Paper ID: 216

Use of Security Culture to Contribute on Enterprise Information Security for the Small and Medium Scale Enterprises (SMEs)

HPAI Pathirana

No 100,Kandawala Road, Ratmalana, Sri Lanka
asanka.pathirana@gmail.com

Abstract: The great use of technologies and flexible work environment introduce complex scenarios to consider for enterprises to assure Enterprise Information Security (EIS). Further the success/failure of EIS effectively rely on behaviour of stakeholders of an enterprise irrespective to the available comprehensive enough technical infrastructure. Therefore, the Security Culture (SC) is recommended to implement at the initial phase to reduce the risk of unacceptable behaviour of stakeholders. Moreover, the SC is further important for Small and Medium Enterprises (SMEs), because comprehensive technical implementation to assure information security is not affordable with limited budget, resources and technical staff. The SC can be introduced as iterative process which must start from somewhere based on primary considerations and improve as required through multiple iterations to fulfil EIS need. The frequent evolvement of SC is essential to addresses consequences of technological development. The SC can be introduced as sub culture of organisation culture, because each stakeholder of the enterprise has active part on assuring EIS in their regular tasks. The mature SC delivers the understand of importance of assuring information security, individual responsibility in security aspects which is way over the general organisational culture, as people is the weakest(only link) for EIS(the technology). Further, people is the first line of defence in any attack, so they must be aware and prepared to represent "Human Firewall". As a result, analyzing assets, analyzing threats, analyzing vulnerabilities, risk assessment, standards and framework, policies and procedures, responsibility, maintenance, stakeholder awareness aspects should be prioritized for implementing SC. Nevertheless, the effective ways to deliver awareness among stakeholders within a SME for enterprise security management should be identified. The successful implementation of SC contributes to EIS for SME effectively.

Key Words: Security Culture, EIS, SME, Vulnerabilities, Threats, Human Firewall,

Introduction

The Enterprise Information Security (EIS) is a problem of people, and it is not just a problem of technology, because people implements and maintains the technological environment(Waly, Tassabehji, & Kamala, 2012). Nevertheless, technology is tool to either use or misuse by the people. The 2%~3% of annual profit of an enterprise is potentially lost due to the poor EIS, nevertheless it influences on reputation of an enterprise having bad impression on customers(Buckley, Nurse, Legg, Goldsmith, & Creese, 2014). Unfortunately, the insider has intentionally/unintentionally involved in most of the incidents, and many studies have same conclusion of the negative involvement of insiders (Buckley et al., 2014; da Veiga & Eloff, 2010; Furnell & Clarke, 2005). Considering those aspects, the enterprises is essential to focus on cultivating understand among stakeholders against the complex uncertain and dynamic characteristics of

insider. Consequently, the Security Culture (SC) is the overlap of needs of organisation culture and EIS as shown in Figure 1, which illustrates SC is part of organisation culture focusing behaviour of stakeholders while contributing to EIS.

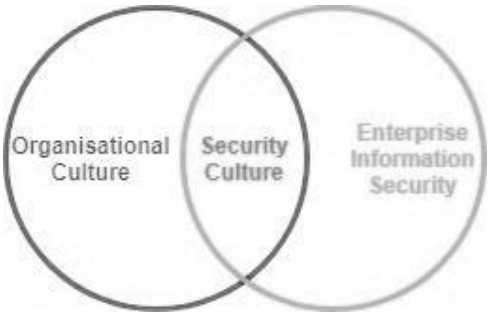

Figure 2: Representation of Security Culture
Source: Author

The enterprise uses interconnected technologies to fulfil business needs effectively in an enhanced level to compete among the competitors, because the business process is significantly influenced with the evolution of technologies(Dhillon, Syed, & Pedron, 2016). As a result, employee is not essential to come to the office regular basis, and customer is served either remotely or in their premises for example. Moreover, many flexible innovative initiatives are introduced with technological enhancement. So the information security is a prior consideration for enterprise at the start-up(Alnatheer, 2015; Dhillon et al., 2016). However there is no enough attention on assuring information security at most of the time, and it introduces challenges to continue business in return(Waly et al., 2012). Assuring information security is global problem for the businesses.

The implementation of technologies and relevant procedures purely contribute to EIS, however large number of incidences are introduced by stakeholders of enterprise due to the negligence or poor knowledge(Dhillon et al., 2016). A one way of defining information security culture is "The collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in [an] organization with the aim of influencing employees' security behaviour to preserve information security''(AlHogail, 2015). Although, the stakeholders represents as the weakest link in the field of EIS by some researchers(da Veiga & Martins, 2017; Sarkar, 2010), the effective implementation of security culture leads for stakeholders to behave as human firewall, since stakeholders do not allow to breach security requirements(Alfawaz, Nelson, & Mohannak, 2010). It is essential to convince stakeholder about the importance of secure behaviour in both work life and personal life through effective implementation of SC.

The most of large scale enterprises maintain better technical implementation adequately by recruiting relevant technical skill staff, because there is no budget constraints, however Small and Medium Enterprises(SMEs) experience in challenges on finance, staffing factors to implement and maintain technical infrastructure(Williams & Manheke, 2010). More often, SMEs consider that information security is not a challenge for them, because they are small, and they rely only on implicit work ethics and trust(Lim, Chang, Maynard, & Ahmad, 2009). Nevertheless, limited staff is responsible for many task which introduces shared resource environment. This research paper is organised to convince SMEs about the importance of assuring EIS and to introduce them effective techniques to implement an SC with priority in their operational environment.

Background

The enterprise security management is evolution process assuring the information security(Waly et al., 2012). The assets are prioritised considering the business value of them to identify what is essential to be

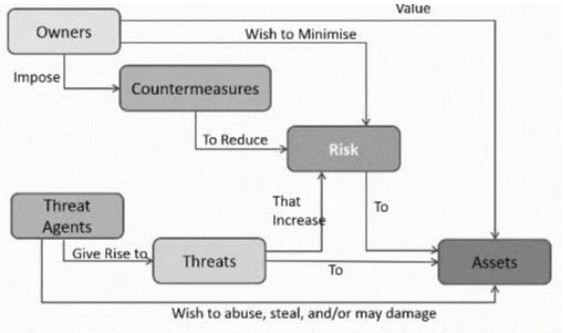

Figure 2: Enterprise Security Management Ecosystem
Source: de Vries, 2016

protected, and risk assessment conducts to identify the risk by introducing countermeasures to reduce the likelihood of exploiting threats(Nasir, Arshah, & Ab Hamid, 2017). Further, financial commitment for a countermeasure must be lesser than the losses against the information security breaches. An enterprise security management ecosystem is shown in the Figure 2 illustrating causalities among different entities(de Vries, 2016). The SC is a cost effective countermeasure correcting behaviour of people, so the SC is important to consider at the start-up.

A. Technoloy and People

Information represents both the hard copies and data in the systems, and people access information in for ways; directly, through systems, over networks and the Internet. A foundation for the security framework is in the Figure 3; sphere of security(Whitman & Mattord, 2011), and the possible countermeasures are illustrated in both technology and people aspects. Nevertheless, contingency planning is essential for addressing security consequences; Incident Recovery, Disaster Recovery, Business Continuity. The evolving technology is a threat for available technological implementation of an enterprise to assure information security(Waly et al., 2012), so it is necessary to acknowledge the stakeholders through effective implementation of SC as describe at next.

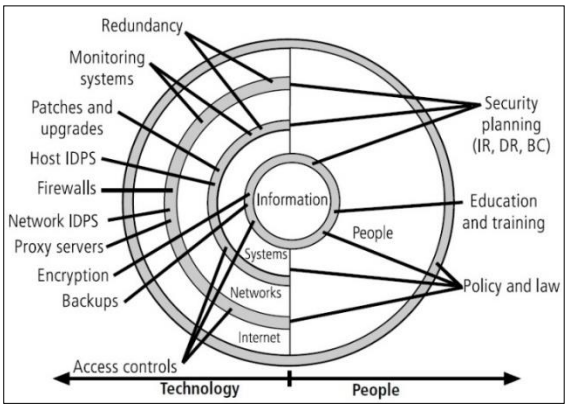

Figure 3. Sphere of Security
Source: Whitman & Mattord, 2011

B. Human Factors

The possible human factors have been identified affecting negatively on EIS, and those are not able to address via technical implementation, where security culture is vital important. Human factors are listed as finding of the literature with the relevant description (Ashenden, 2008; Buckley et al., 2014; da Veiga & Martins, 2017; Nasir et al., 2017; Sarkar, 2010).

1)Improper Use of Passward: Share password, write down password, repeat password are rely on human nature, however use of poor password must be addressed over password policy.

2) Forget to Logout of Systems: The stakeholders are responsible for logging out from the systems after use, however technical configuration is allowed on automatic log out within short time.

3) Theft /Lost of devices: The portable devices; smart phone, laptop, tablet, are not in control of physical security. Consumer must protect the device with priority.

4)Insecure storage: The storage spaces; physical and electronic, must not be accessible for unauthorised stakeholders due to any reason.

5) Insecure Disposal and Reuse: The hard copies of sensitive data; customer details for example, might be used for wrapping something, moreover old laptop might be

sold without deleting data in hard disk. Nevertheless there are techniques to recover deleted data from digital storage. These aspects must be considered closely before dispose or reuse.

6) Resource Misuse: Technologies may be misused in BYOT support; share devices, open WiFi access for convenience for example.

7) Compromise Contractor: The contractor for specific work must be dealt in separate way as untrusted stakeholder by not allowing privileged access to sensitive data.

8) Ignorance of Popup System Warning: The technical implementation to acknowledge stakeholders is available, but stakeholders are not considered them due to poor understand.

9)Accepting Spam Email: The spam email is able to filter technically, however there may be spams rarely, so human firewall must be capable to differentiate them accordingly.

C. The SC Implementation

The implementing EIS is a challenge for most of the enterprises due to the financial, time and staffing factors for example(da Veiga & Martins, 2017), further the SMEs penalised in various manner due to those aspects having limited resources compared to large enterprises(Ng, Ahmad, & Maynard, 2013; Williams & Manheke, 2010). The effective implementation of SC is best possible solution for SMEs with adequate level of policies and technologies implementation as per enterprise requirements after the proper risk assessment(Alnatheer, 2015). nevertheless stakeholders must be acknowledged about the importance of assuring information security adequately as significant part of SC(Furnell & Clarke, 2005).

1)Risk Assessment: The risk assessment goes first in any secure implementation to evaluate the available assets, possible threats/vulnerabilities(Alnatheer, 2015; Nasir et al., 2017), because the critical assets are essential to treat with priority against highly influencing threats/vulnerabilities in affordable manner. Further, the high level risks must be addressed, but medium risks can be transferred by having insurance for example(Whitman & Mattord, 2011). Nevertheless some risks are accepted, since the cost to address that is higher than the impact due to the breaches. Further, some risk can be ignored considering the minor potential impact.

The SMEs are essential to conduct risk assessment at first. Although there are technical implementations are available as countermeasures, SMEs are important to consider implementing effective SC as most effective countermeasure for assuring EIS.

2) Policy Needs Addressing SC for EIS: The enterprise wide information security policy document is essential to introduce in enterprise security management(Furnell & Clarke, 2005; Waly et al., 2012), further implementation of ISO/IEC 27002 to fulfil information security need introduces common language globally(Disterer, 2013). Policy addresses both technical and non-technical implementation requirements of EIS, but this paper focus is about non-technical implementation for effective SC. The primary policy would be focusing on behaviour of stakeholders to introduce best practices; user policy which address the different group of people incorporate with enterprise as stakeholders (Buckley et al., 2014), and it is included with legislation requirement in the event of misconduct. Further the scope of policy depends on enterprise needs, and procedures are introduced based on policy for operational environment.

For example, BYOD is increasing demand of stakeholders due to the comfortable work environment(Miller, Voas, & Hurlburt, 2012), however it allows many vulnerabilities to appear, if there is no extra attention on

devices. It is further expanded into Bring Your Own Technology(BYOT)(Miller et al., 2012). BYOT policy introduces required attention in the use of them addressing the security issues; migration of malware into company network, migration of sensitive data into personal devices, open up security holes, physical security, and the privacy issues; leak of company confidential information, customer personal information.

3) Awareness of Stakeholders: The implementation of technology and policy is effective on active contribution of the stakeholders with better awareness(Furnell & Clarke, 2005; Waly et al., 2012). The requirement for EIS must be known to the stakeholders adequately, and the objective of awareness, training and education programs are conducted to deliver required information/knowledge/insight in theory(Whitman & Mattord, 2011). The awareness program focus on immediate needs on what/things to follow by delivering relevant information for exposure through interactive media, whereas training program focus on average needs on how/approaches to follow by delivering relevant knowledge for skill through hands-on experiences. Nevertheless the education program focus on strategic long term objectives on why/reasons to follow by imparting relevant insight for understanding through theoretical understand. However, specific needs of SME utilise available approaches to deliver proper awareness among stakeholders(Ng et al., 2013).

Methodology

This research is a review and an analysis based on available literature relevant to the SC to find out effective implementation the SC. Both technology and people aspects are evaluated to emphasis enterprise security requirement in background study. Then SC implementation techniques are analysed in different aspects, and the contribution of successful implementation of SC is considered to EIS for SMEs at the end.

A. Research Design

The research design has been introduced based on methodology, and this research follows qualitative approach based on available literature. The motivation of this research to address the global problem to EIS for SMEs by analysing available approaches to implement SC.

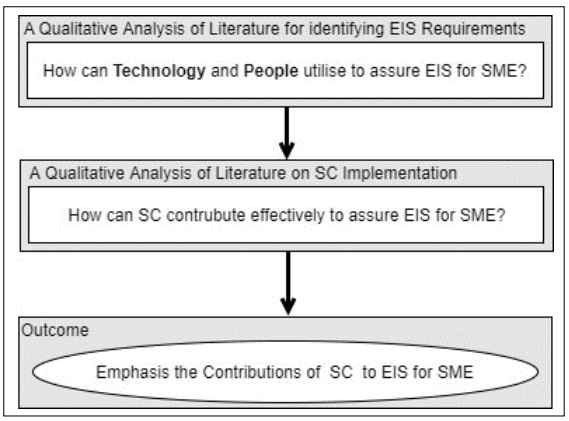

Figure 4: Research Design
Sourcec: Author

Results

The EIS focuses information security needs in an enterprise, and it is supported by security policy as per strategic plan. The SC is significant branch of that considering the complexity of involvement of human. The risk assessment is a main attempt to identify the required technical implementation and other requirements as countermeasure to assure the EIS, and the primary focus of SME is implementation of the SC as countermeasure. The available standards and frameworks assist on developing enterprise specific plan to implement the SC. The budget is a major constrain for SMEs. The SC requirements are primarily addressed through policies and procedures, and the legislation requirements are also enforced. The responsibilities are assigned

Table 1: Research Paper Findings

Paper	Contributing Aspects									Awareness Delivery Approaches									
	Analysing Assets	Analysing Threats	Analysing Vulnerabilities	Risk Assessment	Standards and Frameworks	Policies and Procedures	Responsibility	Maintenance	Stakeholder Awareness	Videos	Posters	Leaflets/ News Letters	Employee Agreements	Self-Studies	Punishments and Rewards	Lectures/ Workshops	Courses	Hands on Practices	Assessments and Reports
(Furnell & Clarke, 2005)					x	x	x	x	x		x	x	x	x		x	x	x	x
(Ashenden, 2008)				x	x	x	x	x	x										x
(Lim et al., 2009)					x	x	x	x	x				x	x	x	x		x	x
(Alfawaz et al., 2010)		x	x			x	x		x										
(Da Veiga & Eloff, 2010)				x	x	x	x		x										
(Sarkar, 2010)	x	x	x	x	x	x	x	x	x				x	x	x				x
(Whitman & Mattord, 2011)	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
(Waly et al., 2012)		x	x	x		x	x		x										x
(Disterer, 2013)	x	x	x	x	x	x	x	x	x				x					x	x
(Buckley et al., 2014)					x	x	x		x										
(AlHogail, 2015)				x	x	x	x		x										
(Alnatheer, 2015)	x	x	x	x		x	x		x					x				x	
(Dhillon et al., 2016)					x	x	x	x	x						x				x
(da Veiga & Martins, 2017)	x			x	x	x	x	x	x		x	x	x	x	x	x	x	x	x
(Nasir et al., 2017)				x	x	x	x	x	x										

explicitly, and it is essential to maintain expected level of SC appropriately. The implementation of security measures is further effective with the appropriate awareness of stakeholders though effective awareness programs. Many researchers have discussed on those as indicated in Table 1.

A) Aspects of effective security culture implementaion

The findings in Table 1 are evaluated further for introducing the better understand of influence of different aspects.

1) Analysing Assets: The available assets must be prioritised through thorough analysis to treat for information security.

2) Analysing Threats: The significance of possible threat decides the requirement of secure implementation.

3) Analysing Vulnerabilities: The significance of available vulnerabilities decides the requirement of secure implementation.

4) Risk Assessment: Risk assessment is comprehensive process to finalise the need of implementing countermeasures as fact findings.

5) Standards and Frameworks: It is not necessary to start from outset, because available standards and frameworks guides need of SC in effective manner. Many SME do not focus on them.

6) Budget: Budget is a major concern of SMEs, as EIS is not part of main business process. The countermeasure implementation must not exceed the lost due to security breaches.

7) Policies and Procedures: The policies provide the guidelines, and procedures are introduced to cultivate best practices for behaviour of the stakeholder. Law enforcement must be addressed.

8) Responsibility: Each stakeholder has an active part to play for effective SC implementation. The legislation, rewards and punishments are explicitly disclosed though an agreement for extra attention. Further, report on any incident is one common responsibility.

9) Maintenance: The present mature implementation becomes obsolete at next moment with evolving technology, so it is essential to conduct periodic audit for maintenance.

10) Stakeholders Awareness: The effective awareness program is essential to convey the need of assuring information security in understandable way. It is essential to focus on individuals.

B) Approaches to deliver the stakeholders awareness

There are 10 approaches listed here to deliver awaresness effectively among the stakeholders.

1) Videos: The videos explain important scenarios in effective manner.
2) Posters: Poster can be displayed in common area with graphical contents to understand easily.
3) Leaflets/ News Letters: A unique concern is acknowledged to the stakeholders, and graphics may help to understand the problem.
4) Employee Agreements: The employee agreement is addressed a legal point, so it becomes part of the job role and responsibilities.
5) Self-Studies: The relevant news articles, online publications about real time scenarios are shared among stakeholders to emphasis the significance of EIS.
6) Punishments and Rewards: This motivates the stakeholder not contribution on security breaches, since it is personally addressed.
7) Lectures/ Workshops: Lecture is organised deliver theoretical knowledge, whereas workshop may focus on case study.
8) Courses: The long term security objectives are addressed educating technical staff for implementing and maintaining secure systems.
9) Hands on Practices: The training sessions guides how to interact with technology in practice through hands on experience.
10) Assessments and Reports: The periodic approach to evaluate stakeholders is recommended to have some understanding of them and report accordingly.

Discussion

A SME has unique challenges to focus on something else in addition to main business process, so they consider EIS as acceptable risk for them assuming no one interest on their information. This research focuses on contribution of SC to EIS for SME as cost effective approach as motivation for SMEs. As initiatives, some aspects are easy to implement with the fundamental approaches since the limited stakeholders in a SME, but continuing the iterative approach towards the successful implementation of EIS is a challenge due to fair reasons attached with finance. This is all about affordability of SME, but it may not the poor interest to assure EIS.

The 10 aspects have been identified in this research serious consideration in SC implementation analysing available literature, and the importance of considering those is also disclosed in broad sense having general understand of SMEs. Nevertheless, 10 approaches are listed with the relevant description to deliver awareness among stakeholders, because the SC is able to establish effectively in operational environment with the awareness of stakeholders improving perceptions, attitudes, values, assumptions, and knowledge of stakeholders.

This paper is about contribution of SC to EIS for SME in general. However there are different sectors of enterprises like education, medical, sales, food, agriculture, production for example(Bolek, Látecková, Romanová, & Korcek, 2016; Gebrasilase & Lessa, 2011; Sari & Nurshabrina, 2016), and certain aspects are emphasised in one sector whereas those are not important for another sector. It is essential to continue this study focusing different sectors in future researches.

Conclusion

The technology implementation to assure the EIS can be established as per the essential requirements of a SME, but mature technical implementation to assure the EIS is not affordable for SMEs in general. The best approach would be dealing with technology in secure manner without introducing vulnerabilities and without allowing threats to exploit. As a result, the SC is the appropriate solution to address human factors instead of technical factors. The SC must be strategically adopted into the operational environment as part of organisation culture to rely on behaviour of stakeholders. Further, the active contribution of each stakeholder is utterly important to achieve this goal, so everyone must have better understand on their responsibilities.

The 10 aspects to consider in effective implementation of SC and the 10 approaches to deliver awareness of stakeholders are tool for implementing mature level of SC. The SC promotes via values, knowledge, artefacts and assumptions relevant to information security, and it is effective if stakeholders act accordingly against any negative incidents according with better understand. Finally, this research filled the gap of the poor understanding of SC implementation by critically evaluating available literature for effective implementation.

The effective implementation of the SC guarantees on addressing information security breaches without introducing vulnerabilities, nevertheless "Human Firewall" is extremely strong enough to prevent from exploiting newly introduced threats which are still not addressed technically. The future work focuses adding value on present findings considering the nature of enterprise due to the unique EIS requirements among them.

References

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: a behaviour compliance conceptual framework. Paper presented at the Proceedings of the Eighth Australasian Conference on Information Security-Volume 105.

AlHogail, A. (2015). Design and validation of information security culture framework. Computers in human behavior, 49, 567-575.

Alnatheer, M. A. (2015). Information security culture critical success factors. Paper presented at the Information Technology-New Generations (ITNG), 2015 12th International Conference on.

Ashenden, D. (2008). Information security management: A human challenge? Information security technical report, 13(4), 195-201.

Bolek, V., Látecková, A., Romanová, A., & Korcek, F. (2016). Factors Affecting Information Security Focused on SME and Agricultural Enterprises. AGRIS on-line Papers in Economics and Informatics, 8(4), 37.

Buckley, O., Nurse, J. R., Legg, P. A., Goldsmith, M., & Creese, S. (2014). Reflecting on the ability of enterprise security policy to address accidental insider threat. Paper presented at the Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop on.

da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196-207.

da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. Computers & Security, 70, 72-94.

de Vries, D. (2016). COMP 9721 - Enterprise Information Security - Topic Manual. Flinders Learning Online (FLO): Flinders University.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: an organizational transformation case study. Computers & Security, 56, 63-69.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4(02), 92.

Furnell, S., & Clarke, N. (2005). Organisational security culture: embedding security awareness, education and training. Computer Security Journal, 21(3), 12.

Gebrasilase, T., & Lessa, L. F. (2011). Information security culture in public hospitals: the case of Hawassa referral hospital. The African Journal of Information Systems, 3(3), 1.

Lim, J. S., Chang, S., Maynard, S., & Ahmad, A. (2009). Exploring the relationship between organizational culture and information security culture. Paper presented at the Australian information security management conference.

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. IT Professional, 14(5), 53-55.

Nasir, A., Arshah, R. A., & Ab Hamid, M. R. (2017). Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture: A Conceptual Framework. Paper presented at the Proceedings of the 2017 International Conference on Information System and Data Mining.

Ng, Z. X., Ahmad, A., & Maynard, S. B. (2013). Information security management: Factors that influence security investments in SMES.

Sari, P. K., & Nurshabrina, N. (2016). Factor analysis on information security management in higher education institutions. Paper presented at the Cyber and IT Service Management, International Conference on.

Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. Information security technical report, 15(3), 112-133.

Waly, N., Tassabehji, R., & Kamala, M. (2012). Improving organisational information security management: The impact of training and awareness. Paper presented at the High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on.

Whitman, M., & Mattord, H. (2011). Principles of information security: Cengage Learning.

Williams, P. A., & Manheke, R. J. (2010). Small Business-A Cyber Resilience Vulnerability. Paper presented at the International Cyber Resilience Conference: Perth

Author Biographies

I graduated in B.Sc.Eng.(Hons) Computer Engineering from the Facullty of Engineering, Univetsity of Peradeniya, Sri Lanka, and I did my M.Sc (Computer Science) at the School of Computing , Flinders University, Australia. I am teaching at the University of Vocational Technology as a senior lecturer in the computing related module. Information Secturity is my interesting research area due to the significant impact to the sensitive information.