What Can We Learn from the Analysis of Information Security Policies? The Case of UK's Schools

Martin Sparrius, Moufida Sadok, Peter Bednar

What can we learn from the analysis of information security policies? The case of UK's schools

Martin Sparrius[1[0000-0001-8586-6767]], Moufida Sadok[1[0000-0003-2981-6516]] and Peter Bednar[1[0000-0002-3631-2626]]

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

Abstract. Security standards consider that developing a security policy is a cornerstone in information security management. In practice, the development of a security policy is contextually dependent and there is no agreement on what organisations should include in their security policies. This paper argues that analysing information security policy documents could potentially provide new insights into existing issues with security practices. The paper explores and analyses the content and form of 100 UK schools' information security policies to assess their scope and accessibility. The key findings show that the content varied widely between schools but tended to have a technical focus, many security policies had not been updated to address changes to work practices due to the Covid-19 situation and many policies have poor readability scores preventing readers from engaging with them.

Keywords: Information Security, UK Schools, Information Security Policy, Readability score, Covid-19, ISO 27002

1 Introduction

Based on risk analysis, an information security policy (ISP) determines the critical assets that need to be protected, and includes procedures and control measures to prevent and respond to security incidents and breaches. ISO/IEC 27002 [1] stipulates that the objective of security policy is to provide management direction and support for information security in agreement with business requirements and relevant laws and regulations. The security standard also recommends that the statement of ISP objectives and scope should be fully documented. The document should provide information and instructions about how to implement the ISP and should include for example, authentication procedures, roles and responsibilities definition, awareness and training programs planning, business recovery measures and sanctions associated with policy violations. Specific parts of the security policy documents should be communicated to all users and relevant external partners.

Previous research [2] has highlighted the importance of using metrics to assess the quality of an ISP. In this paper, we argue that the analysis and review of security policy documents have the potential to provide useful information about the main features of an organisation's vision on information security management.

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 studies that data breaches and cyber-attacks targeting educational organisations have been on the rise [3, 4]. In their Data Breaches Investigation from 2021, Verizon found that 96% of the cyber-attacks involving educational organisations were financially motivated and that they specifically targeted personal data held by these organisations, with Social Engineering being the most common method of attack (47%) [5]. Subsequent to the implementation of the GDPR, it was found that the UK education sector was more likely than other UK sectors to have an ISP in place (75%) [6]. There appears to however been no independent academic research into the nature and quality of the content of UK school ISPs or how staff interact with them.

This paper reports the results of content analysis of 100 UK schools to assess their scope, the relevance of their components and the accessibility of their contents. It is organized as follows: the next section provides some theoretical background to this research. The third section details how ISPs were selected and analysed. The last section discusses the key findings and includes concluding remarks.

2 Background

While there is a wide recognition that an ISP is a key component of an effective information security governance, research in information security suggests that there are different views of what the content of an ISP is supposed to cover [7] and the form these policies take [2]. Some argue that ISP directives need to be detailed in a well-elaborated document [8–10]. Others suggest that only particular aspects of information use need to be covered such as remote working and security incident reporting. The content of an ISP can also address human behaviour and target different groups of users [11]. In this context, ISP document specifies guidelines and procedures that employees must adhere to in their daily interactions with the IT system [12]. The identification of the rights and responsibilities of the organisation members is particularly useful to assist with future decisions when handling information [13].

An ISP document may also outline the specific actions to prevent, respond to and mitigate security incidents. This could include detailed description of monitoring, mitigation and investigation activities that should be assigned to an incident response team (IRT). Monitoring is particularly important since security attacks are growing in frequency, severity and impact and the role of an IRT is crucial in gathering, analysing and archiving digital evidences. When it comes to guides for ISP content, organisations can choose from many different frameworks and could for example refer to security standards such as ISO27002 and/or EU directives for processing personal information. It is, however, challenging in practice to craft a fit-for-purpose ISP as this requires a

thorough contextual analysis of an organisation's strategy, structure and culture. Karyda et al.[14] suggest that contextual factors such as organisational structure, organisational culture, management support, users' participation in the formulation process, training and education influence the formulation and implementation of ISPs. Karlsson et al. [15] found that employees experienced difficulties in following policies due to inadequate explanation and use of terms, inconsistent explanations of the controls, and unexplained policy architecture. A critical analysis of a sample of security policies from the UK's National Healthcare Service by Stahl et al. [16] concluded that security policies can privilege certain groups of stakeholders such as managers and information technology (IT) professionals and do not sufficiently integrate the views and concerns of doctors and nurses about medical matters. Inadequate involvement of staff makes it even less likely that the existence of security policies will lead to effective implementation or relevance from users' perspective [17]. Although an ISP document could include rich and useful information about an organisation's vision of information security, it has been noted that how the policy is constructed can also have a dramatic effect on its effectiveness [2]. In addition, collecting ISPs documents for analysis is very challenging [18], with many organizations regarding the analysis of this documentation as very intrusive [3] and there is still a substantial gap in understanding what organisations include in their ISPs.

In the 2021 UK government survey of schools and colleges it was found that approximately 75% of schools had developed an ISP [6]. However, 47% of the surveyed schools reported multiple security breaches, with phishing (85%), malware (12%) and DDoS (12%) attacks forming the bulk of successful attacks [19]. This discrepancy between having an ISP and still suffering high levels of successful attacks has been highlighted in previous research [3]. This is a cause for concern and it is possible that UK schools ISPs have the same inherent problems over content and form that have been highlighted in other sectors. This paper argues that the analysis of both the content and form of ISPs from UK primary and secondary schools will provide insights into existing issues with security practices within schools.

3 Data collection and analysis

UK schools generally publish their policies for parental review and therefore are accessible in the public domain. The ISPs for the study were obtained using two different search engines (Google and Duck Duck Go), allowing the use of different searching algorithms to produce different search results. The keywords used in this search were "Information Security", "Policy" and "UK School", with other variations and additions as the search progressed. To ensure the policies were up to date each policy was double-checked on the school's website by either 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 primary focus on students, rather than on 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 ISP [3]. The final sample comprised a total of 100 policies from 73 primary schools and 27 secondary schools which is broadly in line with the expected ratio of UK primary and secondary schools [19]. Next, the UK Government school database [19] 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. Initial coding used two categories: Security Management (Organisational Philosophy, Information Security Structure) and Computer Security (Technical Controls, Specific User Responsibilities). These categories were based on Weidman and Grossklags' analysis of university ISPs [3], then the coding was refined using an iterative analysis of a sample of 10 policies. Coding was assigned to content that met the required criteria, irrespective of the potential quality or accuracy of the content. Each policy was then entered into a website readability calculator, Readable, to obtain the word count, Flesch Reading Ease and Simple Measure of Gobbledygook (SMOG) scores. These results were then added to the attribute date for each policy.

3.1 Content of ISPs

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 desired content. For each age focus (primary and secondary schools), the sum of policies which contained the specific content code was divided into the total number of policies for that age focus. The results are presented in Tables 1 and 2.

Table 1. Percentage of schools ISPs containing Security Management content

Content code	**Primary Schools**	**Secondary Schools**
Clearly states who issued policy	59%	**88%**
Has a next review date	57%	68%
Has an effective from 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 2. Percentage of schools ISPs containing Computer Security content

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%

3.2 Accessibility

Accessibility is generally recognised as how easy it is for a person to read and understand a piece of text [20]. To extend upon the work done by Weidman and Grossklag [3] the same measures of accessibility (readability and word count) were investigated. To calculate the readability score, Flesch Reading Ease was used due to its popularity in research [21], and Simple Measure of Gobbledygook (SMOG) due to its recommended use by the UK's National Health Service [20]. Flesch Reading Ease bases its results on word/sentence length ratios and syllables/word ratios. The scoring ranges from 0-100, and Flesch has a recommended target of 30-50 [3]. 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 [20]. The accessibility results are presented in Table 3.

Table 3. Accessibility analysis of ISPs

	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

The mean Flesch Reading Ease (42.7) and SMOG scores (12.9) both fall within the recommended targets, but have a high standard deviation with outlier policies tending to occur in the regions of lower readability. The average ISP consisted of approximately 10 pages of content, but the standard deviation for this was very high and there were a number of policies sitting at the extreme ends of the range. Based on the results from Weidman and Grossklags' study[3], further analysis was conducted to see if there was a correlation between readability and either wordcount or technical content [3]. 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 (Table 4). This confirmed Weidman and Grossklags' findings that an increased word count resulted in improved readability [3].

Table 4. Bivariate Analysis of Word Count against Readability Scores (Note *p<0.01; **p<0.001)

	Flesch Reading Ease	SMOG Score
Word count of ISP	.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 5 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 [3].

Table 5. 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*	

3.3 Updating of ISPs

The outbreak of Covid-19 has created new challenges and working conditions within UK schools. These schools have had to shift to working from home during the Covid-19 outbreak and staff and schools have had to make use of programs, such as Microsoft Team and Google Meet, with which they have potentially had relatively little or no training. To examine if this work shift was mirrored within the school's ISPs, all 100 ISPs were revisited one year after the initial collection. Each original policy was examined to see if it had been due an update, either as stipulated by a published review date or if two years had passed since the last published change. Policies with no included dates were placed in a separate category. Each policy was examined to see if there had been changes in any of the following: dates and names, structure/writing style, content, changed into a new type of policy. The final analysis placed each policy into one of three groups: due, an update, not due an update and no date mentioned. Each of these categories was sub-divided into five categories: No Change – policy was identical to original policy; Superficial change – a date or person's name was changed; Meaningful – Substantial content change was present (both positive and negative); Different policy – such as becoming an Acceptable Use or GDPR policy; No longer present – policy has been removed and can no longer be found on the website or via Google search.

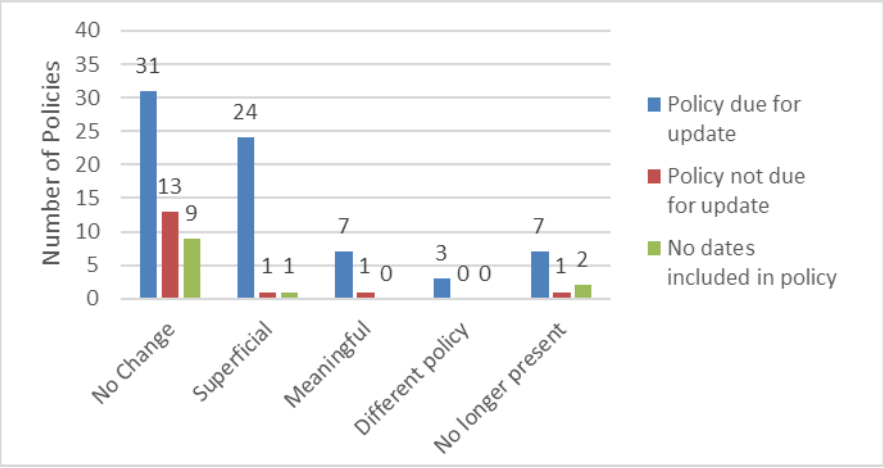

Fig. 1. Results of the update analysis

Figure 1 shows that 72 of the 100 policies were due to be updated, with 41 of those policies having received some form of revision. Of the remaining 28 policies that either lacked any date information or were not due to be revised only three had been revised.

4 Discussion and conclusions

The results from the content analysis revealed a wide variation between ISPs in terms of both organisational and technical content. Analysis of the technical controls found that controls regarding passwords, physical security, encryption, locking workstations and information security 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 [22]. 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 least common items deal with security issues that involve staff interactions with the broader IT world such as spam/phishing attacks, public Wi-Fi usage and awareness of IS threats. There is little indication within the policies of why these are under-represented but considering that Multi-Factor Authentication is effectively non-existent 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 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 for the Social Engineering attacks that UK government has identified as the most likely to affect UK schools [4].

ISP content differed between Primary and Secondary schools. Primary schools focused more on justifying content (93% vs 88%) and explaining roles (70% versus 52%) while Secondary schools tended focus more on policy administration, such as dates (78% vs 92%) and technical controls, such as monitoring staff accounts (54% vs 68%). 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 management, 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.

Accessibility analysis of the school ISPs found that there was substantial variation in the readability 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 scores, the average policy would require 11 years of education to reliably access the content and would exclude approximately 50% of the UK population [19]. 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 [23]. Using that same value, it was

calculated that an ISP with the mean word count of just under 4000 words would take 16 minutes to read. Though most of the policies cluster on the short side, there are six policies that would take an hour or more to read.

In conclusion, there are some good examples within the sample of ISPs that have high accessibility, cover attacks targeting the human factors and have evolved to keep track of current threats. Most of the ISPs however are static and focus primarily on routine technical content. This is to some extent alarming as human factors are equally important in ensuring effective security practices. According to Cyber Security Breaches Survey 2021 [6], the largest number of breaches involve staff interaction with the broader IT environment (redirects, phishing, malware), which correspond to the least common items in the school ISP (spam/phishing attacks, public Wi-Fi usage and awareness of security threats). This implies that the current ISPs have a substantial weakness involving human-IT interactions. This result is consistent with previous research highlighting that actual work practices and routines of most employees were often ignored in the development and operation of security management efforts [24]. Further, the accessibility analysis of the analysed ISPs found that they are on average difficult to access and require a substantial time commitment due to policy length. This raises concerns around the effective implementation of the ISP as the staff are unlikely to engage with the content. Future research could explore the interaction of teachers with ISPs, their perception about their usefulness, and to what extent they reflect and address teachers' work practices in their everyday situation. In addition, further research needs to be conducted into how UK schools can develop their ISPs in order to meet the challenges of managing information security and engaging staff successfully.

5 References

1. Standard, I.: ISO/IEC 27002 - Code of practice for information security management. (2005)
2. Goel, S., Chengalur-Smith, I.N.: Metrics for characterizing the form of security policies. J. Strateg. Inf. Syst. 19, 281–295 (2010). https://doi.org/10.1016/j.jsis.2010.10.002
3. 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)
4. 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
5. Verizon: 2021 Data Breach Investigations Report. Verizon Bus. J. (2021). https://doi.org/10.1057/s41280-018-0097-z
6. Department for Digitial, Culture, M.& S.: Cyber Security Breaches Survey 2021 - Education institutions findings annex. (2021). https://doi.org/10.1016/s1361-3723(20)30037-3
7. 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

8. David, J.: Policy enforcement in the workplace. Comput. Secur. 21, 506–513 (2002). https://doi.org/10.1016/S0167-4048(02)01006-4
9. Klaić, A.: Overview of the state and trends in the contemporary information security policy and information security management methodologies. MIPRO 2010 - 33rd Int. Conv. Inf. Commun. Technol. Electron. Microelectron. Proc. 1203–1208 (2010)
10. Pathari, V., Sonar, R.: Identifying linkages between statements in information security policy, procedures and controls. Inf. Manag. Comput. Secur. 20, 264–280 (2012). https://doi.org/10.1108/09685221211267648
11. Doherty, N.F., Anastasakis, L., Fulford, H.: The information security policy unpacked: A critical study of the content of university policies. Int. J. Inf. Manage. 29, 449–457 (2009). https://doi.org/10.1016/j.ijinfomgt.2009.05.003
12. Cram, W.A., Proudfoot, J.G., D'Arcy, J.: Organizational information security policies: A review and research framework. Eur. J. Inf. Syst. 26, 605–641 (2017). https://doi.org/10.1057/s41303-017-0059-9
13. Baskerville, R., Siponen, M.: An information security meta-policy for emergent organizations. Logist. Inf. Manag. 15, 337–346 (2002). https://doi.org/10.1108/09576050210447019
14. Karyda, M., Kiountouzis, E., Kokolakis, S.: Information systems security policies: A contextual perspective. Comput. Secur. 24, 246–260 (2005). https://doi.org/10.1016/j.cose.2004.08.011
15. Karlsson, F., Hedström, K., Goldkuhl, G.: Practice-based discourse analysis of information security policies. Comput. Secur. 67, 267–279 (2017). https://doi.org/10.1016/j.cose.2016.12.012
16. Stahl, B.C., Doherty, N.F., Shaw, M.: Information security policies in the UK healthcare sector: A critical evaluation. Inf. Syst. J. 22, 77–94 (2012). https://doi.org/10.1111/j.1365-2575.2011.00378.x
17. Dhillon, G., Torkzadeh, G.: Value-focused assessment of information system security in organizations. Inf. Syst. J. 16, 293–314 (2006). https://doi.org/10.1111/j.1365-2575.2006.00219.x
18. Kotulic, A. G. and J. G. Clark (2004). "Why there aren't more information security research studies. Information and Mnagement. 41 (5), 597–607.
19. Department for Education: Schools, pupils and their characteristics: January 2019, https://www.gov.uk/government/statistics/schools-pupils-and-their-characteristics-january-2019
20. 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
21. 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)
22. Department for Education: Statutory policies for schools and academy trusts - GOV.UK, https://www.gov.uk/government/publications/statutory-policies-for-schools-and-academy-trusts/statutory-policies-for-schools-and-academy-trusts
23. McDonald, A., Cranor, L.: The cost of reading privacy policies. Isjlp. 4, 543–568 (2008). https://doi.org/10.1136/bmj.c2665

24. Sadok M, Alter, S. and Bednar P. (2020). It is not my job: exploring the disconnect between corporate security policies and actual security policies in SMEs. Information & Computer Secuirty, Vol. 28 No. 3, pp. 467-483.