Information Security and Practice: The User's Perspective

Nathan, Clarke[1,4]; Fudong Li[1]; Steven, Furnell[1,4]; Ingo, Stengel[2]; Giorgio, Ganis[3]
[1]Centre for Security, Communications and Network Research, Plymouth University, Plymouth, United Kingdom
[2]University of Applied Sciences Karlsruhe Germany
[3]Faculty of Health & Human Sciences, Plymouth University, Plymouth, United Kingdom
[4]Security Research Institute, Edith Cowan University, Western Australia
info@cscan.org

Abstract: The use of Information Technology (IT) has become common practice in our everyday lives both for business and private purposes. While people enjoy the convenience that IT offers, it also poses various security threats if not used properly, including malware, hacking, and information disclosure. Unfortunately, the scale and consequence of cyber threats has increased significantly year-on-year despite various security controls having been developed and deployed. It is evident that end users play a significant role within the information security domain, as they are frequently the primary target and the main force behind incidents. Nonetheless, whilst there are annual security surveys for organisations, less effort were given regarding assessing how individuals practice information security by the research community. Therefore, this paper presents a survey that investigates user's IT security practice and behaviour. In total, 400 respondents were surveyed during a five month period (i.e. November 2014 – March 2015). Overall, the results demonstrate that end users practice better IT security than typically thought although it appears only at a relatively basic level. For example, whilst a reasonably good proportion of participants (66%) claimed that they never share their passwords with others, 76% have used the same password on multiple sensitive accounts. Almost three quarters (72%) of responders never click on links or attachments within emails from unknown sources, but this is significantly reduced (to 36%) when someone they knew sent the email. Two-thirds of users (65%) do appreciate the importance of antivirus software as they always keep their antivirus software updated; however, less care is given to other applications/systems as only 44% would do the same and more alarmingly 65% even cancel or delay the security update process. Over two thirds (68%) of participants do not always backup their data, and only half of the participants (53%) claimed that they always destroy their data before hardware disposal. The results of the survey suggest that whilst levels of awareness are improving, there is still a significant gap between existing and required levels of information security knowledge and practice. Arguably, users are currently being overwhelmed by the burden being placed upon them to remain secure. The range of technologies they use (60% using more than 3 devices), the widespread use of online services (89% using at least 5 IT services) highlight users are becoming or have become technology dependent but perhaps without being security savvy.

Keywords: end-user, IT security, survey.

1. Introduction

The use of Information Technology (IT) is common practice in our everyday lives. Individuals can use IT to conduct their daily activities, such as online shopping and e-banking; and companies are reliant upon their IT infrastructure to ensure business continuity (e.g. managing customer records). According to figures from the Eurostat's Information Society database, 75% of individuals within the European Union had access to computers and broadband Internet in 2014 (Eurostat, 2014). While society enjoys the convenience that IT offers, it also poses various security threats, including spam, malware, Denial of Service (DoS), hacking, and social engineering.

Unfortunately, the scale of threats has increased significantly on an almost annual basis despite an array of security mechanisms (e.g. antivirus software, firewall, authentication, and encryption) becoming widely deployed and utilised. PwC's Global State of Information Security Survey (2015b) states that the total number of information security incidents reported grew to 42.8 million in 2014 globally, a 48% increase upon 2013. For the UK alone, 70% of businesses experienced information security breaches in the same year (PwC, 2014). Consequences of these information security incidents can also result in huge damages to individuals and businesses. Based upon a FBI Internet Crime report, 262,813 individuals were victimised in 2013, resulting a total loss of $781,841,611 (FBI, 2013). The Kaspersky IT Security Risks Survey (2014) suggests that the damage of a single information security incident could cost a business on average of $720,000; if the damage on reputation and brand were also considered, the cost could be more severe.

Traditionally, the majority of cyberattacks against information systems were executed in a more technical manner – focussing upon the attacking the IT system. However, the landscape of security incidents has changed dramatically over the last few years as attackers have increased their focus and involvement with end users. From the attacking perspective, more attacks (including phishing, spam, and ransomware) are being constantly utilised to target end users for their sensitive information and data. From the defending side, more than half of organisations worry that their employees could be the most likely source of an attack (EY, 2014). According to the PwC's 2015 Information Security Breaches survey, 75% of large businesses and 31% of small companies suffered staff-related security breaches in the UK in 2015 (PwC, 2015a). Also, the IT security risks survey by Kaspersky Lab suggests that within organisations unintentional and intentional data leaks by staff were 29% and 21% respectively. Moreover, several research studies demonstrate that careless or malicious actions of internal users are the main source of threat to information security (Pfleeger and Caputo, 2012; Posey et al., 2011).

It is well evidenced that end users play a significant role within the information security system as they are often the primary target and also the main concern of internal security incidents. If they were able to correctly protect their information systems, many of the security incidents could be avoided. Nonetheless, little focus has been given to assessing how individual's practice information security in comparison with yearly published security survey reports by leading global organisations. To this end, this paper presents a survey study that investigates user's IT security practice from several perspectives, including authentication, data management, and their behavioural use.

The remainder of the paper is structured as follows: Section 2 reviews existing survey studies within the information security domain. Section 3 demonstrates the research methodology of the survey study. Section 4 illustrates the survey result in details, followed by the discussion that is presented in Section 5; and conclusions are highlighted in Section 6.

2. Existing IT Security survey studies

In order to obtain an accurate view of past incidents and predict future protection directions, various IT security surveys are conducted each year around world. Based upon the scale and focus, existing studies can be categorised into two types: organisational oriented and end user focused; details of these two categories will be discussed as below.

For organisational oriented survey studies, their focus is to present an overview of the current IT security domain. Normally, these studies are produced by multinational corporations, government departments, or security expert groups (e.g. Computer Emergency Response Teams (CERT)) annually, including Symantec's Internet Security Threat Report (Symantec, 2015), PwC's Information Security Breaches Survey (PwC, 2015a), Kaspersky's IT Security Risks Survey (Kaspersky, 2014), FBI's Internet Crime Report (FBI, 2015), and CERT-UK Annual Report (CERT- UK, 2015). In general, organisational survey studies cover a wide range of IT security related topics, such as IT security threat trends at the global level, types of security incidents within organisations, and/or remedies for enhancing organisational IT security defence. Their focus is often business-related, offering an understanding of the impact of incidents on a company's bottom line. Whilst many highlight the key role the employee (user) plays in effective security and the weaknesses introduced by them, they fail to explore in detail what the issues are.

Regarding end user focused survey works these are largely undertaken by researchers to obtain an end user's perception on a specific IT security topic. For instant, a number of papers, including Clarke and Furnell (2005), Hoonakker et al. (2009), Kurkovsky and Syta (2010), and Voyiatzis et al. (2011), studied user's password usage; other studies, such as Karakasiliotis et al. (2007), Workman (2007), and Flores et al. (2014) investigated user's perceptions of phishing under the wider topic of social engineering attacks. Generally, end user focused surveys offer in-depth knowledge, detailed analysis, and comprehensive discussion on the proposed topic. More importantly, they represent first hand examples of user's IT security practice in real life. They tend however to be focussed upon one/two aspects of the domain rather than providing a more holistic appreciation of current security practice and behaviour.

3. Research methodology

With the aim of investigating user's current security practice and behaviour from a more holistic perspective a quantitative-oriented survey was devised. The survey contained a total of 19 core questions and they were structured under three sections:

- Demographic: to establish an understanding of respondents' background information.
- IT usage: to appreciate the type and level of technology and services which respondents utilise.
- IT security practice: to understand end user's IT security practice from several aspects, including password usage, phishing, networking, data management, and security software.

The survey was implemented via a popular online survey tool (i.e. LimeSurvey) hosted from the authors' research centre. It was active from November 2014 to March 2015. During the aforementioned period, the survey was mainly disseminated in the form of email invitations, which were sent to students and colleagues of the authors, several research communities within authors' institution, as well as through social networking channels (e.g. Facebook, LinkedIn).

4. Survey findings

A total of 400 completed surveys were received during the five month period. An analysis of the demographic questions shows a number of skews that need to be taken into account when analysing the survey questions. On gender, age and education, the population sample was skewed – largely dependent upon access the authors had to participants. Indeed, the skew was towards men (73%), 18-30 (62%) with a degree (62%), and a focus in the IT profession (65%). Whilst this fundamentally does not undermine the results, it is worth noting that any technology usage or security behaviour would more likely be higher within this population than would be experienced from the population as a whole.

4.1 Use of technology and services

User's technology and IT services usage could provide a number of indicators to reveal their susceptibility to potential security threats to their information. As illustrated in Figure 1, Windows based desktop/laptop, iPad/iPhone, and Android Tablet/Smartphone were the top three used technologies with 91%, 73%, and 60% of the participants respectively; in comparison, less than 10% of the participants utilised BlackBerry based devices or a smartwatch. This result is somewhat expected and inline with market analysis. More notable, when analysing how many of these devices a participant has, 60% have 3 or more devices. This highlights two interesting trends: first of all, users no longer rely upon a single computer or device but access services across a range of technologies, providing a wider range of potential attack vectors for hackers; secondly, the nature of the devices utilised are varied (from mobile, laptops to smart TVs and game consoles). These differing platforms require users to be knowledgeable about maintaining security across different operating systems, applications, and devices – arguably significantly increasing the knowledge burden upon the user.

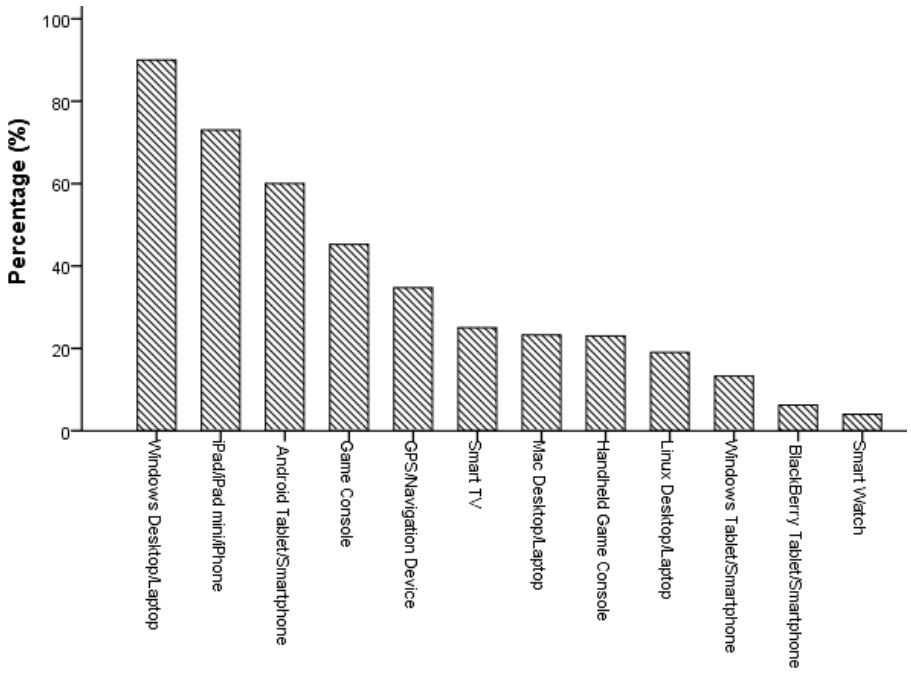

Figure 1: Users' usage upon technology

To further explore how people use technology, participants were asked about their use of online services. Their usage across twelve popular IT services is illustrated in Figure 2. In general, more than 70% of the participants use email, information gathering, instant messenger, social networking, online streaming, and office applications (e.g. word processing) on an always/often basis; particularly, end users were obsessive about their emails as 80% of them claimed that they were always using it; these figures are at least 15% higher than findings of the European Commission's Special Eurobarometer 423 report on the same services (European Commission, 2015). It is also notable that the proportion of participants who responded never to any of these services is relatively low (i.e. less than 8.8%) – apart from online gaming (30.5%) and Peer to Peer sharing (P2P) (28.5%). Moreover, 89% of participants access at least 5 services on an often/always basis, highlighting the high level of engagement users have with various online IT services.

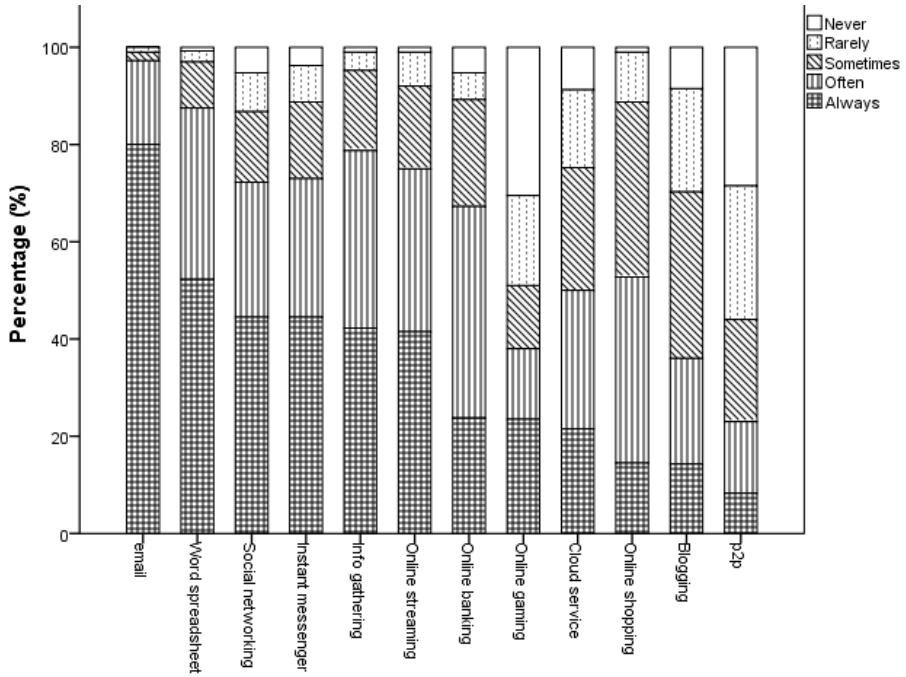

Figure 2: Users' usage upon IT services

4.2 User IT security practice

IT security is considered essential (30%) or a high priority (50%) by a significant proportion of participants, highlighting the importance of security within the minds of participants. When asked about their prior experience with security incidents, 89% of participants had experienced at least one security incident (e.g. malware infection (58%), hardware failure (52%), data loss (34%), and phishing (32%)). Therefore, these users, having experienced an issue (and given their relatively educated backgrounds), should be more focussed upon practising better security than those who have never experienced an incident before. Based upon the user's overall IT usage, their security practice was assessed in several areas, including authentication, application usage, and data management.

The password is one of the most deployed authentication techniques, providing the first (and in many cases the only) line of defence for various IT services and their data. Therefore, it is mission critical for users to conduct good password practices. However, almost 35% of participants had less than 6 passwords for all their devices and services, giving an early indication of password reuse amongst them as a majority (91.2%) of the participants had access to at least 10 IT services (as illustrated in Figure 3). Also, it is well known that strong passwords can protect users against password cracking tools; nevertheless, only 24.5% of the participants met the strong password requirement (e.g. containing lower and upper cases characters, numbers, symbols and is 8 characters or more) for the majority (between 81 to 100%) of their passwords. Almost 40% of the participants do not change their password within 6 months and 38% of the participants only change their passwords if they are forced to do so.

Other good password practices also include never sharing or storing passwords, and never using the same password on multiple accounts. Nonetheless, Figure 3 shows that 44% of participants shared their passwords with others and 76% of participants used the same password on multiple sensitive accounts, providing opportunities for attackers who can obtain their passwords through the hacking of one system obtaining access to several other systems. Significantly, 61% of the participants stored their passwords; regardless how the password is stored, this approach could make the user's systems and information vulnerable if the stored passwords were discovered by others or the owners were denied access by their own password storage facility. Given the participants are skewed towards being more technical savvy and educated than the general population, their use of authentication practices fall short of what is required. However, it is debatable whether the user is truly at fault, as the demands and subsequent burden placed upon them has increased significantly and arguably system designers need to consider and develop more usable yet secure solutions.

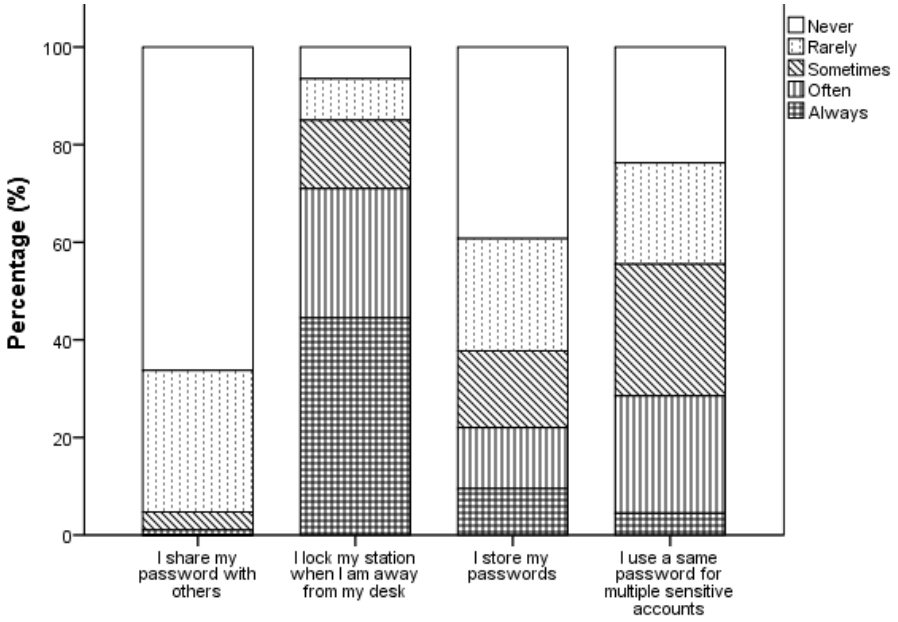

Figure 3: Password security practice

In order to maintain a high level of security for computer systems, users' actions upon applications/systems should also be considered. One of the common practices is to keep applications/systems updated, as unpatched software will offer opportunities for hackers to exploit vulnerabilities. As illustrated in Figure 4, users do appreciate the importance of antivirus software as 65% of participants always keep their antivirus software updated; in comparison, less care is given to other applications/systems as only 44% of participants always install latest security patches, and 65% of them even cancel or delay the security update process. A comparison of these results highlights a potential trend. Participants are happy to use antivirus software, an application that is now typically pre-installed and enabled prior to purchase – the task or burden upon the user to do anything is removed (or at least reduced). Conversely, with patching, the user is in involved in the process (whether to approve an update or the hassle of waiting whilst an automated patch is installed – often impacting upon their ability to undertake the task at hand). The usability of the approach is essential to acceptance.

Another good application security practice is to avoid using illegal software as they are often packed with spyware and vulnerabilities. Nevertheless, 60% of the participants claimed that they have experience of installing/using pirate software on their computing devices.

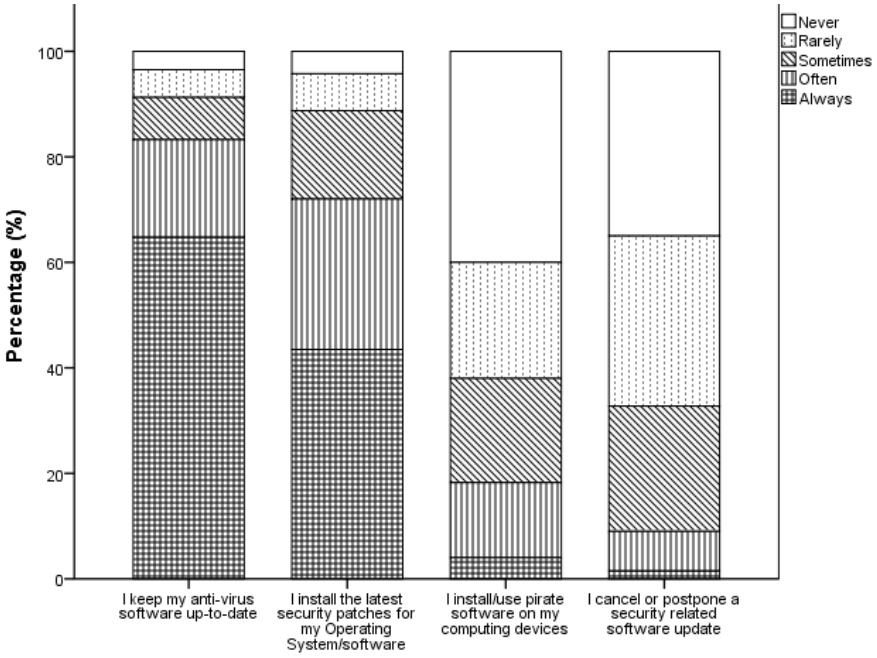

Figure 4: User software usage

Email is one of the most used IT applications by end users, potentially containing a large amount of sensitive information. Nonetheless, it is also a prime channel for cybercriminals (e.g. launching phishing and malware attacks) (Symantec, 2014). As shown in Figure 5, a large proportion of participants (72%) claimed that they can identify potential threats if emails were sent by unknown sources; however, only 36% would do the same if the email was sent by someone they knew. This could become problematic if the sender's email account was compromised or spoofed. Participants' behaviour when dealing with suspicious emails is broadly good with 63% of participants always deleting them. However, only 14% of them always notify the IT support despite the notification would alarm other users from being victimised. Whilst it is unclear why participants do not report the incident, the frequency of such attacks is likely to lead to participants merely ignoring such email. This apathy towards such attacks is both a symptom and cause which is challenging to overcome.

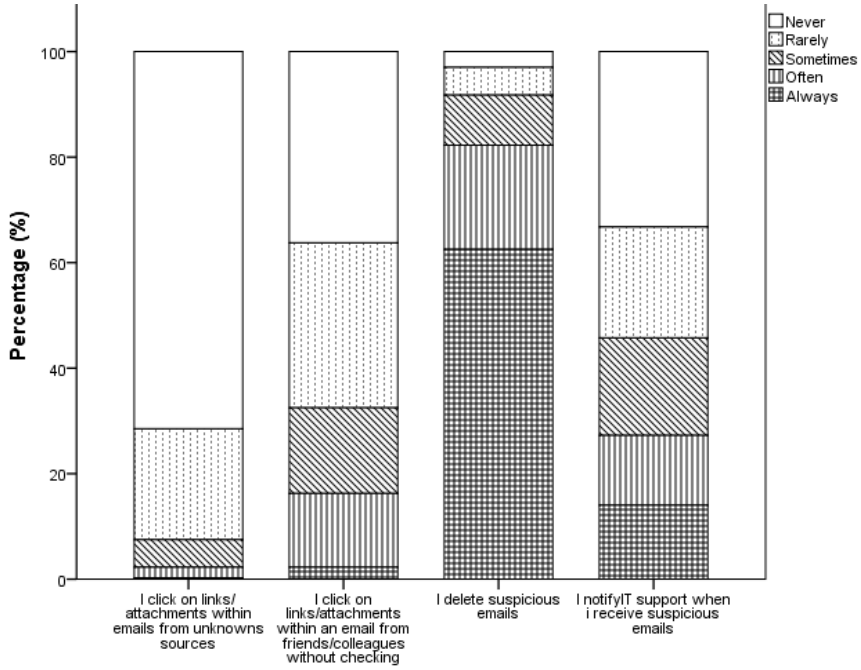

Figure 5: User email security practice

Data plays a significant role within IT systems and often holds sensitive and/or private information. However, data could be damaged, lost, stolen, or neglected during transmission, storage, or removal if it is not handled properly. Data backup is a simple yet effective solution against a data loss incident; with encryption being a long established protection for securing the confidentiality of data. It is envisaged that users should always take the advantage of both methods to protect their data. Nevertheless, as demonstrated in Figure 6, 68% of participants do not always backup their data on a regular basis; 50% of participants never use an encrypted USB to transfer files and 35% never encrypt their sensitive information. In comparison, more actions would be taken by users if they know they will lose the control of their data. Indeed, 53%, 16.8%, and 12.8% of participants claimed that they always, often, and sometimes (respectively) destroy their data before disposing of hardware.

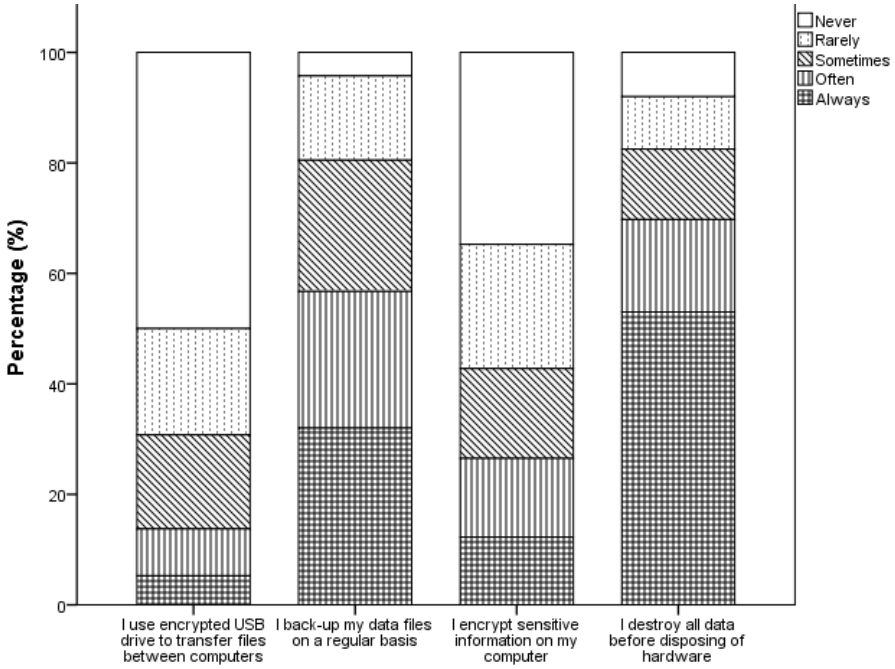

Figure 6: User data management

5. Discussions

As highlighted in the last section, results need to be considered with respect to the sample population. Whilst arguably a skew exists towards to the top end of the IT user spectrum, it is clear that there are significant gaps in participant's practice that would lead to security breaches. Whilst some good behaviour is noted, handling email from unknown sources, backup, antivirus, patching, and data deletion upon disposal, there are a wide range of practices that require significant improvement. Also, some of the answers are perhaps more reflective of the participants' confidence in their ability to perform good security rather than a definitive statement that they can do it correctly.

Arguably the need to practise good security behaviour can be linked to how a person uses technology. High usage would demand a higher level of practise or risk the significant consequences. An additional analysis was undertaken based upon participant's use of services (i.e. low (33%), medium (34%), and high (33%) based upon the number of services and the frequency of usage (as illustrated in Section 4.1)). Encouragingly, users with high service usage typically practise better IT security in comparison with low and medium users. Less encouraging was the relationship between medium and low usage, with very little difference overall experienced. Whilst an argument could be made for it not being essential for people with a low usage to practise good security (albeit not a strong one!), that cannot be said for those in the medium usage category. The results would serve to highlight that more effort towards improving practise would arguably benefit those in the medium usage category. Users with low service usage did outperform others regarding the usage of password and pirate software; nonetheless, these could be caused by limited used services (hence less passwords were required) and little usage of the computer system.

Table 1: User's good IT security practice comparison based upon their service usage level

	Low	Medium	High
I *never* share my passwords with others	65.9%	63%	*69.9%*
I *always* lock my station when I am away from my desk	44.7%	34.8%	*54.1%*
I never store my passwords	37.9%	*43%*	36.8%
I never use a same password for multiple sensitive accounts	*29.5%*	18.5%	23.3%
I always keep my anti-virus software up-to-date	57.6%	60.7%	*75.9%*
I *always* install the latest security patches for my OS/software	40.2%	31.1%	*59.4%*
I *never* install/use pirate software on my computing devices	*53%*	40.7%	26.3%
I *never* cancel or postpone a security related software update	34.1%	20.7%	*50.4%*
I *never* click on links/attachments within an email from unknown sources	68.9%	*74.1%*	71.4%
I *never* click on links/attachments within an email from friends/colleagues without checking	33.3%	30.4%	*45.1%*
I *always* delete suspicious emails	63.6%	60%	*63.9%*
I *always* notify IT support when I receive suspicious emails	13.6%	11.1%	*17.3%*
I *always* use encrypted USB drive to transfer files between computers	4.5%	3%	*8.3%*
I *always* back-up my data files on a regular basis	26.5%	27.4%	*42.1%*
I *always* encrypt sensitive information on my computer	*12.9%*	11.1%	12.8%
I *always* destroy all data before disposing of hardware	50%	46.7%	*62.4%*

Analysis of the results suggests users do have a working knowledge of security and good basic security practices – as the results indicate a good level of practise across a range of domains. They also certainly consider it to be important (80%). Their weakness in practise could be due to:

- Lack of more comprehensive knowledge about how to improve their security practise
- Knowledge of good security behaviour but a conscious decision not to practise it – perhaps based upon a risk-based decision to do so
- An inability to practise good security behaviour due to the burden placed upon the user

Whilst the survey does not provide any evidence to suggest what proportions of impact these factors have, there is evidence to suggest each of these are having an impact. For example, participants' use of email and taking appropriate care when opening attachments even from known senders is mostly linked to a lack of detail knowledge and understanding that email communication tends to be insecure and open to misuse such

as this. Examples of risk-based practise come through with the regularity of practise – how frequent they backup their data, how they dispose of their data, or their use of password strength. The inability to practise good security is highlighted most significantly when looking at their use of passwords. The widespread use of password stores, the inability to use strong passwords (whilst arguably understanding what one is) and utilising a small collection of passwords to manage access to a wide range of services.

Of the three outcomes, participants taking a risk-based approach are potentially okay; it is after all the approach taken by information security practitioners when analysing organisations. This would help ensure commensurate security for the asset being protected. However, more questionable is the ability of the individual to make the correct assessment – after all, security practitioners do this with a solid working knowledge of the domain. To what extent can this be said of end-users in general? Significant further education would be required.

The lack of knowledge could be improved via a variety of awareness raising schemes and education. Given the efforts made thus far, this would be slow process and arguably one that would struggle to keep up with the pace of change within the domain (in terms of technology, threat vectors, and security practises) (Niekerk and Solms, 2013). Awareness raising and education would only ever be able to provide a baseline understanding and appreciate of information security.

The third outcome is arguably the only area where significant enhancement could be made. Technology is currently failing users – their use of passwords being the most recognisable and widespread example. An approach which, when applied to a standalone system or single service might be more than appropriate becomes completely inappropriate when used across their technology usage. Whilst technology itself cannot provide complete security (a principle well understood for more than 20 years), it is clear that technology must play an increasingly more important role. However, rather than focusing upon detection and mitigation strategies, technology must focus upon usability and the human aspects. Technology must provide usable solutions, such as providing interfaces that educate and inform users and controls that are “intelligent” and remove the cognitive burden being placed upon users. Efforts in this space are being experienced – interfaces are becoming more form over function – with usability being a key factor being considered in the design phase (Yee, 2004; Flechais et al., 2007; Ibrahim et al., 2010). Trends can also be seen in the development of intelligent systems that seek to manage and monitor users and provide holistic security across devices and services (Hocking et al., 2013). However, the research undertaken in this space falls significantly short of what is required by the domain.

6. Conclusions

The paper has presented a survey investigating end users’ IT security practice in various areas, including authentication, application, and data management practice. The survey results suggest that a baseline security knowledge is now being practised amongst end-users (albeit those with better education and use of IT than the general population); however significant gaps still exist that will result in the compromise of information.

The solution to closing the gaps is not a simple one and requires effort from a range of stakeholders. The survey suggests users do consider security to be important but their practice is suggestive that they are only willing to go so far in contributing to that protection. More thought and consideration must be given to the development of technology solutions that work with the user to ensure their behaviour and practises are secure.

References

CERT-UK (2015) “Annual Report Apr 2014 – Mar 2015”, available at: https://www.cert.gov.uk/wp-content/uploads/2015/05/Annual-Report-including-4th-Quarter-FINAL.pdf, date accessed: 26 May 2015

Clarke, N.L., Furnell, S.M. (2005) “Authentication of users on mobile telephones—a survey of attitudes and practices”, Computer and Security, 24(7), 519–527

European Commission (2015) “” Special Eurobarometer 423 Cyber security report”, available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf, date accessed 20 May 2015

Eurostat (2014) “Eurostat information society database”, available at: http://ec.europa.eu/eurostat/web/information-society/data/database, date accessed 20 May 2015

EY (2014) “Get ahead of cybercrime”, available at: http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf, date accessed: 21 May 2015
FBI (2013) "2013 internet Crime Report", [online] http://www.ic3.gov/media/annualreport/2013_ic3report.pdf, date accessed: 5 March 2015
FBI (2015) "Annual Reports ", available at: http://www.ic3.gov/media/annualreports.aspx, date accessed: 10 April 2015
Flechais, I., Mascolo, C. and Sasse, M.A (2007) “Integrating security and usability into the requirements and design process”, International Journal of Electronic Security and Digitial Forensics, Vol. 1, Issue 1, pp 12-26, January 2007.
Flores, W.R.; Holm, H.; Nohlberg, M.; Ekstedt, M., "An Empirical Investigation of the Effect of Target-Related Information in Phishing Attacks," Enterprise Distributed Object Computing Conference Workshops and Demonstrations (EDOCW), 2014 IEEE 18th International , vol., no., pp.357,363, 1-2 Sept. 2014
Hocking, C., Furnell, S., Clarke, N. and Reynolds, P. (2013) “Co-operative user identity verification using an Authentication Aura”, Computer & Security, Vol. 39, Part B, pp 486-502
Hoonakker, P., Bornoe, N. and Carayon, P. (2009) “Password Authentication from a Human Factors Perspective: Results of a Survey among End-users”, proceedings of the Human Factors and Ergonomics Society 53rd Annual meeting, pp459-463
Ibrahim, T., Furnell, S.M., Papadaki, M. and Clarke, N.L. (2010) “Assessing the usability of end-user security software”, Proceedings of 7th International Conference, TrusBus 2010, pp 177-189, 2010.
Karakasiliotis A, Furnell SM, Papadaki M (2007), “User security awareness of social engineering and phishing” Advances in Network & Communication Engineering 4, ISBN: 978-1-84102-180-5, pp191-198, 2007
Kaspersky (2014) “IT Security Risks Survey 2014”, available from: http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf, date accessed 10 May 2015
Kurkovsky, S., Syta, E.(2010) “Digital natives and mobile phones: A survey of practices and attitudes about privacy and security”, Proceedings of the IEEE International Symposium on Technology and Society (ISTAS), pp. 441–449 (2010)
Niekerk, J. and Solms, R. (2013) “Bloom’s Taxonomy For Informationsecurity Education”, Information Assurance and Security Education and Training, IFIP Advances in Information and Communication Technology Volume 4026, pp 280-287
Pfleeger, S and Caputo D (2012) “Leveraging behavioural science to mitigate cyber security risk”, Computers & Security, Vol. 31 issue 4 page 597-611
Posey, C., Bennett, R and Roberts, T. (2011) “Understanding the mindset of the abusive insider: An examination of insiders’ causal reasoning following internal security changes”, Computer & Security, vol.30 issue6-7, pp. 486-497
PwC (2015a) “2015 Information Security Breaches Survey”, available at: http://www.pwc.co.uk/assets/pdf/2015-ISBS-Technical-Report-blue-digital.pdf, date accessed: 18 August 2015
PwC (2015b) “Managing cyber risks in an interconnected world”, available at: http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf, date accessed: 23 April 2015
Symantec (2014) “Internet Security Threat Report”, available at: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf, date accessed: 20 June 2015
Symantec (2015) “Security Response Publications”, available at: http://www.symantec.com/security_response/publications/threatreport.jsp, date accessed: 16 May 2015
Yee, K. (2004) “Aligning security and usability”, Security & Privacy, IEEE, vol.2, no.5, pp.48-55, Sept.-Oct. 2004
Voyiatzis, A.G.; Fidas, C.A.; Serpanos, D.N.; Avouris, N.M., "An Empirical Study on the Web Password Strength in Greece," Informatics (PCI), 2011 15th Panhellenic Conference on , vol., no., pp.212,216, Sept. 30 2011-Oct. 2 2011
Workman, M. (2007) “Wisecrackers: a theory grounded investigation of phishing and pretext social engineering threats to information security”, Journal of the American Society of Information Science and Technology (59) (2007), pp. 662–674