International Journal of Computer Networks and Applications (IJCNA)
Volume 2, Issue 4, July – August (2015)

RESEARCH ARTICLE

The Provision of Information Technology Security Considerations by Legal Prescripts: South African Case

Ntjatji Gosebo
Department of Public Service and Administration, South Africa
ntjatji@gosebo.za.net

Sipho Seepe
Ministry of Human Settlements, South Africa
Sipho_Seepe@yahoo.com

Abstract – The purpose of this paper is to establish whether IT security considerations are provided for, in the case of South Africa, by legal prescripts on each computer-based Information Systems' component. A descriptive research approach was employed to accomplish the aim of this paper. Findings are that avoidance IT security consideration is the least covered by legal prescripts, while the deterrence IT security consideration is comprehensively covered by legal prescripts. While legal prescripts related to deterrence IT security consideration are almost similar, they prescribe different punishments for the same violation. A further study is needed to establish whether IT security considerations not covered by legal prescripts are mitigated by other means, and a different further study to determine the efficacy of deterrence without detection is also needed. A consolidated IT security legal prescript might deliver a better remedy to prevailing disjointedness and duplications. This paper develops a rubric or model that guides a comprehensive and systemic assessment of IT security considerations, and provides an evaluation of IT related legal prescripts of South Africa.

Index Terms – IT Security, Legal Prescripts, Security Considerations, Computer-Based Information Systems

1. INTRODUCTION

Nowadays information is a very important asset for any modern organization, and keeping the organization's sensitive internal data from falling into the hands of competitors is every Chief Information Officer's worst nightmare. Network outages, data compromised by hackers, computer viruses and other incidents affect our lives in ways that range from inconvenient to life-threatening. As the number of mobile applications, digital applications and data networks increase, so do the opportunities for criminal exploitations. Therefore protecting information security is very important and is becoming a top priority for many organizations [1].

Security concerns are at the heart of information systems, both at technological and organizational levels [2]. The media is abound with tales of planes that were brought down by rogue code, snoops spying on your security cameras, and secretive undetectable code that can turn any Universal Serial Bus (USB) drive into an unstoppable malware vessel. Therefore, the use of IT as a strategic tool of service delivery will depend on the adequacy of the attendant information security.

The pervasiveness of personal computer and Internet use and the blurred line between work and home, infers that IT security breaches on personal computers can cause harm not only to individuals, but also to organizations [3]. Hacking into corporate IT systems and individuals' computers is no longer a sport for bragging rights, but a major organized economic activity aiming for significant profits controlled largely by underground networks of criminals and organized crime on a global scale [4].

Users currently experience different levels of protection when accessing the Internet via their various personal devices and network connections, due to variable network security conditions and security applications available at each device [5]. Trends such as the influx of consumer devices into the workplace will require more flexible and creative solutions from IT staff for maintaining security while enabling access to collaborative technologies [6].

The widespread of internet usage and development of various systems software enables users to gain more from IT, but, leads to the augmentation of virtual attacks that increases the importance of network security [7]. Subsequently, a process that can illegally elevate itself to root privileges, within the operating system or systems software, can gain access to any sensitive data on the host computer [8].

The effectiveness of other elements in the security system, such as security technology (i.e. software, data, hardware, and networks), organizational policies and procedures, as well as government regulations, are largely dependent on the effort of the human agents, especially those who work within the organizations [3, 4, 9]. Many organizations recognize that their employees, who are often considered the weakest link in information security, can also be great assets in the effort to reduce risk related to information security [9].

RESEARCH ARTICLE

Securing information system resources is extremely important to ensure that the resources are well protected; but, information security is not just a simple matter of having usernames and passwords [1]. It is indispensable to continuously evaluate the compliance regarding information security standards and the effectiveness of already existing control implementations, to maintain a holistic security program [10].

The objective of this paper is to find out whether the IT security considerations (i.e. avoidance, deterrence, prevention, detection, correction, and recovery) under each Computer-Based Information Systems (CBIS) element are provided for in the case of South African IT security legal prescripts. The ensuing sections of this paper are organized into: Literature Review, Research Approach, Results, Discussion of Results, and Conclusion and Recommendations.

2. LITERATURE REVIEW

Risk avoidance is the threat assessment technique that entails eliminating hazards, activities and exposures that place an organization's valuable assets at risk [3, 11, 12]. The IT security related behavior is predicted by avoidance motivation, which, in turn, is determined by perceived threat, safeguards effectiveness, safeguard cost, and self-efficacy [3]. Risk and uncertainty avoidance are factors that significantly affect the success of internet buying [11]. Only extreme IT security related warranties are legally guaranteed, such as the respect for private life or the avoidance of exposure to arbitrary or unlawful interference [12].

The deterrence doctrine suggests that perceived threat of sanctions influence personal behaviors through the certainty and severity of punishment; as punishment certainty and punishment severity are increased, the level of illegal behavior should decrease [13]. Organizations should punish serious violations to the full extent possible because such punishment would deter other such behavior [9]. Hu, Xu, Dinev & Ling [4] emphasize by calling for the establishment of clear and swift sanctions against security misconduct to deter and reduce future violations.

Intrusion prevention is a pre-emptive approach of IT security used to identify potential threats and respond to them swiftly [9, 14]. Enhancement of social bonds through organizational factors (attachment, commitment, involvement, and norm) is an effective mechanism in preventing computer abuse [9]. Organizations may rely heavily on controls to prevent employee computer crime [14].

The IT security detection is a process used to quickly identify and mitigate threats [13, 15]. Moreover, monitoring techniques enable the detection of more serious and deliberate misuse incidents that are likely subject to severe punishment [15]. Some kinds of monitoring and detection mechanisms are necessary to make certain that employees are acting in accordance with the security policies [13].

as natural disasters can never be prevented, hence, it is better to direct more resources to the recovery from loss, rather than to try and defend against them [16]. There must be adequate provision for disaster recovery and business continuity planning to protect the continuity of the services being delivered [17]. With the proliferation of networked technologies, researchers have begun to focus on the constituent elements of networks, with the eventual aim of leveraging the power of network elements in providing information as a way of mitigating the impacts of and speeding up the recovery from extreme events [18].

Correction in IT security is about something given, done, or proposed as a substitute for what is wrong or inaccurate [19, 20, 21]. Where there is an urgent need for corrective measures to be implemented; corrective measures are essential to protect the information systems against threats [21]. Security-related incidents (e.g. attempts to change/manipulate financial data, etc.) identified within the organization's processing of information are communicated in a timely manner and that corrective action is taken for any exceptions identified [19]. Response takes appropriate corrective actions against identified attacks [20].

Fenz [10] observed that several IT-security metrics approaches have been developed, but, a methodology for automatically generating IT security metrics is missing. Traditionally, IT security countermeasures have been categorized into four types, which include deterrence, prevention, detection, and recovery [14]. This paper intends to determine whether the rudiments of IT security considerations (i.e. avoidance, deterrence, prevention, detection, correction, and recovery) under each CBIS element, are provided for in the case of the South African legal prescripts.

3. RESEARCH APPROACH

The descriptive research is used to fulfill the goal of this paper; because, descriptive research is a basic research method that examines the situation, as it exists in its current state [22, 23]. The characteristics used to describe the situation or populations are usually some kind of categorical scheme also known as descriptive categories. Descriptive categories of this paper are: (i) Legal instruments relating to IT security, (ii) Computer-based Information Systems (CBIS) components (i.e. People, Processes and Procedures, Applications Software, Systems Software, Hardware, and Network), and (iii) IT security considerations (i.e. avoidance, deterrence, prevention, detection, correction, and recovery).

South Africa is used as a case study whereupon each of the IT security related legal instruments is mapped in accordance with applicability to the CBIS components. The procedural

RESEARCH ARTICLE

process for the content analysis study is designed to achieve the highest objective analysis possible and involves identifying the body of material to be studied and defining the characteristics or qualities to be examined [23].

The above outcome gets refined according to applicability to the descriptive category of IT security considerations. Purpose of refinement is to make results more easily understood, implementable, and easily measured in an organization by stakeholders [20].

4. RESULTS

There are 32 IT security related legal prescripts in South Africa and are listed in the table hereunder.

Legal Instrument		Acronym
i.	Air Services Licensing Act, 1990 (Act 115 of 1990)	ASL
ii.	Constitution of the Republic of South Africa, 1996 (Act 108 of 1996)	CRSA
iii.	Copyright Act, 1978 (Act No. 98 of 1978)	CA
iv.	Correctional Services Act, 1998 (Act 111 of 1998 CS computers	CS
v.	Criminal Law Amendment Act, 2007	CLA
vi.	Criminal Procedure Act, 1977 (Act No. 51 of 1977)	CP
vii.	Documentary Evidence From Countries in Africa Act, 1993 (Act 62 of 1993)	DEFCA
viii.	Electronic Communications and Transactions Act, 2002 (Act 25 of 2002)	ECT
ix.	Films and Publications Act, 1996 (Act 65 of 1996)	FP
x.	Financial Advisory and Intermediary Services Act, 2002 (Act No. 37 of 2002)	FAIS
xi.	Financial Intelligence Centre Act, (Act 38 of 2001)	FICA
xii.	Financial Markets Act, 2012 (Act 19 of 2012)	FMA
xiii.	International Air Services Act, 1993 (Act 60 of 1993);	IAS
xiv.	Magistrates Courts Act, 1944 (Act 32 of 1994)	MC
xv.	National Key Points Act, 1980 (Act 102 of 1980)	NKPA
xvi.	National Prosecuting Authority Act, 1998 (Act 32 of 1998)	NPA
xvii.	National Strategic Intelligence Act, 1994 (Act 39 of 1994)	NSI
xviii.	Prevention and Combating of Trafficking in Persons Act, 2013 (Act 7 of 2013)	PCTP
xix.	Prevention and Combatting of Corrupt Activities Act, 2004 (Act 12 of 2004	PCC
xx.	Prevention of Organised Crime Act, 1998 (Act 121 of 1998)	POCA
xxi.	Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act 33 of 2004)	PCDATR
xxii.	Protection of Personal Information Act, 2013 (Act 4 of 2013)	PPI
xxiii.	Public Service Act, 2007 (Act 30 of 2007)	PSA
xxiv.	Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act 70 of 2002),	RICA
xxv.	Securities Services Act, 2004 (36 of 2004)	SS
xxvi.	Sexual Offences and Related Matters) Amendment Act, 2007 (Act 32 of 2007)	SOA
xxvii.	South African Police Service Act, 1995 (Act 68 of 1995)	SAPS
xxviii.	Protection of Personal Information Act [No. 4 of 2013	POPI
xxix.	State Information Technology Agency Act, 1998 (Act 88 of 1998)	SITA
xxx.	Statistics Act, 199 (Act 6 of 1999)	SA
xxxi.	Minimum Information Security Standards, 1996	MISS
xxxii.	National Archives Act, 1996 (Act 45 of 1996)	NA

Table 1 - IT Security Related Legal Instruments

Half of South African legal prescripts thought to relate to IT security did not have clear associations with any of the CBIS elements. Consequently, table 2 represents a mapping of legal prescripts that address at least one CBIS element. Findings reveal that the people related CBIS element is covered by legal prescripts across all IT security considerations, while networks related CBIS element is only covered by legal prescripts on deterrence IT security consideration.

RESEARCH ARTICLE

		Computer-based Information Systems (CBIS) Elements					
		People	Applications Software	Systems Software	Databases	Hardware	Networks
IT Security Considerations	Avoid	• CRSA • MISS • PSA					
		9.375%	0%	0%	0%	0%	0%
	Deter	• POPI • NPA • SAPS • CS • ECT • RICA • POPI • SOA • CA • PCDTR	• SAPS • NPA • CS • POPI • PCC • PCDTR	• SAPS • NPA • CS • PCC • PCDTR	• ECT • POPI • SAPS • NPA • CS • PCC • PCDTR	• POPI • SAPS • NPA • CS • ECT • PCC • PCDTR	• ECT • RICA • POPI • PCDTR
		31.25%	18.75%	15.625%	21.875%	21.875%	12.50%
	Prevent	• PSA • CRSA • MISS • SITA • PCTP	• SITA		• PSA • ECT • PPI • SITA	• RICA	
		15.625%	3.125%	0%	12.50%	3.125%	0%
	Detect	• MISS • PSA • ECT		• MISS	• MISS • ECT		
		9.375%	0%	3.125%	6.25%	0%	0%
	Correct	• PSA • CA	• PSA		• ECT		
		6.25%	3.125%	0%	3.125%	0%	0%
	Recover	• MISS		• MISS	• ECT		
		3.125%	0%	3.125%	3.125%	0%	0%

Table 2- Final Results from Synthesizing the Three Descriptive Categories

The cross-tabulation (see table 2 above) encapsulates final results from synthesizing the three descriptive categories of this paper; namely, CBIS elements, IT security considerations, and IT security related legal prescripts. Percentages are used in table 2 to give a sense of prevailing coverage of legal prescripts. Legal prescripts for a given IT security control and given CBIS element are represented as a percentage of the 32 legal instruments from table 1.

General findings reveal that half of the IT security controls aspects are not covered by the current legal prescripts. Findings are presented, hereunder, in accordance with IT security considerations (i.e. avoidance, deterrence, prevention, detection, correction, and recovery).

4.1. Avoidance of IT Security Violations

Only the people element of the CBIS elements has legal prescripts that seek to avoid IT security breaches. Legal prescripts that cover the avoidance of IT security (i.e. PSA and MISS) are limited to civil servants (as a class of people). The Constitution of South Africa has provisions that loosely relate to avoidance of IT security violations, but, there are no laws that clarify the intent on people other than civil servants.

RESEARCH ARTICLE

Legal prescripts related to the avoidance of IT security violations do not exist for CBIS components other than the people element. Therefore, CBIS elements that are not covered by legal prescripts on the avoidance of IT security violations are either neglected or avoidance is unimportant for CBIS elements that are not covered by legal prescripts.

4.2. Deterrence against IT Security Violations

Deterrence is the only IT security consideration that is covered by legal prescripts across all CBIS elements. Accordingly, jail term and fines, if the perpetrator is convicted, are the only forms of deterrence provided by the current legal prescripts.

When the legal prescripts are analyzed per CBIS element, a pattern emerges where several legal prescripts duplicate criminalization of the same offense. Such duplications of legal prescripts present an undesirable situation where differing, sometimes unfair; punishments are prescribed for the same IT security violation. Unfortunate perceptions of corruption or favoritism may be created where differing punishments are meted for the same offence.

The justice and security agencies tend to be leading in prescribing deterrence for IT security violations. However, legal prescripts related to justice and security agencies are wont to focus exclusively on the prescribing agency. The internally focused IT security legal prescripts of justice and security agencies tend to aggravate the proliferation of differing punishments for the same crime.

4.3. Prevention of IT Security Violations

Prevention of IT security violations is covered by existing legal prescripts for most of the CBIS elements, but, both systems software and networks elements of the CBIS are not covered by current legal prescripts. Given that both systems software and networks elements of CBIS are prominent in cybersecurity concerns; the foregoing finding reveals a potentially momentous deficiency of current IT security legal prescripts on the prevention of IT security violations.

Conceivably, products in the market are deemed adequate to prevent IT security violations in both systems software and networks. Then again, lack of legal prescripts may be exposing both systems software and networks to needless security violations.

4.4. Detection of IT Security Violations

There are no legal prescripts for detecting IT security violations in applications software, hardware, and networks. This finding is against the backdrop of applications software, systems software and networks elements of CBIS being predominant in cybersecurity anxieties. Thus, the finding of lack of legal prescript for detecting IT security violations in applications software, hardware, and networks reveal a potentially serious shortcoming of current IT security legal prescripts on the detection of IT security violations.

The foregoing makes it difficult to comprehend how jail terms and fine types of deterrence can be possible without detection or proof. It might be the case that detecting IT security violations in applications software, hardware, and networks is not a valid consideration. Otherwise, legal prescripts are needed to cover the detection of IT security violation in applications software, hardware, and networks.

4.5. Correction of IT Security Violations

Systems software, hardware, and networks do not have legal prescripts that deal with correction of IT security violations. Prominent elements of CBIS in cybersecurity are systems software, hardware, and networks; therefore, the foregoing finding reveals a potentially severe inadequacy of current IT security legal prescripts on the correction of IT security violations.

It is conceivable that the detection of IT security violations for systems software, hardware, and networks is unimportant, whence the correction of their IT security violations become moot. Alternatively, systems software, hardware, and networks may not be accommodated through legal prescripts due to the fact that they are proprietary and corrections by a developing country are infeasible. Otherwise, systems software, hardware, and networks need to be covered by legal prescripts to accommodate the correction of IT security violations.

4.6. Recovery from IT Security Violations

Legal prescripts for recovery from IT security violations have similar findings to those on detection of IT security violations; namely, that applications software, hardware, and networks are not covered by current legal prescripts. Similarly, the finding of lack of legal prescript for recovering from IT security violations in applications software, hardware, and networks reveal a potentially grave weakness of current IT security legal prescripts on the recovery from of IT security violations.

Possibly recovering from IT security violations in applications software, hardware, and networks is not a concern, due to their proprietary nature and developing countries' dispositions. Else, legal prescripts are desirable to provide for recovery from IT security violation in applications software, hardware, and networks.

5. DISCUSSION OF RESULTS

Results of this paper aim to establish whether IT security controls are provided for, in the case of South Africa, by legal prescripts under each CBIS component. Discussion of

RESEARCH ARTICLE

abovementioned findings are organized, hereunder, in accordance with IT security considerations (i.e. avoidance, deterrence, prevention, detection, correction, and recovery).

5.1. Avoidance Considerations

The avoidance of IT security violations on the people element of the CBIS is the only one covered by current legal prescripts. This finding endorses the observation [3] that IT security related behavior is foretold by avoidance motivation.

There is nothing to avoid hazards, activities and exposures that place an organization's valuable assets at risk [3, 11, 12]. Risk and uncertainty avoidance are factors that significantly affect the success of using IT as a tool for service delivery [11], and this is confirmed by the fact that legal prescripts on the avoidance of IT security violations is absent for most CBIS elements.

5.2. Deterrence Considerations

Deterrence is the only IT security consideration that is covered by legal prescripts across all CBIS elements. As a result, this finding supports the assertion that perceived threat of sanctions influence personal behaviors through the certainty and severity of punishment; as punishment certainty and punishment severity are increased, the level of illegal behavior should decrease [13]. Furthermore, this finding supports the contention [9] that organizations should punish serious violations to the full extent possible because such punishment would deter other such behavior.

In order to deter through penalties and jail terms, the legal prescripts rely on court prosecutions; yet, most of the legal prescripts that provide for deterrence are seriously lacking in detecting IT security violations. There is a need for a further investigation on the rate of conviction from legal instruments that provide for deterrence without detection, and this paper anticipates the conviction rate to be dismal.

The deterrence legal instruments against IT security violations are almost similar, but, penalties are dissimilar for the equivalent IT security crime where a punishment depends on a legal instrument used. Therefore, rationalization of all legal prescripts on deterrence against IT security violations under one legal instrument on IT security may bring coherence, and may address perceptions on unfairness and corrupt courts.

Another observation from legal instruments that provide deterrence for IT security violations is that justice and security agencies tend to provide only for deterrence against their own internal CBIS elements. Hence, the IT security legal instruments of justice and security agencies may need to be rationalized under one legal instrument, which extends beyond internally focused concerns of security and justice agencies.

5.3. Prevention Considerations

The prevention of IT security violations on both systems software and networks elements of the CBIS elements are not covered through current legal prescripts, whereas both networks and systems security are at the core of cyber security. The foregoing finding is not supported by the observation [8] that a process can illegally elevate itself to root privileges, within the operating system or systems software, thus, can gain access to any sensitive data on the host computer.

The widespread of internet usage and development of various systems software enables users to gain more from IT, but, leads to the augmentation of virtual attacks that increases the importance of network security [7]. Evidently, appropriate legal instruments are needed to prevent IT security violations.

The CBIS element related to people is covered by legal instruments, amongst others, and validates the assertion [14] that organizations may rely heavily on controls to prevent computer crime by employees.

5.4. Detection Considerations

Monitoring and detection mechanisms are necessary to make certain that employees are acting in accordance with the security policies [13]. Nonetheless, findings reveal that there are no legal prescripts for detecting IT security violations in applications software, hardware, and networks.

Monitoring techniques enable the detection of more serious and deliberate misuse incidents that are likely subject to severe punishment [15]. Without legal prescripts that cover detection of IT security, how will the legal prescripts secure jail terms and fines in CBIS elements of applications software, hardware, and networks?

It is unlikely that detecting IT security violations in applications software, hardware, and networks is not a valid IT security consideration. Consequently, legal prescripts are needed to cover the detection of IT security violation in applications software, hardware, and networks.

5.5. Correction Considerations

Corrective measures are essential to protect the information systems against threats [21], but, findings are that systems software, hardware, and networks do not have legal prescripts that deal with correction of IT security violations. Hence, there are no opportunities for response to take appropriate corrective actions against identified attacks on systems software, hardware, and networks [20].

Security-related incidents (e.g., attempts to change/manipulate financial data, etc.) identified within the organization's processing of information should be communicated in a timely manner and that corrective action is taken for any exceptions identified [19]. Consequently, systems software,

RESEARCH ARTICLE

hardware, and networks need to be covered by legal prescripts to accommodate the correction of IT security violations.

5.6. Recovery Considerations

Legal prescripts for recovery from IT security violations in applications software, hardware, and networks are absent; and this finding is similar to the IT security consideration for detection. Vulnerabilities such as natural disasters can never be prevented, so, the recovery from loss is critical [16]; notwithstanding, legal prescripts do not cater for applications software, hardware, and networks IT security considerations.

Disaster recovery is vital to protect the continuity of the services being delivered [17]. As a result, legal prescripts are desirable to provide for recovery from IT security violation in applications software, hardware, and networks.

6. CONCLUSION AND RECOMMENDATIONS

This paper is establishing whether IT security considerations are provided for, in the case of South Africa, by legal prescripts under each CBIS component. A descriptive research was employed to achieve the purpose of this paper through examining the case of South African legal prescripts related to IT security. Half of South African legal prescripts regarded as IT security related, had nothing to do with any of the CBIS elements. The avoidance IT security consideration is the least covered by legal prescripts, while the deterrence IT security consideration is remarkably covered by legal prescripts. The people related CBIS element is covered by legal prescripts across all IT security considerations, whereas the networks related CBIS element is only covered by legal prescripts on deterrence IT security consideration.

Legal prescripts related to deterrence IT security consideration are almost similar; however, each prescribes a different punishment for the same violation. Most legal prescripts that possess deterrence IT security consideration are not complimented by a legal prescript related to detecting IT security violations. Thus, the deterrence IT security consideration might be ineffective.

Further studies are needed to establish whether IT security considerations not covered by legal prescripts are mitigated by other means, and to determine whether deterrence is possible without detection. A consolidated IT security legal prescript is needed to provide: (i) comprehensive IT security considerations, (ii) consistent sanction for the same violation, (iii) rigorous detection IT security considerations to enable the success of deterrence, and (iv) solutions for weaknesses identified in this paper on current IT security legal prescripts.

This paper develops a rubric or model that guides a comprehensive assessment of IT security considerations, and provides an evaluation of IT related legal prescripts of South Africa.

REFERENCES

[1]. Susanto, H., Almunawar, M. N., & Tuan, Y. C. “Information security management system standards: A comparative study of the big five”. 2011

[2]. Dubois, É., Heymans, P., Mayer, N., & Matulevičius, R. “A systematic approach to define the domain of information system security risk management”. *In Intentional Perspectives on Information Systems Engineering*, 2010, pp. 289-306. Springer Berlin Heidelberg.

[3]. Liang, H., & Xue, Y. “Understanding security behaviors in personal computer usage: A threat avoidance perspective”. Journal of the Association for Information Systems, 2010, 11(7), 394-413.

[4]. Hu, Q., Xu, Z., Dinev, T., & Ling, H. “Does deterrence work in reducing information security policy abuse by employees?” *Communications of the ACM*, 2011, 54(6), 54-60.

[5]. Lioy, Antonio, Antonio Pastor, Fulvio Risso, Roberto Sassu, and Adrian L. Shaw. "Offloading security applications into the network." *In eChallenges e-2014*, 2014 Conference, pp. 1-9. IEEE.

[6]. Thomson, G. “BYOD: enabling the chaos”. *Network Security*, 2012, (2), 5-8.

[7]. Huang, C. C., Lin, F. Y., Lin, F. Y. S., & Sun, Y. S. “A novel approach to evaluate software vulnerability prioritization”. Journal of Systems and Software, 2013, 86(11), 2822-2840.

[8]. Park, Y., Lee, C., Kim, J., Cho, S. J., & Choi, J. “An Android security extension to protect personal information against illegal accesses and privilege escalation attacks”. *Journal of Internet Services and Information Security (JISIS)*, 2012, 2(3/4), 29-42.

[9]. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. “Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness”. *MIS quarterly*, 2010, 34(3), 523-548.

[10]. Fenz, S. “Ontology-based generation of IT-security metrics”. In Proceedings of the 2010 ACM Symposium on Applied Computing, 2010, (pp. 1833-1839).

[11]. Al Kailani, M., & Kumar, R. “Investigating uncertainty avoidance and perceived risk for impacting internet buying: a study in three national cultures”. International Journal of Business and Management, 2011, 6(5), p76.

[12]. Weber, R. H. (2011) “Internet of Things–New security and privacy challenges”. Computer Law & Security Review, 26(1), 23-30.

[13]. Herath, T., & Rao, H. R. “Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness”. Decision Support Systems, 2009, 47(2), 154-165.

[14]. Warkentin, M., & Willison, R. “Behavioral and policy issues in information systems security: the insider threat”. European Journal of Information Systems, 2009, 18(2), 101.

[15]. D'Arcy, J., Hovav, A., & Galletta, D. “User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach”. Information Systems Research, 2009, 20(1), 79-98.

[16]. Dlamini, M. T., Eloff, J. H., & Eloff, M. M. “Information security: The moving target”. Computers & Security, 2009, 28(3), 189-198.

[17]. Kandukuri, B. R., Paturi, V. R., & Rakshit, A. “Cloud security issues”. In Services Computing, SCC'09. IEEE International Conference on, 2009, (pp. 517-520). IEEE.

[18]. Tapia, A. H., Bajpai, K., Jansen, B. J., Yen, J., & Giles, L. “Seeking the trustworthy tweet: Can microblogged data fit the information needs of disaster response and humanitarian relief organizations”. In Proceedings of the 8th International ISCRAM Conference, 2011, (pp. 1-10).

[19]. Otero, A. R., Otero, C. E., & Qureshi, A. “A multi-criteria evaluation of information security controls using Boolean features”. International Journal of Network Security & its application (IJNSA), 2010, 2(4).

[20]. Ahmad, A., Maynard, S. B., & Park, S. “Information security strategies: towards an organizational multi-strategy perspective”. Journal of Intelligent Manufacturing, 2014, 25(2), 357-370.

RESEARCH ARTICLE

[21]. Lo, C. C., & Chen, W. J. "A hybrid information security risk assessment procedure considering interdependences between controls". Expert Systems with Applications, 2012, 39(1), 247-257.
[22]. Ross, S. M., & Morrison, G. R. "Experimental research methods". In D. H. Jonassen (Ed.), Handbook of research on educational communications and technology (2nd ed). 2004, Mahwah, New Jersey: Lawrence Erlbaum Associates, Inc.
[23]. Williams, C. "Research methods". Journal of Business & Economics Research (JBER), 2011, 5(3).