Issues and Trends in Information Security Policy Compliance

Surayahani Hasnul Bhaharin
Centre for Cyber Security
Faculty of Information Science & Technology,
Universiti Kebangsaan Malaysia (UKM)
Selangor, Malaysia
surayahanihasnul@gmail.com

Rossilawati Sulaiman
Centre for Cyber Security
Faculty of Information Science & Technology,
Universiti Kebangsaan Malaysia (UKM)
Selangor, Malaysia
rossilawati@ukm.edu.my

Umi Asma' Mokhtar
Centre for Cyber Security
Faculty of Information Science & Technology,
Universiti Kebangsaan Malaysia (UKM)
Selangor, Malaysia
umimokhtar@ukm.edu.my

Maryati Mohd Yusof
Centre for Software Technology & Management
Faculty of Information Science & Technology,
Universiti Kebangsaan Malaysia (UKM)
Selangor, Malaysia
maryati.yusof@ukm.edu.my

***Abstract*— In the era of Industry 4.0 (IR 4.0), information leakage has become a critical issue for information security. The basic approach to addressing information leakage threats is to implement an information security policy (ISP) that defines the standards, boundaries, and responsibilities of users of information and technology of an organization. ISPs are one of the most commonly used methods for controlling internal user security behaviours, which include, but not limited to, computer usage ethics; organizational system usage policies; Internet and email usage policies; and the use of social media. Human error is the main security threat to information security, resulting from negligence, ignorance, and failure to adhere to organizational information security policies. Information security incidents are a problem related to human behaviour because technology is designed and operated by humans, presenting the opportunities and spaces for human error. In addition to the factor of human error as the main source of information leakage, this study aims to systematically analyse the fundamental issues of information security policy compliance. An analysis of these papers identifies and categories critical factor that effect an employee's attitude toward compliance with ISP. The human, process, technology element and information governance should be thought as a significant scope for more efficiency of information security policy compliance and in any further extensive studies to improve on information security policy compliance. Therefore, to ensure these are properly understood, further study is needed to identity the information governance that needs to be included in organizations and current best practices for developing an information security policy compliance within organizations.**

Keywords—compliance, information security policy, security behaviour, information security, information governance, threats, information security management

I. INTRODUCTION

Information security management is a crucial endeavour in ensuring that an organization's information is kept safe from any security threat. The protection and security of organizational information are increasingly challenging in the era of Industry 4.0, due to sophisticated security threats. Information security management plays an important role in ensuring that the functions and operations of the public service business are implemented efficiently, effectively, and securely [1]–[3]. Information security management is necessary to safeguard an organization's information and information systems from unauthorized access, disclosure, disruption, and destruction, while preserving confidentiality, integrity, and availability (CIA) [4], [5]. According to [6], up until the early 1980s, solutions to information security had focused mainly on technical issues. However, experts are now aware that technological solutions alone cannot guarantee organizational information security [7]. In fact, a 100% security guarantee is impossible as there are risks, threats, and vulnerabilities that may be unknown [8]. Risks, threats, and weaknesses are evolving and changing over time as information and communication technology (ICT) advances. Information security issues need to be addressed from a broader, holistic approach, to the maintenance of CIA information. In recent years, many studies on information security have begun to incorporate human and management aspects, and are no longer limited to the technical issues that need to be addressed in the current landscape of security threats [4], [9], [10]. These include the components of governance, where top management plays a very important role in managing information security within the organization [1], [9] to address business risks and ICT [11]. Several remaining issues should be explored in future research, as this research stream moves forward.

This paper is aimed at further understanding of what the trends or issues in information security policy compliance among the employees by synthesising the existing literature. This paper provides an overview of information security policy compliance issues. The successful implementation of an information security policy is related to the challenges in areas such as enforcement, dissemination, employees' awareness, and their behaviour. Several factors influence employees' behaviour to comply with the organization's ISP, i.e. the human, the process, and the technology factors. The purpose of this paper is to investigate and better understand the issues related to information security policy compliance.

The remainder of this paper is organized as follows: Section II discusses related works in ISP compliance, Section III discusses the research method, Section IV describes the issues of ISP compliance in detail, whereas the discussion of this paper is offered in Section V. Finally, Section VI concludes this paper, along with the recommendation for future work.

978-1-7281-6726-8/19/$31.00 ©2019 IEEE

II. Related Works

The Information and Communication Technology (ICT) revolution has made a huge impact on organizations, including the public service. These developments have led to the emergence of new technologies, such as CYOD (Choose Your Own Device), Internet-of-Things (IoT), data warehousing, BYOD (Bring Your Own Device), cloud-based computer systems and Industry 4.0. Generally, new technologies pose risks to vulnerability [12] and present unexpected security risks. Even with the high reliance on technology for a competitive advantage, security issues are a major challenge in achieving organizational goals.

Advances in web-based technologies and services occur at a high pace, worldwide. However, information security is still a major issue among experts and users. Organizations and consumers are concerned about cyber-attacks and are constantly working to minimize information security risks [7], [13]. Although the implementation of technological controls is important, the reliance on technological solutions is insufficient in reducing security risks, especially information leakage. IBM X-Force Research (2017)[14]; InfoWatch (2017)[15]; Ponemon Institute (2018)[16]; and Symantec Corporation (2019)[17] reported that the number of security incidents is increasing. Previous security threats entail no more than the physical loss of data and the malfunction of mobile equipment as a result of user neglect [18]. Data leakage is now more complex because it transpires online and is difficult to detect. In fact, intruders are financially funded and security breaches are carried out on a large scale [19]–[21]. New threats, such as cryptojacking, formjacking, powershell, ransomware, and malicious emails are aimed at obtaining sensitive information illegally [17].

Technology-based solutions, such as outbound content compliance (OCC), extrusion prevention (EP), data loss prevention (DLP)content monitoring and protection (CMP), information leak prevention and detection (IDLP), content monitoring and filtering (CMF) and information protection and control (IPC), do not guarantee the security of organizational information [22]–[24]. Furthermore, technology-based approaches often increase administrative and maintenance costs, as well as security risks [25]–[27]. Employees find that the implementation of such technologies is unsettling because there is an information gap between software and hardware in the usage of the information system. [28] also argued that despite large investments, software and hardware still do not reduce the security problems faced by organizations. Therefore, investments in various security technologies have little impact on the efficacy of information security [29]–[31].

Experts believe that the mere aspect of technology in information security does not guarantee a safe environment, and that information security (human) behaviour should be taken into account [4], [32]. The importance of the human element in the information security domain cannot be underestimated [7]. Information security management should consider users and their perceptions as significant factors in providing a safer environment. In other words, users are central to security. Reducing and protecting against information security risks need to be addressed at several levels; thus, behavioural science performs a significant impact on the development, architecture, maintenance t, and of web-based systems [33]. An increase in the number of security incidents in an organization indicates that technological control is insufficient in preventing information security breaches.

Past researchers have argued that security issues should be addressed in a more comprehensive way, taking into account the human, organizational, cultural, ethical, policy, and legal elements [9], [34], [35]. Whereas [36]–[38], on the other hand, viewed that the practice of information governance (IG) is just as important as the implementation of technological controls in providing better protection of organizational information. IG organizations rely on various aspects, such as the success and application of security planning, procedures, guidelines, and security measures, as well as the consideration of human aspects as one of the key components [4], [39], [40].

The importance of good management practices in protecting organizational information sources has also been recognized. For example, there is a great deal of literature on the importance of security policies and their role in security programmes, security risk management, security awareness, incident response, security culture, and higher management involvement, with many security programmes discussed in previous studies. In addition, international standards, such as the ISO 27000 series, the National Institute of Standards and Technology (NIST), Special Publication 800, and Control Objectives for Information and Related Technology (COBIT), have been developed to assist organizations in establishing good information security management. However, there is still a lack of research to consider all the crucial elements of information security, namely, the people, the processes, and technologies that are the axis of information security. In addition, previous studies have examined those elements, though they were expressed separately [9], [41], [42], and the proposed solutions are still practical in solving current problems.

Empirical studies have shown there is an essential need for integrating domain information security and information governance (IG) [43]–[47]. The concept of IG is often discussed in various disciplines, such as record management, freedom of information, e-discovery and privacy of information, and in all activities involving data [44]. The concept of information governance began to emerge in the late 1990s and was a major focus of health-care information in the United Kingdom. Since the mid-2000s, the IG has been active in various disciplines involving information-based services. As a result, the definition of IG is unclear and signifies different meanings in various disciplines [44]. Changes in corporate governance, new global laws and regulations relating to information, and the increasing amount of information used in organizations have led to the need for a clear IG model/framework with a consistent definition, an appropriate disciplinary integration, and suitable approaches to implementation [44], [48]. The lack of a comprehensive IG framework has led organizations to redesign their records management and information programmes into IG programmes without realizing that the IG involves various concepts, such as risk management, legal compliance, information security, and business intelligence [49].

III. Method

This paper conducted a review based on several scientific research from different academic databases, such as ScienceDirect, IEEE, WoS and Springer. The review was applied to papers published from 2014 to 2018, by using a keyword relevant to information security policy compliance. The content analysis was carried out to select and organize the papers appropriately.

As a result, the search identified various topics on ISP compliance and its framework, which include the definition of ISP compliance, key factors influencing ISP compliance, challenges of ISP compliance, the cultivation process for implementing ISP, assessment instrument for ISP compliance, and general issues regarding ISP compliance. Several studies have explored on ISP compliance and included data collection and analysis.

IV. Information Security Policy Compliance

Information security policy compliance is more important than ever before in the face of increasingly complex cyber-attacks. Among the efforts to protect the organization against cyber-attacks are the enforcement of guidelines, security frameworks, and frequently-cited standards, such as ISO 27001, COBIT 5, and ITIL. However, efforts such as compliance with standards and use of technology are often hindered by security issues and incidents [50]. The success and impediment of information security programmes within the organization are based on three main contexts, namely Human, Process, and Technology [51]. The human context is often considered the weakest link that poses a threat to cyber security and organizational information [52]–[54], while the process context relates to the organization's readiness to implement information security plans, including training of workers, enforcement of policies, and special budgets for security programmes [55], [56]. The use of technologies, such as information security systems, helps organizations to implement security policies and to control security incidents. However, rapid technological developments and system weaknesses pose challenges to organizations in improving information security [51], [56], [57]. To better understand the issues, evaluating the findings on information security policy compliance in previous research is important. Table I presents an overview of related literature.

TABLE I: Review of Information Security Policy Compliance in The Contexts Of Human, Process, and Technology

Source	Context			Information security Themes	Key Findings
	H[a]	P[b]	T[c]		
[58]	/			Information security, insider threats, deterrence, motivation, risk,	Perceived sanctions certainty and severity significantly influence employees' attitudes
[32]	/			human, Information security policy, user behaviour, information security management, Compliance management	Information security policy promotion, security policy noncompliance, security policy management, and shadow security are challenges to information security policy compliance
[59]		/		IT management, Information security, Organisational policy, International standards, Individual behaviour	Factors that determine security behaviour are top management participation, adapting individual characteristics, accepting the cultural context, inspring employees to comply, and respecting the cost of compliance.
[29]	/	/		information security, human factor, awareness delivery methods, social engineering, information security programme	Mixed technique approaches enhance individual security awareness.
[4]	/			Information security, security behaviour, awareness, risk	Lacking information security awareness (ISA) as a cause of many reasons and it's important to improve users' ISA continuously.
[7]	/			Information security, Conscious care behaviour, Awareness, Risk	Good information security behaviour, or information security conscious care behaviour, reduces the employees' behavioural errors.
[52]	/		/	Human factors, Information security policy User behaviour, Information security management, Compliance management,	The author developed a prototype system to replicate the proposed model to work as a real system that responds to the behaviour of users (violations and compliance behaviour)
[24]	/		/	Security behaviour, Information security policy compliance	The environment, technology, type of business, and legal environment, affected security behaviour
[60]	/			Information security, Information security policy compliance	Intention to comply with information security policies influence on actual compliance policies. The top management has to remind the employees of the significance of information security and how it is important.

[a.] Human, [b] People, [c] Technology

Security incidents involving organizational sensitive information have been widely discussed lately in industry, academia, and politics. Threats to organizational information are categorized into two perspectives [61], technical and non-technical. Although technical aspects have been widely discussed in previous studies, the solution to the reduction of security incidents is still uncertain [62]. [63] considered machine learning to dominate previous studies but the majority of these studies failed when tested with real data sets. The findings also show that the previous studies were conducted separately on the technical and non-technical aspects. In fact, the studies carried out a breakdown of each other's key elements of human security, processes, and technology. Technology-based studies are simply ineffective because real threats are not identified in the early stages, such as internal user security behaviours. Therefore, the need for better technology is in line with security policy requirements, fostering consumer security behaviours and systematic information management i5n the face of increasingly complex information security threats.

Individual security behaviours, as a significant mechanism, influence organizational policy compliance [37], [52], [64]. However, an argument in the same stream posits that compliance remains a challenge in protecting organizational information technology assets [60]. Relevant studies focus on human factors that determine compliance [65] and integrate specific behavioural theories to assess levels of compliance within an organization [37], [39], [52]. Although existing models and frameworks provide useful guidance in the study of security behaviours, they are complex and they address an issue separately. In reality, security management requires a holistic view in developing an information security culture, where security habits as a part of the organization. [6], [24], [59].

This study of current ISP compliance research presents the need for additional studies outside the contexts of human, process, and technology. IG has become increasingly imperative due to the availability of data in various formats at various levels of the organization. Good IG programmes produce quality data, improve delivery systems, and support strategic decision-making management [66], [67]. Despite the importance of the IG, the lack of a clear information management framework in the development, integration, and use of various information security technologies has led to high investment in technology, yet the results have not been satisfactory. A holistic model is therefore needed to integrate the IG principles outlined by the Association of Managers and Records Administrators (ARMA) and to detail how information should be governed in the contexts of human, process, and technology.

V. Discussion

The need for more relevant studies on employee security behaviours and other values in organizations, such as IG, as well as the use of technology, is crucial in building a better understanding of addressing information security issues [61], [68]. Therefore, the understanding of the theoretical relationship of behaviour with other elements allows for the development of a more holistic model in studying security behaviour factors, as well as exploring how levels of compliance can be enhanced within organizations with practices and procedures in protecting information technology assets. The need for employees to understand the issue of compliance with information security policies is also vital; one way to understand it is by integrating human elements (security behaviours), supported by process elements (policies) and technologies. Although [22], [58], [69] anticipated the potential integration of various elements in raising the level of compliance with information security policies, it has not been empirically proven that such integration can contribute to the reduction of organizational security incidents. IG's ability to support other information security contexts requires further research and should be explored in depth for the purpose and process of increasing the information security level in an organization [43].

VI. Conclusion

In conclusion, this study highlights the current issues in information security policy compliance. The attitude in complying with information security organizational policies also has a significant effect on information security compliance behaviour. However, technology and organizational factors also positively effect employees' intention to adhere to information security policy. Future developments are intended to improve this ISP compliance even more. The study on ISP compliance should focus on extended methods for enhancing employees' attitude in complying with information security organizational policies.

Acknowledgment

We are pleased to express our gratitude to Public Service Department of Malaysia and Universiti Kebangsaan Malaysia (DCP-2013-013/6) for the financial support of this study.

References

[1] R. Abdul Munir, Nurul Nuha Abdul Molok, and S. Talib, “Exploring the Factors influencing Top Management Involvement and Participation in Information Security,” in Pacific Asia Conference on Information Systems, 2017.

[2] M. Burdon, B. Lane, and P. Von Nessen, “Data breach notification law in the EU and Australia - Where to now?,” Comput. Law Secur. Rev., vol. 28, no. 3, pp. 296–307, 2012.

[3] S. Suhaiza and M. Y. Zawiyah, “Public sector ict strategic planning: framework of monitoring and evaluating process,” Asia-Pacific J. Inf. Technol. Multimed., vol. 6, no. 1, pp. 85–99, 2017.

[4] M. Alohali, N. Clarke, S. Furnell, and S. Albakri, “Information security behavior: Recognizing the influencers,” in 2017 Computing Conference, 2018, no. July, pp. 844–853.

[5] J. Paliszkiewicz, “Information Security Policy Compliance: Leadership and Trust,” J. Comput. Inf. Syst., vol. 59, no. 3, pp. 211–217, May 2019.

[6] R. von Solms and S. H. (Basie) von Solms, “Information Security Governance: A model based on the Direct–Control Cycle,” Comput. Secur., vol. 25, no. 6, pp. 408–412, Sep. 2006.

[7] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, A. G. Norjihan, and H. Tutut, “Information security conscious care behaviour formation in organizations,” Comput. Secur., vol. 53, pp. 65–78, 2015.

[8] K. Kaur, I. Gupta, and A. K. Singh, “A Comparative Study of the Approach Provided for Preventing the Data Leakage,” Int. J. Netw. Secur. Its Appl., vol. 9, no. 5, pp. 21–33, 2017.

[9] Z. A. Soomro, M. H. Shah, and J. Ahmed, “Information security management needs more holistic approach: A literature review,” Int. J. Inf. Manage., vol. 36, no. 2, pp. 215–225, 2016.

[10] N. Vithanwattana, G. Mapp, and C. George, “Developing a comprehensive information security framework for mHealth: a detailed analysis,” J. Reliab. Intell. Environ., vol. 3, no. 1, pp. 21–39, 2017.

[11] A. Singh and B. Kapoor, “Analysis of the Human Factor behind Cyber Attacks,” Int. Res. J. Eng. Technol., vol. 3, no. 14, pp. 1166–1172, 2016.

[12] T. Pereira, L. Barreto, and A. Amaral, “Network and information security challenges within Industry 4.0 paradigm,” Procedia Manuf., vol. 13, pp. 1253–1260, 2017.

[13] H. Noor Hafizah and I. Zuraini, “A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment,” Procedia - Soc. Behav. Sci., vol. 65, pp. 1007–1012, Dec. 2012.

[14] IBM X-Force Research, “Security trends in the information and communication technology industry,” 2017.

[15] InfoWatch, “Data leaks. ASEAN countries, India, South Korea,” 2017.

[16] Ponemon Institute, “2018 Cost of a Data Breach Study : Global Overview,” IBM Secur., no. July, pp. 1–47, 2018.

[17] Symantec Corporation, “Internet Security Threat Report Volume 24,” 2019.

[18] P. Gordon, “Data Leakage - Threats and Mitigation,” 2007.

[19] G. Cascavilla, M. Conti, D. G. Schwartz, and I. Yahav, “The insider on the outside: a novel system for the detection of information leakers in social networks,” Eur. J. Inf. Syst., vol. 9344, pp. 1–16, 2017.

[20] I. Ghafir, P. Vaclav, A. Ahmad, and H. Mohammad, “Social Engineering Attack Strategies and Defence Approaches,” in IEEE 4th International Conference on Future Internet of Things and Cloud, 2016.

[21] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, “Investigating the impact of cybersecurity policy awareness on employees ’ cybersecurity behavior,” Int. J. Inf. Manage., vol. 45, no. October 2018, pp. 13–24, 2019.

[22] N. S. Safa and C. Maple, “Human errors in the information security realm – and how to fix them,” Comput. Fraud Secur., vol. 2016, no. 9, pp. 17–20, 2016.

[23] M. J. Alotaibi, S. Furnell, and N. Clarke, “A Novel Model for Monitoring Security Policy Compliance,” J. Internet Technol. Secur. Trans., vol. 5, no. 3/4, September/December 2016, pp. 505–514, 2016.

[24] I. Topa and M. Karyda, “Identifying Factors that Influence Employees’ Security Behavior for Enhancing ISP Compliance,” in Computer Systems Science and Engineering, vol. 9264, no. 6, S. Fischer-Hübner, C. Lambrinoudakis, and J. López, Eds. Cham: Springer International Publishing, 2015, pp. 169–179.

[25] B. Bulgurcu, H. Cavusoglu, B. Izak, and Benbasat, “Information Security Policy Compliance : An Empirical Study Of Rationality-Based Beliefs and Information Security Awareness,” MIS Q., vol. 34, no. 3, pp. 523–548, 2010.

[26] K. Gillon, L. Branz, M. J. Culnan, G. Dhillon, R. Hodgkinson, and A. MacWillson, “Information Security and Privacy: Rethinking Governance Models,” Commun. Assoc. Inf. Syst., vol. 28, no. 1, p. 38, 2011.

[27] M. Siponen and J. Iivari, “Six Design Theories for IS Security Policies and Guidelines,” J. Assoc. Inf. Syst., vol. 7, no. 7, pp. 445–472, 2006.

[28] S. Pahnila, M. Siponen, and A. Mahmood, “Employees ’ Behavior Towards IS Security Policy Compliance,” in Proceeding of the 40th Hawaii International Conference on System Science, 2007, pp. 1–10.

[29] J. Abawajy, “User preference of cyber security awareness delivery methods,” Behav. Inf. Technol., vol. 33, no. 3, pp. 237–248, Mar. 2014.

[30] K. Jansson and R. von Solms, “Phishing for phishing awareness,” Behav. Inf. Technol., vol. 32, no. 6, pp. 584–593, Jun. 2013.

[31] R. Von Solms, K. L. Thomson, and P. M. Maninjwa, “Information security governance control through comprehensive policy architectures,” in 2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference, 2011.

[32] M. J. Alotaibi, S. Furnell, and N. Clarke, “Information security policies: A review of challenges and influencing factors,” in 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 2016, pp. 352–358.

[33] K. Padayachee, “Taxonomy of compliant information security behavior,” Comput. Secur., vol. 31, no. 5, pp. 673–680, Jul. 2012.

[34] B. Lundgren and N. Möller, “Defining Information Security,” Sci. Eng. Ethics, pp. 1–23, 2017.

[35] E. Niemimaa and M. Niemimaa, “Information systems security policy implementation in practice: from best practices to situated practices,” Eur. J. Inf. Syst., vol. 26, no. 1, pp. 1–20, Jan. 2017.

[36] M. Carcary, K. Renaud, S. McLaughlin, and C. O’Brien, “A Framework for Information Security Governance and Management,” IT Prof., vol. 18, no. 2, pp. 22–30, Mar. 2016.

[37] A. Da Veiga, “Comparing the information security culture of employees who had read the information security policy and those who had not,” Inf. Comput. Secur., vol. 24, no. 2, pp. 139–151, Jun. 2016.

[38] M. R. Fazlida and S. Jamaliah, “Information Security: Risk, Governance and Implementation Setback,” Procedia Econ. Financ., vol. 28, no. April, pp. 243–248, 2015.

[39] W. Rocha Flores, E. Antonsen, and M. Ekstedt, “Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture,” Comput. Secur., vol. 43, pp. 90–110, Jun. 2014.

[40] A. Zauwiyah, T. S. Ong, H. L. Tze, and N. Mariati, “Security monitoring and information security assurance behaviour among employees,” Inf. Comput. Secur., p. ICS-10-2017-0073, Feb. 2019.

[41] M. Alshaikh, “Information Security Management Practices in Organisations,” university Of Melbourne, 2018.

[42] J. S. Lim, A. Atif, S. Chang, and S. B. Maynard, “Embedding Information Security Culture Emerging Concerns and Challenges,” Pacis 2010, pp. 463–474, 2010.

[43] E. Lomas, “Information governance: information security and access within a UK context,” Rec. Manag. J., vol. 20, no. 2, pp. 182–198, 2010.

[44] P. A. Mullon and M. Ngoepe, “An integrated framework to elevate information governance to a national level in South Africa,” Rec. Manag. J., vol. 29, no. 1/2, pp. 103–116, Mar. 2019.

[45] M. Silic and A. Back, “Factors impacting information governance in the mobile device dual□use context,” Rec. Manag. J., vol. 23, no. 2, pp. 73–89, 2013.

[46] P. P. Tallon, R. V. Ramirez, and J. E. Short, “The Information Artifact in IT Governance: Toward a Theory of Information Governance,” J. Manag. Inf. Syst., vol. 30, no. 3, pp. 141–178, 2014.

[47] S. L. Xie, “A must for agencies or a candidate for deletion:A grounded theory investigation of the relationships between records management and information security,” Rec. Manag. J., vol. 29, no. 1/2, pp. 57–85, Mar. 2019.

[48] J. Hagmann, “Information governance – beyond the buzz,” Rec. Manag. J., vol. 23, no. 3, pp. 228–240, Nov. 2013.

[49] R. F. Smallwood, “Information Governance Principles,” in Information Governance for Healthcare Professionals, T. Reuters, Ed. Boca Raton, FL : Taylor & Francis, 2018.: Productivity Press, 2018, pp. 19–30.

[50] S. Smith, D. Bunker, Donald Winchester, and R. Jamieson, “Circuits of Power: A Study of Mandated Compliance to an Information Systems Security ‘De Jure’ Standard in a Government Organization,” MIS Q., vol. 34, no. 3, p. 463, 2010.

[51] E. Soja and P. Soja, “Exploring Root Problems in Enterprise System Adoption From an Employee Age Perspective: A People-Process-Technology Framework,” Inf. Syst. Manag., vol. 34, no. 4, pp. 333–346, 2017.

[52] M. J. Alotaibi, S. Furnell, and N. Clarke, “A framework for reporting and dealing with end-user security policy compliance,” Inf. Comput. Secur., vol. 27, no. 1, pp. 2–25, Mar. 2019.

[53] K. M. Parsons, D. Calic, M. R. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, “The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies,” Comput. Secur., vol. 66, pp. 40–51, 2017.

[54] R. Torten, C. Reaiche, and S. Boyle, “The impact of security awarness on information technology professionals’ behavior,” Comput. Secur., vol. 79, pp. 68–79, Nov. 2018.

[55] A. Alkalbani, H. Deng, and B. Kam, “A Conceptual Framework for Information Security in Public Organizations for E-Government Development,” in 25th Australasian Conference on Information Systems, 2014.

[56] C. S. Teoh, A. K. Mahmood, and S. Dzazali, “Cyber Security Challenges in Organisations : A Case Study in Malaysia,” in 2018 4th International Conference on Computer and Information Sciences (ICCOINS), 2018, pp. 1–6.

[57] S. Alneyadi, E. Sithirasenan, and V. Muthukkumarasamy, “A survey on data leakage prevention systems,” J. Netw. Comput. Appl., vol. 62, pp. 137–152, 2016.

[58] N. S. Safa et al., “Deterrence and prevention-based model to mitigate information security insider threats in organisations,” Futur. Gener. Comput. Syst., vol. 97, pp. 587–597, Aug. 2019.

[59] I. Topa and M. Karyda, “From theory to practice: guidelines for enhancing information security management,” Inf. Comput. Secur., vol. 27, no. 3, pp. 326–342, Jul. 2019.

[60] M. Siponen, Adam Mahmood, and S. Pahnila, “Employees’ adherence to information security policies: An exploratory field study,” Inf. Manag., vol. 51, no. 2, pp. 217–224, 2014.

[61] A. Onumo, A. Cullen, and I. Awan, “Integrating Behavioural Security Factors for Enhanced Protection of Organisational Information Technology Assets,” in Proceedings - 2018 IEEE 6th International Conference on Future Internet of Things and Cloud, FiCloud 2018, 2018, pp. 128–135.

[62] F. Ullah, M. Edwards, R. Ramdhany, R. Chitchyan, M. A. Babar, and A. Rashid, “Data exfiltration: A review of external attack vectors and countermeasures,” J. Netw. Comput. Appl., vol. 101, pp. 18–54, Jan. 2018.

[63] S. Walker-Roberts, M. Hammoudeh, and A. Dehghantanha, “A Systematic Review of the Availability and Efficacy of

Countermeasures to Internal Threats in Healthcare Critical Infrastructure," IEEE Access, vol. 6, no. 1, pp. 25167–25177, 2018.

[64] Z. Muhamad Khairulnizam, M. Mohamad Noorman, A. S. Mad Khir Johari, and A. Norizan, "Theoretical Modeling of Information Security: Organizational Agility Model based on Integrated System Theory and Resource Based View," Int. J. Acad. Res. Progress. Educ. Dev., vol. 7, no. 3, pp. 390–400, 2018.

[65] Bulgurcu, Cavusoglu, and Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," MIS Q., vol. 34, no. 3, p. 523, 2010.

[66] L. Dong and K. Keshavjee, "Why is information governance important for electronic healthcare systems? A Canadian experience," J. Adv. Humanit. Soc. Sci., vol. 2, no. 5, pp. 250–260, Oct. 2016.

[67] Mohammad Reza Rasouli, J. J. M. Trienekens, R. J. Kusters, and P. W. P. J. Grefen, "Information governance requirements in dynamic business networking," Ind. Manag. Data Syst., vol. 116, no. 7, 2016.

[68] W. R. Flores and M. Ekstedt, "A Model for Investigating Organizational Impact on Information Security Behavior," in WISP 2012 Proceedings, 2012.

[69] P. B. Lowry and G. D. Moody, "Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies," Inf. Syst., vol. 25, no. 5, pp. 433–463, 2015.