SENRA Academic Publishers, British Columbia
Vol. 8, No. 3, pp. 3125-3129, October 2014
Online ISSN: 1920-3853; Print ISSN: 1715-9997

Canadian Journal of pure&applied sciences

EFFECTIVENESS OF DETECTIVE AND PREVENTATIVE INFORMATION SECURITY CONTROLS IN INFORMATION SYSTEMS ORGANIZATIONS

Muhammad Asif Khan
College of Computer Science and Engineering, Taibah University
Madina al Munawwara, Saudi Arabia

ABSTRACT

Information Systems (IS) organizations are experiencing a mounting pressure to contribute organizational success and to secure information asset, therefore, protection of information assets has become a paramount concern in IS organizations. IS organizations are more active in implementing technology and know the significance of IS audit and security controls in order to eliminate the risks for their IS asset and infrastructure. The aim of this paper is to analyze and demonstrate the effectiveness of network security controls in IS organizations that are implemented to ensure security and integrity of information assets. Also, the study evaluates the level of implementation of the detective and preventative security controls in organizations. In the present study we have collected data through survey from different organizations in Saudi Arabia. The purpose is to compare between the approaches for IS audit being used by these organizations and the industry standards of IS audit and controls set by organizations.

Keywords: Information systems organizations, security controls, audit and controls, information systems security controls.

INTRODUCTION

Organizations are becoming more dependent on information systems to provide fast, better and reliable services to their customers and to facilitate decision making and business strategy within the organizations. This trend is increased in the businesses with the advent of internet and electronic business and has grown IS security issue as a prime concern for organizations. Our business institutions are worldwide connected and rely on automated control systems (Warkentin and Willison, 2009). IS security is a process that protects information and maintains its integrity; however, it has not been a serious concern for the top management comparing to other IS issues (Brancheau *et al*., 1996). Most of the organizations do not provide IT security training to their employees and less than 50% of 459 CIOs and IT directors have said that they had IT security knowledge and training programs for their employees (Verton, 2002). For effective corporate governance a proper system of internal controls is essential and it is important to make sure the integrity of financial systems of organization remains intact without compromising and internal control is in place.

In organizations, there are external and internal security functions. External security functions consist of employees, administrative and physical while software and hardware are employed as internal security functions.

Corresponding author email: asifkhan2k@yahoo.com

It is reported that personnel in organizations cause key problem in information security (Puhakainen, 2006). Employees do not implement security controls seriously and poor compliance of security policies cause security breaches (Santon *et al*., 2005; Myyry *et al*., 2009). Deterrent measures attempt to deter people from using IS assets illegally. The deterrent measures can be policy statements or guidelines of using IS assets of an organization. Deterrent measures have been useful in keeping away people from unauthorized use of IS assets but a new theoretical model based on neutralization theory has been introduced (Siponen and Vance, 2010) that highlights neutralization as an important factor in order to implement and develop organizational security policies.

Preventive measures become effective when people do not pay attention to the deterrent measures and these measures are implemented by controls. Various security software are implemented in organizations to prevent unauthorized access to the IS assets. The security software provides different levels of access controls to IS assets (Weber, 1998). At basic level security software set in operating systems can enforce access to user account or any specific files. Security software in a middle level is set in database systems in order to access control of any particular records in a database. However, security software at an advanced level provides access control through high transaction means integrating audit and extensive security breach reports.

In organizations IS assets such as hardware, software, people and data are at risk of abuse by hackers through searching and exploiting vulnerabilities (Sun and Srivastava, 2006). Usually information is at risk during transmission over internet or information being stored in database of organization or information being stored in customers' computer. In financial institutions IS plays a strategic and significant role as compare to different business organizations. Therefore, financial institutions devote extra resources in IS in order to obtain more benefits than other organizations. Many companies face information security problems because senior management does not have a commitment and responsibility towards information security. Usually at management level absence of support from management is not considered in security rather information security is deemed a technical problem. Information security managers always find difficulties in implementing information security plans that take into account all security dimensions including human dimension, awareness dimension, policy dimension, measuring and monitoring dimension etc (Solms, 2001).

An effectiveness of information security depends on some organizational factors such as type of business, management interest and size of organization. To develop an effectiveness of information security, detective and preventive measures are taken into account. Organizations implement preventive security software that is assessed in terms of their sophistication.

There is no independent body that could conduct a systematic testing for the effectiveness of information security controls and usually the results of effectiveness testing carried out by vendors are never published. In a study Khan and Turki (2008) effectiveness of IS audit and control has been presented and an analysis of the effectiveness and efficiency of IS audit in reducing risks, vulnerabilities and security issues that are found within IS organizations is presented.

MATERIALS AND METHODS

In the present study we used a research survey instrument to collect data from various small to large organizations. We mailed out the survey instrument to 93 IS managers associated with small to large professional organizations. We followed up the survey by sending emails and phone calls whenever necessary. Out of 93 IS managers, 41 complete surveys were received and have been used for this study.

In the survey instrument we grouped questions in four categories in order to measure the IS security effectiveness in the organizations i.e. implementation of detective security controls, implementation of preventative security controls, management interest and open ended questions for respondents. We delivered the pilot questionnaires to few organizations in order to get the feedback. Based on the feedback we altered some questions, their wording and order before finalizing the survey instrument for the study.

To assess the implementation of detective security controls i.e. firewalls, intrusion detection system (IDS), encryption, check sums, logs/audit trails, capacity management, performance monitoring and anti-virus procedures, we formed questions to finding out any breach or abuse of IS security and the severity of actions taken by the organization: no abuse – no action - 0, little abuse – warning – 1, serious abuse – strict action – 2, destructive abuse – prosecution – 3. The detective efforts were measured using total man-hours expended on IS security purposes per week (Straub and Welke, 1998).

To evaluate the preventative security controls i.e. policies and procedures, honey pots, configuration management, incident handling, review of audit trails/logs, encryption and performance monitoring, we formulated questions to finding out the software for security used in the organization: software for security built in operating systems – 1, software for security built in databases – 2, software for security (special) – 3. The preventative efforts were measured using the level of sophistication of security software used in the organization.

We determined the size of an organization using the number of employees in the organization. We collected the nominal and ordinal data for this study. We used questions to find out involvement of top management in decisions with regard to security and security related activities. The questions have been helpful to know management's pro-active support for security functions within organizations. We asked these questions on Likert's scale i.e. from Strongly Agree - 5, Agree - 4, Neutral - 3, Disagree - 2 and Strongly Disagree - 1.

Perceptual responses from the respondents to six questions were used to measure the IS security effectiveness. The six questions were based on: preventative effect, detective effect, effect in hardware protection, effect in software protection, effect in data protection and effect in computer services protection. All questions were anchored on a Likert's scale i.e. from 'Maximum' (5), 'High' (4), 'Medium' (3), 'Low' (2) and 'Minimum' (1). Table I depicts the statistics of the organizations participated in the study:

Table 1. Statistics of participatory organizations.

Organization Type	Number of Organizations	% of Response Received
Banks, Financial Institutions	12	38.7
Manufacturing	3	9.6
Others	16	51.6

Since we have small size of sample nominal and ordinal data, we have used partial least square (PLS) method because this method does not require homogeneity and normality on data (Hair *et al.*, 1998).

RESULTS AND DISCUSSION

The questions in our survey instrument were based on different ensembles and the table 2 depicts the data

Based on our survey instrument it was determined that albeit many organizations recognize the importance of IS security effectiveness, but many of them had not properly placed IS security controls within the organizations. As we discussed above the effectiveness of network security controls was measured on Likert's scale, the table 3 depicts the IS effectiveness in organizations.

Reliability of the questions were tested by looking into the loadings of questions provided by PLS. Adequate reliability was proposed by Hair *et al*. (1998) as 0.5. On Cronbach's alpha, evidence of composite reliability could also be obtained. Nunnaly (1978) proposed the reliability of a construct should be at least 0.7. As an indication of adequate variance extracted 0.5 is a good indicator (Fornell, 1982). Table 4 depicts the results.

In this study we have used data collected from different types of organizations ranging from small to large conglomerates in Saudi Arabia where organizational culture, organizational maturity and employees behavior are generally varied. We suggest that this type of study should be carried out with different set of organizations and additional deterrent and preventive controls in order to generalize the results. This study has assessed various security controls and their effectiveness in different organizations. We have observed that small organizations do not have adequate security controls as compare to large organizations, and it is suggested to organizations to improve IS security effectiveness in future in order to prevent from a great damage.

As organizations are increasingly depending on IS and becoming more networked, further awareness of security controls is essential especially to the top management in order to have security measures in place.

A better IS security effectiveness is contributed by greater deterrent and preventive efforts. Many managers in organizations are either reluctant or unwilling to employ deterrent and preventive efforts to reduce risks in their organizations. The reason is they are unaware of the benefits of detective and deterrent measures and effects of preventive counter-measures. Since the penalty for IS abusers is not that high as compare to other crimes, organizations should take further steps to increase efforts for deterrent and preventive measures. The awareness of

Table 2. Ensembles and organizations data.

Ensemble	No. of Organizations	% of Organizations
Deterrent efforts (per day)		
Less than 1 hour	10	32.3
More than 1 but less than 3 hours	7	22.5
More than 3 but less than 9 hours	8	25.8
More than 9 hours	6	19.3
Deterrent Action		
No action	9	29.0
Warning	12	38.7
Suspension of services/ duties	8	25.8
Litigation/Prosecution	2	6.45
Preventive Action		
Security software	21	64.7
Operating systems	3	9.6
Database management systems	7	22.5

Table 3. Effectiveness of security controls in IS organizations.

Security Control	No. of Organizations	% of Organizations	Mean Significance of Security Control	Mean Security Control Effectiveness
Policies & Procedures	18	58.06	5	3
Firewalls	27	87.09	5	5
Intrusion Detection System	12	38.70	4	5
Honeypots	8	25.80	2	1
Encryption	22	70.97	4	4
Checksums	16	51.61	4	1
Audit Trails	13	41.93	5	2
Configuration Management	20	64.51	5	3
Incident Handling	24	77.41	4	3
Problem Escalation	17	54.83	4	4
Capacity Management	18	58.06	5	1
Performance Monitoring	25	80.64	5	1
Anti Virus Procedures	27	87.09	5	3

IS security effectiveness among top management is insufficient and it is suggested that some form of education may be useful in IS security context. Management should be emphasized different aspects of preventive efforts and the legitimate and illegitimate use of IS assets. It is important that IS auditors should have good experience in order to conduct audit on regular basis. Management should also be aware of security software to protect IS assets.

It is observed that small organizations do not invest in deterrent efforts as they believe and trust in employees while large organization invest more in deterrent efforts. It is advised to small organizations that they reassess their deterrent efforts to ensure there is assets are secure. Financial institutions tend to invest more for deterrent and preventive efforts due to large potential losses that may happen from IS security breach. The organizations which are related to other than financial business have lower IS security effectiveness as they are low deterrent efforts. These organizations must raise deterrent efforts to enhance IS security effectiveness as the businesses are increasingly adopting electronic networks in future.

REFERENCES

Brancheau, C., Janz, D. and Wetherbe, C.1996. Key Issues in Information Systems Management: 1994-95 SIM Delphi results MIS Quarterly. 20(2):225-242.

Fornell, C. 1982. A Second Generation of Multivariate Analysis. Methods, 1. New York, USA.

Hair, F., Anderson, E., Tatham, L. and Black, C. 1998. Multivariate Data Analysis with Readings. Englewood Cliffs, Prentice Hall, NJ, USA.

Khan, MA. and Turki, S. 2008. Evaluation of Software Development Controls in Information Systems Organizations. Canadian Journal of Pure and Applied Sciences. 2(2):463-468.

Myyry, L., Siponen M., Pahnila,S.,Vartiainen, T. and Vance, A. 2009. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems. 18:126-139.

Nunnally, C. 1978. Psychometric theory. (2nd edi.). McGraw-Hill, New York, USA.

Puhakainen, P. 2006. A Design Theory for Information Security Awareness. University of Oulu, Oulu, Finland.

Siponen, M. and Vance, A. 2010. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly. 34(3):487-502.

Solms, B. 2001. Corporate Governance and Information Security. Computers and Security. 20:215-218

Stanton, J., Stam, K., Mastrangelo, P. and Jolton, J. 2005. Analysis of End User Security Behaviors. Computers and Security. 24(2):124-133.

Straub, W. and Welke, J. 1998. Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly. 22(4):441-469.

Sun, l. and Srivastava, R. 2006. An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions. Journal of Management Information Systems. 22(4):109-142.

Verton, D. 2002. Disaster Recovery Plan Still Lags. Computer World. 36(14):10.

Warkentin, M. and Willison, R. 2009. Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems. 18:101-105.

Weber, R. 1998. EDP auditing: Conceptual foundations and practice. McGraw Hills, NY, New York, USA.

Received: June 5, 2014; Accepted: Sept 6, 2014