AL-'ABQARI العبقري
USIM
ISSN 2232-0431 / e-ISSN 2504-8422
UNIVERSITI SAINS ISLAM MALAYSIA
VOL. 17 (SPECIAL EDITION) FEB. 2019: 28-38
Journal of Islamic Social Sciences and Humanities
مجلة الثقافة الإسلامية و الإنسانية

Submission date: 04/09/2018 Accepted date: 25/12/2018

CURBING MISBEHAVIOUR WITH INFORMATION SECURITY MEASURES: AN EMPIRICAL EVIDENCE FROM A CASE STUDY

Mengawal Ketidakpatuhan Tingkah Laku dengan Pelan Tindakan Keselamatan Maklumat: Penemuan Empirikal dari Kajian Kes.

Hanifah Abdul Hamid & Nuradli Ridzwan Shah Mohd Dali
Universiti Sains Islam Malaysia

hanifah@usim.edu.my

Abstract

Organisations generally are still struggling with information security breaches despite various technical protections to secure their valuable information which is especially stored in cloud applications. The fact that human behaviour is the weakest link of the security chain. Security compromise causes substantial financial and nonfinancial losses to the organisations which jeopardise organisations' reputation. Technical protection alone is seemed insufficient to ensure information safety. Therefore, this research takes it from the socio-technical perspective to strengthen information security. Addressing these factors are significant to help successfully create a healthy security culture in the organisation. Nevertheless, human behaviour is subjective in nature. Their behaviour depends upon the way they think feel and act towards security issues which needs an in depth understanding towards their security behaviour. Hence, adapting the sequential exploratory mixed-method approach, through the theoretical lens of social cognitive theory and security measures from extended deterrence theory, this study examines the information security behaviour of employees at an IT department of a public university, as the case study. Partial least square was used to analyse data collected via survey. Study shows that personal values and behaviour, apart from the effective technical security measures, are important factors towards inculcating information security compliance behaviour.

Keywords: cloud computing, information security, behaviour, measures.

Abstrak

Pada umumnya, organisasi masih bergelut dengan pelanggaran keselamatan maklumat walaupun terdapat pelbagai perlindungan teknikal untuk mendapatkan maklumat berharga mereka yang terutama disimpan dalam aplikasi awan. Ini disebabkan hakikat bahawa tingkah laku manusia adalah pautan paling lemah dalam rangkaian keselamatan. Kompromi keselamatan menyebabkan kerugian kewangan dan bukan kewangan yang besar kepada organisasi yang menjejaskan reputasi organisasi. Perlindungan teknikal sahaja tidak mencukupi untuk memastikan keselamatan maklumat. Oleh itu, kajian ini mengambilnya dari perspektif sosio-teknikal untuk mengukuhkan keselamatan maklumat. ini meneliti tingkah laku keselamatan maklumat pekerja di jabatan IT universiti awam dalam bentuk kajian kes. Model "Partial Least Square" digunakan untuk menganalisis data yang dikumpulkan melalui tinjauan kajiselidik. Kajian menunjukkan nilai-nilai peribadi dan tingkahlaku, selain daripada pelan

tindakan keselamatan teknikal yang dijalankan Menangani faktor-faktor ini penting untuk membantu mewujudkan budaya keselamatan yang sihat dalam organisasi. Walau bagaimanapun, tingkah laku manusia bersifat subjektif. Tingkah laku mereka bergantung kepada cara mereka berfikir dan bertindak terhadap isu keselamatan yang memerlukan pemahaman mendalam terhadap tingkah laku keselamatan mereka. Oleh itu, menyesuaikan pendekatan kaedah campuran bercampur-gugur, melalui teori teori kognitif sosial dan langkah-langkah keselamatan dari teori pencegahan yang diperpanjang, kajian secara efektif, adalah faktor penting untuk menanamkan tingkah laku pematuhan keselamatan maklumat.

Kata kunci: perkomputeran awan, keselamatan maklumat, tingkah laku, pelan tindakan.

INTRODUCTION

The emerging of cloud computing has uplifted the information technology to the more advanced level. In the Software as a Service (SaaS) environment for instance, everything is served in and around the cloud to which people are not required to bring their own storage devices, since data can be saved in the clouds. Nevertheless, study shows that security is a major hindrance of cloud adoption (Abdul Hamid & Mohd Yusof, 2015; Abdul Hamid & Yusof, 2016). Scientists have come up with an abundant of technical solutions to solve information security problems, yet security incidents still happen because humans have been the weakest link of security chain (AlHogail, 2015; Connolly, Lang, & Tygar, 2014). Security incompliance, either accidentally or intentionally, causes substantial costs to the organisation, both tangibly and intangibly.

Hence this study will approach the information security compliance behaviour (ISCB) from the socio-organisational perspective. Previous studies discussed the factors inculcating security culture in the organisation (Alfawaz, Nelson, & Mohannak, 2010)(Hassan & Ismail, 2015)(Hassan & Ismail, 2012) but there is no first-hand evidence that could prove the claim. The aim of this paper is to empirically examine the driving factors of security compliant behaviour in the organisation. Specifically, this paper, as part of the whole ISCB research, will seek to answer this question: How significant are the social and information security control management factors in deterring security misbehaviour?

Adapting Social Cognitive Theory (SCT), as well as extended deterrent theory (DT) as our framework, this study will examine the impact of security control management (SCM), personal values (PV), environment (ENV) and employees' behaviour (BHV) towards information security compliance behaviour (ISCB). SCT is a three dimensional complementary model that is used to determine human behaviour which consists of cognitive or personal factors, environmental factors and behavioural factors (Albert Bandura, 1989). The theory founder (Albert Bandura, 1989) further accentuates that "expectations, beliefs, self- perceptions, goals and intentions give shape and direction to behaviour. What people think, believe, and feel, affects how they behave (Albert Bandura, 1986, 1989). He nevertheless argued that behaviour cannot easily change the environment much like it is influenced by the environment unless the behaviour first change itself. The DT of punishment can be traced to the early works of classical philosophers such as Thomas Hobbes (1588–1678), Cesare Beccaria (1738–1794), and Jeremy Bentham (1748–1832) (Lieberman, 2010). Rooted from school of criminology, DT advocates that individual choose to commit crime when the benefits of the action outweigh the costs (Herath & Rao, 2009b). Deterrence has been indicated significant in decreasing negative practices and has likewise been observed to be a viable instrument in administration (Herath & Rao, 2009a). In Information System (IS) research, DT has been extended by integrating some security control as a measure to deter security breaches (J D'Arcy & Hovav, 2009).

METHODOLOGY

Hypotheses Development

To ensure successful information security in the organisation, the SCM is vital. Past scholars have highlighted on the important roles of SCM in making sure that employees act according to the standards and procedure, and rules and regulations (Connolly, Lang, & Tygar, 2015; John D'Arcy, Hovav, & Galletta, 2009). Security awareness (Alnatheer, 2015; Bozic, 2012; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014), as well as security training and education (Alnatheer, 2015; Alnatheer & Nelson, 2009; Bozic, 2012; Soomro, Shah, & Ahmed, 2016) are among the most basic factor needed in inculcating information security culture in the organization which must be given much attention by the top management. Employees must be aware that their behaviour must always in accordance to the rules and regulations to avoid security breaches that may occur accidently or intentionally. However, in today's technology advancement where threats are rising almost from any angle, security awareness is still lagged behind (Furnell & Moore, 2014). The lack of security awareness causes security incompliance in the cloud environment, which makes outsourcing arrangement of IT services becomes more complex (Bachlechner, Thalmann, & Maier, 2014). Without proper security education, training and awareness (SETA) programmes, people do not know if they have committed security breaches. It was found out that SETA programmes has positive influence on managing and deterring security behaviour (John D'Arcy et al., 2009).

In addition, the organisations that have proper information security policies and procedures (SPP) are better at guiding employees to good security behaviour. Research shows that complying with organisation security policy can shape and mitigate the risk of employees misbehaviour (Sohrabi Safa, Von Solms, & Furnell, 2016). However, employees must be aware of the information security policies in place in order to have an effective deterrence factor(John D'Arcy et al., 2009). It is also a critical factor to consider setting up ethical conduct policy (Da Veiga & Eloff, 2010) in building up security culture in the organisation. It is argued that previous research in ISCB did not give attention on ethical conduct due to different organisations have different kinds of values and culture(Alnatheer, 2015).

Another security control is risk analysis assessment and management (RAM). The organization will be able to identify areas that are highly critical for information security and to improve the security effectiveness. Information is secured with the three triads of information system – confidentiality, integrity and availability. However, in nowadays computing, cloud computing for instance, has exposed information to more security risks and challenges issues. Information is at risks of the existence of vulnerability and threats. It is claimed that organizations which have security RAM in place are being more aware of their losses due to security breaches (Alnatheer, 2015).

The fourth factor for SCM is physical security monitoring (PSM) which is essential to control the security behaviour of employees in the organisation (J D'Arcy & Hovav, 2009). While technical threats are easier to detect and rectify, the human threats are proven to be difficult to identify. Thus, the uses of PSM activities are said to be effective in controlling the behaviour of the employees with regards to the safety of information. Past research examined how PV have been a significant driving factor in complying with security regulations. This includes their attitude (Safa et al., 2015; Siponen, Adam Mahmood, & Pahnila, 2014), security knowledge (Parsons et al., 2014; Thomson, von Solms, & Louw, 2006; Van Niekerk & Von Solms, 2010), religious and ethical beliefs (Al-Hamar, Dawson, & Guan, 2010; Leiwo & Heikkuri, 1998) as well as level of trust (Al-Hamar et al., 2010; Colella, Castiglione, & Santis, 2014). Humans act

according to their habitual conducts. When human do things repeatedly, these actions become a habit and are stored in the subconscious minds.

Depending on the individual preference towards an object (person, event, thing, time, activity), attitude can be expressed positively or negatively. Attitude has been proven to have a positive effect on employee security compliance behaviour (Safa et al., 2015) and self-efficiency in attitude help cultivates ISCB (Bozic, 2012). The ENV plays an important role is shaping a positive behaviour of a person. This can be either internal or external environment that influence from within and outside organisation. As an individual, people tend to adapt themselves to the particular situation for the fact that they are unable to change the environment alone. In this situation, the government plays an important role to ensure the information security is at the highest priority.

The Personnel Data Protection Act 2010 was enacted by the Malaysian Government for these reasons. It was suggested that the enforcement of the act will help shaping the behaviour of the people with regards to information security (Alnatheer, 2015). The influence of regulation with regards to information security culture should be empirically tested (Alfawaz, Nelson, & Mohannak, 2010). Another ENV element is social norms. Individuals' behaviours are very much shaped by their ENV such as peer influence. The colleagues and immediate supervisor, other departments' behaviour, the mechanism for rewarding good behaviour and punishing bad behaviour are constructing factors which influence the security behaviour of the employees in the organisation (Bozic, 2012; Herath & Rao, 2009a). It is argued that among others, ENV factors that influence the security behaviour of people are still yet to be explored (Topa & Karyda, 2015), (Alfawaz, Nelson, & Mahannak, 2010),(AlHogail, 2015).

BHV is the conduct of a person towards a particular situation which is based upon the ENV as well as the personality traits one owns. The BHV elements which includes skills, practice and self-efficacy (SESE) of employees are formed gradually in such a long span of time and cannot be obtained overnight. ISCB research found out that security conscious behaviour has a significant impact towards the safety of information in the organisation (Alfawaz, Nelson, & Mahannak, 2010; Connolly et al., 2015; Van Niekerk & Von Solms, 2010). Good security behaviour will result in security compliance thus reduce security breaches. In long term this good behaviour will become norms which exhibit security culture of the organisation. The skills to measure risks and recognise threats are crucial for information safekeeping. Those who possess lower skills in recognizing and detecting threats are more vulnerable to the attacks.

Good security practice will likely reduce security incidents as users take all the precaution steps to comply with security policies and procedures. Experience in information security context means one's familiarity with the skills or knowledge in the field of information security, which were acquired over a period of time through actual exercise and apparently has enhanced better ability or grasp in behaving according to the security rules and regulations (Munteanu & Fotache, 2015). Using social bond theory (Hirschi, 1986), (Sohrabi Safa et al., 2016) found out in their study that the experience and involvement of employees have significant effect on their attitude towards complying with security policy. Self-efficacy is a person's certainty of his or her ability to perform required behaviours to achieve certain accomplishments (A Bandura, 1977).

Self-efficacy is a form of self-evaluation that can be the most influential apparatus of human agents in motivating and regulating human behaviour. Many studies in information technology and information systems adoption in various domains claimed that self-efficacy is an influencing factor for users to adopt such technology and systems. Self-efficacy has been found to have a significant relationship towards information security behaviour of the employees

(Herath & Rao, 2009a; Ng, Kankanhalli, & Xu, 2009; Safa et al., 2015; Vance, Siponen, & Pahnila, 2012). Hence, we posit the following hypotheses:

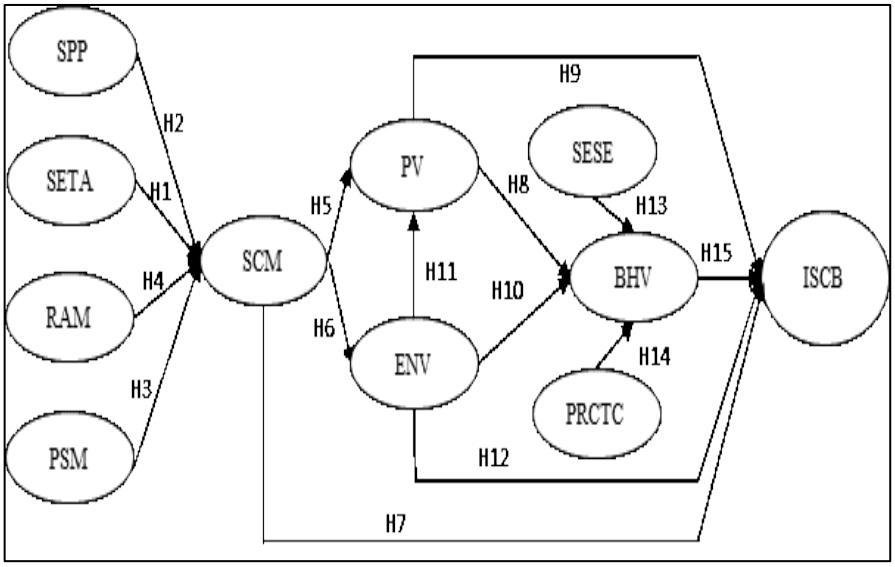
H1: SETA programme has a positive impact towards SCM.
H2: The SPP has positive impact towards SCM.
H3: The PSM has a positive impact towards SCM.
H4: The RAM has a positive impact SCM.
H5: SCM has positive impact towards PV.
H6: SCM has positive impact towards the ENV.
H7: SCM has a positive impact towards ISCB.
H8: PV have positive impact towards BHV.
H9: PV have positive impact towards ISCB.
H10: ENV has positive impact towards BHV.
H11: ENV has a positive impact towards PV.
H12: ENV has positive impact towards ISCB.
H13: SESE have positive impact towards BHV.
H14: PRCTC has positive impact towards BHV.
H15: BHV has positive impact towards ISCB.

METHOD

The survey instruments were adapted from the work of (Parsons et al., 2014; Siponen et al., 2014; Thomson et al., 2006; Van Niekerk & Von Solms, 2010) for cognitive factors using reflective measurement. The security control management instruments were adapted from (John D'Arcy et al., 2009) using formative measurement. All items were measured on a 5-point Likert-scale from 1- strongly disagree to 5- strongly agree. The case study was conducted at an IT department at a public university. The survey was conducted online to all IT employees in this organisation, from February to March 2017. Google doc was used as the platform of the survey.

Potential respondents were contacted through email messages to which the link of the survey was attached to the messages. Convenience sampling was used as the sampling method. Respondents were informed about the purpose of the study and given option to quit answering at any time. Screening questions were asked to identify the correct respondents. Respondents were asked about the usage of mobile devices such as laptops or smartphones for their job-related tasks. Respondents were also questioned about their exposure to cloud applications such as cloud storage, social media networks as well as email applications. Altogether, there were 94 people responded to the questions (All staff responded). Screening the missing data, 90 data was useful for empirical analysis. Partial Least Square (PLS) was used to analyse the ICSB model as shown in the following figure.

Figure 1: Conceptual Model



RESULTS AND DISCUSSION

The demographic profiles of the employees were obtained during the survey and the results are shown as at the following Table 1:

Table 1: Demographic Profiles

Item		N	Valid %
Gender	Male	41	45.6
	Female	49	54.4
Age	21-30	39	43.3
	31-40	45	50.0
	41-50	5	5.6
	51-60	1	1.1
Education	High school	5	5.6
	Diploma	27	30.0
	Degree	46	51.1
	Master	7	7.8
	PhD	5	5.6
Experience	<= 5 years	34	37.8
	6-10 years	32	35.6
	11-15 years	17	18.9
	16 above	7	7.8

Role	Top management	4	4.4
	Management	13	14.4
	Administrative	17	18.9
	Technical	56	62.2

Based on Table 1 above, there were 54.4% of female employees compared to 45.6% of male employees. In terms of their age, 50% was in the range of 31-40 years old, 43.3% was in the ranger of 21-30 years of age, followed by 41-50-year-old (5.6%) and 51 and above (1.1%). 51.1% had bachelor's degree, followed by 30 % whom were diploma holders, 7.8 % with master's degree, 5.6% with PhD and high school education, as their highest education level respectively.

Their working experience varied where 37.8% had below 5 years of experience, 35.6% had 6 – 10 years of experience, 18.9% had 11-15 years of experience and 7.8 % had more than 16 years of working experience. Based on the position, 4.4% of them were the top management, 14.4% were at the managerial level, 18.9% were administrative staff and 62.2% were the technical support staff.

Table 2: SaaS Cloud Applications Exposure

Frequency/ Item & (%)	E (%)	CS (%)	MA (%)	SSO (%)	SM (%)	ES (%)
None	0 (0)	2 (2.2)	2 (1.1)	1 (1.1)	0 (0)	4 (4.4)
Very Limited	4 (4.4)	13 (14.4)	8 (8.9)	8 (8.9)	7 (7.8)	15 (16.7)
Some Experience	10 (11.1)	25 (27.8)	20 (22.2)	20 (22.2)	7 (7.8)	37 (41.1)
Quite a Lot	46 (51.1)	37 (41.1)	49 (54.4)	48 (53.3)	49 (54.4)	30 (33.3)
Extensive	30 (33.3)	13 (14.4)	11 (12.2)	13 (14.4)	27 (30)	4 (4.4)

Based on Table 2, respondents were also asked about their exposure towards software -as-a-service applications (SaaS). In terms of email (E), 51.1% of users had quite a lot experience, 33.3% had extensive experience, as opposed to those with some experience (11.1%) and very limited experience (4.4%). The users' exposure to cloud storage also varied; 41.1% users had quite a lot experience, followed by those with some experience (27.8%), extensive usage (14.4%), very limited experience (14.4%) and no experience at all (2.2%).

The users were also asked about their experience with mobile apps (MA). It shows that 54.4% of them had quite a lot experience and 22.2% had some experience using mobile apps. Only 12.2% of the users used mobile apps extensively, and 8.9% of them had very limited experience and 1.1% had no experience with mobile apps at all. The survey also asked the employees about their exposure to the SSO portal. 53.3% of them had quite a lot experience

with SSO portal, followed by 22.2% with some experience, 14.4% with extensive experience, 8.9% with limited experience, and 1.1% with no experience at all.

Employees were also asked about their social media (SM) usage such as Facebook, Instagram and Twitter. It shows that 54.4% of the them had quite a lot experience with social media, 30% used the social media extensively, followed by those with some experience and limited experience at 7.8% each.

Lastly, the employees were queried about their usage of e-services (ES) such as e-filing or e-billing. Approximately 41.1% of the employees had some experience of using e-services, followed by 33.3% with quite a lot experience, and 16.7% with limited experience. There are only 4.4% of them having extensive experience with e-services as well as inexperienced e-services users respectively.

Table 3: Significance Testing Results of the Structural Model Path Coefficients

H	Paths	Path Coefficient	T Values	SIG Level	P Values	Confidence Interval (92.5 -97.5%)	R
H1	SETA -> SCM	0.183	1.679	*	0.09	[-0.026 - 0.417]	MS
H2	SPP -> SCM	0.758	4.73	***	0	[0.436 - 1.062]	S
H3	PSM -> SCM	-0.094	0.61	NS	0.54	[-0.304 - 0.296]	NS
H4	RAM -> SCM	-0.052	0.61	NS	0.54	[-0.243 - 0.080]	NS
H5	SCM -> PV	0.364	3.921	***	0	[0.183 - 0.553]	S
H6	SCM -> ENV	0.659	6.743	***	0	[0.440 - 0.815]	S
H7	SCM -> ISB	0.229	1.611	NS	0.11	[0.007 - 0.554]	NS
H8	PV -> BHV	0.123	1.521	NS	0.13	[-0.007 - 0.296]	NS
H9	PV -> ISCB	0.31	3.206	***	0	[0.118 - 0.496]	S
H10	ENV -> BHV	-0.007	0.043	NS	0.97	[-0.279 - 0.342]	NS
H11	ENV-> PV	0.183	0.984	NS	0.32	[-0.157 – 0.532]	NS
H12	ENV -> ISCB	-0.102	0.689	NS	0.49	[-0.431 - 0.145]	NS
H13	SESE -> BHV	0.781	6.071	***	0	[0.478 - 1.015]	S
H14	PRCTC -> BHV	0.174	1.687	*	0.09	[-0.011 - 0.371]	MS
H15	BHV -> ISCB	0.434	3.354	***	0	[0.54 – 0.89]	S

Note: S- Supported, MS- Marginally Supported, NS- Not Supported; *** denotes significant at 1%, * denotes significant at 10%.

Table 3 exhibits the results of path coefficients of ISB model for the case study conducted at GIC. The paths of SPP->SCM, SCM->PV, SCM->ENV, PV->ISB, SESE->BHV and BHV->

ISB are significant at 1%. Other paths such as SETA->SCM and PRCTC-> BHV are significant at least at 10% (marginally significant). Following the results, there are 8 hypotheses which are supported in this case study such as H1, H2, H5, H6, H9, H13, H14 and H15. On the other hand, there are 7 other paths which show insignificance and hence rejection of hypotheses of H3, H4, H7, H8, H10, H11 and H12.

The result shows that SETA programmes as well as security policies and procedures are perceived important by the employees, which are consistent with D'Arcy [10]. Nevertheless, in contrary, the physical security monitoring and risks analysis and management are found insignificant in this study as employees did not find that that these measures however important, are not being properly implemented in their organization. Further assessment shows that security measures play an important role in encouraging secured environment and enhancing personal values towards information security compliance behaviour. It also shows that personal values and behaviour of employees strongly influence information security compliance behaviour, but not the environment. This is consistent with Bandura's social cognitive theory that environment cannot change one's behaviour unless one's changes the behaviour which gradually alters the environment.

CONCLUSIONS

In conclusion, personal values and behaviour are important factors towards inculcating information security compliance behaviour. In addition, from security measures perspective, the physical security monitoring and risks analysis and management should be properly implemented to effectively inculcate information security compliance behaviour in the organization. This can be done by the management by forming up a professional security team specifically handling information security matters and building up strategic security plans which are aligned with the organisation's objectives. As this work was conducted in the public education environment, future work may consider other domains from different perspective.

ACKNOWLEDGMENT

The authors are grateful to Universiti Sains Islam Malaysia and Ministry of Education Malaysia for their support in this study.

REFERENCES

Abdul Hamid, H., & Mohd Yusof, M. (2015). State-of-the-Art of cloud computing adoption in Malaysia: A review. *Jurnal Teknologi (Sciences and Engineering)*, *77*(18), 1–6. http://doi.org/http://dx.doi.org/10.11113/jt.v77.6499.

Abdul Hamid, H., & Yusof, M. M. (2016). Conceptualizing global cloud landscape: A review of adoption issues and challenges. *Research Journal of Applied Sciences*, *11*(6), 333–339. http://doi.org/10.3923/rjasci.2016.333.339.

Al-Hamar, M., Dawson, R., & Guan, L. (2010). A culture of trust threatens security and privacy in Qatar. *Proceedings - 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software and Systems, ICESS-2010, ScalCom-2010*, (Cit), 991–995. http://doi.org/10.1109/CIT.2010.182.

Alfawaz, S., Nelson, K., & Mahannak, K. (2010). QUT digital repository : Information security culture : A behaviour compliance conceptual framework. In *Security, Information Aisc, Conference*.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information Security culture: A behaviour compliance conceptual framework. In *AISC '10 Proceedings of the Eighth Australasian Conference on Information Security - Volume 105* (pp. 47–55). Brisbane: Australian Computer Society, Inc.

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575. http://doi.org/10.1016/j.chb.2015.03.054

Alnatheer, M. a. (2015). Information Security Culture Critical Success Factors. *2015 12th International Conference on Information Technology - New Generations*, 731–735. http://doi.org/10.1109/ITNG.2015.124

Alnatheer, M., & Nelson, K. (2009). Proposed framework for understanding information security culture and practices in the Saudi context. In *Proceedings of the 7th Australian Information Security Management Conference* (pp. 6–17). Perth, Western Australia: Edith Cowan University.

Bachlechner, D., Thalmann, S., & Maier, R. (2014). Security and compliance challenges in complex IT outsourcing arrangements: A multi-stakeholder perspective. *Computers & Security*, *40*, 38–59. http://doi.org/10.1016/j.cose.2013.11.002.

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

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. (National Inst of Mental Health Rockville MD US, Ed.). Englewood Cliffs, NJ, US: Prentice-Hall series in social learning theory.

Bandura, A. (1989). Social cognitive theory. *Annals of Child Development*, *6*(Six theories of child development), 1–60.

Bozic, G. (2012). The role of a stress model in the development of information security culture. *Proceedings of the 35th International Convention MIPRO, May 2012*, 1555–1559.

Colella, A., Castiglione, A., & Santis, A. De. (2014). The Role of trust and co-partnership in the societal digital security culture approach. *2014 International Conference on Intelligent Networking and Collaborative Systems*, 350–355. http://doi.org/10.1109/INCoS.2014.142.

Connolly, L., Lang, M., & Tygar, D. (2014). Managing Employee security behaviour in organisations: The role of cultural factors and individual values. *ICT Systems Security and Privacy Protection*, *428*, 417–430.

Connolly, L., Lang, M., & Tygar, J. D. (2015). Investigation of employee security behaviour: A grounded theory approach. *IFIP Advances in Information and Communication Technology*, *455*, 283–296. http://doi.org/10.1007/978-3-319-18467-8_19

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, *89*, 59–71. http://doi.org/10.1007/s10551-008-9909-7.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. http://doi.org/10.1287/isre.1070.0160.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*. http://doi.org/10.1016/j.cose.2009.09.002.

Furnell, S., & Moore, L. (2014). Security literacy: The missing link in today's online society? *Computer Fraud and Security*, *2014*(5), 12–18. http://doi.org/10.1016/S1361-3723(14)70491-9.

Hassan, N. H., & Ismail, Z. (2012). A conceptual model for investigating factors influencing information security culture in healthcare environment. *Procedia - Social and Behavioral Sciences*, *65*(ICIBSoS), 1007–1012. http://doi.org/10.1016/j.sbspro.2012.11.234.

Hassan, N. H., & Ismail, Z. (2015). A conceptual model towards information security culture in health informatics. In *The Malaysia-Japan Model on Technology Partnership* (pp.

187–196). Springer Japan. http://doi.org/10.1007/978-4-431-54439-5.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. http://doi.org/10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*. http://doi.org/10.1057/ejis.2009.6.

Hirschi, T. (1986). On the compatibility of rational choice and social control theories of crime. *The Reasoning Criminal: Rational Choice Perspectives on Offending*, 105–118.

Leiwo, J., & Heikkuri, S. (1998). An analysis of ethics as foundation of information security in\ndistributed systems. *Proceedings of the Thirty-First Hawaii International Conference on System Sciences*, *6*(c). http://doi.org/10.1109/HICSS.1998.654776

Lieberman, P. E. (2010). Deterrence theory. *Billboard*, *1*(45), 8–8. http://doi.org/doi: http://dx.doi.org/10.4135/9781412952514.

Munteanu, A.-B., & Fotache, D. (2015). Enablers of information security culture. *Procedia Economics and Finance*, *20*(15), 414–422. http://doi.org/10.1016/S2212-5671(15)00091-X.

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

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–176. http://doi.org/10.1016/j.cose.2013.12.003.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78. http://doi.org/10.1016/j.cose.2015.05.012.

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management*, *51*(2), 217–224. http://doi.org/10.1016/j.im.2013.08.006.

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. http://doi.org/http://dx.doi.org/10.1016/j.cose.2015.10.006.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. http://doi.org/10.1016/j.ijinfomgt.2015.11.009

Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10), 7–11. http://doi.org/10.1016/S1361-3723(06)70430-4.

Topa, I., & Karyda, M. (2015). Identifying factors that influence employees' security behavior for enhancing ISP compliance. In S. Fischer-Hübner, C. Lambrinoudakis, & J. López (Eds.), *Trust, Privacy and Security in Digital Business*. Valencia, Spain: Springer.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476–486. http://doi.org/10.1016/j.cose.2009.10.005.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4), 190–198. http://doi.org/10.1016/j.im.2012.04.002.