An analysis of United Kingdom Schools' Information Security Policies: A socio-technical approach

Martin Sparrius[1][0000-0001-8586-6767] and Moufida Sadok[1][0000-0003-2981-6516]

[1] University of Portsmouth, Portsmouth, United Kingdom
martin.sparrius@port.ac.uk

Abstract. UK schools collect and store large amounts of data on their students, parents, and staff. This makes them attractive targets for both external and internal attackers. To respond to and manage security risks, many schools have developed and implemented Information Security policies. This paper explores and analyses the content of 100 UK schools' security policies with an aim to examine the extent to which these policies address security risks faced by schools. Such exploration has the potential to assess the effectiveness and the relevance of security policies. The key findings show that many security policies are primarily centered on traditional technology-focused solutions and not on threats targeting the human elements in their organisations. In addition, it could be argued that between poor readability scores and large word counts, these policies are not very accessible to staff. This paper proposes that a socio-technical approach to information security would potentially result in better understanding of the role and application of security policies in schools and, therefore, improved information security.

Keywords: Cyber Security, UK Schools, Information Security Policies, Socio-technical Approach

1 Introduction

Schools within the United Kingdom (UK) collect and store large amounts of data on their students, parents and staff. This makes them an attractive target for cyber-attacks, and it has been noted by previous researchers that data breaches and cyber-attacks targeting educational organisations have been on the rise [1, 2]. In their Data Breaches Investigation from 2019, Verizon found that 79% of the cyber-attacks involving educational organisations were financially motivated and that they specifically targeted personal data held by these organisations [3]. The report further notes that internal threat actors are still a major threat to educational organisations, accounting for 45% of the total breaches, with unintentional actions that led to a security incident comprising 35% of the incidents reported by these organisations.

In response to the general rise in cyber-attacks, the UK implemented the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 in May 2018 to encourage improved Information Security (IS) within UK organisations. Since then,

30% of UK business and educational organisations are reported to have made changes to their cyber security and of these changes, 60% focused on the creation of new policies [4]. Additionally, it became a statutory obligation for UK schools to create and annually review a Data Protection policy [5].

This focus on policy creation meshes with research that has identified that the 'construction and implementation of strong technology and information policies' forms a key component in the improvement of an organisation's IS [6]. Subsequent to the implementation of the GDPR, it was found that the UK education sector was more likely than average to have an IS policy in place (57%) [4] and while self-reported data identified a general increase in IS content [4], there has been no independent academic research into the nature and quality of this content or how staff interact with school IS policies. This research plans to use a series of qualitative and quantitative analysis to answer the following research questions:

- RQ1: What organisational and technical content is contained within school policies?
- RQ2: How accessible are these policies to the teaching staff?
- RQ3: To what extent does the IS policy content address the current threat landscape faced by schools?

2 Background

This literature review focuses on three themes: the use of the socio-technical approach within Information Security, the use of policies within IS and research involving Information Security within educational organisations for students aged 5-16.

2.1 The use of the socio-technical approach within IS

The interplay between the technical and human elements within an organisation performs an important role in the effectiveness of security measures within the organisation. Research has been undertaken within each of these elements and their combinations, with Siponen observing that each field has developed its own research community [7]. While the positivist orientation within computer science is more common within the UK, there is an increasing realisation that a more interpretivist orientation within Information Security has an important role to play in the development of security practices [7]. Coles-Kemp described the need for more research to be undertaken into how the human, organisational and technical elements relate to each other and how these elements impact on IS [8].

In their investigation of the human aspects of security, Furnell and Clarke and found that investment was targeted at technological solutions and different forms of security control, such as awareness, was lagging behind [9]. Researchers have even detailed how failing to consider the ways in which caseworkers operate in an organisation led to the IS procedures of that organisation proving to be a hinderance to legitimate work. This resulted in employees actively circumnavigating security controls to

effectively perform their required duties [10, 11]. In a following paper, Coles-Kemp and Hansen discussed how real-world security problems developed from the consequences of human interactions with the technology within an organisation and that separating out the social and technical elements was unadvisable; however, they noted this was still a dominant theme in IS policy creation [12].

2.2 The use of policies within IS

As discussed by Weidman and Grossklags, a policy is "designed to set the strategic direction, scope and tone for an entire organisation regarding a particular topic" [1]. In terms of the content of an IS policy, this would include a description, important dates for the policy, describe IT procedures and key personnel who are critical to IS within the organisation. It is also expected that an organisational security policy addresses specific areas such complying as with regulatory frameworks and using of new technologies. There is a widespread belief in IS literature that enforcing compliance with the IS policy is a solution for security effectiveness [13]; however, this this can be counterproductive [14]. This focus on employee compliance in policy research has been due to many researchers considering employees the 'weak link' within an organisation [15, 16]. However, it is also recognised that with proper motivation, these self-same employees can, instead, be a vital part of an organisation's IS and this motivation can come in the form of feeling that they are part of the IS solution by building in value congruence [17, 18].

As Weidman and Grossklags note, an effective IS policy needs to recognise the internal threat posed by employees by including suitable technical and organisational controls while not making the employees feel like an enemy of their own organisation [1]. This realisation is missing from many organisations, though, and as Albrechtsen and Hovden observed, there is a "digital divide" between the security managers who are designing these policies and the users to whom the policies apply [19]. This, in turn, leads to development of security policies that are independent of the needs of users within the organisation who then, ironically, breach the system security to perform their job to a satisfactory standard [20, 21] or become distrustful and resentful towards the organisation [14]. The impact of these policy creation decisions and how organisations are adapting their policies in an evolving environment is, however, still insufficiently researched [22].

2.3 The Analysis of Information Security and IS Policies within educational organisations

IS within primary and secondary schools, organisations which serve students aged 5-16, appears to be an under-researched topic. A few authors around the world have studied different aspects of IS. Chou and Chou investigated Taiwanese teachers' perceptions of their own IS behaviour and found the perceived inconvenience of taking preventative measures resulted in poor IS behaviour amongst primary and secondary teachers [23]. Moyo et al. looked at how an optimised risk assessment exercise in two South African secondary schools could lead to improved appreciation of IS amongst

the staff of these schools [24]. In the United States of America (USA), Pusey and Sadera investigated whether trainee teachers felt comfortable with cybersecurity and found that most of their respondents did not feel prepared to model or teach this topic [25]. Shen et al., in their study of data breaches within USA schools, found that data security still focused on basic measures, such as password use, and that staff lacked an understanding of cybersecurity [26].

The consensus amongst these researchers is that there is a lack of effective IS within educational organisations and there is a persistent and increasing threat of IS breaches involving these organisations. An understanding of IS work done in other fields is being used to jump start research into the IS of educational organisations, but at this stage it appears fragmented and localised to specific countries.

In 2020, the UK government conducted its first Data Breach Survey of UK schools, where schools were asked to respond to a series of questions relating to IS and data breaches. It found that approximately 87% of schools possessed an IS policy. 52% of the surveyed schools reported multiple security breaches, with 92% of these schools suffering at least one breach due to fraudulent emails or website redirects, 24% reporting successful phishing or malware attacks and 10% suffering at least one breach a week [12]. These findings support the concerns raised by researchers investigating IS in schools and present an increasingly threatening security landscape for these schools.

3 The Study

3.1 Data selection and collection

Researchers in the field have found that collecting policies for analysis is incredibly difficult [19], with many organisations regarding the analysis of this documentation as very intrusive [1]. To find a more accessible source of IS policies, some researchers chose to focus on educational organisations, in particular universities, as they appear to be more likely to host IS policies on their websites to guide their staff and students [1,20]. In this study on schools, initial Information Security policy collection was also attempted in this manner. The online policy section of the top 100 schools within the researchers' local county was searched. This involved both checking each relevant policy webpage or performing a search using the website's search tool. E-Safety and Safe Internet use policies were disregarded as having a focus on students, rather than the staff. Additionally, policies which were too specific in nature (BYOD, GDPR, Use of Mobile Phones) were also disregarded because, as Weidman and Grossklags noted, while smaller, issue-specific policies are useful for an organisation, it is important to have a consolidated high-level policy to provide a foundation for an organisation's IS [1]. Only one school in the first 50 listed an Information Security policy and the search was adjusted to instead make use of popular internet search engines to search for IS policies hosted by schools within the whole of England.

This search used two different search engines (Google and Duck Duck Go) to make use of different searching algorithms to produce different search results. The core terms used in this search were "Information Security", "Policy" and "UK

School", with other variations and additions as the search progressed. The search was concluded once 100 policies were found, which met the criteria used for the initial school-by-school search. Next, the UK Government database was used to collect data on each school, such as school capacity and organisation type. The policies where then loaded into an NVivo database and relevant data for each school added as attributes prior to the initial coding.

3.2 Qualitative coding and readability analysis

Initial coding used the 4 item categories that were based on Weidman and Grossklags' analysis of university IS policies, as well as iterative analysis of a sample of 10 policies. This coding was binary in nature and only focused on the presence of the stipulated code within the policy. Once the coding criteria had been identified, the whole set of policies was coded, checked for coding errors, and then was rechecked using keywords identified in the initial coding run. To differentiate policies which contained detailed technical instruction, the code of "has detailed technical terms" was allocated to relevant policies. Each policy was then entered into a website readability calculator, Readable, and the word count, Flesch Reading Ease and Simple Measure of Gobbledygook (SMOG) scores added to the attribute date for each policy.

4 Data analysis of selected components from the IS policies

4.1 School Characteristics

State-funded English schools are generally split into age groups that correspond to 5-11 years (Primary) and 11-16 (Secondary). This distinction is important as funding for these schools is on a per pupil basis and differs based on the age focus of the school [27]. Official government data was obtained by accessing the Department of Education website [28].

Table 1. Relative Age Focus proportions of UK schools

Age Focus	Proportion of Sample	UK Government Data
Primary Schools	75%	83%
Secondary Schools	25%	17%

Table 2. Mean school capacities of UK schools

School Capacity	Number of Students (Mean)	Standard Deviation	UK Government Data (Mean)
Primary Schools	318	231	282
Secondary Schools	991	135	965

4.2 Content of IS policies

As previously stated, coding only notes the presence of content that corresponds to the relevant code. All 100 policies had some relevant text; however, no single policy had all the searched-for content. For each age focus, the sum of policies which contained the specific content code was divided into the total number of policies for that age focus and presented in Tables 3 and 4.

Table 3. Relative Age Focus proportions of coded organisational content in school IS policies

Content code	Primary Schools	Secondary Schools
Clearly states who issued policy	59%	88%
Has a next review date	57%	68%
Has an effective date	78%	92%
Explicitly provides motivation or justification for policy	93%	88%
Clearly states who is affected by the policy	93%	88%
Defines responsibilities for standard roles	42%	32%
Defines responsibilities for specific roles	70%	52%
Mentions methods of enforcement	54%	68%
Mentions nature of sanctions	70%	72%
Has detailed technical items	55%	48%
Has Information Security definitions	16%	28%
References Computer Misuse Act	35%	48%
References GDPR or Data Protection	82%	80%
Refers to other school policy documents	86%	88%

Table 4. Relative Age Focus proportions for coded technical content in school IS policies

Use of:	Primary Schools	Secondary Schools
Account control	54%	48%
Anti-virus or malware	64%	56%
Awareness campaign	42%	28%
Backups	53%	44%
BYOD conditions	64%	60%
Encryption	69%	76%
Firewalls	42%	44%
Locking stations	62%	72%

Multi-Factor Authentication	4%	8%
Passwords	85%	88%
Patching schedule	24%	40%
Physical security procedures	73%	80%
Public Wi-Fi usage restrictions	14%	8%
Definitions for security breaches	22%	44%
IS incident response guidelines	80%	88%
Software licensing and software restrictions	66%	60%
Spam or Phishing emails guidance	22%	32%

4.3 Accessibility

Two measures of readability were investigated. Flesch Reading Ease, due to its popularity in research [29], and Simple Measure of Gobbledygook (SMOG) due to its recommended use by the UK's National Health Service [30]. Flesch Reading Ease bases its results on word/sentence length ratios and syllables/word ratios. The scoring ranges from 0-100, with a higher value representing text which is easier to read. Flesch has a recommended target of 30-50 [1]. SMOG examines the number of polysyllabic words, perceived as being difficult words, compared to the number of sentences in the text. SMOG ranges from 1 to 20, with a higher score being harder to read, and a recommended target of 12-13. The NHS suggests that a score of 14 or higher would result in most adults battling to read the text [30]. For the SMOG results, a standard deviation of 1.43 places nearly 15% of the policies over this recommended threshold.

Table 5. Readability analysis of school IS policies

	Mean	**Standard Deviation**	**Minimum**	**Maximum**
Flesch Reading Ease	42.7	7.9	18.1	65.2
SMOG	12.9	1.43	10.1	15.5
Word Count	3962	3327	424	20352

5 Key Findings and Discussion

5.1 Demographic Characteristics of Schools and their impact on their Information Security

Despite using an internet search to obtain the IS policies, school characteristics for English schools compare favourably with the UK government's statistics in Table 1. These characteristics are important as state funding for English schools is on a per-pupil basis and depends on the age focus of the school. As shown in Table 2, primary schools tend to be substantially smaller than secondary schools and this is likely to

have a knock-on effect in terms of their financial resources and staffing resources. This difference in resources will lead to a split in how primary and secondary schools approach their Information Security, with secondary schools more likely to have the resources to develop a dedicated IT team and assign a senior manager to deal with Information Security. Primary schools, with their smaller number of employees, are likely to have staff assume numerous roles with a wider set of responsibilities and may not be as focused on their Information Security policy.

To test this assumption, analysis of the coding with a primary and secondary division was conducted and it found that there was a distinct difference in their respective policies. Some of the key differences were:

- Primary schools were more likely to try to persuade staff with justifications (93% versus 88%) and explain what specific roles involved (70% versus 52%)
- Administration of policies was less consistent in primary schools:
  - Review date present (57% versus 68%)
  - Effective from date present (78% versus 92%)
  - Stating who was responsible for the policy (59% versus 88%)
- Primary schools are less likely to focus on monitoring staff IT usage (54% versus 68%)

These findings indicate that primary schools rely more on informal measures which consist mainly of persuading their staff of the importance and role of IS, while secondary schools are more focused on administrative details and the monitoring of staff members.

5.2 Technical Content

Analysis of the technical controls found that controls regarding passwords, physical security, encryption, locking workstations and IS incident response guidelines are the most encountered items within the policies. This is in line with the requirements for GDPR compliance and is a legal obligation for UK schools to avoid financial penalties in the event of a data breach [5]. Additional technical items referring to account control, anti-virus, backups, patching and firewalls occur inconsistently, with several policies implying their presence but not providing any detail. The tone of this content consists largely of admonishments to not interfere with the technology.

The least common items deal with security issues that involve staff interactions with the broader IT world: spam/phishing attacks, public Wi-Fi usage and awareness of IS threats. There is little indication within the policies of why these are underrepresented, but considering that Multi-Factor Authentication is effectively nonexistent in the surveyed policies, it is possible that the policies are focusing on aspects which are deemed to be of a higher priority or are more easily managed. This is consistent with the findings in previous research where Furnell and Clarke observed that the selection of controls in an IS policy were based on the criteria that "they target a defined threat and deliver a more easily measurable return" [9].

This skewed focus in the studied policies is concerning, particularly in regards to raising awareness (35% across all schools) and defining what exactly a security

breach is (33% across all schools), as it leaves the staff unprepared and guessing about the nature of cyber-attacks. This, in turn, leaves the schools unprepared to face evolving security threats. It is likely that this will be seen in the breach data from the period where UK schools had to shift to working from home during the Covid-19 outbreak as staff and schools had to suddenly make use of programs, like Microsoft Team/Google Meet, with which they had relatively little or no training.

5.3 Accessibility

Analysis of the school IS policies found that there was substantial variation in the accessibility of the policies, representing a wide range of writing styles. With a mean Flesch reading ease of 42.7 and a SMOG score of 12.9, the policies can be considered to have an average or higher readability difficulty. For these figures, the average policy would require 11 years of education to access reliably and exclude approximately 50% of the UK population [30]. While UK teachers must all possess an undergraduate degree, this still presents a substantial barrier to interacting with the policy on anything besides a superficial level.

During the analysis, it was also noted that there was a large variation in word count for the policies. In their analysis of policy accessibility, McDonald and Cranor used a value of 250 words per minute to find the time spent reading a policy [31]. Using that same value, it was calculated that an IS policy with the mean wordcount of just under 4000 words would take 16 minutes to read. Though most of the policies cluster on the short side, there are 6 policies that would take an hour or more to read.

Based on the results from Weidman and Grossklags' study, further analysis was conducted to see if there was a correlation between readability and either wordcount or technical content [1]. Bivariate analysis of the word count and reading difficulty revealed that there was a significant positive correlation between the word count of the policies and improved readability. This confirmed Weidman and Grossklags' findings that an increased word count resulted in improved readability [1].

Table 6. Bivariate Analysis of Word Count against Readability Scores (Note *p<0.01; **p<0.001)

	Flesch Reading Ease	**SMOG Score**
Word count of IS policy	.386**	-.202*

Bivariate analysis of the coded content and the readability scores was also conducted to see if the presence of technical content significantly decreased accessibility. Selected results with significant correlations are reported in Table 7 and confirm, particularly for the Flesch Reading Ease score, that the presence of a coded technical control increased with readability. While there are only a few contrary correlations in the SMOG results, this analysis still appears to indicate that the presence of the content does not in itself make the text harder to access. This result contrasts with Weidman and Grossklags' result and suggests that other factors are decreasing the readability [1]. It was noted during coding that many of the policies use very precise

language for the technical content, as demonstrated by this example, “Do not click on links in emails unless you know they are from a trusted source and never provide passwords in response to email requests”. To confirm this further research would need to be conducted into the impact of the writing style of the policies.

Table 7. Bivariate analysis of the presence of technical content against Readability Scores (Note *p<0.01; **p<0.001)

	Flesch Reading Ease score	**SMOG score**
Has detailed technical items	.294**	.211*
Mentions account control		.293**
Mentions anti-virus or malware	.296**	
Mentions BYOD conditions	.280**	.243*
Mentions locking stations	.249*	
Mentions passwords	.553**	
Mentions physical security	.274**	
Mentions security breaches or incidents	.244*	

5.4 Content versus breach data

In 2020 the UK government conducted a survey encouraging educational organisations to report on the state of Information Security within their organisation and the incidence of security breaches over the last year. This data has proved incredibly useful as prior to this survey the only breach data benchmarks in the UK were based around UK businesses [32].

It should be noted that the UK government survey is focused on technological controls in its questioning and it uses self-reported data submitted that is likely to have been reported by the school’s IT manager. A case could be made that these are the schools which feel confident in reporting their breaches and represent a best-case scenario.

Key points from this report are that:

- 11% of Primary and 13% of Secondary schools have an attack at least once a week
- 23% of Primary and 32% of Secondary schools reported material losses
- 41% of Primary and 65% of Secondary schools had to devote time or delay work to deal with these breaches
- 80% of Primary and 92% of Secondary schools have an IS policy

The report highlights that secondary schools are substantially more proactive than the average UK business (46% versus 76%) about identifying breaches due to GDPR; however, it should be noted that these breaches can range from an email redirect to a ransomware attack. The increased number of attacks reported by secondary schools in

Table 8 is likely to be because secondary schools have a different threat profile from primary schools. Secondary schools have an increased internal threat from students, hold more financial and personal data due their larger size and have the funding for IT resources to detect security incidents.

When the technical controls in this investigation's policy sample are contrasted against the data in the UK government's survey, there is a noticeable discrepancy in policy content. It is apparent in Table 8 that the controls reported by the schools are not reflected in many of the surveyed policies. This may be because some of these controls are not listed in schools' IS policies as these policies are primarily drawn up for staff members who are perceived as not needing to know the technical details. If this is the case, then these schools are taking a centralised approach to security that relies heavily upon the background technical controls and the competence of the IT managers to handle IS in the school.

Table 8. Relative Age Focus proportions for UK schools' policy content and UK government survey content [32]

Rules or controls in place	Primary Schools	Primary Schools (Government)	Secondary Schools	Secondary Schools (Government)
Patching	24%	97%	46%	99%
Anti-virus/Malware	64%	94%	54%	100%
Firewalls	42%	100%	46%	96%
Strong password policy	85%	97%	100%	93%
Account Control	54%	99%	46%	100%
Backup (Physical)	53%	69%	46%	82%
BYOD restrictions	64%	84%	54%	56%
Monitoring	54%	77%	85%	93%

When considering both the breach and content data, it is clear that the largest number of breaches involve staff interaction with the broader IT environment (redirects, phishing, malware), while the least common items in the school IS policy (spam/phishing attacks, public Wi-Fi usage and awareness of IS threats) also deal with staff interactions. This implies that the current IS policies have a substantial weakness involving human-IT interactions that is leading to increased cyber-attacks directed towards the human elements of the school organisation.

6 Conclusion

For this paper, 100 IS policies from UK primary and secondary schools were collected and analysed for their readability and content. It was found that 98% of these policies contained technical content, with the most common content items focusing on technical solutions, like password security. While there were some encouraging ex-

amples of schools realising that there was more to IS than technical controls, items dealing with security issues around the interactions of staff with IT, like spam/phishing attacks and awareness of IS threats, were substantially less common.

Despite the high occurrence of content rich IS policies, relative to UK businesses, security breaches are still rising in UK schools and this suggests that these policies are not as effective as they could be. As noted by other researchers, the presence of an IS policy, even one which meets industry standards, does not mean it has any relevance to those whom it applies and they may choose to ignore or work around it [11]. The research from this investigation also suggests two other possible factors for this ineffectiveness. Readability analysis of these IS policies found that they are on average difficult to access or a substantial time commitment due to policy length. Additional comparison with UK IS breach data also found a mismatch between the policy content and evolving threats that target the human element within an organisation, such as phishing emails and website redirects.

This has created a possible scenario where UK schools have derived a false sense of security from the presence of a policy which is not up to date with the evolving threat landscape and which does not engage the staff it is meant to inform.

There are, however, some examples within the sample of IS policies which have high readability scores, cover evolving threats targeting the human factors and keep the policy within a manageable wordcount. Further research could be conducted into the writing style, particularly the tone, of these policies and how teachers engage with and implement the content. The lessons from these further investigations could then be used to inform and improve IS policy creation by UK schools.

7 References

1. Weidman, J., Grossklags, J.: What's in your policy? An analysis of the current state of information security policies in academic institutions. 26th Eur. Conf. Inf. Syst. Beyond Digit. - Facet. Socio-Technical Chang. ECIS 2018. 1–16 (2018)

2. Laszka, A., Farhang, S., Grossklags, J.: On the Economics of Ransomware. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 10575 LNCS, 397–417 (2017). https://doi.org/10.1007/978-3-319-68711-7_21

3. Verizon: 2019 Data Breach Investigations. (2019)

4. Department for Digital, Culture, M. and S.: Cyber Security Breaches Survey 2019. (2019)

5. Department for Education: Statutory policies for schools and academy trusts, https://www.gov.uk/government/publications/statutory-policies-for-schools-and-academy-trusts/statutory-policies-for-schools-and-academy-trusts

6. Ponemon Institute: 2016 Cost of Cyber Crime Study and the Risk of Business Innovation. 1–37 (2016)

7. Siponen, M.T.: Analysis of modern IS security development approaches: Towards the

next generation of social and adaptable ISS methods. Inf. Organ. 15, 339–375 (2005). https://doi.org/10.1016/j.infoandorg.2004.11.001

8. Coles-Kemp, L.: Information security management: An entangled research challenge. Inf. Secur. Tech. Rep. 14, 181–185 (2009). https://doi.org/10.1016/j.istr.2010.04.005

9. Furnell, S., Clarke, N.: Power to the people? the evolving recognition of human aspects of security. Comput. Secur. 31, 983–988 (2012). https://doi.org/10.1016/j.cose.2012.08.004

10. Kolkowska, E., Dhillon, G.: Organizational power and information security rule compliance. Comput. Secur. 33, 3–11 (2013). https://doi.org/10.1016/j.cose.2012.07.001

11. Sadok, M., Bednar, P.M.: Understanding Security Practices Deficiencies: {A} Contextual Analysis. Ninth Int. Symp. Hum. Asp. Inf. Secur. {&} Assur. {HAISA} 2015 ,Lesvos, Greece, July 1-3, 2015, Proceedings. 151–160 (2015)

12. Coles-Kemp, L., Hansen, R.R.: Walking the line: The everyday security ties that bind. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 10292 LNCS, 464–480 (2017). https://doi.org/10.1007/978-3-319-58460-7_32

13. Chen, Y., Ramamurthy, K., Wen, K.W.: Organizations' information security policy compliance: Stick or carrot approach? J. Manag. Inf. Syst. 29, 157–188 (2012). https://doi.org/10.2753/MIS0742-1222290305

14. Balozian, P., Leidner, D.: IS security menace: When security creates insecurity. 2016 Int. Conf. Inf. Syst. ICIS 2016. 1–17 (2016)

15. Durgin, M.: Understanding the Importance of and Implementing Internal Security Measures, https://www.sans.org/reading-room/whitepapers/policyissues/understanding-importance-implementing-internal-security-measures-1901

16. Gordon, L., Loeb, M., Lucyshyn, W., Richardson, R.: 2006 CSI/FBI computer crime andsecurity survey. Comput. Secur. J. 22, 1 (2006)

17. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Q. 34, 523–48 (2010)

18. Kolkowska, E., Karlsson, F., Hedström, K.: Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inf. Syst. 26, 39–57 (2017). https://doi.org/10.1016/j.jsis.2016.08.005

19. Albrechtsen, E., Hovden, J.: The information security digital divide between information security managers and users. Comput. Secur. 28, 476–490 (2009)

20. Adams, A., Sasse, M.A.: Users Are Not The Enemy. Commun. ACM. 42, 40–46 (1999). https://doi.org/10.1145/322796.322806

21. Koppel, R., Smith, S., Blythe, J., Kothari, V.: Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient? IOS Press (2015)

22. Paananen, H., Lapke, M., Siponen, M.: State of the art in information security policy development. Comput. Secur. 88, 101608 (2020). https://doi.org/10.1016/j.cose.2019.101608

23. Chou, H.L., Chou, C.: An analysis of multiple factors relating to teachers' problematic information security behavior. Comput. Human Behav. 65, 334–345 (2016). https://doi.org/10.1016/j.chb.2016.08.034

24. Moyo, M., Abdullah, H., Nienaber, R.C.: Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems. 2013 Inf. Secur. South Africa. 1–6 (2013). https://doi.org/10.1109/ISSA.2013.6641062

25. Pusey, P., Sadera, W.A.: Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference. J. Digit. Learn. Teach. Educ. 28, 82–85 (2011). https://doi.org/10.1080/21532974.2011.10784684

26. Shen, L., Chen, I., Su, A.: Cybersecurity and Data Breaches at Schools. (2018)

27. Department for Education: Schools, colleges and children's services : School and college funding and finance, https://www.gov.uk/topic/schools-colleges-childrens-services/school-college-funding-finance

28. Department for Education: Schools, pupils and their characteristics: January 2019, https://www.gov.uk/government/statistics/schools-pupils-and-their-characteristics-january-2019

29. Feng, L., Jansche, M., Huenerfauth, M., Elhadad, N.: A comparison of features for automatic readability assessment. Coling 2010 - 23rd Int. Conf. Comput. Linguist. Proc. Conf. 2, 276–284 (2010)

30. NHS: Use a readability tool to prioritise content - NHS digital service manual, https://service-manual.nhs.uk/content/health-literacy/use-a-readability-tool-to-prioritise-content

31. McDonald, A., Cranor, L.: The cost of reading privacy policies. Isjlp. 4, 543–568 (2008). https://doi.org/10.1136/bmj.c2665

32. Department for Digitial, Culture, M.& S.: Cyber Security Breaches Survey 2020 - Education Annex. (2020)