to support both those transitioning from a primary career into the sector's security community, as well as an onward learning journey of technical competency development. Role definitions should then form the Hierarchy of Security to lend a framework for how the security community is structured.
9) Academia should collaborate with the security profession, and with forums and associations, to identify the key learning goals of the sector. This will help define how academic studies might advance the security and resilience professional in developing research, and in forming

strategic areas of competency. It will also offer the opportunity for individuals to expand the scope of their capabilities, and in the process gain recognition from their peers.

10) A recognized community of security practitioners and professionals, and more broadly resilience professionals (including those from non-security related fields) should be developed to establish a body of professional knowledge. This will provide a mechanism for sharing standards, practices, knowledge, and experiences.

CONCLUSION

CHAPTER 9

The research focused on the field of organizational resilience within the humanitarian aid and development community, an area of increasing importance as humanmade conflict and natural disasters create growing societal instabilities, with a heightened level of beneficiary reliance on humanitarian assistance and development support. Thematic areas were used to examine the sector's approach to resilience, addressing what risks the sector faces and what resilience therefore means, how the security community plays a key role in addressing complex risks, how standards create consistency and structure within resilience strategies, the value of forums and awarding bodies, and how education enables the professionalization of the security and wider resilience practice.

Existing literature focused specifically on organizational resilience within the sector was examined, and where gaps were identified the research remit was expanded to draw out data from similar fields which might offer transferable value. The literature review identified a very clear gap within both academic and practitioner studies on strategic resilience within the sector, while operational and tactical security risk management was addressed extensively. Other related fields, such as supply chain resilience, the production of knowledge and communities of practice, was also extensively covered, as was resilience within conflict and disaster affected communities.

The main research question asked: "what risks does the sector face, what is driving change, and how can the sector professionalize its resiliency strategy". The research looked specifically at: 1) what threats exist, what are their impacts, and what constitutes resistance against these vulnerabilities, 2) how can practitioners from different backgrounds enter and develop in the field of security risk management and organizational resilience, 3) how are standards and practices codified and shared within the community through recognized document systems, 4) how can forums, associations and commercial resources enable resilience at both the individual and organizational levels, and 5) how are standards and practices operationalized through credible educational and exercising programs.

The research findings evidence that an escalation of natural disasters and humanmade crises are increasingly drawing the sector into high-risk situations, which necessitates effective organizational resilience measures. Gibbons et all (1994) models of knowledge production influenced the action-based outcome goals, seeking to support both academic as well as practitioner advancement. Empirical realism allowed data to be gathered through first-hand observation and experience, while Blumer's concept of

social interactionism was important as the data reflected the personal deep-seated beliefs and experiences of those participating within the data-gathering instruments, and in a wider context, how the culture of security views resilience. The research offers the *Hybrid Model of Security and Resilience*, incorporating four key concepts focused on: 1) mechanisms for knowledge production, 2) a formal structuring of security roles and responsibilities, 3) a recognition of defined professional convergence points, and 4) the need to both implement and evidence professional standards.

The online survey was used to draw largely quantitative data from two groups to form an understanding of how the sector might differ from its government and commercial peers. From the lessons learned a sector-focused semi-structured interview approach was used to further explore thematic areas of interest. Finally, a focus group was then used to specifically explore how a competency framework might turn standards into practice. This approach offered a significant range of data from which findings were established, allowing the research to then offer recommendations as part of an action-based research outcome.

The humanitarian aid and development community face a significant conundrum: how to protect its own interests while concurrently implementing an undisrupted and timely flow of aid to disaster-affected communities. This is especially important as: "disaster loss is on the rise with grave consequences for the survivability, dignity and livelihood of individuals, particularly the poor, and hard-won development gains… points to a future where disasters could increasingly threaten the world's economy, and its population…." (**Hyogo Framework for Action 2005-2015,** p.1). The **Sendai Framework for Disaster Risk Reduction 2015–2030** report more recently continued discussions by the United Nations General Assembly on societal disaster risk management, and yet also fails to address the requirement for implementing partners to have a commensurate level of internal resilience in order to best support donors and beneficiaries of aid. As such, there is an urgent need to enhance sectoral resilience, not only to meet the increasing threats implementing partner organizations face, but also to meet the rise in beneficiary demands within problematic environments.

Barnett (2000, p.257) states: "a complex world is one in which we are assailed by more facts, data, evidence, tasks and arguments that we can easily handle within the frameworks in which we have our being. By contrast, a super-complex world is one in which the very frameworks by which we orient ourselves to the world are themselves contested". The lack of rigorous and agreed upon standards requires the security community to become a learning society, embracing flexibility, adaptability, and self-reliance. To be effective, resilience must coalesce around agreed upon standards, bringing together

stakeholders from diverse technical, experiential, and cultural backgrounds. And, risk owners must meet at specific touch-points to form a mutually-supportive hybrid community of practice to address the increasing risks the sector faces. Resilience must build order and stability, moving the community from a super-complex to a complex world, but without being so rigid as to snap under the effects of chaos. To operationalize this, the production of knowledge (Gibbons et al., 2002) needs to weave together academic and vocational learning, security profession concepts and practices, as well as resilience standards into the way in which the security community can both articulate and implement appropriate and scalable measures to control, or manage, risk—either at the point of a contract award, or where programs are implemented.

The practical implementation of a sector-wide resilience approach is complex, requiring focus, substantial effort, and investment. The solution must be multi-pronged, involving academia, the security community, both sector specific and out-of-sector forums, as well as awarding and standards defining bodies. The approach must bring together donors and implementing partners to establish points of mutual interest. It must bring together the technical and experiential knowledge of security professionals from both within—as well as outside—of the sector. It must incorporate a diverse range of forums and bodies which espouse standards and best practice, regardless of whether they are sector or commercially focused. The sector must leverage existing standards and resources to expedite the process of professionalization, recognizing where a transferal of knowledge or best practice is appropriate. And, it must support those seeking to transition into the field of security, and support and recognize their onward learning journey. The solution spans millions of organizations, and hundreds of millions of employees and volunteers operating globally, and within a myriad of shifting risk environments, and it must overcome the complexities of language, culture, and resource limitations.

In order to build lasting resilience within the sector further research into the steps and resources needed to form a standards-based approach to the professionalization of the security community, and specifically for those responsible for leading in the area of security risk management, is required.

References

ACA. (2014). *Global Humanitarian Overview Status Report*. United Nations Office for the Coordination of Humanitarian Affairs (OCHA). Retrieved from: https://reliefweb.int/sites/reliefweb.int/files/resources/Global_Humanitarian_Overview-Status_Report-Aug_2014.pdf (accessed 4th July 2018).

Alexander, D.E. (2013). *Resilience and disaster risk reduction: an etymological journey*. Natural Hazards and Earth System Sciences. Retrieved from: https://nhess.copernicus.org/articles/13/2707/2013/nhess-13-2707-2013.pdf (accessed 12th August 2019)

Allen, M.A., Kovacs, G., Masini, A., Vaillencourt, A., & Wassenhove, L.V. (2013). *Exploring the link between the humanitarian logistician and training needs*. International Journal of Physical Distribution and Logistics Management, Vol 3, Issue 2, pp.129-148.

Annawitt, P. (2010). *Global Security and Regional Responses: Conflict Management in a Fractured World*. Geneva Center for Security Policy.

Bacon, F. (1625). *Sylva Sylvarum: or of Natural History in ten Centuries*. Kessinger Publishing.

Barnett, R. (2000). *Realizing the university in an age of supercomplexity*. Buckingham: Society for Research in Higher Education and Open University Press.

Beal, H. L. (2014). *Military Foreign Humanitarian Assistance and Disaster Relief (FHA/FDR Evolution: Lessons Learned for Civilian Emergency Management Response and Recovery Operations*. International Journal of Mass Emergencies and Disasters.

Becker, H.S. (1982). *Culture: A Sociology of Deviance*: New York: Free Press.

Behn, O., & Kingston, M. (2010). *Whose risk is it anyway? Linking operational risk thresholds and organizational risk management*. European Interagency Security Form.

Below, R., & Wirtz, A. (2009). *Disaster Category Classification and Peril Terminology for Operational Purposes*. Universite catholique de Louvain. Belgium.

Bickley, S. (2017). *Security Risk Management: a basic guide for smaller NGOs*. European Interagency Security Forum.

Blumer, H. (1986). *Symbolic Interactionism: Perspective and Method* (Edition 1): University of California Press.

Boris, E.T. (2013). *The Nonprofit Sector in the United States: Size and Scope.* Center on Nonprofits and Philanthropy. Washington, D.C.

Boyatzis, R.E. (1982). *The Competent Manager: A Model for Effective Performance*. John Wiley & Sons, New York, NY.

Boyatzis, R. (2008). *Competencies in the 21st Century*. Journal of Management Development. Vol 27, No 1, pp. 5-12.

Brabant, K.V. (2001). *Mainstreaming the Organisational Management of Safety and Security.* Overseas Development Institute. HPG Report 9.

Brech, V., & Potrafke, N. (2014). *Donor ideology and types of foreign aid.* Journal of Comparative Economics, Vol 42, No 1, pp. 61-75.

Briggs, R., & Edwards, C. (2006). *The Business of Resilience: Corporate security for the 21st century*. Demos.

Brooks, J. (2018). *Humanitarian Under Attack: Tensions, Disparities, and Legal Gaps in Protection*. ATHA. Retrieved from: https://reliefweb.int/sites/reliefweb.int/files/resources/atha-humanitarians_under_attack.pdf (accessed 4th January 2020).

Bryman, A. (2016). *Social Research Methods (5th Edition)*. Oxford University Press.

Burkle, F.M., Martone, G., & Greenough, P.G. (2014). *The Changing Face of Humanitarian Crises*. Brown Journal of World Affairs, Vol XX, Issue 11.

Buth, P. (2010). *Crisis Management of Critical Incidents.* European Interagency Security Forum.

Camburn, J. (2013). *Competency-Based Standardized Training for Humanitarian Providers: Making Humanitarian Assistance a Professional Discipline.* ResearchGate.

CARRI. (2013). *Definitions of Community Resilience: An Analysis*. Community & Regional Resilience Institute.

Chi, Bassock, Lewis, Reimann & Glaser. (1989). *Self-Explanations: How Students Study and Use Examples in Learning to Solve Problems.* John Wiley and Sons. New York.

Childs, A. K. (2013). *Cultural Theory and Acceptance-Based Security Strategies for Humanitarian Aid Workers*: The Berkeley Electronic Press. Retrieved from: http://scholarcommons.usf.edu/jss/vol6/iss1/9/ (accessed 5th August 2019).

Christopher, M., & Peck, H. (2004). *Building the Resilient Supply Chain*. The International Journal of Logistics Management, Vol 15, No. 2, pp. 1-14.

Craik, F.M.I., & Lockhart, R.S. (1972). *Levels of Processing: A Framework for Memory Research.* University of Toronto.

Creswell, J.W., & Guetterman, T.C. (2019). *Educational Research. Planning, Conducting, and Evaluating Quantitative and Qualitative Research*. Pearson. New York. NY.

Davies, J., & Reilly, L. (2017). *Security to go: a risk management toolkit for humanitarian aid agencies*. European Agency Security Forum.

De Smet, H.D. (2017). *Disaster management within the framework of a changing disaster landscape*. Datawyse / Universitaire Pers Maastricht.

De Vus. D. (2014). *Surveys in Social Research*. Routledge.

DeLoach, J., & Thomson, J. (2014). *Improving Organizational Performance and Governance.* COSO.

Department for International Development. (2012). *Promoting innovation and evidence-based approaches to building resilience and responding to humanitarian crises: a DFID Strategy Paper*. Retrieved from: http://www.dfid.gov.uk/Documents/publications1/prom- innov-evi-bas-appr-build-res-resphum-cris.pdf (accessed 14th October 2019).

Department for International Development. (2014). *Operational Plan 2011-2016: Conflict, Humanitarian and Security Department*. DFID.

DG ECHO. (2006). *NGO Security Collaboration Guide*. DG ECHO. Retrieved from: https://gisf.ngo/wp-content/uploads/2014/09/0640-Bickley-2006-NGO-Security-Collaboration-Guide.pdf (accessed 18th October 2019).

Dilley, M., Chen, R., Deichmann, U., & Lerner-Lam A. (2005). *Natural Disaster Hotspots A Global Risk Analysis*. Disaster Risk Management Series No 5. World Bank.

Drake, P., & Heath, L. (2011). *Practitioner research at doctoral level: developing coherent research methodologies*: Routledge.

Duijnhoven, H., & Neef, M. (2014). *Framing Resilience. From a model-based approach to a management process*. Elsevier B.V. Retrieved from: https://core.ac.uk/download/pdf/82058353.pdf (accessed 4th December 2019).

ECHO. (2004). *Report on Security of Humanitarian Personnel. Standards and practices for the security of humanitarian personnel and advocacy for humanitarian space.* Retrieved from: https://reliefweb.int/sites/reliefweb.int/files/resources/14B8FB85F0FB1CDBC1256F510039BF2F-security_report_echo_2004.pdf (accessed 14th June 2019).

Egeland, J., Harmer, A., & Stoddard, A. (2011). *Stay and Deliver: Good practice for humanitarians in complex security environments*. Office for the Coordination of Humanitarian Affairs: Policy Development and Studies Branch (OCHA).

Elsea, J., Schwartz, M., & Nakamura, K. (2008). *Private Security Contractors in Iraq: Background, Legal Status, and Other Issues*. Congressional Research Service.

Engestrom, Y. (2001). *Expansive learning at work: toward an activity theoretical reconceptualization*. Journal of Education and Work, Vol 14, No 1.

Eraut, M. (1994). *Developing professional knowledge and competence*. London: Falmer Press.

Fairbanks, A. (2017). *Demystifying Security Risk Management*. European Interagency Security Forum.

Faraj, S., & Xiao, Y. (2006). *Coordination in fast-response organizations*. Management Science. Vol 58, No 8, pp. 1155-1169.

Fast, L., & O'Neill, M. (2010). *A closer look at acceptance.* Retrieved from http://odihpn.org/magazine/a-closer-look-at-acceptance/ (accessed 18th August 2019).

Field, C.B., Barros, V., Stocker, T., & Dahe, Q. (2012). *Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation: A Special Report of Working Groups I and II of the IPCC*. Cambridge University Press, Cambridge and New York, NY.

Fischer, R. J. & Green, G. (2004). *Introduction to security.* 7th ed., Boston: Butterworth Heinemann.

Garrett, C. (2004). *Developing a Security-Awareness Culture – Improving Security Decision Making*. SANS Institute. Information Security Reading Room.

Garrett, S. (2015). *Are Natural Disasters Increasing*. The Borgen Project. Retrieved from: https://borgenproject.org/natural-disasters-increasing/ (accessed 3rd October 2019).

Gibbons, M., Limoges, C., Nowotny, H., Schwartzman, S., Scott, P. & Trow, M. (2002). *The new production of knowledge: the dynamics of science and research in contemporary societies.* SAGE. London.

Gosling. B.R., Marturano. A., & Dennison. P. (2003). *A review of leadership theory and competency frameworks*. Centre for Leadership Studies. University of Exeter.

Guardian. (2020). Trump's Blackwater pardons an affront to justice, say UN experts. Retrieved from: https://www.theguardian.com/us-news/2020/dec/30/trumps-blackwater-pardons-an-affront-to-justice-say-un-experts (accessed 12th January, 2021).

Guha-Sapir, D., & Below, R. (2002). *The quality and accuracy of disaster data: a comparative analysis of three global data sets.* WHO Center for Research on the Epidemiology of Disasters. University of Louvain School of Medicine.

Guttry, A., Frulli, M., Greppi, E., & Macchi, C. (2018). *Duty of Care of the EU and Its Member States towards Their Personnel Deployed in International Missions*. Springer Books.

Haas, P.M. (1992). *Introduction: Epistemic Communities and International Policy Coordination.* International Organization: Cambridge University Press.

Haase, T.W., Ertan, G., & Comfort, L. (2017). *The Roots of Community Resilience: A Comparative Analysis of Structural Change in Four Gulf Coast Hurricane Response Networks*. Homeland Security Affairs, Vol 13, Issue 9, No 1.

Harding, A., Walker-Cillo. G.E., Duke, A., Campos, G.J., & Stapleton. J. S. (2013). *A framework for creating and evaluating competencies for emergency nurses*. Journal of Emergency Nursing. Vol. 39 Issue 3, pp. 252–264.

Harmer, A. (2018). *Aid worker deaths: the numbers tell the story*. Office for the Coordination of Humanitarian Affairs.

Hoelscher, K., Miklian, J., & Nygard, H.M. (2015). *Understanding Violent Attacks against Humanitarian Aid Workers.* SSRN.

Horey, J., Fallesen, J., Morath, R., Cronin, B., Cassella, R., Frank Jr, W., & Smith, J. (2004). *Competency Based Future Leadership Requirements.* United States Army Research Institute for the Behavioral and Social Sciences. Retrieved from:

https://play.google.com/books/reader?id=JH3fAAAAMAAJ&hl=en&pg=GBS.PA5 (accessed 15th December 2020).

Horne, J.F., & Orr, J.E. (1998). *Assessing Behaviors that Create Resilient Organizations*. Employment Relations Today.

Independent Panel. (2003). *Report of The Independent Panel on the Safety and Security of UN Personnel in Iraq.* Retrieved from: https://www.voltairenet.org/IMG/pdf/fr-Panel_on_security_in_Iraq_Oct_03.pdf (accessed 24th June 2019).

INSSA (2017). *Competency Framework*. Global Interagency Security Forum.

International Organization for Standardization. (2016). *Security and Resilience – Guidelines for Organizational Resilience.* International Organization for Standard.

International Organization of Standard. (2016). *ISO 22316, Security and resilience – Guidelines for organizational resilience*. ISO.

International Organization of Standard. (2009). *ISO 31000, Risk Management-Principles and Guidelines*. ISO.

International Organization of Standard. (2011). *ISO 22320, Societal Security – Emergency Management – Requirements for Incident Response*. ISO.

International Organization of Standard. (2012). *ISO 22320, Societal Security – Business Continuity Management Systems – Guidance*. ISO.

International Organization of Standard. (2015). *ISO 18788, Management system for private security operations – Requirements with guidance for use*. ISO.

International Organization of Standard. (2015). *ISO 22317, Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA).* ISO.

International Organization of Standard. (2016). *ISO 34001.4, Security and resilience – Security management system for organizations assuring authenticity, integrity and trust for products and documents*. ISO.

Jackson, A., & Zyck, S.A. (2016). *Presence & Proximity: To Stay and Deliver, Five Years On.* Office for the Coordination of Humanitarian Affairs.

Jayawickrama, S. (2011). *Developing Managers and Leaders: Experiences and Lessons from International NGOs*. Harvard Humanitarian Initiative.

Kemp, E., & Merkelbach, M. (2011). *Can you get sued? Legal liability of international humanitarian aid organizations towards their staff*. Security Management Initiative.

Khorany, K. (2017). *International NGOs' Security Manager: Mindset, Attributes, Skills and Knowledge of Today's Humanitarian Security Professional*. University of Portsmouth.

Kingston, M. (2009). *Joint NGO Safety and Security Training*. European Interagency Security Forum.

Kingston, M., & Behn, O. (2010). *Risk Thresholds in Humanitarian Assistance*. European Interagency Security Forum.

Kingston, M. (2010). *Joint NGO Safety and Security Training*. European Interagency Security Forum.

Kirkpatrick. J.D. & Kayer. W. (2016). *Kirkpatrick's four levels of training evaluation*. Atd Press. Virginia.

Klamp & Associates. (2019). *Legal Liability in the Humanitarian Sector*. Klamp Law. Retrieved from: https://www.hg.org/legal-articles/legal-liability-in-the-humanitarian-sector-27150 (accessed 5th August 2020).

Kovacs, G., & Spens, K.M. (2007). *Humanitarian logistics in disaster relief operations*. Journal of Humanitarian Logistics and Supply Chain Management, Vol 37, Issue 2, pp. 99-114.

Kovacs, G., & Spens, K.M. (2011). *Humanitarian logistics and supply chain management: the start of a new journal.* Journal of Humanitarian Logistics and Supply Chain Management, Vol 1, Issue 1, pp. 5-14.

Kovacs, G., &Spens, KM. (2011). *Trends and developments in humanitarian logistics – a gap analysis.* International Journal of Physical Distribution & Logistics Management, Vol 41, Issue 1, pp. 32-45.

Kravitz, D., & O'Molloy, C. (2014). *A risky business: Aid workers in danger*. Devex. Retrieved from: https://www.devex.com/news/a-risky-business-aid-workers-in-danger-84373 (accessed 18th March 2019).

La Porte, T.R. (1996). *High Reliability Organizations: Unlikely, Demanding and At Risk*. Journal of Contingencies and Crisis Management, Vol 4, Issue 2, pp. 51-72.

Lave, J., & Wenger, E. (1991). *Situated Learning: Legitimate peripheral participation*. Cambridge University Press.

MacAskill, K., & Guthrie, P. (2014). *Multiple interpretations of resilience in disaster risk management*. Elsevier. B. V.

Manyena, S.B. (2006). T*he concept of resilience revisited*. Disaster's publication. New York. Willey and Sons.

Maren, M. (1997). *The Road to Hell: The Ravaging Effects of Foreign Aid and International Charity.* New York: Free Press.

Maslow, A. (1942). *A theory of human motivation*. Psychological Review, Vol 50, Issue 4.

Mathan, A., & Izumi, T. (2015). *Malaysian Experiences: The Private Sector and NGO Collaboration in Risk Reduction*: Retrieved from: https://link.springer.com/chapter/10.1007%2F978-4-431-55414-1_16#page-1 (accessed 18th June 2019).

Matyas, D., & Pelling, M. (2014). *Positioning resilience for 2015: the role of resistance, incremental adjustment and transformation in disaster risk management policy*. John Wiley and Sons. New York.

McKinley Advisors. (2018). *Security Industry Career Pathways Guide – Practitioners and Suppliers*. ASIS and Security Magazine.

Merkelbach, M., & Daudin, P. (2011). *From Security Management to Risk Management: Critical Reflections on Aid Agency Security Management and the ISO Risk Management Guidelines*. Security Management Initiative.

Metcalfe, V., Martin, E., & Pantuliano, S. (2011). *Risk in humanitarian action: towards a common approach?* Humanitarian Policy Group.

Moeller, R.R. (2011). *COSO Enterprise Risk Management: Establishing Effective Governance, Risk and Compliance Processes.* John Wiley and Sons. New York.

Murre. M.J., & Dros, J. (2014). *Replication and Analysis of Ebbinghaus Forgetting Curve*. US National Library of Medicine National Institutes of Health.

Musila, G. (2019). *The Spread of Anti-NGO Measures in Africa: Freedoms Under Threats.* Freedom House.

Narayanan, U. (2016). *Review and Development of Core Humanitarian Competencies Framework Report for CHS Alliance and Start Network Talent Development Project.* Consortium of British Humanitarian Agencies: Start Network.

Narli, S. (2010). *Is constructivist learning environment really effective on learning and long-term knowledge retention in mathematics? Example of the infinity concept*. Dokuz Eylul University.

NHI (2020). *Principles of Adult Learning & Instructional System Design*. NHI Instructor Development Course Guide.

Normandin, J.M., & Therrien, M.C. (2016). *Resilience Factors reconciled with Complexity: The Dynamics of Order and Disorder.* Journal of Contingencies and Crisis Management, Vol 24, Issue 2, pp. 1-12.

Oloruntoba, R. & Kovacs, G. (2015). *A commentary on agility in humanitarian aid supply chains*. Supply Chain Management: An International Journal, Vol 20, Issue 6, pp. 708-716.

Pelling, M. (2011). *Adaptation to Climate Change: From resilience to transformation*. Routledge.

Persaud, C. (2014). *How to Create Effective Security Training for NGOs*. European Interagency Security Forum.

Polanyi, M. (2009). *The Tacit Dimension*. The University of Chicago Press.

Reilly, L., & Llorente, R.V. (2015). *Organizations Risk Management in High-Risk Programs, The Non-Medical Response to the Ebola Outbreak*. Humanitarian Practice Network.

Robson, C. (2011). *Real World Research*. New York. NY. John Wiley and Sons.

Ross, J., & Sidebotham, T.L. (2017). *Crisis Management for Non-Profits, NGOs, and Mission Organizations*. Telios Law, PLLC.

Rutter, L. (2011). *Core Humanitarian Competencies Guide, Humanitarian Capacity Building Throughout the Employee Life Cycle*. ActionAid.

SAGE. (2019). *Learn to Use an Exploratory Sequential Mixed Method Design for Instrument Development.* SAGE Publications Ltd.

Schein, E. (1985). *Organizational Culture and Leadership*. Jossey-Bass.

Schon, D. (1983). *The reflective practice: how professionals think in action*. HarperCollins Publishers.

Schneiker, A. (2015). *Humanitarian NGOs, (In) Security and Identify Epistemic Communities and Security Governance*. Routledge.

Schneiker, A. (2016). *Humanitarian NGOs, (in) Security and Identify: Epistemic Communities and Security Governance*. Routledge.

Schwartz, M., & Swain, J. (2011). *Department of Defense Contractors in Afghanistan and Iraq: Background and Analysis.* Congressional Research Service.

Scott, D., Brown. A., Lunt. I., & Thorne. L. (2004). *Professional Doctorates: Integrating Professional and Academic Knowledge.* Society for Research into Higher Education & Open University Press. New York. NY.

Semb, G.B., Ellis, J.A. (1994) *Knowledge taught in school: What is remembered*? SAGE Journals, Vol 64, Issue 2.

Smet, H.D., Schreurs, B., & Leysen, J. (2015). *The Response Phase of the Disaster Management Life Cycle Revisited Within the Context of "Disasters Out of the Box"*. Homeland Security and Emergency Management.

Sphere Project (2011). Humanitarian Charter and Minimum Standards in Humanitarian Response. Hobbs the Printers, Hampshire, United Kingdom

Stoddard, A., Harmer, A., & Czwarno, M. (2017). *Behind the attacks: A look at the perpetrators of violence against aid workers*. Aid Worker Security Report 2017 – Humanitarian Outcomes.

Stoddard, A., Haver, K., & Czwarno, M. (2016). *NGOs and Risk: How international humanitarian actors manage uncertainty.* Humanitarian Outcomes.

Tabaklar, T., Halldorsson, A., Kovacs, G., & Spens, K. (2015). *Borrowing theories in humanitarian supply chain management*. Journal of Humanitarian Logistics and Supply Chain Management. Vol 5, Issue 3, pp. 281-299.

Talas, R. (2010). *The Efficient Relationship between Residual Security Risk and Security Investment for Maritime Port Facilities*. Doctoral thesis City University.

Thacker, M. (2017). *Duty of Collaboration: The Changing Personality of NGO Security*. Safe Travels Magazine.

Timmermann, P. (1981). *Vulnerability, Resilience and the Collapse of Society*. Institute of Environmental Studies, University of Toronto, Toronto.

Tabaklar, T. (2015). *The Regression Level of Constructivist Learning Environment Characteristics on Classroom Environment Characteristics Supporting Critical Thinking*. Eurasian Journal of Educational Research, Issue 60, pp. 181-200.

UNDP. (2018). *Standard Operating Procedure for Immediate Crisis Response.* UNDP.

UNDSS. (2006). *Saving Lives Together: A Framework for Improving Security Arrangement Among IGOs, NGOs and UN in the Field*. Office for the Coordination of Humanitarian Affairs.

UNDSS. (2017). *United Nations Security Management System – Security Policy Manual*. UNDSS.

UNDSS. (2020). *SSAFE course advert*. Retrieved from: https://www.unssc.org/courses/safe-and-secure-approaches-field-environments-ssafe-surge-deployment-september/ (accessed 8th February 2021).

UNICEF. (2000). *Standing Operating Procedures for Crisis Management and Emergency Operations.*

United Kingdom Government. (2020). *Government Functional Standard GovS 007: Security*. Government Security Group.

United Nations International Strategy for Disaster Reduction. (2005). *Hyogo Framework for Action 2005– 2015: Building the Resilience of Nations and Communities to Disasters*. Retrieved from: http://www.unisdr.org/files/1037_ hyogoframeworkforactionenglish.pdf (accessed 18th March 2019).

USAID. (2006). *Operational Security – General Information. An Additional Help for ADS Chapter 303*.

USAID. (2012). *USAID Building Resilience to Recurrent Crisis: USAID Policy and Program Guidance*.

USAID. (2018). *Safety and Security Sector Update*. USAID/OFDA Safety and Security Activities.

USAID. (2018). *U.S Agency for International Development Risk Appetite Statement – June 2018*.

Van Maanen, J. (1988). *Tales of the Field: On Writing Ethnography*. University of Chicago Press.

Venton, C.C., & Fitzgibbon. (2012). *Understanding Community Resilience: Findings from Community-Based Resilience Analysis (CoBRA) Assessments*. United Nations Development Programme's Drylands Development Center (UNDP DDC).

Vygotsky, L.S. (1980). *Mind in society: The development of higher psychological processes*. Harvard University Press.

Wainwright, R. (2017). *European Union Terrorism Situation and Trend Report.* European Union Agency for Law Enforcement Cooperation.

Wenger, E. (2017). *Communities of Practice: Learning, Meaning and Identity.* Cambridge University Press.

Wenger, E., & Lave, J. (1991). *Situated learning: legitimate peripheral participation*. Barnes and Noble.

White, L. (2015). *21 years of regulatory innovation through professional standards*. Australian Professional Standards Councils.

Windle, G. (2010). *What is resilience? A review and concept analysis*. Cambridge University Press.

Wright. (1992). *Pluralist theories*. Bloomsbury

Wu, J. (2013). *Hierarchy Theory: An Overview*. ResearchGate.

BIBLIOGRAPHY

Abdallah, M.N. (2011). *Darfur kidnapping victim sues aid group that sent her*. Reuters. Retrieved from: https//www.reuters.com/article/us-newyork-kidnap-idUSTRE74I70A20110519 (accessed 24th March 2019).

AED USAID fraud incident (2011). Retrieved from: http://www.slate.com/articles/news_and_politics/politics/2011/03/contract_killer.html (accessed 24th March 2019).

Al Jazeera (2018). *Why are aid organizations increasingly targeted?* Retrieved from: http://www.aljazeera.com/programmes/insidestory/2018/01/aid-organisations-increasingly-targeted-180125120842862.html (accessed 17th April 2019).

Albawaba News. (2019). *NGOs sued over Litani pollution crackdown*. The Daily Star. Retrieved from: https://www.albawaba.com/news/300-syrians-lebanons-litani-river-are-being-evicted-1275136 (accessed 24th April 2019).

Ammour, L.A. (2012). *New Security Challenges in North Africa after the "Arab Spring"*. GCSP.

Anderson, M. (1996). *Do No Harm: Supporting Local Capacities for Peace through Aid*. Cambridge, MA: The Collaborative for Development Action.

Armstrong, J. (2013). *The Future of Humanitarian Security in Fragile Contexts*. European Interagency Security Forum.

Auletta-Young, C., Maclin, B., Kelly, J., & Cragin, W. (NA). *We Mobilize Ourselves*. Harvard Humanitarian Initiative.

Axe. J. (2010). Darfur kidnapping victim sues aid group that sent her. Reuters. Retrieved from: https://www.reuters.com/article/us-%09newyork-kidnap-idUSTRE74I70A20110519 (accessed 14th June 2019).

Ayre, R. (NA). *The Information Management Challenge: A Briefing on Information Security for Humanitarian Non-Governmental Organisations in the Field*. European Interagency Security Forum.

BBC (2016), *Burkina Faso hotel siege: Like a scene out of a movie*. Retrieved from: https://www.bbc.com/news/world-africa-35333617 (accessed 26th November 2020).

Beam, C. (2011). *Contract Killer.* Slate. Retrieved from: http://www.slate.com/articles/news_and_politics/politics/2011/03/contract_killer.html (accessed 13th June 2019).

Behn, O., & Kingston, M. (2010). *Whose Risk is it Anyway?* European Interagency Security Forum.

Behn, O., Kingston, M., & Singh, I. (2012). *Security Management and Capacity Development, International Agencies Working with Local Partners*. European Interagency Security Forum.

Béné, C., Newsham, A., & Davies, M. (2013). *Making the most of resilience*. IDS In Focus Policy Briefing 32. Retrieved from http://www.ids.ac.uk/publication/making-the-most-of-resilience (accessed 15th August 2019).

Bernstein, B.B. (1999). *Vertical and horizontal discourse: an essay*. British Journal of Sociology of Education. Vol 20, No 2.

Birkmann, J. (2006). *Measuring Vulnerability to Natural Hazards*. United Nations University Press, Paris.

Boin, A., & Byander, F. (2014). *Explaining success and failure in crisis coordination*. Swedish Society. for Anthropology and Geography.

Bosch, D. (2015). *Our Partnership with HEAT Trainings*. Headington Institute.

Brabant, K.V. (1997). *Security and Protection: Beyond Technology*. London, UK: Overseas Development Institute, Relief and Rehabilitation.

Brabant, K.V. (2000). *Operational Security Management in Violent Environments*. ODI.

Brabant, K.V. (2010). *Managing Aid Agency Security in an Evolving World: The Larger Challenge*. European Interagency Security Forum.

Brabant, K.V. (2010). *Operational security management in violent environments, Good Practice Review 8*. Humanitarian Practice Network at OD.

Brabant, K.V. (2012). *Incident Statistics in Aid Worker Safety and Security Management: Using and Producing Them.* European Interagency Security Forum.

Brand, F.S., & Jax, K. (2007). *Focusing the meaning(s) of resilience: resilience as a descriptive concept and a boundary concept*. Ecology and Society.

British Standards Institute. (2018). *Crisis Management – Guidance for developing a strategic capability.*

Brooks, J. (2015). *Humanitarian Under Attack: Tensions, Disparities, and Legal Gaps in Protection.* ATHA White Paper Series.

Brosschot, J.F., Verkuil, B., & Thayer, J.F. (2018). G*eneralized Unsafety Theory of Stress: Unsafe Environments and Conditions, and the Default Stress Response*. International Journal of Environmental Research and Public Health, Vol 15, Issue 3.

Brown, K., & Westaway, E. (2011). *Agency, capacity, and resilience to environmental change: lessons from human development, well-being, and disasters*. Annual Review of Environment and Resource.

Brown, L. (1997). *InterAction/OFDA training pilot – Health in complex humanitarian emergencies, IHL and Humanitarian Principles*. OFDA/InterAction Health Training Task Force, Washington, D.C.

Buth, P. (2017). *Abduction and Kidnap Risk Management*. European Interagency Security Forum.

Buth. P., Bickley, S., Goddin, W., Hughs, H., Wood. P., Kok. W., Quinn, R., Reilly, L., Wagner. M., & Williams. S. (2018). *Managing the Security of Aid Workers with Diverse Profiles*. European Interagency Security Forum.

Carroll, A.B., & Nasi. J (1997). *Understanding Stakeholder Thinking, Themes from a Finnish Conference.* Business Ethics. Vol 6, No 1.

Cederberg, A., & Eronen, P. (2015). *How can Societies be Defended against Hybrid Threats?* Geneva Centre for Security Policy.

Chenoweth, L., & Stehlik, D. (2001). *Building resilient communities: Social work practice and rural Queensland.* Australian Social Work.

Cerna, E.S.D., Ibias Jr., P., & Raymundo, A.M.S. (2019). *Traditional e-Learning vs. Immersive Learning: A Perception Study Among Maritime Students.* IJODeL.

Coles, E., & Buckle, P. (2004). De*veloping community resilience as a foundation for effective disaster recovery*. Australian Journal of Emergency Management. Vol 19, Issue 4.

Community and Regional Resilience Institute (CARRI, 2013*). Definitions of community resilience: an analysis*. Oak Ridge National Laboratory.

Curtis, P., & Carey, M. (2012). *Risk Assessment in Practice*. COSO.

Cutter, S.L., Burton, C.G., & Emrich, C.T. (2010). *Disaster resilience indicators for benchmarking baseline conditions*. Journal of Homeland Security and Emergency Management. Vol 7, Issue 1.

Cutts, M., & Dingle, A. (1995). *Safety First: Protecting NGO Employees who Work in Areas of Conflict*. Save the Children.

Daccord, Y. (2018). *The humanitarian #MeToo crisis: the really hard work is just beginning*. ODI HPN.

Davidson, S., & French, E. (2013). *Family First: Liaison and support during a crisis*. European Interagency Security Forum.

Davis, J. (2015). *Security to go: a risk management toolkit for humanitarian aid agencies*. European Interagency Security Forum.

Davydoff, D. (2019). *Brining Different backgrounds to Your Intelligence Team*. ASIS, Security Magazine.

Dell'Amico, M., & Good, J. (2009). *Security Risk Management*. UNHCR.

DeLoach, J. & Thomson, J. (2019). *Improving Organizational Performance and Governance*. COSO.

Dilley, M et al. (2005). *Natural Disaster Hotspots A Global Risk Analysis*. Disaster Risk Management Series No 5. World Bank.

Dworken, J.T. (2014). *Vulnerability Assessment Training Module for NGOs Operating in Conflict Zones and High-Crime Areas*. OFDA/InterAction PVO Security Task Force.

Ebbinghaus, H. (1885). *Memory. A Contribution to Experimental Psychology*. Teachers College, Columbia University. New York City.

ECHO (2006) *NGO Security Collaboration Guide*. European Commission: Humanitarian Aid.

Edge, S. (2013). *Office Closure*. European Interagency Security Forum.

Edwards, S. (2018). *Sexual assault and harassment in the aid sector: Survivor stories*. Inside Development.

European Union Agency for Law Enforcement (2017). *European Union terrorism Situation and Trend Report: 2017*.

Fairbanks, A. (2018). *Duty of Care under Swiss law – How to improve your safety and security risk management processes*. European Interagency Security Forum.

Fairbanks, A., Marron, E., Reilly. L., & Weerden. M.V. (2019). *Managing Sexual Violence against Aid Workers: prevention, preparedness, response and aftercare*. European Interagency Security Forum.

Fast, L., Rowley, E., O'Neill, M., & Freeman, F. (2011). *The Promise of Acceptance*. Save the Children.

Field, C.B., et al. (2012). *Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation: A Special Report of Working Groups I and II of the IPCC*. Cambridge University Press, Cambridge and New York, NY.

Field, C.B., V. Barros, T.F. Stocker, D. Qin, D.J. Dokken, K.L. Ebi, M.D. Mastrandrea, K.J. Mach, G.-K. Plattner, S.K. Allen, M. Tignor, and P.M. Midgley (Eds.) (2012). *Managing the risks of Extreme Events and Disasters to Advance climate Change Adaptation.* Cambridge University Press. Retrieved from: https://www.ipcc.ch/report/managing-the-risks-of-extreme-events-and-disasters-to-advance-climate-change-adaptation/ (accessed 14th June 2019).

Finucane, C. (2013). *Security Audits*. European Interagency Security Forum.

Finucane, C. and Kingston, M. (2009). *Humanitarian Risk Initiatives: Index Report December 2009*. European Interagency Security Forum.

Fisher, D. (2015). *Drummond sues NGO & others for accusing firm of collaborating with Colombian paramilitaries; intl. NGOs issue statement*. Business & Human Rights Recourse Centre.

Foucault, M. (1997). *Discipline and punish*. London: Penguin.

Garrett, C. (2004). *Developing A Security-Awareness Culture-Improving Security Decision Making*. SANS Institute.

Garrett, C. (2005). *Developing A Security-Awareness Culture-Improving Security Decision Making*. SANS Institute.

Glaser, B.G., & Strauss, A.L. (1967). T*he Discovery of the Grounded Theory: Strategies for Qualitative Research*: Barnes and Nobel.

Glaser, M.P. (2011). *Engaging Private Security Providers*. European Interagency Security Forum.

Goffman, E. (1963). *Stigma: Notes on the Management of Spoiled Identity*: Harmondsworth: Penguin.

Gonsalves, A. (2015). *Applying Serious Gaming to Humanitarian Security, A Framework For Mixed-Reality Training*. European Interagency Security Forum.

Greenaway, S. & Harris, A. (1998). *Humanitarian Security: Challenges and Responses*. Harvard University. Cambridge USA.

Gronlund, T. & Sjostedt, P. (2016). *The Military Instructor's Handbook.* Royal Danish Defense College.

Guha-Sapir, D., Hargitt, D., & Hoyois, P. (2004). *Thirty Years of Natural Disasters 1974-2003: The Numbers*: Center for Research on the Epidemiology of Disasters, UCL Presses Universitaires De Louvain.

Haavisto, I. & Kovacs, G. (2014). *Perspectives on Sustainability in Humanitarian Supply Chains*. Emerald Insight. Journal of Humanitarian Logistics and Supply Chain Management. Vol 1 Issue: 1, pp. 5-14.

Handmer, J.W., & Dovers, S.R. (1996). *A typology of resilience: rethinking institutions for sustainable development*. *Organization and Environment*. SAGE Journals, Vol 9, Issue 4.

Harmer, A. (2010). *A decade on: a new Good Practice Review on operational security management.* Retrieved from http://odihpn.org/magazine/a-decade-on-a-new-good-practice-review-on-operational-security-management

Hodgson, L. (2014). *Security Risk Management and Religion: Faith and Secularism in Humanitarian Assistance*. European Interagency Security Forum.

Horobin, D. (2019). *Critical Incident Management*. GCSP.

Humanitarian Outcomes (2016). *NGO Risk Management Principles and Promising Practice Handbook.* Retrieved from: https://www.interaction.org/documents/ngo-risk-management-principles-and-promising-practice-handbook/ (accessed 14th June 2019).

Igoe, M. (2019). *USAID mulls proposal to train aid workers as special forces*. Devex. Retrieved from: https://www.devex.com/news/usaid-mulls-proposal-to-train-aid-workers-as-special-forces-94321 (accessed 15th June 2019).

International Federation of Red Cross and Red Crescent Societies. (2008). *A Framework for Community Safety and Resilience: In the Face of Disaster Risk.* IFRC, Geneva.

International Red Cross and Red Crescent Societies and ICRC. (NA). *Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief*. Retrieved from: https://www.icrc.org/en/doc/assets/files/publications/icrc-002-1067.pdf (accessed 17th August 2019).

IRD and USAID fines over serious misconduct. Retrieved from :https://www.washingtonpost.com/investigations/usaid-suspends-ird-its-largest-nonprofit-contractor-in-iraq-and-afghanistan/2015/01/26/0cafe16a-a599-11e4-a2b2-776095f393b2_story.html (accessed 3rd June 2019).

Irish Aid. (NA). *Irish Aid Guidelines for NGO Professional Safety & Security Risk Management*. Retrieved from: https://www.irishaid.ie/media/irishaid/allwebsitemedia/20newsandpublications/irish-aid-guidelines-for-ngo-professional-safety-and-security-risk-management.pdf (accessed 1st September 2019).

Jamjoom, M. (2018). *Why are aid organization increasingly targeted*? Al Jazeera News. Retrieved from: http://www.aljazeera.com/programmes/insidestory/2018/01/aid-organisations-increasingly-targeted-180125120842862.html (accessed 14th August 2020)

Johns, K. (2012). *Disaster Assistance Improvement Program (DAIP)*. U.S. Department of Homeland Security.

Johnson, K. (2019). *Pilot Study of Humanitarian e-Learning shows promising signs of performance improvements and impact*. Humanitarian U, Humanitarian Leadership Academy, and MEDAIR.

Kolb, D. (1984). *Reflective Model*. Retrieved from: https://study.cardiffmet.ac.uk/AcSkills/Documents/Guides/AS_Guide_Reflective_writing_Kolb.pdf (accessed 14th June 2020).

Kolb, D. (2000). *Learning Styles and Experiential Learning Model*. Retrieved from: http://nwlink.com/~donclark/hrd/styles/kolb.html (accessed 14th June 2020).

Koons, A. (2016). *Why is There a Humanitarian and Development Divide*? The University of Texas at Austin.

Kowalski, M., & Vaught, C. (2020). *Judgement and decision-making under stress: An overview for emergency managers*. National Institute for Occupational Safety and Health: Pittsburg Research Laboratory.

Kumar, M. (2017). *Digital Security of LGBTQI Aid Workers: Awareness and Response*. European Interagency Security Forum.

Lave, J. (1988). *Cognition in practice: mind, mathematics and culture in everyday life*. Cambridge University Press.

Llorente, R.V. and Wall, I. (2016). *Communications Technology and Humanitarian Delivery – Challenges and Opportunities for Security Risk Management*. European Interagency Security Forum.

Lockton. (2015.) *Duty of Care: Protecting Traveling Employees.* Retrieved from: https://www.lockton.com/whitepapers/Duty_of_Care.pdf (accessed 14th May 2019).

Lomborg, B (2013). *How Much Have Global Problems Cost the World?: A Scorecard from 1900 to 2050*. Cambridge University Press.

Macrae, J. and Zwi, A. (1994). *War and Hunger: Rethinking International Responses to Complex Emergencies.* London, UK: Zed Books

Mallak, L. (1998). *Resilience in the Healthcare Industry*. Paper presented at the Seventh Annual Engineering Research Conference, Banff, Alberta, Canada.

Maslow, A.H. (1942). *The Dynamics of Psychological Security-Insecurity*. Journal of Personality. Vol. 10, Issue 4, pp. 331-334.

McKay, L. (2011). *Building Resilient Managers in Humanitarian Organizations: Strengthening Key Organizational Structures and Personal Skills that Promote Resilience in Challenging.* People in Aid.

Menier, M. (2017). *Security Incident Information Management Handbook*. RedR UK, Insecurity Insight, European Interagency Security Forum.

Merkelbach, M. (2017). *Voluntary Guidelines on the Duty of Care to Seconded Civilian Personnel*. Swiss Federal Department of Foreign Affairs, Stabilisation Unit and Center for International Peace Operations.

Merkelbach, M., & Kemp, E. (2016). *Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications*. European Interagency Security Forum.

Merton, R. (1949). *On Sociological Theories of the Middle Range*. The Free Press.

Merton, R. (1967). *On Social Structure and Science*: The University of Chicago Press, Chicago and London.

Miller, F. et al. (2010). *Resilience and vulnerability: complementary or conflicting concepts?*. Ecology and Society.

Mills, C.M. (1959). *The Sociological Imagination*: Oxford University Press.

Mwaiwa, F.M. and Odiyo, W.O. (2015). *The Role of Disaster Preparedness on business Continuity Management for Corporate Organisations: A Case of Equitol Bank, Kenya*. International Journal of Managerial Studies and Research.

North, C.S et al. (1999). *Psychiatric disorders among survivors of the Oklahoma City bombing*. Journal of the American Medical Association. Vol 282, No 8, pp 709-806.

OCHA. (2014). *Global Humanitarian Overview, Status Report*. OCHA. Retrieved from: https://www.unocha.org/sites/unocha/files/Global%20Humanitarian%20Overview%20Final%2022%20Aug%202014.pdf (accessed 23rd September 2019).

Olson, A., Anderson, J. (2016). *Resiliency scoring for business continuity plans*. Journal of Business Continuity & Emergency Planning. Volume 10, No 1.

Oscar, N. (1972). *Defensible Space: crime prevention through urban design*. Macmillan, New York.

Page, S. and Lewer, N. (2015). *Duty of Care: Protecting Traveling Employees*. Lockton Companies. Retrieved from: https://www.lockton.com/whitepapers/Duty_of_Care.pdf (accessed 3rd October 2019).

Palacios, G.D. (2018). *Managing security-related information: a closer look at incident reporting systems and software*. European Interagency Security Forum.

Parker, B. (2019). *Oxfam faces $160 million legal threat over Palestine aid project*. The New Humanitarian.

Paton, D., & Johnston, D. (2001). *Disasters and communities: vulnerability, resilience, and preparedness*. Disaster Prevention and Management.

Paul, R., & Thompson, C. (2006). *Employee assistance program responses to large scale traumatic events: lessons learned and future opportunities*. Journal of Workplace Behavioral Health. Retrieved from: https://www.tandfonline.com/doi/pdf/10.1080/15555240.2020.1821206?needAccess=true (accessed 29th July 2019).

Pelling, M. (2011). *Adaptation to Climate Change. From Resilience to Transformation*. Routledge.

Persaud, C. (2012). *Gender and Security – Guidelines for Mainstreaming Gender in Security RiskManagement*. European Interagency Security Forum.

Polanyi, M. (1967). *The Tacit Dimension*. The University of Chicago Press.

Prendergast, J. (1996). *Frontline Diplomacy: Humanitarian Aid and Conflict in Africa*. Lynne Rienner Publishers

Presant, D., Farrington, A., and Henderson, S. (2019). *Supporting and Strengthening Humanitarians Everywhere.* HPass.

Rayment, B., & Sanders, D. (2015). *21 Years of Regulating Innovation Through Professional Standards.* Australian Professional Standards Councils.

Relief Web. (2020). *Aid Security and COVID-19*. Retrieved from: https://reliefweb.int/report/world/aid-security-and-covid-19-bulletin-5-6-may-2020 (accessed 14th July 2019).

Richards, B.A. & Frankland, P.W. (2017). *The Persistence and Transience of Memory*. PubMed.gov. Retrieved from: https://pubmed.ncbi.nlm.nih.gov/28641107/ (accessed 14th July 2019).

Ripley, A (2008). *The Unthinkable: Who Survives When Disaster Strikes—and Why.* Three Rivers Press. NY.

Shafer. J. (2015). *Interaction and the MOSS*. Retrieved from: https://www.interaction.org/document/interaction-minimum-operating-security- standards-and-suggested-guidance-language (accessed 9th June 2019).

Schafer, J., & Murphy, P. (2006). *Security Collaboration, Best Practices Guide*. InterAction.

Schein, E. (1996). *Organizational Culture and Leadership*, 3rd edn. Jossey-Bass.

Schmidt, M. (1997). *Recommendations for Improving the Security of Humanitarian Workers*. International Review of the Red Cross.

Schroder, H.M. (1989). *Managerial Competence and Style*. JSTOR. Vol 15, No 4, pp. 713-715.

Scott, E.K.M. (2019). *Yes, aid workers are getting killed more often. But why?* The Washington Post.

Scott et al. (2004). *Professional doctorates: integrating professional and academic knowledge*. Maidenhead: Society for Research in Higher Education and Open University Press.

Secretary General. (2016). *Report of the open-ended intergovernmental expert working group on indicators and terminology relating to disaster risk reduction*. United Nations General Assembly.

Sidebotham, T.L. (2017). *The Blood of the Martyrs and Legal Liability*. Telios Law PLLC.

Source 8. (2015). *Office Opening – A Guide for Non-Government Organisations*. European Interagency Security Forum.

Stoddard, A. (2003). *Humanitarian NGOs, Challenges and Trends*. Humanitarian Policy Group.

Stoddard, A., Harmer, A., Czwarno, M. (2017). *Behind the attacks: A look at the perpetrators of violence against aid workers*. Humanitarian Outcomes.

Stoddard, A., Harmer, A., & DiDomenico, V. (2009). *Providing aid in insecure environments: Update Trends in violence against aid workers and the operational response*: HPG Policy Brief, 34. Retrieved from: http://www.odi.org.uk/resources/download/3250.pdf (accessed 15th June 2019).

Stoddard, A. Harmer, A., and Ryou, K. (2014). *Unsafe Passage: Road attacks and their impact onhumanitarian operations*. Humanitarian Outcomes.

Swords, S. (2006). *Emergency Capacity Building Project Staff Capacity Initiative*. Humanitarian Competencies Study.

Tatham, P., Wu, Y., Kovacs, G., and Butcher, T. (2017). *Supply chain management skills to sense and seize opportunities*. Emerald Insight.

Technical Committee CEN-TC 391. (2018). *Crisis Management – Guidance for Developing A Strategic Capability.* British Standards Institute.

Terada, Y. (2017). *Why Students Forget – and What You Can Do About It*. Edutopia.

Tiedemann-Nkabinde, R. and Davydoff, D. (2019). *Why Reputational Risk is a Security Risk and What to Do About It*. Security Solutions for Enabling and Assuming Business.

Teitelbaum, P. (2019). *Pilot evaluation to assess the impact of elearning on humanitarian aid work – Final Report.* Humanitarian U. Retrieved from: file:///C:/Users/MBlyth/Downloads/HU_Pilot_Study_Report_web-version.pdf (accessed 14th June 2020).

Twigg, J. (2009). *Characteristics of a disaster resilience community: a guidance note, version 2*. DFID Disaster Risk Reduction Interagency Coordination Group. Retrieved from: http://www.abuhc.org/Publications/ CDRC%20v2%20final.pdf (accessed 8th September 2019).

UNCHR eCentre. (2009). *Security Risk Management, Learning Module*. UNHCR.

UNDSS. (2020). *SSAFE course advert*. Retrieved from: https://www.unssc.org/courses/safe-and-secure-approaches-field-environments-ssafe-surge-deployment-september/ (accessed 10th July 2020).

United Nations CTED. (2020). *The impact of the COVID-19 pandemic on terrorism, counter-terrorism and countering violent extremis*. United Nations Security Council publication.

United Nations International Strategy for Disaster Reduction. (2012). *Towards a Post-2015 Framework for Disaster Risk Reduction*. Retrieved from: http://www.preventionweb.net/files/25129_towardsapost2015frameworkfordisaste.pdf (accessed 18th July 2019).

United Nations International Strategy for Disaster Reduction. (2017). *Disaster terminology*. Retrieved from: https://www.unisdr.org/we/inform/terminology (accessed 18th May 2019).

United Nations. (2006). *United Nations Field Security Handbook*: UNDSS. Retrieved from http://psm.du.edu/media/documents/international_regulation/united_nations/other/un_field_security_handbook.pdf (accessed 12th June 2019).

UNSECOORD, UNICEF, WFP, UNHCR, and UNDHA. (1997). *Presentation to the Humanitarian Liaison Working Group.* Mimeo, Geneva.

USAID. (2018). *U.S. Agency for International Development Risk Appetite Statement – June 2018*.

USAID. (2019). *What We Do – Safety and Security*. USAID. Retrieved from: https://www.usaid.gov/what-we-do/working-crises-and-conflict/responding-times-crisis/how-we-do-it/humanitarian-sectors/safety-and-security (accessed 4th June 2019).

USAID. (2019). Section H of a subcontract award. (RSM PLSO Nigeria contract – confidential).

U.S. Department of Homeland Security. (2012). *Disaster Assistance Improvement Program (DAIP)*. Retrieved from:

https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_fema_daip_20121116.pdf (accessed 14th January 2021).

Vineburgh, NT. (2004). *The power of the pink ribbon: raising awareness of the mental health implications of terrorism*. Journal of Psychiatry. Vol. 67, Issue 2.

Viravaidya, M., & Hayssen, J. (2001). *Strategies to Strengthen NGO Capacity in Resource Mobilization Through Business Activities*. PDA and UNAIDS Joint Publication.

Wildavsky, A. (1991). *Searching for Safety.* Transaction, New Brunswick NJ.

Wolcott, H.F. (1999). *Ethnography: A Way of Seeing*. AltaMira Press.

Yang, T., & Che, H. (2017). *Quantum Mechanics and Multi-World Interpretation – A Dialogue between a Cat and Everett*. Scientific Research Publishing.

Yin, R. (1994). *Case Study Research: Design and Methods*. 2nd Ed., SAGE Publications.

Young. H. (2015). *Steve Dennis and the court case that sent waves through the aid industry*. Guardian. Retrieved from: https://www.theguardian.com/global-development-professionals-network/2015/dec/05/steve-dennis-court-case-waves-aid-industry (accessed 24th July 2019).

ZeeNews. (2020). *Kenya arrests aid workers for wooden rifles training exercise*. Available at: https://zeenews.india.com/news/world/kenya-arrests-aid-workers-for-wooden-rifles-training-exercise_1612285.html (accessed 15th April 2020).

Zumkehr, H.J., and Finucane, C. (2013). *The Cost of Security Risk Management for NGOs*. European Interagency Security Forum.

Zutphin, T.V., and Damerell, J. (2011). *Humanitarian Charter and Minimum Standards in Humanitarian Response.* The Sphere Project.

APPENDIX 1: PARTICIPANT ONLINE-SURVEY

Dear Potential Participant,

I would like to invite you to participate in a research study related to international business resiliency and continuity management. This study is part of an academic program focusing on international security and risk management.

> **Study Title:** Determining the foundation for business resiliency success against the common shortfalls and vulnerabilities found at the organizational level.

Why have you been invited to participate

You have been selected as a participant based on your international experience relating to safety, security, business resiliency, continuity and recovery, and risk and emergency management, and your ability to comment (from a leadership perspective), on business resiliency and continuity management needs, and how different international organizations address these needs in a dynamic and increasingly dangerious world.

The purpose of the study

This project will form part of my doctoral program to meet 'research' requirements and will be used purely for educational purposes. The data in the research cannot be used for performance, business or human resource purposes. This research is owned concurrently by both the researcher (Mike Blyth), as well as Portsmouth University.

The purpose of this survey is to explore the level and manner by which risk, resiliency and business continuity is incorporated into how organizations manage all forms of risk, and what strengths or weaknesses participant's see within organizational and sector approaches to ensuring the protection of people, business interests, operational activities, facilities and assets, information, stakeholder needs and reputation.

Do you have to take part

If you wish to participate then it would be greatly appreciated if you could the *Survey Form* which can be returned with ***no personal information included*** on it. This can be sent via email to either up840253@myport.ac.uk or alternatively to mike.blyth@rsmconsulting.us at your earliest convenience. This survey will also be available through the following online link: https://portsmouth.onlinesurveys.ac.uk/michael-blyth-business-resiliency-survey

A Consent Form is included – ***it is very important that this is also completed and returned to me*** **s**o that the data you provide can be used for this study.

If you do not wish to participate then you do not need to respond to this letter. Participation within this study is purely elective and fully I understand that for various reasons participation may prove problematic for you.

Will your taking part in the study be kept confidential

Your participation in this study, and any information provided will be considered 'confidential' and will be used ONLY as part of this academic study. No information you provide will be attributed to you or your organization.

The University of Portsmouth will not know the identity of those who send in completed surveys.

The information you provide will be retained within a password protected and an encrypted laptop (Symantec Endpoint Encryption), and any hard copy data will be secured in an industrial grade gun safe and will be shredded once reviewed. All measures possible will be used to ensure that your information is kept anonymous.

> **Important Note:** Research in the University of Portsmouth is looked at by independent group of people, called an Ethics Committee, to protect your interests. This study has been reviewed and given a favourable opinion by the Portsmouth University Ethics Committee. The final study will also be subject to review before being released to ensure the high ethical standards of the Portsmouth University are adhered to.

What will happen if you take part

If you decide to participant then the survey will take anywhere between 15-30mins, depending on how much information you would like to provide in the Survey Form. Within this document is the Survey Form itself (Appendix 1) which provides guidance on how to complete the survey. There is also a Consent Form in Appendix 2 which I would ask that you complete, and if you would like to see the results of the study then you can request this information via email and it will be provided once completed, or you can submit the Request Slip found in Appendix 3.

Specific consent will be requested if published material from the study might directly or indirectly identify you or your organization – care will be taken to ensure that any observations are sanitized and remain completely anonymous.

The study includes the following steps:

1. Identify a pool of participants willing to offer their insights and experiences to the study
2. Send out invitation letters, survey forms and consent forms – or make these available online
3. Review the statistical data, analysing this in the context of organizational business resiliency
4. Review any narrative provided to establish a contextual understanding of the data provided
5. Explore the collective findings, trends and pertinent data and establish an opinion
6. Capture the findings within a written study

You are only requested to submit a written response and will not be asked, for this survey, to participant in interviews.

It is requested that you submit your response within 14 days of the request being made, if this is possible. This will allow for time to be taken to assess the responses and complete the study in time for submission to the University of Portsmouth.

All data received, once assessed, will be stored in a password and encrypted flash-drive, or a locked safe, before being deleted or shredded.

The paper resulting from this study will be presented as part of my doctoral evaluation requirements and may be published; but will not include any information identifying you or your organization, and any data and observations included will be none attributable and anonymous in nature (noting you will be one of approx. 25-50 participates from which data is drawn).

The risks and benefits

The risks associated with participation relate to making statements which could be linked to you or your organization, and which might be considered inappropriate in nature. As such, I would ask that you depersonalize any observations and offer them from a ***career experience*** perspective, rather than necessarily from the perspective of your current employer. I will also ensure that any comments are sanitized and are not attributed to an individual or organization to ensure all aspects of the data provided is confidential and anonymous.

The benefits of participating include receiving the findings of a wide-ranging study, from multiple vantage points, on international business resiliency, continuity and recovery. This may be useful in terms of providing professional insights which might be valuable to you or your organization.

Who is organizing and funding the research

This research is being directly organized (with support from the University of Portsmouth) by the researcher (Mike Blyth) and is self-funded. No other stakeholders or participants are involved in this study.

Asking questions or lodging complaints

You can also contact me on 001 571 242 9044 if you have any questions relating to this research study. If you wish to verify that this study is purely for the purposes of the doctoral program, and that information will be treated with the strictest of confidence then please feel free to contact my tutor (located in the UK) with any questions, or if you have any complaints relating to this survey:

- Name: Dr Alison Wakefield
- Email: alison.wakefield@port.ac.uk
- Phone Number: +44 (0)23 9284 3942

The head of the Portsmouth University Complaints Department can also be contacted if you feel that any aspect of this study has been conducted in an inappropriate manner.

Regardless of whether you are able to support, or not, I thank you for your time and consideration.

Best wishes,

Mike Blyth

Email: mike.blyth@rsmconsulting.us

Mobile: 571-242-9044

Mainline number: 571-719-6950 Ext 301

Skype: michael.blyth2

The Survey Form

Study Title: Determining the foundation for business resiliency success against the common shortfalls and vulnerabilities found at the organizational level.

Name and Contact Details of Researcher

- Name: Mike Blyth
- Email: mike.blyth@rsmconsulting.us (for initial correspondence)
- Email: up840253@myport.ac.uk (for survey response correspondence)
- Phone: 001 571 242 9044 (USA)

Name and Contact Details of Supervisor

- Name: Dr Alison Wakefield
- Email: alison.wakefield@port.ac.uk
- Phone Number: +44 (0)23 9284 3942 (UK)

Invitation

Thank you for reading this. I would like to invite you to take part in my research study by completing this questionnaire. It is entirely up to you whether you participate, but your responses would be valued if you do.

My study is designed to explore the level and manner by which risk, resiliency and business continuity is incorporated into how international organizations manage all forms of risk, and what strengths or weaknesses participants see within their sector's approach to ensuring the protection of people, business interests, operational activities, facilities and assets, information, stakeholder needs and reputation.

You are invited to speak from experience and not necessarily in direct relation to your current employer's resiliency levels, nor their methods for ensuring the protection of people, business, operations, assets and reputation. You are asked to avoid including any privileged or case study specific information which could compromise you, or your organization, in any manner. Rather, you are requested to speak from a wider experiential perspective as a professional within the sector.

You are requested to complete this online if at all possible, using the following link: https://portsmouth.onlinesurveys.ac.uk/michael-blyth-business-resiliency-survey

If this is not possible then you can use the form below to complete the survey.

Your rights in research

- You will remain anonymous throughout this study and no identifying data will be kept on record.
- You have the right to withdraw your response data before 1st July 2017 (after this date, your response data will be collated into the overall dataset for this project and unable to be withdrawn).
- You are welcome to see the results and findings once the research is complete.
- At completion of the study, and when the research findings are published, you are welcome to express your feelings about the research, the researchers and your participation.
- Your anonymised, aggregated data will be kept on file in a secure, encrypted and password protected location.

This survey has been approved by the University of Portsmouth Ethics Department.

I neither need your name nor any identifying details; the questionnaire can be completed anonymously and all reasonable steps will be taken to ensure confidentiality, whether in written format (emailed back) or online. Responses from completed questionnaires will be collated for analysis; once this is complete the original questionnaires will be retained purely for the purposes of my doctoral studies; and once completed, all materials will then be destroyed. Up to this stage, completed questionnaires will be stored electronically within a password protected and encrypted laptop. The University of Portsmouth will not be provided information on the identity of participants to further protect your identity.

If you wish to learn more about the results of the research please complete the slip provided in Appendix 3 of this document; I would be happy to share this with you.

Survey instructions

You are requested to complete as many questions as possible, where you feel you can offer insights and opinions; these will help offer context to the study.

The goal is to draw both qualitative and quantitative data from this survey. You are requested to grade the current measures in place to support a scoring system:

Strongly agree (5) Agree (4) Neither agree or disagree (3)

Disagree (2) Strongly disagree (1)

You are also requested to offer succinct comments against key strengths, weaknesses or general observations behind your scoring to lend context to your evaluation of key areas of organizational resiliency.

Contextual Information

1. Please indicate the role closest to your position title below

Executive		Director		Manager		Consultant	

2. Please indicator the sector in which you work which is closest to yours

NGO		Faith based		Oil and Gas		Security		Media		Government	
IT		Construction		Transport		Consulting		Hospitality		Education	

3. Please indicate whether your experience in domestically based, internationally based, or both

Domestic		International		Both	

4. Please indicate your gender: Male / Female / Transgender
5. Please indicate your years of professional experience: insert here
6. Please indicate any previous government related experience below

Military		Police		Intelligence		Emergency Services		None	

7. Please indicate any academic qualifications you have related to business continuity management, risk or security management:

Professional Doctorate		Masters' Degree		Bachelor's Degree	
PHD		MBA		Diploma	
No related academic qualifications					

8. Please indicate any non-academic industry or sector qualifications you have related to business continuity management, risk or security management:

ISO Standards		ILM		Skills for Security	
ASIS		CSMP		No related professional qualifications	

Please include other standards used here: insert comments

Question 9: Organizational Resiliency Levels

The concept of resiliency means different things to different people and organizations. The ability for organizations to resource required resiliency levels can also be challenging, leading to potentially known and accepted vulnerabilities. From your experience please grade and comment on the following statement.

A. Organizations are highly resilient to human-made and natural threats.
Grading: Insert grade here

Observations: Insert comments here

Question 10: Application of Recognized Standards

Understanding and working towards recognized standards arguably indicates that organizations are aware of, and seeking to meet, best in class standards as part of their strategy for managing organizational risks. From your experience please grade and comment on the following statements.

A. Organizations fully understand and are compliant with ISO standards associated with Enterprise Risk Management, Business Continuity Management Systems, and ICT DR resiliency; or use comparable standards.
Grading: Insert grade here

Observations: Insert comments here

B. Organizations see value in seeking to be aligned with, or certified to, recognized standards.
Grading: Insert grade here

Observations: Insert comments here

C. Organizations see value in key representatives for risk and business continuity management having qualifications or certifications in associated and recognized educational programs.
Grading: Insert grade here

Observations: Insert comments here

Question 11: Document Structuring, Depth and Application

Documents are the repository of institutional knowledge, experience and best practice; codifying knowledge, standards, structures and processes. Arguably they form the bedrock of effective and consistent risk management and business resiliency strategies. From your experience please grade and comment on the following statements.

A. Organizations have an overarching document bringing together all organizational risk and resiliency needs.
Grading: Insert grade here

Observations: Insert comments here

B. Documents effectively address the need to establish context for knowledge led decision making.
Grading: Insert grade here

Observations: Insert comments here

C. Organizational management structures and roles and responsibilities are clearly defined in documents.
Grading: Insert grade here

Observations: Insert comments here

D. Organizational documents address preparedness and prevention, response and management, and transition and recovery requirements effectively.
Grading: Insert grade here

Observations: Insert comments here

E. Organizational documents typically bring together stakeholder needs, functions and activities.
Grading: Insert grade here

Observations: Insert comments here

F. Documents typically address ALL FORMS of risk effectively.

Grading: Insert grade here

Observations: Insert comments here

G. Documents are typically clearly owned, and are maintained effectively.
Grading: Insert grade here

Observations: Insert comments here

H. Documents are repetitively used or applied in a consistently structured and applied manner.
Grading: Insert grade here

Observations: Insert comments here

Question 12: Integration of Risk and Resiliency Measures

The integration of risk and resiliency strategies brings together internal and external stakeholders to ensure stakeholder and transdisciplinary needs, influences and activities work collaboratively to support a unified outcome. From your experience please grade and comment on the following questions.

A. Organizations seek to integrate risk management across different organizational functional areas.
Grading: Insert grade here

Observations: Insert comments here

B. Risk management is included in business planning from the outset.
Grading: Insert grade here

Observations: Insert comments here

C. Risk management is included at the point where new activities or programs are initiated.
Grading: Insert grade here

Observations: Insert comments here

D. The response to a crisis is integrated effectively with governmental, community, peer and other stakeholders.

Grading: Insert grade here

Observations: Insert comments here

Question 13: The Importance of Training, Exercising and Testing

Building knowledge and ensuring that this is translated into effective action operationalizes risk and resiliency management, and systems are only as good as the practitioners who apply them. From your experience please grade and comment on the following statements.

A. Organizations place great importance in raising the knowledge and skill of executive leadership on resiliency and continuity management.

Grading: Insert grade here

Observations: Insert comments here

B. Organizations place great importance in identifying and supporting a lead or champion on risk and resiliency responsibilities.

Grading: Insert grade here

Observations: Insert comments here

C. Organizations place great importance on designating, educating and supporting departmental representatives on risk and resiliency management.

Grading: Insert grade here

Observations: Insert comments here

D. Organizations place great importance on building the knowledge, skill and confidence of the broader staff population of risk management at a personal level.

Grading: Insert grade here

Observations: Insert comments here

Thank you for completing the questionnaire.

If you have any concerns regarding this research please contact me or my supervisor in the first instance.

If you are not entirely happy with a response, please contact the Portsmouth University ***Complaints Officer.***

If you are not completing this online then please return through the following email: up840253@myport.ac.uk

APPENDIX 2: SEMI-STRUCTURED INTERVIEWS

Thank you again for agreeing to participant in this interview. The interview will last between 30 to 45mins. I would like to reconfirm that you consent to participating and using any observations for my doctoral thesis – and possible academic journal and professional magazine articles.

Please let me know if you do NOT want the data from this interview used for any one of these three purposes.

I would like to remind you that you can withdraw your data within 3 months of this interview. After that point the information will be used within my thesis and potentially for academic and magazine articles. During this interview please do not mention your name - your employer - Name any organization which might place you, or them, at business, liability or reputational risk. Your inputs will be anonymous.

All information provided today will be kept in the utmost confidence. Your name will not be listed on any recordings, and these recordings and transcripts will be held separate of a name to code list. These will be stored in a security envelop, with a security seal, and in a safe.

A transcript of this interview will be provided to you as well – you are free to redact sections of the transcript before the data is used within a period of 3 months. Or, you can tell me to strike any comments during the interview itself.

The objective of this interview is to explore your personal experiences and to draw upon your professional observations. As such, I will only seek to ask confirmatory questions, or to seek further insights into the main thematic areas of the research. The goal is for you to speak for the majority of the interview period.

My goal is a positive and action-based outcome which provides tangible and effective contributions to strengthening organizational resiliency within the sector. Ideally, the findings will add to the research available for the broader community and may assist the sector at large.

Do you have any questions at this time?

Ok, I will now present a series of questions and appreciate your candid observations – please do ask me if any question is unclear:

1. What do you believe are the current and emergent risks, and their impacts, the sector faces in terms of: People – Business – Operations - Assets and facilities – Information - Reputation

2. From your experience can you explain how well, or badly, risk management and business resiliency is incorporated into organizational leadership structures, including: At the headquarters level - Within organizational core functions - At the field or location level

3. Can you explain what importance, or lack of importance, is placed on security or risk practitioners within organizations?

4. Can you explain what mechanisms exist to support those entering into the security risk management field from a primary career?

5. What strengths and weaknesses are associated with a professional coming from a military, police or government background, compared to those coming in with an academic or civilian background?

6. Can you explain to what extent are recognized standards applied to manage risk, and your professional opinion of these standards as they relate to the sector, including: The MOSS - The

acceptance model - ISO standards on business continuity and emergency management - Other standards

7. Can you explain how knowledge and practice is effectively, or ineffectively, operationalized and implemented through credible training for: Security and risk practitioners - The executive leadership team - Core functions - including HR, finance, legal, programs, communications etc - Field or locational leadership teams, including security and safety focal points - Individuals - including international and local, fellows, consultants and volunteers - Support staff - such as drivers / guards etc - Vulnerable groups (such as women and the LGBTQIA community)

8. Can you offer solutions which might reduce risks and vulnerabilities within the sector?

9. Do you have any other observations or recommendations you would like to make?

APPENDIX 3: FOCUS GROUP QUESTIONNAIRE

Thank you for offering to participate in "Competency Framework" Focus Group study.

A Competency Framework aligns educational programs and job performance exceptions to standards. Please offer your professional observations and experiences on competency frameworks as they relate to:

1) the value and importance of the competency framework.

2) problems you have seen with establishing or implementing competency frameworks.

3) successes you have seen in establishing and implementing competency frameworks.

Please return your observations no later than the 10th June 2020.

Any comments you offer will remain anonymous and may be used for subsequent publications [articles/reports].

With your permission, we would like to name you as a contributor to this important study within further articles and publications. You will not be named within the thesis paper. .

APPENDIX 4: THESIS ETHICAL SUBMISSION

Application for Ethics Review – Staff and Postgraduate Students

1. Study Title and Key Dates

1.1 Title
EVALUATING HUMANITARIAN AID AND DEVELOPMENT SECTOR RESILIENCE: FINDING SOLUTIONS TO COMPLEX PROBLEMS
1.2 Key Dates
Date of original submission to ethics committee: 5th October 2018 Version number of original submission: 1.1 Ethics Committee Reference Number: xxx Intended Start Date of Data Collection: 30th November 2018 Expected Finish Date of Data Collection: 1st July 2019 *When resubmitting an updated application (e.g. in response to ethical review, or an application for substantial amendment):* Date of resubmission to ethics committee: xxx Version number of resubmitted documents: xxx

2. Applicant Details

2.1 Principal Investigator	
Name: Michael Blyth	Title /Role /Course of study: DSyRM
Department: Institute of Criminal Justice Studies	Faculty: ICJS
Telephone: 001 571 242 9044	Email: mike.blyth@rsmconsulting.us

Has the principal investigator attended the graduate school (for students) or researcher development programme (for staff) research ethics training session?	Yes as part of 2017 ART assignment class-based sessions
2.2 Supervisor (if Principal Investigator is a student)	
Name: Dr Risto Talas Title /Role: Lecturer in Security Risk Management Department: Institute of Criminal Justice Studies Faculty: ICJS Telephone: +44 (0)7979 852086 Email: risto.talas@port.ac.uk	
Has the supervisor attended the researcher development programme research ethics training session?	Yes
2.3 Others involved in the work/research including students and/or external collaborators (name, organisation/course, role in the project)	
None.	

3. Details of Peer Review

The project has been reviewed by the course lead Alison Wakefield, and my assigned tutor Risto Talas within the Initial Proposal concept. No peer review has been undertaken within my cohort, nor within my practitioner community.

4. Funding Details

The research will be self-funded. No external funding will be used.

5. Sites/Locations

Interviews will be conducted principally in the US and UK at either:

1) Conference rooms or business spaces in hotels.
2) The researcher's work offices.

6. Insurance/indemnity Arrangements

My company (Risk and Strategic Management, Corp) holds the necessary insurance policies related to both liability risks, as well as workers compensation and health coverages. Further personal insurances are also in place. No special insurances are required due to the nature of the research being conducted.

7. Aims and Objectives/Hypothesis

7.1 Aims

The aim of the research is to draw rich contextual data from experts and leaders within the field of resiliency and business continuity management from the humanitarian aid and development sector so as to explore emergent threats to the sector, how organizations view and address risk, whether the current measures are 'fit for purpose', and how the sector might evolve current, or develop new, resiliency practices to better address their current and future vulnerabilities.

7.2 Primary Objective

To assess the fitness for purpose of current resiliency measures within the humanitarian aid and development community, which might then provide action-based outcomes to address existing and future vulnerabilities.

7.3 Secondary Objective(s)

The secondary objectives of this research include qualitative research to determine:

- What influence does a community of risk practitioners have upon sector resiliency?
- To what extent are recognized standards applied to manage risk?
- How is knowledge and practice operationalized through training?
- What solutions might reduce risks and vulnerabilities within the sector?

The answers to these questions will form the basis of determining vulnerabilities and shortfalls within existing risk management practices. These will then offer potential solutions to enhance organizational resiliency as an outcome of action-based research.

8. Study Summary

8.1 Justification/Summary of Study (no more than one side)

The humanitarian aid and development sector has a higher risk profile than many sectors and industries. Members of the sector commonly operate within fragile states or post disaster environments – which have elevated safety and security risk. And, the demand upon the sector is increasing, with predictions suggesting a dramatic rise in disasters and conflict which will lead to an exponential growth in beneficiary needs. With increasing security risks on humanitarian groups, the sector also faces new stresses from increased stakeholder expectations which further heightens risk.

Despite these challenges, no defined risk management community of practice exists within the sector, standards are inconsistently applied, and knowledge and practice are not effectively operationalized through training. This exposes the sector to avoidable and hazardous risk.

Recent impacts to Oxfam originating from ethical misconduct in Haiti, the dissolution of Academy of Education Development[15] due to fraud, the impacts on International Relief and Development[16]

[15] https://slate.com/news-and-politics/2011/03/usaid-aed-suspension-why-did-usaid-suspend-one-of-its-biggest-contractors-without-any-explanation.html

[16] https://www.washingtonpost.com/investigations/usaid-suspends-ird-its-largest-nonprofit-contractor-in-iraq-and-afghanistan/2015/01/26/0cafe16a-a599-11e4-a2b2-776095f393b2_story.html?noredirect=on&utm_term=.e91f26de319f

due to fiscal misconduct, the lawsuits against Samaritan's Purse[17] and the Norwegian Refugee Council[18] for mishandling kidnap situations all illustrate historic disruptions to the success and the very survivability of other sector groups - suggesting that the current approach to resiliency (often based on the United Nations Minimum Operating Security Standards approach, or the acceptance model) is flawed.

Research to date has also revealed a gap in the literature, with a focus on operational security risk management, supply chain resiliency, and disaster risk management for the beneficiaries of aid, with little to no study on how the implementers of aid and development programs can establish a resiliency strategy for their organizations.

The aim of this research is to determine how organizations both view and approach organizational resiliency, establishing what gaps and vulnerabilities exist, and why, and how to address these areas of weakness. The output will offer insights into why these gaps exist, offering practical solutions by which humanitarian aid and development organizations, and the community at large, might address them.

8.2 Anticipated *Ethical* Issues

The research approach used and outlined within this ethical application will mitigate the potential for information to be inadvertently disclosed to parties outside of the University of Portsmouth in such a manner as to compromise either the participant, or the organization they represent.

To protect participants anonymity will be ensured at all times. In addition, to protect participants from the inadvertent disclosure of sensitive information participants will not be expected to comment on their current role and organization, nor link any observations or experiences with a specific

[17] https://www.reuters.com/article/us-newyork-kidnap/darfur-kidnapping-victim-sues-aid-group-that-sent-her-idUSTRE74I70A20110519

[18] https://odihpn.org/blog/dennis-vs-norwegian-refugee-council-implications-for-duty-of-care/

organization or function in order to protect the interests of employers and other parties. As such, the observations sought will be more macro level, rather than focusing on a specific event or group.

The questioning included within the research interviews will purposely avoid any specific case studies or examples associated with the participant's employers, as these expose the participant and their organization to elevated risks. As such, the lines of questioning are more general and strategic in nature, removing or mitigating the majority of ethical risks, should information integrity be breached.

The researcher uses password protected and encrypted software for the IT assets used to store and work on any provided data as per the instructions listed in https://library.port.ac.uk/researchdata.html.

The researcher will ensure that responses are treated with the utmost confidence, and that anonymity is established within the research participant pool. Any responses which could indicate the participant source, or the identity of their organization, will be scrubbed of any identifying information, or filtered from the research materials.

8.3 Anticipated other *Risks or Concerns*

Risks to participants: None.

Risks to researchers/ university staff/students: None.

Reputational risks: None.

Security risks: Foreign Office Travel Guidelines will be followed and a full risk assessment will be conducted per Portsmouth University guidelines for any international travel where interviews will be conducted.

8.4 Medical Cover (if applicable)

Medical Information: No additional medical cover required.

a. **Medical Category (1-5)**:

This research will be a Category 5 model.

Category **5** No additional medical cover required.

9. Description of Method/ Protocol

The research will be based on grounded theory with an inductive approach for the gathering and interpreting of the data through semi-structured interviews. The researcher will conduct all interviews using an interview protocol to ensure a consistent approach is adopted.

10. Compliance with Laws, Codes, Guidance, Policies and Procedures

It is not anticipated that the research will breach any local laws, codes, guidance, policies and procedures.

11. Recruitment of Participants

11.1 Who are the Research/ Participant Population?

The participants will be selected through an appropriate organizational Gatekeeper from senior level positions within the humanitarian aid and development sector who hold a direct role within organizational resiliency. Consent will be sought from the employers before interviews will be conducted. The researcher will send the Invite Letter, Information Sheet and Consent Form to those who have been identified as the most suitable participants based on the selection criteria of organizational size, nature, operating regions and risk exposure.

11.2 Inclusion/Exclusion Criteria

Inclusion Criteria. Participants will be selected based on the following:

1. Their seniority (Director or Vice President, head of department or executive).
2. Their experience in role (10 years or more within risk, resiliency or security management).
3. Sector experience of 3 or more years
4. Their geographic experience (supporting operations in 5 or more countries).
5. Specific sector experience (working within the sector for more than 3 years).

Exclusion Criteria. The following characteristics will exclude potential participants:

1. A lack of seniority, reflecting only a tactical or operational level of management.
2. Inexperience in role (less than 10 years or more within risk, resiliency or security management).
3. Sector experience of less than 3 years.
4. Geographic inexperience (supporting operations in less than 5).
5. Limited sector experience (working within the sector for less than 3 years).

11.3 Number of participants (include rationale for sample size)

In order to gain sufficient depth and breadth across humanitarian aid and development groups a number of potential of Gatekeepers have been identified with a view to securing up to 20 interviews. In order to achieve a balanced population geographic diversity and sector focus will also be part of the selection rationale.

11.4 Recruitment Strategy (including details of any anticipated use of a gatekeeper in host organizations to arrange/distribute participant invitations)

Gatekeepers will be sought within identified organizations from the security, legal, human resources or program functional areas so as to identify suitable interviewees. Gatekeepers will be asked to identify, and seek consent from, identified candidates. Once participants confirm their ability (or inability) to participate then a formal invitation letter and supportive documentation will be sent ahead of scheduling an interview – including an Information Sheet and Consent Form.

11.5 Payments, rewards, reimbursements or compensation to participants

None.
11.6 What is the process for gaining *consent* from participants?
The consent process will be conducted in 3 steps: 1. Gatekeepers will confirm their organizational interest in participating and nominating potential candidates for interview. 2. The Invitation Letter, Consent Form and Information Sheet will be sent ahead of the interview to the interviewee for formal consent. This will further articulate the objectives and process of the research and which participants can either sign and return ahead of the interview, or at the time of the interview. 3. At beginning of the interview stage it will be repeated that the participants can withdraw at any time, noting the cut-off point for the withdrawal of data within 3 months of the interview being conducted.
11.7 Has or will consent be gained from other organisations involved (if applicable)?
Not applicable as consent will be gained from organization, as described in 11.6.
11.8 Arrangements for translation of any documentation into another language (if applicable)?
N/A.
11.9 Outline how participants can withdraw consent (if applicable), and how data collected up to this point will be handled. Also stop criteria for specific tests (if applicable)?
Before the interview commences they will be notified that they can withdraw from the interview at any time before 3 months of the interview being conducted. Participants will be notified through the consent form, and at the time of interview, that they can withdraw their data up until the time where data is processed for analysis.
11.10 Outline details of re-consent or debrief (if applicable)?
N/A.

12. Data Management

12.1 Description of data analysis
Data will be analyzed using Bryman's 4 stages of thematic coding by attaching codes to pieces of text within the transcripts. By using indexing, categories, codes and themes to the transcript data it can be disaggregated. This will identify repetitive concepts, key words, major themes and unusual issues from the participant's open-ended responses so as to interpret the responses and their meaning.
12.2 Where and how will data be stored?
The audio recordings and written transcripts will be placed on a password protected flash-drive and will be secured at my office within a locked cabinet.
12.3 Destruction, Retention and Reuse of Data
Data will be retained for a period of 10 years unless the participant notifies the researcher that they withdraw consent before the data is analysed. • **Destruction:** Any paper copies of collected data will be shredded after being analysed. • **Retention:** Please see the data storage (above) process and confidentiality (below) process. • **Reuse:** Analysed data will be reused for future article and journal submissions.
12.4 Personal Data – How will confidentiality be ensured (for instance will anonymisation be used)?
All data from interviews will be anonymized.
12.5 How will organisational data (publically unavailable data) be handled (if applicable)?
N/A.
12.6 How will security sensitive data be handled (if applicable)?
N/A.

13. Publication / Impact / Dissemination Plans

The primary purpose of the research is for the doctoral thesis. However, secondary benefits of the research may include use of the data for journal articles.

14. References

Bryman, A. (2016). *Social Research Methods (5th Edition)*. Oxford University Press.

https://slate.com/news-and-politics/2011/03/usaid-aed-suspension-why-did-usaid-suspend-one-of-its-biggest-contractors-without-any-explanation.html

https://www.washingtonpost.com/investigations/usaid-suspends-ird-its-largest-nonprofit-contractor-in-iraq-and-afghanistan/2015/01/26/0cafe16a-a599-11e4-a2b2-776095f393b2_story.html?noredirect=on&utm_term=.e91f26de319f

https://www.reuters.com/article/us-newyork-kidnap/darfur-kidnapping-victim-sues-aid-group-that-sent-her-idUSTRE74I70A20110519

https://odihpn.org/blog/dennis-vs-norwegian-refugee-council-implications-for-duty-of-care/

15. Appendices

Put N/A in version Number column if necessary		
Document	**Date**	**Version No.**
Application Form	6Nov18	1
Invitation Letter	6Nov18	1

Participant Information Sheet(s) (list if necessary) (SEE INCLUDED APPENDIX)	6Nov18	1
Consent Form(s) (list if necessary) (SEE INCLUDED APPENDIX)	6Nov18	1
Advertisement	NA	NA
Peer / Independent Review	NA	NA
Supervisor Email Confirming Application	NA	NA
Evidence From External Organisation Showing Support	NA	NA
Terms of Reference for Steering / Advisory Group	NA	NA
Survey Instrument	NA	NA
Interview Questions / Topic List	6Nov18	1
Focus Group Questions / Topic List	NA	NA
Focus Group Ground Rules	NA	NA
Script for Oral Consent (SEE INCLUDED APPENDIX)	NA	NA
Questionnaire	NA	NA
Observational Data Collection Form	NA	NA
Risk Assessment Form(s)	NA	NA
Other – please describe	NA	NA

16. Declaration by Principal Investigator and Supervisor (if applicable)

1. The information in this form is accurate to the best of my/our knowledge and belief and I/we take full responsibility for it.
2. I/we undertake to conduct the research/ work in compliance with the University of Portsmouth Ethics Policy, UUK Concordat to Support Research Integrity, the UKRIO Code of Practice and any other guidance I/we have referred to in this application.
3. If the research/ work is given a favourable opinion I/we undertake to adhere to the study protocol, the terms of the full application as approved and any conditions set out by the Ethics Committee in giving its favourable opinion.
4. I/we undertake to notify the Ethics Committee of substantial amendments to the protocol or the terms of the approved application, and to seek a favourable opinion before implementing the amendment.
5. I/we undertake to submit annual progress reports (if the study is of more than a year's duration) setting out the progress of the research/ work, as required by the Ethics Committee.
6. I/we undertake to inform the Ethics Committee when the study is complete and provide a declaration accordingly.
7. I/we am/are aware of my/our responsibility to be up to date and comply with the requirements of the law and relevant guidelines relating to security and confidentiality of personal data, including the need to register, when necessary, with the appropriate Data Protection Officer. I/we understand that I/we am/are not permitted to disclose identifiable data to third parties unless the disclosure has the consent of the data subject.
8. I/we undertake to comply with the University of Portsmouth Data Management Policy.
9. I /we understand that records/data may be subject to inspection by internal and external bodies for audit purposes if required.
10. I/we understand that any personal data in this application will be held by the Ethics Committee, its Administrator and its operational managers and that this will be managed according to the principles established in the Data Protection Act 1998 (and after May 2018, the General Data Protection Regulation).

11. I understand that the information contained in this application, any supporting documentation and all correspondence with the Ethics Committee and its Administrator relating to the application:

- Will be held by the Ethics Committee until at least 10 years after the end of the study
- Will be subject to the provisions of the Freedom of Information Acts and may be disclosed in response to requests made under the Acts except where statutory exemptions apply.
- May be sent by email or other electronic distribution to Ethics Committee members.

12. I/we understand that the favourable opinion of an ethics committee does not grant permission or approval to undertake the research/ work. Management permission or approval must be obtained from any host organisation, including the University of Portsmouth or supervisor, prior to the start of the study.

Principal Investigator: Michael Blyth **Date** 19th September 2018

Supervisor (if applicable): Dr Risto Talas **Date 6 November 2018**

APPENDIX 5: INVITE LETTER

Doctoral Research Invitation Letter

Name and contact details of researcher

- Name: Mike Blyth
- Email: mike.blyth@rsmconsulting.us
- Phone: 001 571 242 9044 (USA)

Name and contact details of supervisor

- Name: Dr Risto Talas
- Email: risto.talas@port.ac.uk
- Telephone: +44 (0)7979 852086

Study Title: Evaluating Humanitarian Aid and Development Sector Resilience: Finding Solutions to Complex Problems

REC Ref No: .....

Dear Potential Participant,

Thank you for reading this. I am doctoral student at the University of Portsmouth studying Security and Risk Management, with a specific focus on the humanitarian aid and development community. As part of my thesis paper I would like to invite you to take part in my thesis research study through a 30 to 45 minute interview. Further details are provided within the attached *Information Sheet* attached to this invite letter.

It is entirely up to you whether you participate, however your involvement would be very much appreciated.

My research is designed to explore the manner by which risk, resiliency and business continuity is incorporated into how the humanitarian aid and development sector manages risks to people, business, operations, facilities and assets, information and reputation. The objective is to identify existing strengths, as well as vulnerabilities and weaknesses. My research intends to offer action-based outcomes (in the form of solutions) from which the community might benefit.

The thematic areas which will be included in the interview will include:

- What current and emergent risks are present against:
  - People
  - Business
  - Operations
  - Assets and facilities
  - Information
  - Reputation

- How is risk management and resiliency incorporated into organizational leadership structures?
  - Headquarters
  - Organizational core functions
  - Field or locations
- What importance is placed on security or risk practitioners within organizations?
- To what extent are recognized standards applied to manage risk, including:
  - The MOSS
  - The acceptance model
  - ISO standards on business continuity and emergency management
  - Other standards

- How is knowledge and practice operationalized and implemented through training for:
  - Security and risk practitioners
  - Executive leadership
  - Core functional areas such as HR, finance, legal, programs, communications etc
  - Field or locational leadership teams, including security and safety focal points
  - Individuals - including international and local, fellows, consultants and volunteers
  - Support staff - drivers / guards etc
  - Vulnerable groups - such as women and the LGBTQIA community

- What solutions might reduce risks and vulnerabilities within the sector?

In order to protect both you and your organization you will be asked NOT to comment directly on your existing employer, nor name any previous employer nor party where a conflict of interest may exist. Rather, you are asked to provide professional and experiential observations in terms of strengths, weaknesses and potential solutions.

If you do agree to participate then you will be provided a ***Consent Form*** which will confirm whether the research can be used for:

- My academic doctoral thesis paper
- Professional or academic journals and magazines

As such, you will be able to select how your observations data is used. In addition, an ***Information Sheet*** is also attached to this invite, which provides further information relating to this research.

YOUR RIGHTS IN RESEARCH

If you are able to support this research then a priority is to ensure that your interests are protected. As such:

- You will remain anonymous throughout this study and no identifying data will be kept on record.
- You have the right to withdraw your response data for a period of 3 months after the interview for the thesis. After this date, your response data will be collated into the overall dataset for this project and unable to be withdrawn from the thesis.
- You are welcome to see the results and findings once the research is complete.
- At completion of the study, and when the research findings are published, you are welcome to express your feelings about the research, the researchers and your participation.
- Your anonymised, aggregated data will be kept on file in a secure, encrypted and password protected location. Any recordings or data will be secured in a security envelope with security seals, and this will be stored in a safe.

This research has been approved by the University of Portsmouth Ethics Department. The University of Portsmouth will NOT be provided information on the identity of participants to further protect your identity.

If you agree to participate then we can coordinate a convenient date and time to meet for the interview.

Yours sincerely,

Michael Blyth

APPENDIX 6: CONSENT FORM

INFORMED CONSENT FORM FOR INTERVIEWS

Title of Project: Evaluating Humanitarian Aid and Development Sector Resilience: Finding Solutions to Complex Problems

Name and Contact Details of Researcher(s): Mike Blyth at mike.blyth@rsmconsulting.us on 001 571 242 9044 (USA)

Name and Contact Details of Supervisor (if relevant): Name: Dr Risto Talas at risto.talas@port.ac.uk on +44 (0)7979 852086 (UK)

University Data Protection Officer: Samantha Hill, +44 023 9284 3642 (UK) or data-protection@port.ac.uk

Ethics Committee Reference Number: xxxx

	Please initial box
1. I confirm that I have read and understood the *Information Sheet* for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.	☐
2. I understand that my participation is voluntary and that I am free to withdraw at any time within 3 months of the interview being conducted, without giving any reason.	☐
3. I understand that data collected during this study will be retained in accordance with the University's data retention policy and *could* also be requested by UK regulatory authorities.	☐
4. I allow for the data I provide to be used for the purposes of the doctoral thesis.	☐
5. I agree to the data I contribute being retained for any future research that has been given a favourable opinion by a Research Ethics Committee for professional journals, magazines or other publications.	☐

6. I understand that I can withdraw consent for my data to be used at any time before analysis starts, or within 3 months of the interview being conducted. ☐

7. I agree for the interview to be recorded. ☐

8. I agree to take part in the above study. ☐

Name of Participant: **Date:** **Signature:**

Name of Person taking Consent: **Date:** **Signature:**

APPENDIX 7: INFORMATION SHEET

PARTICIPANT INFORMATION SHEET

Study Title: Evaluating Humanitarian Aid and Development Sector Resilience: Finding Solutions to Complex Problems

Name and contact details of researcher

- Name: Mike Blyth
- Email: mike.blyth@rsmconsulting.us
- Phone: 001 571 242 9044 (USA)

Name and contact details of supervisor

- Name: Dr Risto Talas
- Email: risto.talas@port.ac.uk
- Telephone: +44 (0)7979 852086

Ethics Committee Reference Number: xxx

1. Invitation

I would like to invite you to take part in my doctoral research study. Joining the study is entirely up to you, before you decide I would like you to understand why the research is being done and what it would involve for you. I will go through this *Information Sheet* with you to help you decide whether or not you would like to take part and answer any questions you may have. I would suggest this should take about 15 minutes. Please feel free to talk to others about the study if you wish, and please do ask if anything is unclear.

As you know, I am a doctoral student at the University of Portsmouth studying Security and Risk Management with a focus on the humanitarian aid and development community. This research will contribute directly to my thesis paper.

2. Study Summary

This study is concerned with risk and resiliency within the humanitarian aid and development sector which is important because the sector not only faces increasing security risks as it seeks to provide support to the beneficiaries of aid and development with challenged communities and operating environments, but also as the sector must concurrently manage risks to its business interests and reputation. I am seeking participants who are directly involved within either security risk management or organizational resiliency and business continuity management within the sector at a senior level, and who have a deep understanding of both the sector and the challenges organizations face when implementing programs internationally.

Participation in the research would require you to attend an interview (at your convenience) and it will take approximately 30-45mins of your time.

3. What is the purpose of the study?

The aim of the research is to contribute to available data on both the existing and emergent risks the sector faces, as well as whether current risk, resiliency and continuity measures are effective and so "fit for purpose". The output of the research is intended to provide action based outcomes, providing pragmatic and actionable measures which might assist organizations (and the sector at large) to better manage their risks, or more effectively respond to complex and interrelated crisis events.

The research will be built upon an initial online survey which you may have participated in, a literary review of available studies and research by others (academic and professional practitioners), and a 30-45min interview with leaders with the field of sector security risk management and organizational resiliency and business continuity (you).

The areas of focus for the research include:

- What new and emergent risks are present against organizations within the sector?
- How is risk management and resiliency incorporated into organizational leadership structures?
- The importance placed on security or risk practitioners within organizations?
- To what extent are recognized standards applied to manage risk?
- How is knowledge and practice operationalized and implemented through training?
- What solutions might reduce risks and vulnerabilities within the sector?

Further depth on these topics is included within the *Invite Letter* to help you better contextualize what the interview is seeking to address.

4. Why have I been invited?

You have been invited to participant based on your:

1. Seniority
2. Maturity in role
3. Geographic experience
4. Specific sector experience

It is felt that these qualities will enrich the context of the research with real-life observations on how organizations view, plan against, address and react to multi-faceted risks. The goal of the research is to interview up to 30 participants from across sector organizations, from which both trends and unique views and experiences can be drawn.

5. Do I have to take part?

No, taking part in this research is entirely voluntary. It is up to you to decide if you want to volunteer for the study. I will describe the study in this *Information Sheet.* If you agree to take part, I will then ask you to sign the attached *Consent Form*. You can either email a copy back, or you can sign one when we meet for the interview.

6. What will happen to me if I take part?

If you agree to participate in the interview then the following steps will occur:

1) We will agree a schedule for when we can meet for the interview.
2) You can either sign and return the Consent Form before we meet, or when we meet.
3) I will give you a verbal briefing before the interview starts, and then will walk through the questions outlined within the Invite Letter – the interview will last no more than 45mins.
4) The interview will be recorded – and a transcript will be made. You will be assigned a code so that your transcript is not attached to your name to protect your anonymity.
5) You can indicate during the interview any comments you wish not to be used.

6) You will be provided a written version of the transcript and you again can indicate comments which you would like to be removed.
7) You will have 3 months to indicate whether you wish to withdraw consent after the interview.
8) Your observations, and the observations of the other participants will be used as the backbone of the doctoral thesis paper.

After this process the collective data may be used for journal and magazine publications – at all times with anonymity being in place. You will have 3 months to withdraw your interview if you change your mind.

7. Expenses and payments

There will be no cost to you regards this research process, nor will payment be made for participation.

8. Anything else I will have to do?

You do not have to do anything ahead of the interview.

9. What data will be collected and / or measurements taken?

The interview will be recorded, with your permission. This will be turned into a transcript so that the information you provide can be better leveraged for research. You will have access to both – at any time. No-one else will have access to the recordings, nor the full transcripts. Nor will recordings or transcripts be linked to you in any way. At no time will your name, nor the name of your organization, be used.

10. What are the possible disadvantages, burdens and risks of taking part?

Aside from the use of your time, there are no disadvantages associated with participating. Your identity will never be revealed within any materials resulting from the interview, and any comments which can be associated with you or your employer will be removed from the transcript.

11. What are the possible advantages or benefits of taking part?

The benefits of participating include: 1) you will have access to the research findings and doctoral thesis, 2) this will both directly and indirectly benefit both your organization as well as the community at large, and 3) this may provide insights which help you implement change within your role and organization.

12. Will my taking part in the study be kept confidential?

The priority of this research is to gather information without in any way compromising participants, nor their organizations. As such:

1) Your interview will be issued a code rather than your name.
2) A single printed code to name sheet will be retained in a secure safe and security envelope separate of your interview recording and printed transcript.
3) Any potential linkages between your interview and you will be 'scrubbed' so that no associations can be draw between you and the research.
4) You can also scrub your interview before any data is used.

Anonymity will be maintained at all times, both during the interview and as the data is used. The data, when made anonymous, may be presented to others at academic conferences, or published as a project report, academic dissertation or in academic journals. Anonymous data, which does not identify you, may be used in future research studies approved by an appropriate research ethics committee.

The raw data, which would identify you, will not be passed to anyone outside the study team without your express written permission.

The raw data will be retained for up to 10 years. When it is no longer required, the data will be disposed of securely (*e.g.* electronic media and paper records / images) destroyed.

13. What will happen if I don't want to carry on with the study?

As a volunteer you can stop any participation at any time during the interview, or you can withdraw from the study at any time within 3 months of the interview being conducted, without giving a reason if you do not wish to. If you do withdraw from a study after some data have been collected you will be asked if you are content for the data collected thus far to be retained and included in the study. If you prefer, the data collected can be destroyed and not included in the study. Once the research has been completed, and the data analysed and used for the doctoral thesis it will not be possible for you to withdraw your data from the study.

14. What if there is a problem?

If you have a query, concern or complaint about any aspect of this study, in the first instance you should contact the researcher(s) if appropriate. There will also be an academic member of staff listed as the supervisor whom you can contact. If there is a complaint and there is a supervisor listed, please contact the Supervisor with details of the complaint. The contact details for both the researcher and any supervisor are detailed on page 1.

If you have a concern about any aspect of this study, you should ask to speak to the researcher or their supervisor, who will do their best to answer your questions. The researcher Michael Blyth can be contacted at mike.blyth@rsmconsulting.us or the supervisor/gatekeeper, Dr Risto Talas can be contacted at Risto.Talas@port.ac.uk If you remain unhappy and wish to complain formally, you can do this by contacting the head of school, at Paul.Norman@port.ac.uk or the ICJS Ethics Committee chair on vasileios.karagiannopoulos@port.ac.uk.

If the complaint remains unresolved, please contact:

The University Complaints Officer

Phone: 023 9284 3642 Email: complaintsadvice@port.ac.uk

15. Who is funding the research?

None of the researchers or study staff will receive any financial reward by conducting this study.

16. Who has reviewed the study?

Research involving human participants is reviewed by an ethics committee to ensure that the dignity and well-being of participants is respected. This study has been reviewed by the Portsmouth University Faculty Ethics Committee and been given favourable ethical opinion.

Thank you for taking time to read this information sheet and for considering volunteering for this research. If you do agree to participate your consent will be sought; please see the accompanying Consent Form. You will then be given a copy of this Information Sheet and your signed consent form, to keep.

Interview Format and Script for Oral Consent

Thank you again for agreeing to participant in this interview. The interview will last between 30 to 45mins.

I would like to reconfirm that you consent to participating and using any observations for:

1. My doctoral thesis
2. Possible academic journal and professional magazine articles

   Please let me know if you do NOT want the data from this interview used for any one of these three purposes.

I would like to remind you that you can withdraw your data within 3 months of this interview. After that point the information will be used within my thesis and potentially for academic and magazine articles.

During this interview please do not:

1. Mention your name
2. Mention the name of your employer
3. Name any organization which might place you, or them, at business, liability or reputational risk

All information provided today will be kept in the utmost confidence. Your name will not be listed on any recordings, and these recordings and transcripts will be held separate of a name to code list. These will be stored in a security envelop, with a security seal, and in a safe.

A transcript of this interview will be provided to you as well – you are free to redact sections of the transcript before the data is used within a period of 3 months. Or, you can tell me to strike any comments during the interview itself.

The objective of this interview is to explore your personal experiences and to draw upon your professional observations. As such, I will only seek to ask confirmatory questions, or to seek further insights into the main thematic areas of the research. The goal is for you to speak for the majority of the interview period.

My goal is a positive and action-based outcome which provides tangible and effective contributions to strengthening organizational resiliency within the sector. Ideally, the findings will add to the research available for the broader community and may assist the sector at large.

Do you have any questions at this time?

Ok, I will now present a series of questions and appreciate your candid observations – please do ask me if any question is unclear:

10. What do you believe are the current and emergent risks, and their impacts, the sector faces in terms of:
    - People
    - Business
    - Operations
    - Assets and facilities
    - Information
    - Reputation

11. From your experience can you explain how well, or badly, risk management and business resiliency is incorporated into organizational leadership structures, including:
    - At the headquarters level
    - Within organizational core functions
    - At the field or location level

12. Can you explain what importance, or lack of importance, is placed on security or risk practitioners within organizations?

13. Can you explain to what extent are recognized standards applied to manage risk, and your professional opinion of these standards as they relate to the sector, including:
    - The MOSS
    - The acceptance model
    - ISO standards on business continuity and emergency management
    - Other standards

14. Can you explain how knowledge and practice is effectively, or ineffectively, operationalized and implemented through credible training for:
    - Security and risk practitioners
    - The executive leadership team
    - Core functions - including HR, finance, legal, programs, communications etc
    - Field or locational leadership teams, including security and safety focal points
    - Individuals - including international and local, fellows, consultants and volunteers
    - Support staff - such as drivers / guards etc
    - Vulnerable groups (such as women and the LGBTQIA community)

15. Can you offer solutions which might reduce risks and vulnerabilities within the sector?

16. Do you have any other observations or recommendations you would like to make?