***IBIMA Publishing***
*Communications of the IBIMA*
*http://www.ibimapublishing.com/journals/CIBIMA/cibima.html*
*Vol. 2010 (2010), Article ID 486878, 9 pages*

# Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks

**Abdullah Alshboul**

Argosy University, Chicago, USA

**Abstract**

*Determining the exact requirements for security for a given organization is essential for implementing the proper security measures. Such measures are designed to protect information systems from security breaches. The Internet and computer networking requires a new security measures and policies to reduce the threats and challenges inherent from these new technologies and software applications and network devices. The information security attacks of an organization's assets have high dollar impact, loss of customer confidence, and negative business reputation. An organization must analyze its assets and the threats these assets face from either inside attacks or outside attacks. This paper presents a security assessment method which is designed to enable the organization to reduce security threats by deploying the most proper security measures, countermeasures, and policies.*

**Keywords:** security measures, countermeasures, malicious attacks.

## Introduction

The Internet and computer networking means that there is a need for new security measures and policies to reduce the threats and challenges inherent from these new technologies and software applications and network devices. Information, network equipments, transmission media, computer systems, and servers are subject to threats. "Yet the use of information and communication technologies has increased the incidents of computer abuse." (Backhouse and Dhillon). Security measures and countermeasures are implanted to protect organizations from different security attacks. To guarantee the security requirements of a given organization, it is essential to be able to evaluate the current security demands of an organization as well as the measures taken to achieve such requirements. Security weaknesses cause a negative impact on organizations such as financial loss, reputations, and loss of

 Author contact:
Abdullah Alshboul email: alshboul12@yahoo.com

customer confidence (Kumar, Park, and Subramaniam, 2008). The intention of implementing security measures, controls, and policies is to guard information security objectives and information assets. Information security objectives, which are confidentiality, integrity, and availability, are the main concern in categorizing information security level (Chen , Shaw and Yang, 2006, Johnson, 2008 and. Nyanchama, 2005).

Information security breaches take many forms and could carry disturbing and devastating consequences on both the economy and national security. The Department for Business Enterprise & Regulatory Reform (BERR) in the United Kingdom conducted a survey in 2008 which indicated that the estimated financial losses due to the security breach were several billion pounds a year (Chen, Shaw, and Yang). Richardson found in the annual CSI conducted by FBI that the average financial loss due to the security breach per respondent was $288,618, however; only 144 respondents from 522 were willing to share their financial losses. Security- related losses cost the U.S economy some U.S $117.5 Billion a year (Powner). An organization which could experience a loss of personal information due to the breach of confidentiality, integrity or availability would be categorized as a low, moderate, or high security level. Table 1 illustrates a template example for a high security level of a given organization. Measuring the level of personal, physical and network security will assist organizations in determining the average security level that needs to be implemented in an organization.

The security measures and countermeasures are used in organizations to protect information security objectives. These measures will assist an evaluator to measure the security level. For example the security level is high when an organization implements the most proper, updated measures, policies, and countermeasures to protect its security objectives. The information security level is low when an organization implements up to 49% of the measures and countermeasures to protect its security objectives. The security moderate is high when an organization implements between 50% and up to 79% of the measures and countermeasures to protect its security objectives as shown in table 1.

Table 1: Information Security Level Assessment

| Measuring level | Low | Moderate | High |
|---|---|---|---|
| Personal security | 0-49 | 50-79 | 80-100 |
| Network Security | 0-49 | 50-79 | 80-100 |
| Physical security | 0-49 | 50-79 | 80-100 |
| Assessment/ Average | The average is low | The average is moderate | The average is high |

This tool allows for multiple classifications of an organization. For example, an organization with an average score of 40%, 60%, and 90% for security measures that protects confidentiality, integrity, and availability will be categorized as low, moderate and high on confidentiality, integrity, and availability accounts.

Organizations are required to take appropriate security measures based on their requirements. Security measures can be grouped into three major groups: physical, personal, and network security measures. Each group employs several means for security protection. Within each group, security measures can be further classified into measures aimed at securing the

confidentiality, integrity and availability of the data and system. Banks, on the other hand, have high demand for data confidentiality. Hence, the measures required to protect confidentiality are essential for banks. In essence, an organization may have different security requirements for information security objectives. Similarly, an organization may have different security requirements at different times.

**Information Security Threat and Vulnerability**

Vulnerability is the weakness of information and information systems which can lead to attacks, harm, modification, destruction, disclosure, interruption, and interception.

1. Destruction: occurs when information, hardware, and software are destroyed due to malicious intention.
2. Disclosure: occurs when unauthorized users have access to information or information systems and disclose the confidential information. "Unauthorized disclosure has a serious impact on maintaining security and privacy of the system" (Dhillon).
3. Modification: occurs when unauthorized users change the information held in computer and server systems.
4. Interruption: occurs when a computer network becomes unavailable for access. An example is the denial of service.
5. Interception: occurs when unauthorized users copy information that resides in a computer system or while the data is in transmission mode.

An attack on information systems is a sign of vulnerability. "Vulnerability assessment deals with identifying flaws and weaknesses that could possibly be exploited of the threats" (Dhillon). Vulnerabilities lead to hackers, attackers, and spies who attack the information and information systems. "Threats take advantage of vulnerabilities to cause damage or loss" (Nyanchama, 2005).The weaknesses of information systems are the roots of the breaches in information security which can lead to financial fraud, damage to brand-names, and brand-marks, loss of customer and partner confidence, and could also cause the organization to go out of business.

New threats to information systems occur from unexpected sources when organizations become more reliant on it (Nyanchama, 2005). "Threat is an indication of impending danger or harm" (Johnson, 2008). "A security threat is a condition of vulnerability that may lead to an information security being compromised." (Kumar, Park, and Subramaniam, 2008).

All organizations having information systems, websites, intranet, and Internet are subject to a number of security threats. Organizations are facing an increase of varieties of security threats. As risk level grows and the need for organizational compliance in this field increases, information systems security becomes more important to an organization's overall business approach.

Internet is considered the major threat to organizations because criminals can access valuable information. Many threats are caused by operating System (OS) weaknesses, network operating system (NOS) weaknesses, and default configuration of the OS and NOS, network devices and firewalls, encryption weaknesses, and applications that are poorly written (Ciampa). As the sophistication of security threats continues to evolve, organizations must take steps toward preventing the losses from these threats (John, 2000).Removing threat and eliminating vulnerability is impossible as long as the organizations are connected to the Internet and hackers are breathing (Nyanchama, 2005). However, it is doable to ease the risk and live with both

inside and outside threats (Nyanchama, 2005). A threat is not a risk when vulnerability does not exist. Yet, if there is any possibility of a threat or the root of a threat, weaknesses and vulnerability must be determined and the appropriate measures and controls need to be implemented.

Mitigating vulnerability by deploying measures to reduce security breaches, monitoring news about the new vulnerabilities, developing new risk assessment, deploying new technologies, and employee training can mitigate new threats and protect an organizational asset. The importance of understanding the impact of an organization's security threats is facilitating an organization more efficiently to measure the security risk. The nature of threats to information security has changed due to the hackers and crackers sophistication. Organizations must investigate the information systems vulnerability.

This review of the literature provides substantive solutions to mitigate the information security vulnerabilities. Organizations that measure their security level and determine the weaknesses should be able to reduce threats and improve information security, which is what this study intends to do.

**Information Systems Assets**

Literature indicates that information is considered to be one of the most essential assets to organizations. Backhouse and Dhillon argued that the concerns in regards to the protection of the organizational information assets have increased due to the technology revolution in information systems and communication media (Backhouse and Dhillon).
The main purpose of information security is to protect and safeguard the organizations' assets from threats. "For many organizations, information and the technology that supports it represent the organization's most valuable assets." (John, 2000). Assets are classified into two groups which are tangible and intangible. Schou and Shoemaker (2006) classified information as intangible because it cannot be counted; it is not the same as computer parts or soapboxes where it is possible to establish accurate dollar value. Examples of intangible assets are survey data, trademarks, trade names, licenses, contracts and procedures.

Intangible assets need to be converted into tangible assets to establish a value of the intangible assets, as shown in Table 2. To make a value for intangible assets, the assets need to be documented and the value and the ownership of the assets need to be determined. This will make enforcement of intangible assets achievable and allow the court to protect intangible assets the same way as tangible assets (Schou, and Shoemaker, 2006).

Information and information systems assets are tangible and intangible. Assets vary from one organization to another. Protecting information systems from breaches and preventing information theft is done by defining the information systems assets. Each organization's information assets must be evaluated to determine their information security. Information security is needed for safeguarding the information and information system assets in the organizations. Dhillon mentioned that the purpose of defining and characterizing the organization's assets allows for better determination behind the threat (Dhillon). Documentation of the assets will be beneficial to an organization because it will know what to secure, and it will ensure updates of assets in the case of changes (Schou, and Shoemaker, 2006). Security breaches appear due to the lack of documenting and characterizing the information system assets within organizations. According to Ciampa (Ciampa) an organization not only protects its information by classifying its assets in order to protect them from any threat caused by crackers and hackers, but it also identifies its vulnerabilities.

Table 2: Information Assets

| Assets Name | Asset Background | Asset Category |
|---|---|---|
| Server, desktop, switch , router, connectors, hub | Physical infrastructure | Tangible |
| Cables, cell phone, T.V., DVD, storage devices | Physical infrastructure | Tangible |
| Articles, white paper, press release, music files, patent | Internet | Intangible |
| UPS | Physical infrastructure | Tangible |
| Application programs | Physical infrastructure | Tangible |
| Customer, employees' and suppliers' information (credit card, phone number, SSN#...), Website applications, inventory, supply and demand, marketing software | Internet | Tangible |
| copyright, survey data, trademarks, trade names, licenses, contracts, procedures, programs and procedures. | Internet | Intangible |

**Methodology**

The purpose of this research was to provide a new method for evaluating and assessing the information security level to assist organizations to optimize costs, reduce information security threats. This research intended to evaluate the information security level to assist organizations in identifying the measures that are implemented and help organizations identify any gaps in the current security implementation. This study identified the effects of measuring information security level in organizations. This research examined the results of implementing the most appropriate information security measures and countermeasures in various organizations.
This section describes the model that was utilized in this research to gather the data necessary to answer the research question:
What is the significance of categorizing the information security level in an organization?
The hypothesis of this research are the following:

Hypothesis: Defining the information security level will allow an organization to implement the appropriate security measures.

This research utilized a quantitative approach. A web-based survey was conducted to collect the data to examine the correlation between measuring information security levels and securing confidentiality, integrity, and availability. A total of 56 participants participated in a web-based survey containing 57 questions divided into six sections.

*Research Design*

The research design selected for this study was a web-based survey. The survey was designed by this researcher. The survey was a self-administered questionnaire. A correlation study examined whether or not a relationship exists between dependent and independent variable. With a correlation significant at the 0.05 level (2-tailed).

*Selection of Participants*

The participants for this research were information system professionals from various organizations. Information system professionals who had a major role in information systems security were the primary target. The survey was launched by

a third party company. The name of the third party company is Sendmedia.com.

*Data Collection*

The researcher used a web-based survey to gather data. Surveymonkey.com was chosen as the online survey vendor. The survey questionnaire was emailed by Senditmedia.com to all 100,000 organizations. The gathered data was uploaded into Microsoft Excel and Statistical Package for the Social Sciences (SPSS) for analysis.

Data Analysis

Pearson's correlation was conducted to measure the relationship between the dependent and independent variables, with a correlation significant at the 0.05 level (2-tailed). A total of 56 information security professionals participated in the research from various organizations. SPSS version 17 was used for data analysis.

**Results**

Table 3 illustrates categorizing information security levels in various organizations. In the banking industry 62.5% of participants indicated that their security level was moderate and 37.5% has a high security level. In the education industry, 66.7% of the participants pointed that the security level is moderate, 16.7% indicated that information security level in the education industry was low, and the same percentage of the participants indicated that the level of security was high. In information technology, 50% of participants indicated that the information security level was moderate and the same percentage 50% indicated that the security level was high. In the medical industry, 75% of participants pointed that information security level was high and 25% of participants indicated that security level was moderate. In the retail industry, 14.3% of participants indicated that security level was low, 42.9% of participants indicated that information security level was moderate, and 42.9 of participants indicated that information security level was high. In the transportation industry, 100% of participants indicated that the level of security was moderate. In the telecommunication industry, 58.3% of participants indicated the information security level was moderate and 41.7 of participants indicated that information security level was high.

Table 3: Descriptive Statistics for Information Security Level in Organizations (N-56)

| Industry | Low | Moderate | High | Total |
|---|---|---|---|---|
| Banking | .0% | 62.5% | 37.5% | 100.0% |
| Education | 16.7% | 66.7% | 16.7% | 100.0% |
| Information Technology | .0% | 50.0% | 50.0% | 100.0% |
| Medical | .0% | 25.0% | 75.0% | 100.0% |
| Retail | 14.3% | 42.9% | 42.9% | 100.0% |
| Transportation | .0% | 100.0% | .0% | 100.0% |
| Telecommunication | .0% | 58.3% | 41.7% | 100.0% |

*Research Hypothesis*

The first research hypothesis for this study was: Defining the information security level will allow an organization to implement the appropriate security measures.

Table 4 shows descriptive statistics (minimum, maximum, mean, and standard deviation) for implementing the proper security measures. The mean for implementing the appropriate security measures in organizations is 4.40 (*SD*=.995). The mean of improving overall security by measuring information security is 4.47 (*SD*=.790).

Table 4: Descriptive Statistics for the Dependent Variables for Hypothesis One (N=56)

| | Minimum | Maximum | *M* | *SD* |
|---|---|---|---|---|
| Improving overall security | 1 | 5 | 4.47 | .790 |
| Implement the proper security measures. | 1 | 5 | 4.40 | .955 |

Table 5 Correlation between Defining Information Security Level and Dependent Variables for the Research Question

| | *R* | *p* |
|---|---|---|
| Improving overall security | .345 | .011 |
| Implement the proper security measures. | .430 | .001 |

Table 5 shows the correlation computed to investigate this hypothesis. There was a statistically significant positive correlation between defining information security level and improving overall security (p=.011), as well as implementing the proper security measures (p= .001). This indicates that organizations that measure their information systems security level will implement the proper security measures and improve their overall security. As a result, this hypothesis is supported by this study.

**Summary of Findings**

Information security breaches have a negative impact on organizations One of the main challenges facing organizations is how to reduce information security vulnerabilities and protect information security objectives. Information security objectives are the main concern in categorizing information security levels. These objectives are confidentiality, integrity, and availability. Implementing the proper security measures and measuring their information security levels will assist organizations in protecting and maintaining their data in the proper way.

The first research question of this study was: What is the significance of categorizing the information security levels in an organization? Hypothesis one suggested that an organization that measures its information systems security will implement the most proper information systems security measures. Hypothesis one was supported by the findings. Results of this research indicated that measuring information security levels enable

organizations to implement the appropriate security measures, policies, and countermeasures. The positive correlation between putting in place the proper security measures and improving security indicated that organizations that categorized their security levels utilized the proper security measures. Based on this research there is a clear support for organizations to measure their security levels to improve their security by deploying the most efficient security measures.

In today's global market intranet is connected to Internet and an organization's assets will become a target for various malicious attacks. The need for protecting the organizational information assets has increased due to the technology revolution in information systems and communication media (Dhillon, 2006). The organizations that participated in this research indicated that there was a need to implement proper security measures to protect information assets from malicious attacks. Ensuring information and not securing the tangible assets of an organization can be risky because this separation will create an opportunity for an attacker to cause serious harm by gaining physical access (Schou, and Shoemaker, 2006). Organizations implementing security measures and countermeasures to protect hardware, software, and information, such as antivirus, firewalls, encryptions, password protection, hardening operating systems, hardening network operating systems, hardening network devices, and employee's awareness decreased vulnerabilities and security breaches(Ciampa).

As a result, the answer to the first research question is that there was a statistically significant positive correlation between defining information security levels and utilizing the proper security measures and countermeasures. Measuring information security levels is a method that helps information security professionals manages their enterprise more effectively.

**Conclusion**

This research constructs a method for defining information security levels in organizations. Defining information security levels is based on measuring security layers, which are network security, physical security, and personal security in organizations. Each layer deploys several means for security protection. Within each layer, security measures, policies, and countermeasures can be further classified into measures aimed at protecting the confidentiality, integrity and availability of the information.

This research makes quite a few essential contributions. It illustrates the importance to correlate between an organization's assets, security vulnerability, security attacks, and evaluating information security levels in order to safeguard the confidentiality, integrity, and availability of information. Security measures, countermeasures, policies, procedures and guidelines are implemented in organizations to maintain the desired level of information security level. As a result, organizations will be able to secure their information security objectives.
Organizations are struggling against security attacks. Implementing the most appropriate security measures in organizations assists organizations to protect their information's assets and reduce security vulnerabilities. The results of the research question led the researcher to conclude that defining information security levels enables organizations to implement proper security measures. Implementing security measures helps organizations to decrease possible damage and loss due to security attacks.

**References**

Backhouse, J. and Dhillon, G. (2000). Information system security management in the new millennium. *Communications of the ACM*, *43*, 125-128.

Chen, C. C., Shaw, R. S., and Yang, S.C. (2006). Mitigating information security risks By increasing user awareness: A case study of

information security awareness system. *Information Technology, Learning & Performance Journal*, *24*, 1-14.

Ciampa, M. (2005). *Security+ Guide to network security fundamentals*. (2nd ed.). Boston: Course Technology.

Dhillon, G. (2006). *Principles of information systems security: Texts and Cases* (1st ed.). Hoboken, NJ: Wiley.

John, L. W. (2000). COBIT: A Methodology for Managing and controlling Information and Information Technology Risks and Vulnerabilities. *Journal of Information Systems*, *14*, 21-25.

Johnson, M. E. (2008). Information risk of inadvertent disclosure: An Analysis of File Richardson, R. CSI Computer Crime & Security Survey. *Computer Security Institute.*

Ryan, D. J., and Ryan, J. J., (2005) Proportional hazards in information security. *Risk analysis: An International Journal*, *25*,141-149.

Schou, C., and Shoemaker, D. (2006). *Information assurance for the enterprise: A roadmap to information security (1st ed).* NY: McGraw-Hill Irwin.

sharing risk in the financial chain. *Journal of Management Information Systems, 25*(2), 97-123.

Powner, D. *GAO security report.* [Online], [Retrieved September 22, 2009], http://www.gao.gov/.

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*, 241-279.

Nyanchama, M. (2005). Enterprise vulnerability management and its role in information security management. *Information Systems Security*, 14, 29-56.

[Online], [Retrieved September 22, 2009], http://www.gocsi.com/forms/csi_survey.jht