Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol.4, No.9, 2014

Impact of Information Security Policies on Computer Security Breach Incidences in Kenyan Public Universities

Jerotich Sirma [1*] Monicah Muiru[1] Dr. Cynthia Kipchillat[2]
1.Lecturer, Faculty of Commerce, Department of Accounting Finance and Management Science, Egerton University, Nakuru Town Campus College, P.O Box 13357, Nakuru-Kenya
2.Senior Lecturer, Faculty of Commerce, Department of Business Administration, Egerton University
[*] Email of the corresponding author jerotichk@gmail.com

Abstract
The aim of this study was to investigate the Impact of Information Security Policies on Computer Security Beach incidences in Kenyan public universities. Information security policies are designed to safeguard network resources from security breaches. The study utilized a questionnaire to collect primary data from Information Technology (IT) personnel in public universities with regard to their perceptions of how information security policies affect computer security breach incidents. A simple random sampling was used to identify 200 IT employees from public universities in Kenya. Pearson correlation analysis was used to study the relationships between the variables. Independent t-tests (2-tailed) and ANOVA test were used to determine the level of significance. According to the results of the study, there is a weak relationship between information security policies and security breaches. The study hopes to add to the body of academic knowledge in the public educational institutions in Kenya where information repository is a resource.
Keywords: Information Security Policies, Security Breach Incidences, Kenyan Public Universities

1.0 Background of the study

Information is an important organizational asset that is subject to vulnerability to attacks due to user errors, hackers and crackers, viruses and cyber criminals. The Kenyan public universities are prioritizing the security of their computer systems in order to provide their users with information that is available, accurate and confidential (Doherty & Fulford, 2005). Public Universities are entrusted with highly confidential and privileged client information. Subsequently, public universities have an obligation to maintain, store, and secure this sensitive information and to ensure their clients' privacy (Comerford, 2006). The underlying problem in most institutions is managing information security policies. Information security entails the creation of policy statements used in ranking information risks, identifying acceptable security goals and procedures (Da Veiga & Eloff, 2007; Metzler, 2007; Robinson, 2005; Laudon & Laudon, 2012). Studies have identified good security policies (Dhillon and Torkzadeh, 2006) and frameworks for security governance (Brotby 2009; Da Veiga and Eloff 2007; Vonn Solms and Von Solms 2009), yet there is still lack of understanding by users about how security breach incidents have the potential to weaken the implementation of security policies in public universities. Security breaches are incidents consisting of unauthorized access to sensitive or confidential data (Kraemer & Carayan, 2007). Security breaches can also arise through computer programs that replicate viruses across systems and networks; intrusion of organizational computer systems by unauthorized outsiders who can manipulate data; abuse of systems that contain data; theft of valuable hardware, software and information assets.
Information security polices outline the responsibilities and acceptable user actions of public university employees when using university computers and networks. Security controls include management controls, operational controls, and technical controls. According to Post and Kegan (2007), information security policies are considered to be the management control measures that will define an appropriate security for the network infrastructure. Other management controls include vulnerability assessment and security plans implemented to manage the security of a university (Salmela, 2008). Security policies have clear rules on how a network can be accessed while maintaining confidentiality and identifying the ramifications of a security breach of a university (Greene 2006; Whitman & Mattord, 2008). Operational controls include physical security, personal security, business continuity planning, incident response, hardware and software maintenance, confidential data protection, and security awareness training (Bowen, et al, 2006; Hagen, Albrechtsen, & Hovden, 2008) that are implemented by public university personnel as opposed to computer software automation process.

Technical controls include firewalls, anti-virus, intrusion detection systems (IDSs), intrusion prevention Systems (IPSs), and access controls. Firewalls are software and hardware that prevent unauthorized users from accessing the university network (Weaver, 2007). Anti-virus software scans files for potentially harmful viruses and sequesters these files to prevent their propagation (Lin, 2006) to other computers on the network. IDSs are software programs that identify possible unauthorized access to files (Basta & Halton, 2008). IPSs are software programs similar to IDSs that identify possible access to files but flag activity in real-time (Whitman & Mattord, 2008). According to Comerford (2006), authorized users are those users who have permission to access the computer files and network of the university. Access controls provide permissions to allow users access to

network assets, such as database file or public university networks based on their carefully delineated access privileges, ensuring authorized users are allowed to access certain data on the university's network.

1.1 Statement of the Problem

Most organizations are going digital with the hope of improving service efficiency to their customers and increased productivity from their employees. Public universities in Kenya are no exception in this digital trend. Cases of public university fraud have increased in the past few years and this trend begs for further investigation on security breaches in Kenyan public university computer systems. Currently, organizations are forced to store digital data for longer periods while processing business transactions (Laudon & Laudon, 2012). The risks that organizations face include safeguarding information resources in their networks. Organizations have formulated security policies with the hope of solving the problem of security breaches or to significantly reduce incidences of security breaches. However, systems are still vulnerable to security breaches. The vulnerability may arise from security breaches that could be internal or external to the organization. A security breach can result in the risk of an intrusion into the university's sensitive information (Kramer & Carayan, 2007; Schwartz & Janger, 2007). Johnson (2008) observes that disclosure of information can result to loss of confidence in Public Universities. Therefore, this study hopes to establish whether information security policies assist in preventing unauthorized individuals from accessing university's sensitive information.

1.2 Objectives of the Study

The main objective of the study is to analyze the impact of information security policies on the reduction of computer security breaches in the public universities in Kenya. The specific objectives are to:

i. Investigate the relationship between network security policies and information security breach incidents.
ii. Determine the relationship between server security policies and information security breach incidents.
iii. Investigate the relationship between application security policies and information security breach incidents.
iv. Investigate the impact of information security policies on information security breach incidents.

1.3 Research Hypotheses

$H_0$1 There is no statistical significant relationship between network security policies and information security breach incidences.
$H_0$2 There is no statistical significant relationship between server security policies and information security breach incidences.
$H_0$3 There is no statistical significant relationship between network security policies and information security breach incidences.
$H_0$4 There is no statistical significant relationship between information security policies and information security breach incidences.

2. 0 Literature Review

2.1Information Security Policies

According to Baker and Wallace (2007), security policies define actions that can and cannot be taken with company computers. The policies outline the acceptable actions and use of public university's computers and networks by its employees (Doherty & Fulford, 2005; Metzler, 2007; Verdon, 2006). Information security policies pertain to written documentation outlining the structure of the organization's security posture. The purpose of information security entails the preservation of confidentiality, integrity and availability (Ismail et al., 2011). In addition, authenticity, accountability, non-repudiation and reliability are other elements which pertain to information security. Subsequently, security policies provide guidance with regard to the physical and remote access to data of the public university. Bidgoli (2006) observes that there are three categories of information security policies; network security policies, server security policies and application security policies. Liska (2008) notes that sever security policies help to prevent configuration inconsistencies and helps administrators to react efficiently to security incidents while network security policies aim at securing the network. On the other hand, application security policies aim to consistently enforce application security around an organization application infrastructure (Tipton and Krause, 2008)

Doherty and Fulford (2006) state that information security policies should be in line with the public university's objectives. Verdon (2006) observes that threats continually evolve, and the countermeasures must evolve too. After reviewing the potential threats to public universities' network, the public university Chief Security Officer (CSO) and/or Chief Information Officer (CIO) should develop, implement, and distribute a security policy or policies to all employees. According to Whitman and Mattord (2008) and Greene (2006) an effective security policy must establish key goals for ensuring that authorized users can access the network and information resources. Additionally, the security policy must ensure employees know the penalties of

inappropriate behavior when using information resources. Within the policy, each public university employee's information security responsibilities are to protect the confidentiality, integrity, and availability of the public university and confidential data.

Metzler (2007) suggested using standards or security processes rather than just security policies to cater for the continued need to update the requirements as part of security policy maintenance. According to Metzler (2007), an organization stakeholders' involvement is critical in order to produce longevity and effective security policies. For these security goals to be realized, public universities' IT personnel must be actively involved in developing these policies. If the security failure can be equated to a monetary figure, then the seriousness of developing an applicable security policy is more readily accepted by public universities (Greene, 2006; Whitman & Mattord, 2008). Security policies addresses the following topics: access control, acceptable use, business continuity and disaster recovery, change control management, confidentiality, data classification, data backup and recovery, disposal practices, e-mail practices, encryption, information protection, information systems security, Internet use, network security, privacy, physical security, remote access, system administration security, incident response, and termination (Greene, 2006; Metzler, 2007; Rotvold, 2008; Verdon, 2006).

Metzler (2007) suggests developing a separate security policy for each topic in order to quickly update and approve procedures. Therefore, smaller separate documents rather than one large document would expedite revisions and approval of necessary revisions to the individual policy topics since they would be shorter and therefore easier to review. Furthermore, security awareness is a topic all public university employees must understand so that their actions will not jeopardize confidential data in their possession (Alshboul, 2010). Therefore, public university employees must be informed as to the applicable security policy pertinent to their job and understand why it is important to protect the information located on their computers from unauthorized access (Baker & Wallace, 2007; Chen et al., 2006). Furthermore, insider threats consisting of the disgruntled or curious employee must be addressed in the security policies to outline the ramifications of accessing data not relevant to the public university employee's job description (Gupta & Sherman, 2012; Lin, 2006). Insider threats are one of the most common causes of security breaches (Bowen et al., 2006; Chen et al., 2006; Ramim & Levy, 2006). Incident response procedures and the method for reporting information security incidents relative to insider breaches should be included in the public university security policies (Chen et al, 2006).

2.2 Information Security Threat and Vulnerability

According to Alshboul (2010) vulnerability is the weakness of information and information systems that leads to attacks, harm, modification, disclosure, destruction, interruption, and interception. A successful attack on information systems is a sign of vulnerability (Alahboul, 2010). Vulnerability assessment deals with identifying flaws and weaknesses that could possibly be exploited (Dhillon, 2006). Vulnerabilities open opportunities for hackers and attackers who attack the information and information systems. Nyanchama (2005) points out that threats take advantage of vulnerabilities to cause damage or loss. The weaknesses of information systems leads to security breaches which can lead to financial fraud, damage to brand names, and loss of customer and partner confidence, and can cause the organization to go out of business.

New threats in information systems are a result of unexpected sources when an organization relies on it (Nyanchama, 2005). Threat is an indication of impending danger or harm (Johnson, 2008). According to Kumar, Park and Dubramanian (2008), a security threat is a condition of vulnerability that may lead to an information security being compromised. Currently, organizations that have information systems, websites, intranet, and internet are subjected to various security threats. Moreover, organizations are facing an increase in variety of security threats. As risks emerge, the need for organizational compliance in this field increases thus information systems security becomes more important to an organization's overall business approach (Alshboul, 2010)

2.2.1 Data Threats

Whitman and Mattord (2008) classify threats as accidental, deliberate acts, physical attacks, remote penetration attacks, human errors, technical control failures, operational issues, or social engineering wherein someone is tricked into revealing his/her username and password. According to Bowen et el (2006), environmental, natural, and human threats to public university data adversely impact public university's operations. Environmental threats include inadequate temperatures in public university's server rooms, fires, and power outages. Natural threats to public universities include floods, earthquakes, volcanic explosions, and wild fires (Myler & Broadbent, 2006). Environmental and natural threats also adversely impact the availability of public university data. Subsequently, security breaches results from lost, stolen, or compromised confidential data through unauthorized access to computerized data (Cassini et al., 2008). Human threats, however, whether accidental or intentional can directly compromise confidential data by facilitating unauthorized access to computerized data

2.2.2 Insider Threats

According to Information security breaches survey report (2013), an insider threat arises when a current or

former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data. Also, it is someone who has intentionally exceeded or used that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems. A threat can either be deliberate or come from negligent behavior attributed by lack of training and poor policies. Myler and Broadbent (2006) note that data at rest resides within file systems, databases, desktops, and groupware. Common risks associated with this type of data include lack of visibility into where sensitive data is stored, lack of understanding around who has access to sensitive data, and lack of secure storage for sensitive data to prevent theft and loss. Data at rest are even more at risk than e-mail messages in transit. Unencrypted data on servers and hard drives are at risk to unauthorized retrieval by employees and/or hackers (Comerford, 2006; Gupta & Sherman, 2012; Wiant, 2005). The weakest factor in protecting confidential and sensitive data from unauthorized disclosure is the insider who works for the public university as an employee (Bowen et al., 2006; D'Arcy & Hovav, 2009).

Another insider threat can originate within the IT Department. The sharing of one administrator username and password by the entire IT Department for accessing every network server is categorized as a high threat level practice (Humphreys, 2007). Wiant (2005) notes that an organization can enforce an audit trail using automated monitoring software in order to overcome the threat of sharing administrator username and password. However, when everyone shares the same administrative username and password, there is no audit trail to discover who made specific changes (Kent & Souppaya, 2006). Beside from the login username and password for logging into the network, each member of public university IT department should be assigned a unique username and password for the domain controller accounts (Kent & Souppaya, 2006). Use of the null default passwords poses a high threat level practice that can result in the compromise of confidentiality, integrity, and availability of the network should a disgruntled employee or other unauthorized users initiate changes to the network servers (Wiant, 2005). Thus, individual administrator passwords for each IT Department employee should be changed regularly as should public university's employee passwords.

2.3 Data Breach Incidents

Data security breaches involving personal and sensitive information have significantly grown over the last few years. Data security breaches according to (Gupta & Sherman, 2012) amounts to billions of dollars in the United States to detect and remediate consequences of security breaches which include identity theft frauds and lawsuits. On an estimate, an average company spends $2 million per data breach and therefore this warrants organizations, public universities and individuals to understand the risks and take measures to safeguard personal information.

A number of data breach incidents are not only affecting big firms, but such breaches are also experienced in small firms (Security breaches survey, 2013). On the other hand, public universities collects, uses, distributes, and disposes information which is impacted by identity theft risks associated with unsecured information on public university's computer equipment and networks.

3.0 Research Methodology

3.1 Research Design and Study Population

The study employed survey as its research design. The aim of a survey is to explore and to obtain information that describes existing phenomenon by asking individuals about their perceptions, attitudes and values (Mugenda & Mugenda, 2003). Survey research was used because it provides possible collection of vast amounts of information on a large number of people (Kothari, 2012) and also it gives accuracy within specified ranges of sampling error. The population for the survey consisted of 200 IT personnel from public universities in Kenya

3.2 Sample and Sampling Techniques

IT personnel from public universities in Kenya formed the sample size. Simple random sampling was used to identify 200 employees from public universities in Kenya to validate the hypotheses and to meet the objectives of the study.

3.3 Instruments of Data Collection

The study utilized a survey instrument to analyze responses from IT personnel in public universities in Kenya. Data was collected using a questionnaire because questionnaires were found to be appropriate as they allow much information to be gathered over a short period of time (Mugenda and Mugenda, 2003). Questionnaires with multi-choice questions, demographic questions, and likert-scale questions were utilized.

3.4 Methods of Data Analysis

Descriptive techniques were used to analyze qualitative data. Research hypotheses were tested using both 2 tailed t tests and ANOVA tests. Pearson correlation was conducted in order to test the relationship between

independent variables and dependent variable. Regression analysis was used to show the contribution of each independent variable to the dependent variable.

4. 0 Results and Discussions

The results in table 1 show that 24.4% of the respondents indicated that their university had weak network security policies. Moreover, 40 respondents perceived that their university had strong server security policies. This represented 19.9% of all the respondents.

Table 1 further indicates that 23.8% (48) of the study respondents perceived that their university had weak application policies. Application security policies had a mean of 3.05 and a standard deviation of 1.388. According to the results in table 1, majority of the respondents (23.9%) indicated that their universities had encountered strong information security breach incidences.

Table 1: Level of information security policies and security breach incidences

	Very Weak	Weak	Indifferent	Strong	Very strong	Mean	Std Deviation
Network security policies	40 19.9%	49 24.4%	41 20.4%	40 19.9%	30 15.4%	2.86	1.354
Server security policies	37 18.4%	45 22.4%	37 18.4%	42 21.3%	39 19.5%	3.01	1.402
Application security policies	39 19.5%	48 23.8%	33 16.4%	43 21.9%	37 18.4%	2.96	1.408
Security breach incidents	36 17.9%	44 21.9%	38 18.9%	47 23.9%	35 17.4%	3.01	1.373

According to the results in table 2, there is a negative and a statistically significant relationship between network security policies and security breach incidences as shown by the r value of -0.188 and a p value of 0.008 ($p<0.05$). Therefore, this study rejects the first null hypothesis and concludes that there is a statistical significant relationship between network security policies and security breach incidences. Furthermore, the computed r value on the relationship between server security policies and security breach incidences was -0.059 with a significance value of 0.406. This implies that there is a negative but not a statistically significant relationship between server security policies and security breach incidences in Kenyan public universities. As a result, this study fails to reject the second null hypothesis and concludes that there is no statistical significant relationship between server security policies and security breach incidences. The results in table 2 show that application security policies were negatively correlated with security breach incidences. Nonetheless, the relationship between the two variables was not statistically significant ($r=-0.119$, $p=0.093$). Consequently, this study fails to reject the third null hypothesis and concludes that there is no statistical significant relationship between application security policies and security breach incidences.

Table 2: Pearson Bivariate Correlation Analysis and Test of significance

		Network security policies	Server security policies	Application security policies	Security breach incidences
Network security policies	Pearson Correlation	1	.419**	.437**	-.188**
	Sig. (2-tailed)		.000	.000	.008
Server Security policies	Pearson Correlation		1	.245	-.059
	Sig. (2-tailed)			.000	.406
Application security policies	Pearson Correlation			1	-.119
	Sig. (2-tailed)				.093
Security breach incidences	Pearson Correlation				1
	N	200	200	200	200
**. Correlation is significant at the 0.01 level (2-tailed).					

According to the results in table 3, the correlation co-efficient (R) value was 0.194 with a significance value of 0.057. This means that there is a weak relationship between information security policies and security breach incidences ($r<0.5$). However, the relationship between the two variables was not statistically significant ($p>0.05$). As a result, this study fails to reject the fourth null hypothesis and concludes that there is no statistical significant relationship between information security policies and security breach incidences.

The results in table 3 indicate that information security policies explain only 3.7% of the observed security breach incidences as shown by the coefficient of determination (R^2) value of 0.043. The Durbin-Watson

measure of autocorrelation in this analysis was 1.827 and this signifies that there was no autocorrelation among the independent variables. This is due to the fact that it was within the acceptable levels of 1.5 to 2.5.

Table 3: Multiple Regression Analysis

R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
				R Square Change	F Change	df1	df2	Sig. F Change
.194[a]	.037	.023	1.017	.037	2.545	3	196	.057

a. Predictors: (Constant), Application security policies, Networks security policies, Server security policies
b. Dependent Variable: Security breach incidences

According to table 4, the overall significance of the model was 0.057 with an F value of 2.545. The level of significance was higher than 0.05 and this means that information security policies do not show a statistically significant relationship with security breach incidences.

Table 4: ANOVA[a] Test

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7.902	3	2.634	2.545	.057[b]
	Residual	202.853	196	1.035		
	Total	210.755	199			

a. Dependent Variable: Security breach incidences
b. Predictors: (Constant), Application security policies, Server security policies, Network security policies

The results in table 5 show that the computed significance values in relation to server security policies (p=1.316, p>0.05) and application security policies (p=2.473, p>0.05) did not statistically and significantly influence security breach incidences at 0.05 degree of significance. Nonetheless, network security policies were found to statistically and significantly influence security breach incidences.
The multi-collinearity tests results indicated that none of the Variance of inflation factor was around or equal to 5. This means that there was no multi-collinearity between the independent variables. This is further supported by the fact that the tolerance values were more than 0.2.

Table 5: Regression Co-efficient

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	4.395	.214		20.511	.000		
	Network security policies	-.135	.063	-.178	-2.135	.034	.706	1.417
	Server security policies	.020	.057	.027	.351	.726	.820	1.220
	Application security policies	-.035	.057	-.048	-.613	.541	.805	1.243
a. Dependent Variable: Security breach incidences								

5.0 Summary and Conclusions

The aim of the study was to investigate the impact of information security policies on security breach incidences in Kenyan public universities. The results of the study indicated that there is a negative relationship between network security policies and security breach incidences. This suggests that Kenyan universities can reduce the

impact of security breach incidences by strengthening their network security policies. Furthermore, server security policies were found to be negatively correlated with security breach incidences. This means that the extent of security breach incidences can be significantly reduced by formulating and implementing stronger server security policies. Moreover, the results from correlation analysis indicated that there is a negative relationship between application security policies and security breach incidences. This implies that the level of security breach incidences in Kenyan universities can be reduced by putting in place resilient application policies.

The results from the multiple regression analysis indicated that there is a weak relationship between information security policies and security breach incidences. This indicates that information security policies have a low impact in reducing security breach incidences. However, both the ANOVA test and the individual t tests indicated that the relationship was not statistically significant. Therefore, this study concludes that there is no statistical significant relationship between information security policies and security breach incidences in Kenyan public universities.

6.0 Recommendations for Further Studies

A comparative study should be undertaken in private universities in Kenya to determine whether the findings will be similar. Moreover, further studies should be done to determine the impact of information security policies on security breach incidences in public and private organizations in Kenya. In addition, more studies should also be conducted to determine the impact of IT staff qualifications on security breach incidences.

References

Alshboul, A. (2010) Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks. *Communications of the IBIMA,* 2010

Baker, W. H. & Wallace, L. (2007). Is information security under control? Investigating quality in information security management. *IEEE Security & Privacy*, 5, 36-44.

Basta, A. & Halton, W. (2008). Computer Security and Penetration Testing, Boston, M.A: Thomason Course Technology.

Bowen, P., Hash, J., & Wilson, M. (2006). Information security handbook: A guide for managers. NIST special publication 800-100. Retrieved April 10, 2014, from http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

Cassini, J. A., Medlin, B. D., & Romaniello, A. (2008). Law and regulations dealing with information security and privacy: An investigation study. *International Journal ofInformation Security and Privacy*, 2(2), 70-82.

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. Information Technology, Learning, and Performance Journal, 24(1), 1-14.

Comerford, J. D. (2006). Competent Computing: A lawyer's ethical duty to safeguard confidentiality. *The Georgetown Journal of Legal Ethics*, 19, 629-642.

D'arcy, J. & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics: Supplement*, 89, 59-71.

Da Veiga & Eloff, J. H. P. (2007). An Information Security Governance Framework. *Information Systems Management* 24(4); 361-372.

Dhillon, G. (2006). Principles of Information Systems Security: Texts and Cases (1st ed.), Honoken. NJ:Wiley.

Doherty, N. F. & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal,* 18, 21-39.

Doherty, N. F. & Fulford, H. (2006). Aligning the information security policy with strategic information systems plan. *Computer & Security*, 25, 55-63.

Greene, S.S., (2006). *Security Policies and Procedures: Principles and Practices*, Upper Saddle River, NJ: Pearson Education, Inc.

Gupta & Sherman (2012) Determinants of Data Breaches: A Categorization-Based Empirical Investigation, *Journal of Applied Security Research*, 7, 375-395.

Hagen, J. M., Albrechten, E. & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Information Management & Computer Security, 16, 377-397.

Humphreys, E. (2007). *Implementing the ISO/IEC 27001: Information Security Management System* Standard, Boston, M.A: Artech House

Information security breaches survey (2013) Retrieved March 18, 2014, from http://www.nlondon.bcs.org/pres/cpapr13.pdf

Ismail, Z., et al. (2011). A Framework for the Governance of Information Security for Malaysian Academic Environment, *Journal of Information Assurance & Cybersecurity*.

Johnson, A.C. and Warkentin, M. (2008). Information privacy compliance in the healthcare industry.

Information Management & Computer Security, 16(1), 5-19.
Johnson, M. E. (2008). Information risk of inadvertent disclosure: An Analysis of File Richardson, R. CSI Computer Crime & Security Survey. Computer Security Institute.
Kent, K. & Souppaya, M. (2006). Guide to computer security log management. NIST Special Publication 800-92. Retrieved March 18, 2004, from http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
Kothari, C.R., (2012), *Research Methodology: Methods and Techniques*, 2nd Edition, New AGE International Publishers, New Delhi, India
Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, 38(2), 143-154.
Kumar, R. L., Park, S. and Subramaniam, C. (2008). Understanding the value of countermeasures portfolios in information systems security. *Journal on Management Information Systems*, 25, 243-279.
Laudon, K.C. & Laudon, J. P. (2012). Essentials of Management Information Systems, 10th International Edition, Prentice Hall
Lin, P.P. (2006). System security threats and controls. *The CPA Journal*, 76(7), 58-66.
Liska, A.(2008). The Practice of Network Security: Deployment Strategies for Production Environment. New Jersey, Prentice Hall Publishing.
Metzler, M. (2007). Promoting security policy longevity. *Computer Security Journal. XXIII*, (2/3), 82-94.
Mugenda, O. & Mugenda, A.. (2003). *Research Method, Quantitative and Qualitative Approaches.* African Centre of Technology (A.C.T.).
Myler, E. & Broadbent, G. (2006). ISO 17799; Standard for secutity. The Information Management Journal, 40(6), 43-52.
Nyanchama, M. (2005). Enterprise vulnerability management and its role in information security management. Information Systems Security, 14, 29-56.
Post, G.V. & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access an interfere with user tasks. *Computer & Security*, 26(3), 229-237.
Ramim, M. & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. *Journal of Cases on Information Technology*, 8(4), 24-34.
Robinson, T. (2005). Data security in the age of compliance. *networker*, 9(3), 24-30.
Rotvold, G. (2008). How to create a security culture in your organization. *Information Management Journal*, 42(6), 32-34, 36-38.
Salmela, H. (2008). Analysing business losses caused by information systems risk: A business process analysis approach. Journal of Information Technology, 23(3), 185-202.
Salmela, H. (2008). Analysing business losses caused by information systems risk: A business process analysis approach. *Journal of Information Technology*, 23(3), 185-202.
Schwartz, P. M. & Janger, E. J. (2007). Notification of data security breaches. *Michigan Law Review*, 105(5), 913-984.
Tipton, H., & Krause, M.(2008). Information Security Management handbook. Berlin, CRC Press.
Verdon, D. (2006). Security Policies and the software developer. *IEEE Security & Privacy*, 4(4), 42-49.
Weaver, R. (2007). Guide to Network Defense and Countermeasures Second Edition. Boston, MA: Thomson Course Technology.
Whitman, M.E. & Mattord, H.J. (2008). Management of Information Security Second Edition. Boston, MA: Thomson Course Technology.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar