INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES
HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2222-6990

Identification of key Predicting Factors Affecting Classified Information Assurance in Institutions of Higher Learning

Bello Ahmadu, Ab Razak Che Hussin and Mahadi Bahari

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v12-i7/10563 DOI:10.6007/IJARBSS/v12-i7/10563

Received: *22* April 2022*, **Revised:** 24* May 2022*, **Accepted:** 15* June 2022

Published Online: 29 June 2022

In-Text Citation: (Ahmadu et al., 2022)

To Cite this Article: Ahmadu, B., Hussin, A. R. C., and Bahari, M. (2022). Identification of key Predicting Factors Affecting Classified Information Assurance in Institutions of Higher Learning. *International Journal of Academic Research in Business and Social Sciences. 12(7),* 1 – 11.

Vol. 12, No. 7, 2022, Pg. 1 – 11

http://hrmars.com/index.php/pages/detail/IJARBSS | **JOURNAL HOMEPAGE**

Full Terms & Conditions of access and use can be found at
http://hrmars.com/index.php/pages/detail/publication-ethics

INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES
HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY
EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2222-6990

Identification of key Predicting Factors Affecting Classified Information Assurance in Institutions of Higher Learning

Bello Ahmadu[1,2], Ab Razak Che Hussin[1] and Mahadi Bahari[1]
[1]Department of Information System, Azman Hashim International Business School, Universiti Teknologi Malaysia, Johor Bahru, Malaysia, [2]Academy Library, Nigerian Defence Academy, Kaduna, Nigeria
Email: bahmadu@graduate.utm.my, abrazak@utm.my and mahadi@utm.my

Abstract
The recent escalation in leakages of classified information (CI) has attracted sustained interest from information security scholars and practitioners alike. CI is sensitive information that must be protected from being accessed by unauthorised persons. Thus, the purpose of this research is to identify the key factors that influence CI leakages in Institutions of Higher Learning (IHL). In doing this, we conducted a literature survey with a meta-analysis of 19 articles to identify the Key Predicting Factors (KPFs) that influences CI assurance in IHL. The factors found are categorised to organisational (communication structures), regulatory (enforceability), human (social norms, self-efficacy, training, and awareness of being monitored), and technological (internet of data, access control and storage control). These factors were validated via Delphi method to ascertain its consistency by information security experts. This research contributed to the knowledge by identifying KPFs influencing CI violation in IHL. In view of all factors that have been mentioned so far, there is no single information security theory/model that covers all identified KPFs. Therefore, we suggested for the development of a security violation prevention model to safeguard CI in IHL using KPFs.
Keywords: Classified Information, Information Security Violation, Information Assurance, Information Management, Key Predicting Factors (KPFs)

Introduction

Today, most organisations particularly Institutions of Higher Learning (IHL), fully dependent on classified information (CI) for their daily activities. IHL sit on rich data assets, including students' personal, academic and research data, financial data, and IHL correspondences. In particular, the research data in IHL are immensely valuable. They can make a significant impact by giving those who access them profitability, competitive advantage and also can support national interest in education, industry, health and defence (Pascual, 2009). Indeed, IHL are centres of excellence awash in creative thought and innovation all stored as information in various media and repositories. Thus, IHL have much information to protect, a large portion of which are already stamped CI. However, CI faces many issues across IHL. Several

organisations, most especially during Covid-19, witnessed data security threats as a result of working from home without proper CI protections. CI in IHL across the globe continuous to leaks to unlawful Individuals (Patz, 2017; Safa *et al.*, 2019; Vijandren, 2019). According to (CyberScout, 2019) over 67% of cyber-attacks on IHL are on sensitive information. Again, they observed that about 58% of the attacks are causing organisations more than $500.000 or more. Apart from the financial losses, there are many risks that exposure of CI can cause organisations such as legal reputation (CyberScout, 2019; Wood, 2014) and losses of integrity from sponsor institutions. Therefore, IHLs need to keep their CI and the underlying information system secure against unlawful access. Several theories and models have been developed to ensure the fidelity of CI. However, despite these numerous attempts at providing grounded bases for CI security, unauthorised persons continue to enjoy illegal access.

In view of this, there is a need to use novel approaches in understanding the phenomenon taking cognisance of its contextual peculiarities. Such an approach is all the more expedient in universities as institutions that must simultaneously protect their CI as well as ensure liberal access to knowledge. It is established science that one of the first steps at providing a solution is to identify the real issues surrounding CI violation as accurately as possible. In the same vein, address the spate of CI leakages in IHL requires the development of valid measures of the relevant contextual variables. However, there is a dearth of contextually relevant measures of CI security assurance dovetailed to the university's context. Analysis of the extant literature shows that the bulk of prior research on CI was conducted in several domains (Ahmad, Ong, Liew *et al.*, 2019; Safa *et al.*, 2019; Wall, Lowry, and Barlow, 2016). Hence, this study aims to identify key predicting factors that can promote classified information assurance in IHL.

Methodology

In view of our aim to identified KPFs for CI assurance in IHL, we adopted two major steps. The first step consists of two subsets. We source for relevant literature in reputable journals and the next sub-step is the analysis of the literature to identify KPFs to secure CI and the last step is the validation of the factors by information management experts (practitioners) using Delphi method.

Literature Search

We adopted automated and manual search process to source for published articles to enable us to meet our research objectives. However, these articles went through rigorous filtering based on our study's inclusion and exclusion criteria. Firstly, a series of search queries were made via keywords and phrases related to the study domain via trustworthy databases and search engines such as Scopus, IEEE, Web of Science and Google Scholar.

Literature Analysis

Collated literature was reviewed based on "meta-analysis." We use the same issue to answer each specific article documenting corporate securing CI measurements. The aim of using meta-analysis is to adapt statistics approaches to extract a cumulative approximation nearest to unknown common reality depending on how errors are interpreted. This method has the benefit of examining the whole article's when trying to extract variables. Webster and Watson (2002) also support a literature analysis but with the categorisation of a whole article in order to identify gaps in the literature, pointing out state of the art and explaining past research. To

extract specific knowledge and categorise this, the coding on a textual level of articles is more appropriate in this case.

Validation of Factors using Delphi Method

We adapted Delphi method to validate our review result. It is a structured communication technique to enable researchers to assess the panel of experts' opinion on a critical issue. The approach allows an iterative, written assessment by experts and stakeholders to gain a progressively satisfactory response among experts. Therefore, we design formal questionnaire interrogation, which was sent to a team of experts in the field of information system in Nigeria. This method provides confidential, impartial dialogue and debate among the experts. To avoid bias, the responses are only visible to the moderator and not to the participants. Thus, the same experts were invited for the second round to maintained consistency. All answers are based on anonymity and freedom of judgement.

The Key Predicting Factors

We analysed 19 relevant articles from the search methodology resulted in first-order codes and second-order code. Therefore, each article and their different impact factors were coded. These codes were based on the direct appearance of a variable in the information security mode or theories.

The analysis resulted in 33 first-order codes. We further aggregate the first-order codes to 9 second-order codes. In view of this, the result of our literature analysis identified 9 variables influencing CI assurance in the IHL domain, which we consider as the key predicting factors. They are: "communication structure", "enforceability", "social norm", "self-efficacy", "awareness of been monitor", "training", "internet of data", "access control" and "storage control". Consequently, the breakdown below shows the KPFs with their descriptions based on the literature view and their challenges regarding each factors.

Communications Structure

Information is the essence of communication. It is what is communicated. However, the distinction between one communication and the other lies in the subject of the communications. Some subjects are routine while others carry momentous consequences that measures must be taken to prevent such information from falling into the hands of the wrong people (Wall et al., 2016). However, organisations are wont to employ similar communication structures in transmitting both routine and consequential information. While the formal communication structure is usually designed to handle the flow of official information (Uslu, 2018), the informal structure also serves as an unauthorised conduit for the dissemination of CI among networks of employees (Fischbach et al., 2009). As a result, important information gets leaked in the process. It is therefore essential to consider the extant communication structure in organisations when investigating how consequential information, including CI are being transmitted from one point to another.

Enforceability

Enforceability is a pre-emptive ability of an organisation to irrefutably constrain or compel the actions of staff to defined norms (Breaux *et al.*, 2006). It refers to an organisation's ability to invoke its oversight powers and carry out some of the adverse promises guaranteed for the violation of organisational rules and regulations including extraction of compensation from the violator following the violation of organisational rules and regulations (Reiff, 2005).

Enforceability happens where the organisation can control the system and its behaviours; otherwise, the process to which the rule applies is better contracted out (Steyskal and Kirrane, 2015). However, most institutions of higher learning lack ability to prosecute suspect due to nonexistence of evident. Therefore, we are with the view that monitory of CI management staff would assist in maintaining rules and regulation in academics domain.

Social Norms

According to the social learning theory (Bandura, 1977b), employees tend to learn and accept the dominant social norm in the workplace by observing their colleagues and imitating their behaviour. This learning propensity is based on the people's assumption that what the other co-workers are doing in the workplace is the accepted custom (Chen and Li, 2014). Thus, social norms are, first of all, signals, either indicating what a good practise or bad practice is. Once a given practice is socially established, it becomes the standard of doing what it is meant to shape, thereby imposing a measure of constraint on members of the social unit (Hovav and D'Arcy, 2012). However, constraints of accepted social norms cannot be effective for very long if they are not relayed by social disapproval towards those who transgress the norms (Tene and Polonetsky, 2013). In practice, it was observed that some staff commit a crime with impunity due to corruption. Therefore, it promotes bad behaviours among colleagues.

Self-Efficacy

Self-efficacy is the primary explanatory construct in the social learning theory by Bandura's (1977b, 1986). Self-efficacy explains why people are (or are not) motivated to perform certain behaviours. The theory posits that people are motivated by the expectations about what they can do as well as by the expectations about the likely success of their actions (Bandura, 1977a; Warkentin *et al.*, 2016). In the context of this research, these expectancies define an employee's belief that he or she is capable of complying with CI policies and can safeguard CI under his or her responsibility. Therefore, for this study, we adopt the definition of information security self-efficacy given by Rhee et al (2009): that self-efficacy in the context information security to mean "a belief in one's capability to protect information and information systems from unauthorised disclosure, modification, loss, destruction and lack of availability" (p. 818). However, in practice, it was observed that information management staff do not have self-efficacy due to lack of trust in their IT system and poor IT knowledge (Ng et al., 2009).

Training

Training has been recognised as one of the most effective means of improving employee competencies with regards to managing the security of CI (Abu Bakar et al., 2017; Hwang *et al.*, 2017). It is a tool that organisations routinely use to ensure that employees handling sensitive informational assets are well trained (McIlwraith, 2006), thereby pre-empting avoidable costs associated with CI violation. The essential role of training in the securing of sensitive informational assets of organisations has been empirically validated in the study reported in (Hwang *et al.*, 2017). However, most of the CI management staff in Nigerian universities lack technical skills. Employees may easily do things that can endanger organisational data. For example, people often try to find a more straightforward and easier way to do something, often unaware of the danger they could cause. Human error is often one of the organisation's greatest threats in CI management in any organisations which IHL is

not left out. Therefore, we concur with the view of Hovav and D'Arcy (2012) that effective CIM training is essential to avoid risking CI.

Awareness of Monitoring

Monitoring of staff is a vital function in managing organisations, as it ensures that employees are held accountable for their actions (Hovav and D'Arcy, 2012). In connection to secure CI in organisations, employees are made to be conscious of being monitored through the various oversight mechanisms put in place to keep track of CI access and distribution patterns in organisations. Where employees are conscious of being observed (directly or through digital systems and signatures), the likelihood of employees to engage in deviant behaviours that may compromise the integrity of CI is significantly minimised (Hanus and Wu, 2015). In general, employees tend to comply with CI regulations if they are aware that countermeasures exist that will detect any violation at any time committed (Hanus and Wu, 2015; Torten et al., 2018). However, in Nigeria universities context, it was observed that monitoring apparatus are of less capacity which cannot store graphic.

Internet of Data (IoD)

Data are representations of things, objects, processes, and value which exist in the physical world. However, most data today are in digital form (in binary format). In much the same manner, physical objects are managed and controlled through the internet of things (IoT) (Yang et al., 2010). In addition, data or records can also be managed by embedding digital tags much as RFIDs which keeps track of the data, where they are transmitted, who and how they were transmitted, who access them, and what changes are made in them (Anderl, 2014). IoT has already contributed massively to the development of educational institutions, especially in the areas of teaching and research (Gul *et al.*, 2017). IoD offers exciting possibilities in the field of CI management. In an IoD environment, a datum could be able to contribute towards its protection. In the event of a violation, it could easily help uncover those involved in the violation. IoD can be associated with the infrastructure factor. It is about knowing all systems and software as well as the connections between them and if they are secured or not. However, the challenges are the complex nature of the activity in IoD. Above all, the service provider other stakeholders may have access to the universities CI, which is a threat to information assurance in IHL.

Access Control

Access controls are countermeasures designed to protect CI from risks of disclosure to unauthorised, theft, damage, loss or tampering. The controls may include a combination of physical, technical and procedural controls that effectively insulate CI from persons not authorised to access it (Horne et al., 2016). By far, the most challenging aspect of access control relates to CI kept on digital devices accessible over the Internet. The Internet of Things (IoT), for instance, is a behemoth of billions of devices that interact with each other that comes with daunting access control challenges (Ravidas *et al.*, 2019). Special access software and protocols are therefore needed to control access. The emergence of the IoD is both a solution to some of the existing problems and source of new challenges as well as a source of exciting opportunities for the management of sensitive data. However, in a case where information workers share their password to their colleagues and friends, therefore the aims of access control are overwhelmed.

Storage Control

Storage control refers to the safe-keeping of information, especially classified information (Qi et al., 2012). The storage system includes not only the physical system where CI is kept but also the medium used in keeping and transmitting it. In today's IT-enabled workplaces, storage control is of critical importance to the security of CI because of the easy ways of which digital data could be accessed. CI could be kept in various electronic media: on servers, computer hard-disks, removable devices, cloud-based and the likes (Qi et al., 2012; Zhang *et al.*, 2011). This type of system, though robust, is equally open to both insider and outsider threats (Safa *et al.*, 2019; Walton and Limited, 2006). With the help of smart devices, an insider may use their devices to copy sensitive data for their financial gain. IHL are open to all types of threats facing electronic information storage systems.

Relevance validation of KPFs

The literature was used to determine their relevance of key predicting factors to secure CI in organisations. Consequently, Delphi method was used for validation of KPFs by information security experts. We invited a total of 12 information management experts from Nigerian universities based on their long experience in handling CI in institutions of higher learning. Also, we ensured that they are top management staff. However, in the first round, 10 experts responded to our questionnaire while in the second round, only 8 experts responded.

Accordingly, a 4-point Likert-scale which points out the importance of the factors for securing CI in IHL arena was used. The coding of the scale was from not important to important. In defining the proportion in expert agreement regarding the important of factors, we utilised the “rather important” and “important” as the proportion agreement in the computation. This calculation is figured out as the number of experts that rated factors as important, divided by the total number of the panel. Table 1 shows the computation of factors validity in the second round by experts. Nine factors (range: 0.88 to 1) exceeded the threshold 0.78 level of statistical significance (Mikalef and Pateli, 2016). Indeed, this indicates that KPFs are important factors to measure CI assurance in IHL.

Table 1
Second Round Measurement of factors for Relevance

Factors	Not Important	Rather Not Important	Rather Important	Important	Average	Recommendation
Communication structures	0	0	2	6	1	Recommended
Enforceability	0	0	3	5	1	Recommended
Social norms	0	0	0	8	1	Recommended
Self-Efficacy	0	0	0	8	1	Recommended
Skills	0	1	0	7	0.88	Recommended
Awareness of been monitored	0	0	1	7	1	Recommended
Internet of Data	0	0	0	8	1	Recommended
Access Control	0	0	0	8	1	Recommended
Storage Control	0	0	1	7	1	Recommended

In view of this table, the result supported all factors extracted from the literature. In other words, the proposed factors are valid in their context as well as relevant in practice for

securing CI and thus are now called key predicting factors (KPFs). Therefore, the KPFs would be used in further research for the development of a security violation prevention model (SVPM).

Discussion

Unauthorised disclosure or destruction of public records is on the rise, thus posing serious economic dangers to organisations. Lack of proper information protection can lead to significant consequential effects, including loss irreplaceable information assets, loss of reputation and prohibitive recovery cost after the damage was done (Wood, 2014). Research has shown that there are basic approaches to protecting CI: organisational, regulatory (Wall et al., 2016), technology-based and human-based approaches (Simpson, 2019). It is instructive to note that communication has always been a central issue in matters relating to the management of classified information in organisations. Thus, this study retains the communication structure constructs featured prominently in the Selective Organisational Information Privacy and Security Violations Model (SOIPSVM) (Wall et al., 2016). Indeed, D'Arcy and Greene (2014) emphasise the centrality of communication (in addition to computer monitoring, a critical construct to be investigated in this study) in their Security Compliance Intention Model (SCIM). In another study which developed the Compliance Intention/Non-Compliance Model, the influence of training on bringing about information security was empirically verified (Hwang *et al.*, 2017). In another study, the role played by human factors in the violation and or protection of organisations' information assets was established. Specifically, (Warkentin *et al.*, 2016) established that perceived risks and self-efficacy enables employees' to engage in protective behaviours with regards to the organisation information assets. While in the state-of-the-art of ICT, it plays a significant role to pre-empt vulnerabilities and minimise the adverse consequences of possible attacks on CI in organisations. Therefore, this study suggests practical solutions for information management stakeholders consisting of software firms, IT professionals, Universities, NUC, institutions of higher learning and other researchers with multiple factors affecting CI protection in the context of IHL. We uncover the main predicting constructs, in order to understand the issues surrounding information leakages in Nigerian IHL. Thus, employees who are involved in information management implementation plan can realise that the identified KPFs would be useful as a guide in safeguarding CI in IHL. This is an important step to contribute to our knowledge on CI management. Thus, one of the major issues we discovered in this study is that there is no single information security theory or model that covered all our identified KPFs as independent variables. Therefore, we strongly suggested for the development of SVPM to safeguard CI in educational institutions.

Conclusion

The results of this research identified KPFs of CI assurance in IHL. The KPFs was supposedly based on the literature analysis, and it was further evaluated by IS experts using Delphi survey technique. It implies both practitioners, as well as the literature, supported the need KPFs for the development model to secure CI in organisations. KPFs give a basis for information management workers to take countermeasures to secure CI. However, it would also be useful for information management staff as well as technical employees in the IHL.

References

Abu Bakar, N., Mohd, M., & Sulaiman, R. (2017). *Information leakage preventive training.* Paper presented at the 6th International Conference on Electrical Engineering and Informatics (ICEEI), Langkawi, Malaysia, 25-27 November 2017.

Ahmad, Z., Ong, T. S., Liew, T. H., & Norhashim, M. (2019). Security monitoring and information security assurance behaviour among employees. *Information and Computer Security, 27*(2), 165-188. doi:10.1108/ics-10-2017-0073

Anderl, R. (2014). *Industrie 4.0: advanced engineering of smart products and smart production.* Paper presented at the 19th International Seminar on High Technology, Piracicaba, Brasil, October 9th, 2014.

Bandura, A. (1977a). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191-215. doi:10.1037/0033-295x.84.2.191

Bandura, A. (1977b). *Social Learning Theory*. Englewood Cliffs, New Jersey: Prentice-Hall, Inc.

Bandura, A. (1986). *Social Foundations of Thought and Action*. New Jersey: Prentice-Hall.

Breaux, T. D., Antón, A. I., Karat, C.-M., & Karat, J. (2006). *Enforceability vs. accountability in electronic policies.* Paper presented at the Seventh IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'06), London, Ont., Canada, 5-7 June 2006.

Chen, H., & Li, W. (2014). *Understanding Organization Employee's Information Security Omission Behavior: An Integrated Model of Social norm and Deterrence*. Paper presented at the Pacific Asia Conference on Information Systems (PACIS) 2014 Proceedings.

CyberScout. (2019). 2019 End of the year Data Breach Reports. *Identity Theft Resource Center (ITRC)*.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security, 22*(5), 474-489. doi:10.1108/imcs-08-2013-0057

Fischbach, K., Gloor, P. A., & Schoder, D. (2009). Analysis of Informal Communication Networks – A Case Study. *Business & Information Systems Engineering, 1*(2), 140-149. doi:10.1007/s12599-008-0018-z

Gul, S., Asif, M., Ahmad, S., Yasir, M., Majid, M., & Malik, M. S. A. (2017). A Survey on Role of Internet of Things in Education. *International Journal of Computer Science and Network Security, 17*(5), 159-165.

Hanus, B., & Wu, Y. A. (2015). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management, 33*(1), 2-16. doi:10.1080/10580530.2015.1117842

Horne, C. A., Ahmad, A., & Maynard, S. B. (2016). *A Theory on Information Security.* Paper presented at the Australasian Conference on Information Systems 2016, Wollongong, Australia.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management, 49*(2), 99-110. doi:10.1016/j.im.2011.12.005

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review, 41*(1), 2-18. doi:10.1108/oir-11-2015-0358

McIlwraith, A. (2006). *Information Security and Employee Behaviour: How to Reduce Risk through Employee Education, Training and Awareness*. Aldershot, England: Gower Publishing Limited.

Mikalef, P., & Pateli, A. (2016). Developing and Validating a Measurement Instrument of IT-Enabled Dynamic Capabilities. *AIS Electronic Library (AISeL) Research Papers ECIS, 26*.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825. doi:10.1016/j.dss.2008.11.010

Pascual, R. (2009). Enhancing project-oriented learning by joining communities of practice and opening spaces for relatedness. *European Journal of Engineering Education, 35*(1), 3-16. doi:10.1080/03043790902989234

Patz, R. (2017). Leaking, leak prevention, and decoupling in public administrations: the case of the European Commission. *West European Politics, 41*(4), 1049-1071. doi:10.1080/01402382.2017.1394103

Qi, L., Xiao, S. M., & Tang, F. M. (2012). The Application of Information Flow Control Technology Based on Electronic Confidentiality Level Identifier in the Removable Storage Medium. *Advanced Materials Research, 461*, 182-186. doi:10.4028/www.scientific.net/AMR.461.182

Ravidas, S., Lekidis, A., Paci, F., & Zannone, N. (2019). Access control in Internet-of-Things: A survey. *Journal of Network and Computer Applications, 144*, 79-101. doi:10.1016/j.jnca.2019.06.017

Reiff, M. R. (2005). *Punishment, Compensation, and Law: A Theory of Enforceability*. Cambridge,UK: Cambridge University Press.

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826. doi:10.1016/j.cose.2009.05.008

Simpson, C. J. (2019). *Unauthorized Disclosures of Sensitive and Classified Information: A Meta-Synthesis of Leadership Support, Security Policy, and Security Education, Training and Awareness within the Federal Government Information Security Culture.* (PhD Thesis). Delaware State University,

Steyskal, S., & Kirrane, S. (2015). *If You Can't Enforce It, Contract It: Enforceability in Policy-Driven (Linked) Data Markets.* Paper presented at the 11th International Conference on Semantic Systems – SEMANTiCS 2015, Vienna, Austria, September 15–17, 2015.

Tene, O., & Polonetsky, J. (2013). A theory of creepy: technology, privacy and shifting social norms. *Yale Journal of Law & Technology, 59*, 59-102.

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. *Computers & Security, 79*, 68-79. doi:10.1016/j.cose.2018.08.007

Uslu, B. (2018). The components of communication systems in universities: their influence on academic work life. *Tertiary Education and Management, 24*(1), 34-48. doi:10.1080/13583883.2017.1359662

Vijandren. (2019). Universiti Malaya Staff Personal Data, Banking and Salary Details Leaked Online. *lowyat.net*. Retrieved from https://www.lowyat.net/2019/196895/universiti-malaya-staff-data-leaked-online/#

Wall, J. D., Lowry, P. B., & Barlow, J. B. (2016). Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under

Conditions of Strain and Excess. *Journal of the Association for Information Systems, 17*(1), 39-76.

Walton, R., & Limited, W.-M. (2006). Balancing the insider and outsider threat. *Computer Fraud & Security, 2006*(11), 8-11. doi:10.1016/s1361-3723(06)70440-7

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems, 92*, 25-35. doi:10.1016/j.dss.2016.09.013

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, xiii-xxiii.

Wood, P. (2014). Walls of straw - the cyber risks to higher education. *Insights, 72*(2), 192-197.

Yang, D.-L., Liu, F., & Liang, Y.-D. (2010). *A Survey of the Internet of Things.* Paper presented at the 2010 International Conference on E-Business Intelligence (ICEBI2010), Kunming, Yunnan, P.R.China, December 19-21, 2010.

Zhang, X., Du, H.-T., Chen, J.-Q., Lin, Y., & Zeng, L.-J. (2011). *Ensure Data Security in Cloud Storage*. Paper presented at the 2011 International Conference on Network Computing and Information Security.