https://doi.org/10.48009/1_iis_2011_246-255

Issues in Information Systems

Volume XII, No. 1, pp. 246-255, 2011

INFORMATION SECURITY EFFECTIVENESS: A RESEARCH FRAMEWORK

Sushma Mishra, Robert Morris University, mishra@rmu.edu
Lewis Chasalow, The University of Findlay, chasalow@findlay.edu

ABSTRACT

Information security has taken on increasing importance as the size and complexity of IT issues continues to grow. Research literature in information security suggests that clarity in policies, systems auditing and clear deterrence practices enhance organizational information security effectiveness. In this paper we analyze research framework defining how the three constructs: security policies, deterrence practices and systems auditing impact information security effectiveness. A survey was conducted to collect data, the results of which suggest that there is a significant relationship between security policies and systems audit with security effectiveness.

Keywords: Information security, systems audit, deterrence, policy, regression, survey

INTRODUCTION

An organization has to adequately protect its data from being compromised as the consequences possible security breaches could be significant for the reputation of the company. For businesses, a breach usually entails huge financial penalties, expensive law suits, loss of reputation and business [13]. Recently, TJX clothing company had a security breach in 2007, where over 45 million credit cards and 500,000 records containing customer details (including social security number and driver license details) were compromised. The apparent reason for the compromise was inadequate wireless network protection. The financial cost of the breach was estimated to run over $1 billon [13]. With health care organizations turning to electronic medical records systems, health records have become more vulnerable to being compromised. In another incident, security breaches of personal health data was reported in October 2010, when a computer flash drive containing names and addresses and personal health information of 280,000 people went missing [30]. The breach involved records of Medicaid recipients, nearly two-thirds of the insurers' subscribers, and was the first such Medicaid data breach in Pennsylvania since 1997. The two affiliated Philadelphia companies, Keystone Mercy Health Plan and AmeriHealth Mercy Health Plan issued a public statement expressing regret for the unfortunate incident. The cause of the breach; a hard drive containing crucial information was missing from the corporate headquarters and was apparently used at a local community health fair. The fact that a drive with such a sensitive data would be used at a health fair stresses the careless and irresponsible attitude of the healthcare organizations regarding storing such data. The news of the breach comes at a time when there is more emphasis - and billions of dollars in federal funding - to develop protocols for electronic medical records, with information being shared among providers, insurers, and consumers [30]. Such frequent reports of security and privacy breaches suggest lack of widely accepted security frameworks and weak governance efforts from organizations dealing with sensitive data.

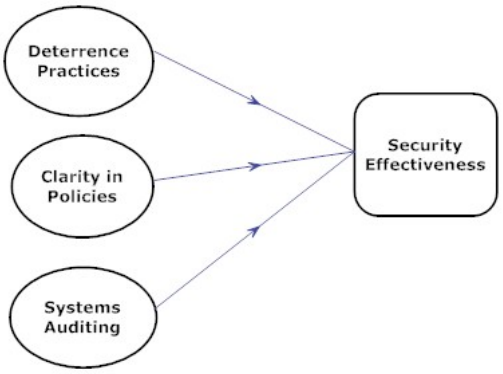
This study is primarily undertaken to understand the impact of security audits, security policies and deterrence activities in organizations on overall security effectiveness in an organization.

The research questions are:
R1: How do deterrence practices impact overall security effectiveness of an organization?

R2: How does clarity in security polices impact overall security effectiveness of an organization?

R3: How does system auditing impact overall security effectiveness of an organization?

Based on research literature in information security, we propose a security effectiveness framework and hypothesize the relationships between the constructs:



Model 1: Security Effectiveness in Organizations

In the following section, the background for the proposed model is discussed and relationship is hypothesized.

LITERATURE REVIEW

The proposed research model (see model 1) has four constructs: security effectiveness (dependent variable), Systems auditing, clarity in security policies and deterrence activities for security (independent variable). The background and justification for each construct is discussed below and the relationship is hypothesized.

Security effectiveness

Information security effectiveness can be seriously questioned as we see high volume of security breach incidents happening often resulting in considerable financial losses. The effectiveness of security measures in reducing the overall risk to information in organizations had been studied extensively over the years. Straub (1990) defined IS security effectiveness as the ability of IS security measures to protect against "the unauthorized and deliberate misuse of assets of the local organizational information system by individuals, including violations against hardware, programs, data, and computer service" (p. 4). D'Arcy and Hovav (2009) indicated that understanding the factors affecting the effectiveness of security countermeasures has been a consistent theme in the literature. Dhillon and Backhouse (2001) called for more empirical research to develop key principles for effective security management. Dhillon and Torkzedeh (2006) identify security policies as a fundamental objective for enhancing information security and deterrence as a means objective for improving effectiveness of security management.

Kankanhalli et al (2003) developed and tested an integrative model of IS security effectiveness. The model comprised constructs such as top management support, greater deterrent efforts and preventive measures as independent variables leading to enhanced security effectiveness, the dependent variable. Chang and Lin (2007) found organizational culture and management support have a positive impact on security effectiveness in a study of IT managers from various industries. The measure of effectiveness in this study was increasing confidentiality, integrity and availability. Though this measure of effectiveness could be argued to be myopic or incomplete at best, the study definitely establishes a relationship between culture, management support and effectiveness. Brady (2011) proposed a theoretical model using management support, security awareness, security culture, and computer self-efficacy to predict security behavior and security effectiveness. The results demonstrated that security awareness, management support, and security culture were significant predictors of security effectiveness and security behavior, with security awareness being the most significant predictor.
To assess security effectiveness, we developed items that capture information about major accomplishments of the security program in organizations. An effective security program would reduce risks, protect IT infrastructure from vulnerabilities, would achieve what it is intended to do and institute the right controls to prevent security breaches. Our items captured all respondents' perceptions about security effectiveness in their organizations.

Deterrence Practices

Deterrent activities are organizational attempts to discourage people from not following rules through the fear of sanctions [12]. Research in this area suggests two characteristics of sanctions that can contribute to the effectiveness of deterrent measures are: certainly of sanctions and severity of sanctions [4]. It is possible that lack of deterrent efforts may lead to people misunderstanding what is acceptable information system use hence resulting information systems abuse [18]. In a survey of 1,211 organizations, Straub (1990) found that deterrent efforts resulted in fewer IS abuses. Kankhalli et al (2003) in a study found that greater deterrent efforts appear to contribute to better IS security effectiveness but deterrent severity, punishments and sanctions, did not affect IS security effectiveness.

Deterrence criteria for security have been emphasized in information systems security research. Dhillon and Torkzadeh (2006) argue for developing deterrence criteria for better security. Straub and Welke (1998) have used the general deterrence theory from criminology, which suggests sanctions to prevent people from committing crimes. The theory suggests that it is prudent to maximize prevention and deterrence and thus minimize abuse. There has not been much work about deterrence criteria in security governance research. Most of the leading standards for security governance such as CobiT or ISO 27000 do not mention deterrence as an objective. Research models in security governance also do not emphasize deterrence activities as an important objective for governance.

To measure our deterrence construct, the items were developed to estimate if employees understand acceptable security actions and behavior in organization. Establishing sound deterrence criteria entails that employees clearly understand the consequences of their actions and results of non-compliance with rules. Employees need to be educated about acceptable security behavior and there should be well established consequences for violation of any policy. It is important that these consequences are communicated to the employees.

Clarity in policies

Security policies, procedures and guidelines are paramount in the implementation of information security governance as they provide direction and support to the organization [16, 17]. Management should have clarity in security policies and procedures to make the implementation of the controls more effective and to get the intended results from the governance process. Clarity in policies and procedures is essential to ensure the proper use of the applications and technological solutions instituted in an organization. Controls should be reflected in the policy document and implemented through procedures.

There is a heavy emphasis on developing clear policies for effective information systems security governance [27, 29]. Ward and Smith (2002) argue that IT security policies also provide the basis for displaying the executive management's commitment to IT security. Moultan and Cole (2003) suggest that policies should be developed in a way that should facilitate the development of the relevant controls for security. In their proposed security governance framework, Moultan and Cole (2003) have identified "policies and procedures" as a security governance objective. Even though there is significant amount of work establishing security policies as a required condition for a good security program, there is not enough work that establishes a relationship between clear security polices and security effectiveness. Even though intuitively this relationship seems logical, there is lack of empirical studies that evaluate this relationship. This study is addressing this gap by proposing a relationship between clear security policies and security effectiveness.

To measure the clarity in security polices construct, items were developed assess if the existent security policies were apprehensible and useable for the employees. Developing clarity in security policies requires that an effective security policy document exists and employees are aware of these policies. It also requires that employees are required to periodically review the policies and are able to understand it. Security policy documents need to be easily accessible and guide employee actions regarding safeguarding information.

Systems auditing

Auditing is an important functionality which provides assurance for risk management, controls and governance structures [14]. Organizations may regard strategy, people, assets and finance as pivotal but equally important are routine day-to-day aspects of an organization including the mechanics of the IT system. It is important to audit the security posture of the systems periodically, either manually or automatically [21]. Auditing is essential component to maintain the security of deployed systems. Systems need to be periodically audited to prevent configurations drifting over time due to entropy or modifications that unknowingly or maliciously change the desired security posture. Such changes could go undetected if corrective measures are not taken [21] resulting in systems that are less secure and more vulnerable.

Thus auditing becomes crucial to provide a reasonable assessment of risks of day-to day jobs in IT and suggest improvements for better security of information systems. It is vital for management to consult experts proactively for them to advise on IT security. Auditing ensures segregation of duties and points out anomalies in normal business transactions. Lack of segregation of roles and auditing of the suspense account were the major cause of the failure of Barings Bank [10]. This is essentially an example of security governance loopholes. Internal auditors are responsible for pointing out management deficiencies negatively impacting the strength of an organization's internal controls [1]. The greatest benefit of the audit function is its unbiased assessment of management adequacy. A strong, independent audit committee can be critically useful in ensuring high quality of reporting and controls and the proper identification and management of risk [31]. There have been several calls in information security research about importance of auditing functionality for security but there are hardly any studies that have studied the relationship between systems auditing and security effectiveness. This study addresses this gap by proposing a positive impact of systems audit on information security effectiveness.

To measure the construct systems auditing, items were developed to assess the frequency and perception of systems auditing in organizations. Systems auditing could have a positive impact on information security effectiveness of an organization if it is performed periodically and considered as a complementary tool that helps finds gaps in the security program and improves it. Auditing should be perceived as an activity that improves security controls and management by identifying issues in the existing plan. The notion of having frequent audits could prevent employees from circumventing security controls. Our survey captured these notions of systems auditing.

Based on the understanding of the research literature and the constructs, following relationships are hypothesized:

H_1: Effective deterrence practices are positively related with effectiveness of security program.

H_2: Clarity in security policies is positively related with effectiveness of security program.

H3: Systems auditing is positively related with effectiveness of security program.

RESEARCH METHODOLOGY

Data Collection

The population to be studied is all employees working with information systems as part of their jobs. For this study we had students enrolled in master's degree programs who are currently employed full time fill out the survey instrument. The sample frame consisted of approximately 120 individuals working is a variety of industries. Out of the surveys sent 54 valid and complete responses were received.

The survey consisted of Likert scaled responses of five or six items per measure. Deterrence, Security Auditing, and Security Effectiveness were each measured using a five item instrument, while Security Policy had a six item instrument. Data was collected using an online survey with IP address screening to limit responses to one per person.

The respondents come from a variety of industries and different sized companies. All of the respondents had at least a bachelor's degree and 40% had a master's degree. The majority of respondents worked for larger organizations, as illustrated below (figure 1):

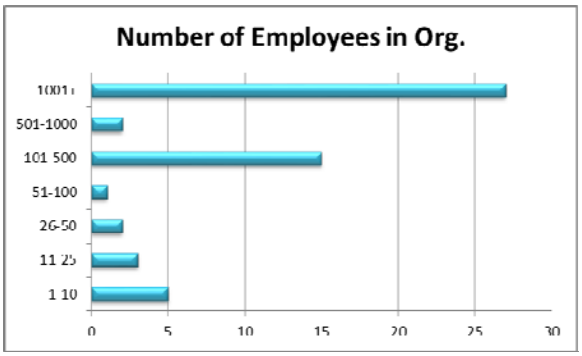


Figure 1: Respondent profile-size of organization

The most frequently mentioned industry in which they worked was financial services at 20%, but nearly 15% worked in the computer industry in some capacity (see figure 2).

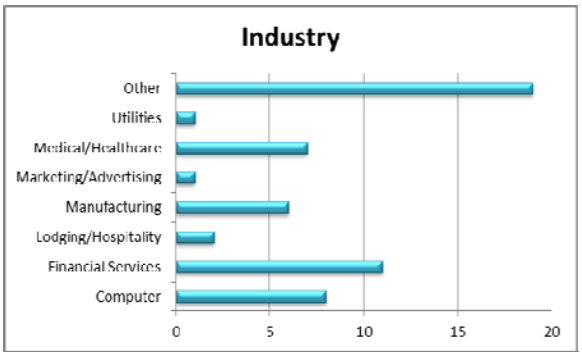


Figure 2: Respondent profile-industry

While the respondents worked in a variety of roles, the majority worked in professional or administrative staff functions (see figure 3 below).

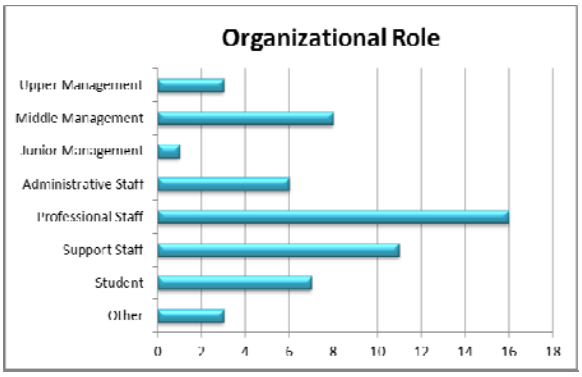


Figure 3: Respondent profile-Roles

While not all of the respondents worked in IT, more than half had more than 2 years of experience working with IT in industry (see figure 4).

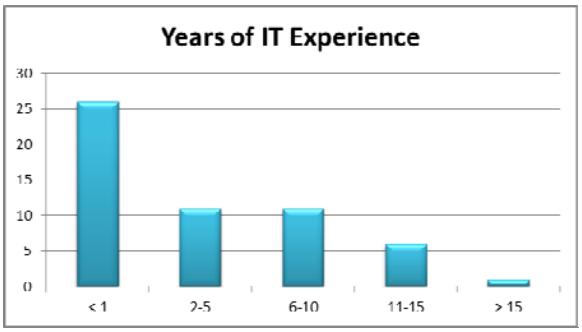


Figure 4: Respondent profile-Experience

Data Analysis

The first step in the analysis was to test the validity of each instrument. Cronbach's alpha was calculated for each item to determine internal consistency. The calculated alpha for each measure were all greater than 0.70m which indicates good reliability in the instruments as illustrated in the table 1 below:

Table 1: Reliability measure

Variable	**Cronbach's Alpha**	**N**
Deterrence	.763	5
Security Policy	.917	6
Security Audits	.865	5
Security Effectiveness	.822	5

All of these indicate good validity of the instruments, but we found that for the effectiveness construct removing one of the questions improved the alpha from .822 to .882. The model was therefore tested using the 4 item scale for security effectiveness.

Our model assumes a direct relationship between each of the independent variables and security effectiveness. This was tested using multiple linear regression. The overall result of the regression using Security Effectiveness as the dependent variable and Deterrence, Security Policy, and Security Audits as the independent variables was significant at the .01 level as shown by the model ANOVA below (table 2):

Table 2: ANOVA of the Regression model w/ deterrence

Model	*Sum of Squares*	*Df*	*Mean Square*	*F*	*Sig*
Regression	*19.309*	*3*	*6.436*	*35.915*	*.000*[a]
Residual	*8.961*	*50*	*.179*		
Total	*28.270*	*53*			

a. Predictors: (Constant), Audits, Policy, Deterrence
b. Dependent Variable: Effectiveness

The R-squared for this model came to 0.683 indicating that nearly 70% of the variation in security effectiveness in our sample could be explained by the variables in the model. However, when looking at the individual coefficients, we found that deterrence was not statistically significant as shown below (table 3):

Table 3: Regression coefficients for model w/ deterrence

Model	*Unstandardized Coefficients*		*t*	*Sig.*
	B	*Std. Error*		
1 (Constant)	*.688*	*.346*	*1.987*	*.052*
Deterrence	*.191*	*.141*	*1.348*	*.184*
Policy	*.254*	*.101*	*2.522*	*.015*
Audit	*.406*	*.110*	*3.700*	*.001*

As a result we re-ran the analysis removing deterrence and found the following results (see tables 4 & 5 below).

Table 4: ANOVA of the Regression w/out deterrence

Model	*Sum of Squares*	*df*	*Mean Square*	*F*	*Sig*
1 Regression	18.983	2	9.492	52.128	.000[a]
Residual	9.286	51	.182		
Total	28.270	53			

a. Predictors: (Constant), Audits, Policy
b. Dependent Variable: Effectiveness

Table 5: Regression coefficients for model w/out deterrence

Model	*Unstandardized Coefficients*		*t*	*Sig.*
	B	*Std. Error*		
1 (Constant)	.932	.298	3.130	.003
Policy	.324	.087	3.717	.001
Audit	.477	.097	4.922	.000

a. Dependent Variable: Effectiveness

The R-squared for this model was 0.672, indicating that the final model still has a very strong effect size. However, it does appear that there is some relationship between the factors used for the deterrence construct and those for the auditing construct. In order to study this further we tested for a mediator or moderator effect between deterrence and auditing using the method suggested by Baron and Kenny (1986). These tests did not indicate a mediation or moderation relationship between deterrence and auditing. However another possible explanation for the effect of deterrence and audit in the model is that they are in fact measuring the same concept. If this were the case one would expect there to be multicollinearity in the model when all variables were included [22]. There are several tests for multicollinearity, the most common being the VIF or its inverse tolerance. However, the VIF for these variables when included in the model came to 2.3 for auditing and 2.8 for deterrence, both less than the normal rule of thumb for significance of 10, but due to the sample size they may be large enough to indicate some issue [24].

Another way to deal with this would be to incorporate a single variable that combined deterrence and auditing into a single variable. When this is done the resulting model has an R-squared of 0.677 with all of the variables being significant, which is slightly larger than the .672 from the model with the pure audit factor included. However, a

more parsimonious model being more desirable [23], we suggest that this combined variable does not add enough explanatory value to be worth including in the model.

DISCUSSION

We hypothesized that effective deterrence, clear security policies, and systems audits together would improve information systems security. While we found that each has a significant relationship with security effectiveness on their own, when taken together the impact of deterrence factors appears to not be significant (see table 6 above). In looking at the specific questions used to model deterrence and auditing it seems clear that there is a relationship between these two constructs. Systems audits are performed to verify that systems processes and outcomes are operating effectively and that the data being generated and stored are accurate and complete. If individuals in the organization are aware that data in key systems will be regularly audited it can have a deterrent effect in addition to auditing's role as a detective control [33]. We believe that it is this mechanism that is at work in our data. It seems clear that knowledge that systems audits are being performed and that they are effective has a deterrent effect that confounds the data with pure deterrence factors.

Table 6: Results

Model	*Decision*
H_1: Effective deterrence practices are positively related with effectiveness of security program.	*Not supported as indicated by an insignificant t test on the regression coefficient*
H_2: Clarity in security policies is positively related with effectiveness of security program.	*Supported at 99.9% on the coefficient t test*
H3: Systems auditing is positively related with effectiveness of security program	*Supported at greater than 99.9% on the coefficient t test*
Overall Model	*Significant at the 99.9% level as indicated by the model F test*

Our findings are consistent with research literature in information systems security. Straub 1990 suggest deterrent activities comprise security briefings on the consequences of illegitimate uses and audits on the use of IS assets. The author considers auditing as a deterrent activity and not a separate factor that influences security effectiveness. This explains the complex relationship between two of our constructs: systems auditing and deterrence activities. Auditing could very well be used as a strategy to prevent fraud and vulnerabilities rather than just detect these loopholes [33]. Frequent audits could result in deterring employees from performing unacceptable actions, as the probability of their getting caught increases. Kanlhalli (2003) concluded that even though greater deterrent activities enhance effectiveness but there seems to be no relationship between severity of deterrence activities and effectiveness. The authors conclude that in the context of IS security, organizations should focus their attention on deterrent and preventive efforts rather than deterrent severity. The construct clarity in policies, according to our data, has a significant impact on security effectiveness of an organization. Eloff and Eloff (2005) place policies as a first priority for an effective governance program. In their proposed security management model, McCarthy and Campbell (2001) identify policies, procedures, documented guidelines and standards as crucial components for proper implementation of security controls. Our results make logical sense and have support from extant research literature in this domain. While the original model as proposed was not shown to be fully accurate, we believe that the elements in the model all do have an impact on increasing the effectiveness of information security outcomes.

CONTRIBUTION AND LIMITATIONS

We have developed a model that identifies the relationship between clear security policies, security auditing practices and security effectiveness. This model suggests that a significant portion of the variation in security effectiveness can be attributed to these two factors. We have also examined the impact of deterrence practices on security effectiveness, and while when taken on their own there is a relationship between such practices and security effectiveness, there appears to be a relationship between the audit practices and security policies as we have defined them that would appear to make them have a similar impact. This model provides strong support for the concepts that having security audits and deterrence processes along with a current, communicated, and complete security policy leads to higher levels of security effectiveness.

This study contributes in several ways. Theoretically, this model is studying the impact of systems auditing and clarity of security policies on security effectiveness. There are few, if any, studies that have investigated these relationships. This study forms a basis for further understanding the complex relationship between the above constructs. The relationship between clear information security polices and effectiveness, even though discussed extensively in literature, can be termed anecdotal at best. This study suggests an empirical relationship between clear security polices and security effectiveness. For practitioners, an understating of relationships between auditing and deterrence activities could lead to potentially strong security programs. Systems auditing should be perceived as a tool to improve security and this knowledge can help business managers assess and design their security posture more effectively. Our study is not without limitations. While our sample size of 54 is large enough to support the analysis that was done [28], it is still relatively small relative to the population and may impact the precision of our results. We plan to refine the instrument based on this information and collect further data to evaluate the proposed model. In particular the instrument for deterrence and security audits needs further refinement to isolate its most significant components.

CONCLUSION AND FUTURE RESEARCH

We started out looking to validate the factors that increase the effectiveness of information security outcomes. We have verified the often repeated contention that effective security policies lead to improved security outcomes. In addition we have found that systems auditing also has a strong relationship with effective information security. An interesting finding in our results is the relationship between deterrence and auditing.

While knowledge that systems audits are taking place seems like a reasonable deterrent factor, this relationship requires further study. We plan to investigate the detailed elements of deterrence and auditing to attempt to develop a richer understanding of the mechanisms by which they interact and impact information systems security effectiveness. This study was done on a relatively small sample of data. In order to improve the precision of our estimate and to refine and validate this model we plan to expand our data collection to encompass a broader cross section of geography and in particular security experiences.

REFERENCES

1. Banks, D.G. "The fight against fraud," The Internal Auditor (61:2) 2004, pp 34-39.
2. Baron, R.M., and Kenny, D.A. "The Moderator-Mediator Variable Distinction in Social Psychological Research," *Journal of Personality and Social Psychology* (51:6) 1986, pp 1173-1182.
3. Brady, J. W. (2011) Securing Health Care: Assessing Factors that Affect HIPAA Security Compliance in Academic Medical Centers, In Proceedings of 44th Hawaii International Conference on System Sciences, January 04-07, Kauai, Hawaii USA
4. Blumstein, A. "Introduction," in *Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates*, Blumstein, A., Cohen, J. and Nagin D. (eds.), National Academy of Sciences: Washington, DC, 1978.
5. Chang, S. E., and C. Lin, "Exploring Organizational Culture for Information Security Management", Industrial Management + Data Systems, 107(3), 2007, pp. 438-458.
6. COBiT (2007) Information Systems Audit and Control Association

7. D'Arcy, J. and A. Hovav, "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures", Journal of Business Ethics, 89, 2009, pp. 59-71.
8. Dhillon, G. and Backhouse, J. (2000). Information system security management in the new millennium, Communications of the ACM , 43(7):125-128
9. Dhillon, G., and Torkzadeh, G. "Value-focused Assessment of information systems security in organizations," Information Systems Journal (16:3) 2006, pp 293-314.
10. Drummond, H. "Did Nick Leeson have an accomplice? The role of information technology in the collapse of Barings Bank," Journal of Information Technology (18) 2003, pp 93-101
11. Eloff, J., and Eloff, M. "Integrated Information Security Architecture " Computer Fraud and Security (11) 2005, pp 10-16.
12. Forcht, K.A. *Computer Security Management*, Boyd and Fraser: Danvers, MA, 1994.
13. Gaudin, S. (2007) T.J. Maxx Security Breach Costs Soar To 10 Times Earlier Estimate, InformationWeek, August 15, retrieved on 05/13/11 http://www.informationweek.com/news/201800259
14. Institute of Internal Auditors, 2011 retrieved on 04/18/11 www.theiia.org
15. ISO "ISO/IEC 17799:2005," International Organization for Standardization 2005
16. ISO 27000, 2011 Retrieved on 04/18/11 http://www.27000.org/
17. Kankanhallia, A., Teo, H., Tan, B., and Wei, K. "An Integrative Study of Information Systems Security Effectiveness," International Journal of Information Management (23) 2003, pp 139-154.
18. Klete, H. "Some Minimum Requirements for Legal Sanctioning Systems Special Emphasis on Detection," in *Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates*, Blumstein, A., Cohen, J. and Nagin, D. (eds.),National Academy of Sciences: Washington, DC, 1978.
19. McCarthy, M., and Campbell, S. *Security Transformation* McGraw-Hill, New York, 2001
20. Moulton, R., and Coles, R. "Applying Information Security Governance," Computers & Security (22:7) 2003, pp 580-584.
21. Noordergraaf, A. and Brunette, G. (2003) Auditing System Security, Sun BluePrints™ OnLine—May 200, Retrieved on 05/13/11 http://www.sun.com/blueprints/0503/817-2881.pdf
22. Pedhazur, E.J., and Schmelkin, L.P. *Measurement, Design, and Analysis: An Integrated Approach* Lawrence Erlbaum Associates, Hillsdale, NJ, 1992.
23. Petter, S., Straub, D., and Rai, A. "SPECIFYING FORMATIVE CONSTRUCTS IN INFORMATION SYSTEMS RESEARCH," *MIS Quarterly* (31:4) 2007, pp 623-656.
24. Sekaran, U., and Bougie, R. *Research Methods for Business*, (5th ed.) John Wiley & Sons, Ltd., Chichester, U.K., 2009.
25. Straub, D. (1990). "Coping with systems risk: security planning models for management decision making.," MIS Quarterly (22:8), pp 441-465.
26. Straub, D.W. and Welke, R.J. "Coping with Systems Risk: Security Planning Models for Management Decision Making," MIS Quarterly (22:4), 1998, pp. 441-469.
27. Swanson, M. and Guttman, B. (1996) "Generally Accepted Principles for Securing Information Technology Systems," National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 1996
28. Tabachnick, B.G., and Fidell, L.S. *Using Multivariate Statistics*, (5th ed.) Allyn & Bacon, 2006.
29. Von Solms, B. "Information Security–A Multidimensional Discipline " Computers & Security (20) 2001, pp 504-508.
30. Von Bergen, J. (2010). Medical-data breach said to be major, October 21, 2010 on Philly.com, retrieved on 02/05/2011 : http://www.philly.com/philly/business/20101021_Medical-data_breach_said_to_be_major.html?page=2&c=y#ixzz1ClrDbbeR
Watch sports videos you won't find anywhere else
31. Wagner, J.K. "Leading the Way," The Internal Auditor (57:4) 2000, pp 34-39.
32. Ward, P., and Smith, C. "The Development of Access Control Policies for Information Technology Systems," Computers & Security (21:4) 2002, pp 356-371
33. Wells, J.T. "New Approaches to Fraud Deterrence," Journal of Accountancy (197:2) 2004, pp 72-76.