https://doi.org/10.48009/1_iis_2012_177-184
Issues in Information Systems
Volume 13, Issue 1, pp. 177-184, 2012

INFORMATION SECURITY POLICIES' CHANGES IN ORGANIZATIONS

Marzie Astani, Winona State University, mastani@winona.edu

ABSTRACT

Computer security issues have been a fact of life since the beginning of electronic information sharing. With the development of the Internet, these issues became global. Computer systems have been under attack by hackers through using several techniques including malicious email attachments. There are various estimates about the cost of damage, but the most recent statistics are stated to be in the range of billions of dollars per year. Organizations have been slow in adopting strategies and developing policies to secure their information resources. Firms' budget allocations appear unaffected by the accelerated rate of computer security incidents. Companies have been slow in spending more money and adopting strategies to secure their information resources. There is a trade-off between security and the budget allocation, and organizations are having a difficult time to find a balance. The initial step in the process of finding a balance is to conduct an analysis of the existing security situation and to understand where the company stands on the information resources risk. This study attempts to explore some of the policy issues with which organizations are faced in securing their information resources. The focus of this study is to show companies' existing security policies situation and compare with those of a decade ago to see whether there have been any changes. The objective is to help organizations to realize their potential security weaknesses.

Keywords: Network security, computer worms, hackers, network administrator, computer acceptable use policy

INTRODUCTION

Prior to the Internet borderless networks, individuals needed physical access to where information was hosted. Today, sensitive data is no longer limited to physical facilities and computer hackers can remotely and anonymously gain access to them (5). This phenomenon has become more significant as countries join together to securely share information at the global level. Information sharing is a major challenge since information content that ranges from the simple to complex (e.g., intelligence reports, financial information, travel records, citizenship records, military positions and logistical data, map data, etc.) is transmitted in a constantly changing environment (17).

Many businesses have flourished doing business online. One consequence of doing business on the Internet is that money attracts criminal activities (6). Throughout the years, there have been many well-publicized information security, network intrusions and computer hacking incidents. In 1988, when the Internet was still in its infancy, the Robert Morris Jr. Internet worm swiftly disabled cyberspace. At that time, Internet was not a common household word, as it is today. Many people did not know it existed, and many users had not considered the impact a security incident might have on their own system and data. When the Michelangelo virus scare headlined the national news in 1991, users had become much more aware of the importance of network security (12). At that time, users were already heavily reliant on the computer's ability to store knowledge and execute business transactions.

A survey released in 2003 showed that nearly half of the nation's fastest-growing companies suffered from a recent information security breach (9). Since viruses, worms, and other network exploits can easily seek and target any vulnerable computer connected to the network, as seen in the cases of MS-Blaster (CERT CA_2003-20) and SQL Slammer (CERT CA-2003-04), it's imperative to secure networks and prevent financial loss. System downtime that results in the system's unavailability of service/operations caused by denial-of-service (DoS) has been directly linked to financial loss. For example, eBay's outage in 2000 has been linked to an unbelievable $5 billion loss, or about $225,000 per hour of downtime (4). In 2005, another major financial damage happened, where the credit information of approximately 163,000 consumers was stolen from ChoicePoint, now a division of LexisNexis. ChoicePoint was a data aggregation that acted as a private intelligence service to government and industry (15). It

was purchased in February 2008 by Reed Elsevier (parent corporation of LexisNexis). ChoicePoint sold the information to identity thieves impersonating business people. The thieves opened ChoicePoint accounts by posting as debt collectors and insurance agents, giving them access to a large database with records on almost every individual in the U.S. Ultimately, more than 800 cases of identity theft were connected to the incident, leading ChoicePoint to agree to a $15,000,000 settlement (21).

Malware has evolved along with the Internet and is now the tool of choice for attacking computers and networks. The key lies in its ability to remain surreptitious: It must enable the attacker to remotely manipulate a system while remaining virtually invisible to standard defenses. There is a specialized class of malware, termed "advanced persistent threats" (APTs), that presents a widely publicized yet little understood security challenges (5). Using this class of malware, attackers can – and do- segregate infected computers into interest areas and modify their methods accordingly. For example, after initial infection by a common downloader, Trojan, subsequent information may be collected from infected machines to identify those systems more likely to lead to sensitive information. Unique web malware encounters increased significantly throughout the first half of 2011, from 72,294 unique encounters in January 2011 to 287,298 in June. Companies in the Pharmaceutical, Chemical, and the Energy and Oil sectors continued to be at highest risk of web malware throughout the first half of 2011. This is followed by Transportation and Shipping, Agriculture and Mining, and Education.

Our awareness of computer security continues to increase with each new security breach. Some suggest that computer security issues we have seen to date might be the tip of a very large iceberg, and it is urgent that organizations take measures to safeguard their networks (14). According to a Computer Security Institute and the Federal Bureau of Investigation Computer Crime and Security Survey, approximately 85% of companies in the USA experienced internal and external security breaches which weakened the financial strength and confidence of the victimized companies. In a small survey conducted by the American Bar Association, 40 percent of the respondents detected and verified incidents of computer crime within their organizations. Respondents of the survey calculated their loss in a single year to a total between $145 million and $730 million (4). Throughout the literature, there are various estimates about the incurred cost of damage for security breach. But the actual situation is even worse. According to several reports, the majority of companies are reluctant to broadcast security failures to customers and shareholders and report only a fraction of the security breaches (14).

This research is an attempt to reveal the current state of computer and information security issues in some organizations. The focus of this study is to show how these companies protect their information resources. The objective is to help organizations realize their security weaknesses. In the following parts of this paper, current security plans and limitations are discussed, followed by the research methodology, analysis of the results, and conclusion.

CURRENT SECURITY PLANS AND LIMITATIONS

There are many security threats to organizational networks; however, they all fall into the four most common categories that can be caused by intentional or unintentional actions. These categories are interruption, interception, modification, and fabrication (16). Interruption, an attack in availability, occurs when an asset of the system becomes lost, unavailable, or unusable. Interruption examples include malicious destruction of a network element, erasure of a software program or data file, cutting of a communication line, and malfunction of an operating system file manager so that it cannot find a particular disk file. Interception, an attack on confidentiality, occurs when an unauthorized person, program or computing system gains access to an asset. Wiretapping to obtain data in a network and passive listening to a wireless radio transmission are examples of this type of intrusion. Modification, an integrity attack, happens when an unauthorized party tampers with an asset. Examples include changing the network configuration values in a database and modifying data being transmitted in a network. Fabrication, an attack of authenticity, occurs when an unauthorized party gains access and fabricates counterfeit objects on a network. Examples include unauthorized access to the network, untraceable malicious activity on the network, the insertion of spurious messages in a network, and the addition of records to an authentication database (13). Ongoing data analysis can help baseline what is normal for the organizations, an important first step in readily identifying

new or previously unseen incidents. According to Cisco 2011 report (5), the majority of network intrusion attacks (72%) occurs through port 80. NUA Research reported (2) that e-mail attachments account for 80 percent of computer virus infections. Denial of service (DoS) attempts increased during the second quarter (5). Phishing levels measured in proportion to all spam increased in the second quarter, reaching 4 percent of the total volume of spam in May 2011.

Software vulnerabilities when exploited cause loss in confidentiality, integrity, and availability of information. Various encryption and encoding techniques have been proposed to protect confidentiality and integrity of information, while redundancy and fault tolerance have been the classical solutions to ensure availability. However, in a network environment when a vulnerability common to all nodes is exploited, redundancy alone is not enough to ensure availability (4). Information security performs four important functions for an organization: 1) protecting the organization's ability to function; 2) enabling the safe operation of applications running on the organization's IT systems; 3) protecting the data the organization collects and uses; and 4) safeguarding the organization's technology assets" (24). Establishing an efficient and effective security strategy and policy allows organizations to successfully safeguard their resources and assets while setting the standards on how to interact with one another in a global environment. On the other hand, an ineffective security strategy increases the possibility of financial burden for firms. Network vulnerabilities reduce efficiency and leave the organization's resources and assets unprotected and compromise the integrity of information systems and resources. In order to strengthen an organization's information systems, an effective computer security plan and policy must be in place.

There are two basic types of policies: authorization and obligation policies (7). Authorization policies are used to define access rights for a subject (management agent, user, or role) and can be either positive (defining the actions subjects are permitted to perform on target objects) or negative (specifying the actions subjects are forbidden to perform on target objects). As such, authorization policies are used to define access control rules implemented by several types of mechanisms in a network security system, such as packet filters, Kerberos, and VPNs. Obligation policies are, in turn, event-triggered condition-action rules that can be used to define the activities subjects (human or automated manager components) must perform on objects in the target domain, i.e., the duties of these subjects. In the network security context, obligation policies can be used to specify the behavior of mechanisms such as logging agents, intrusion detection systems (IDSs), and watchdogs.

Organizations need to establish a set of standards for information sharing in a secure environment that is constantly changing. The best known competing information security management systems (ISMS) are described in ISO/IEC 27001 and ISO/IEC 27002 and related standards published jointly by ISO and IEC. ISO/IEC 27001is a set of policies concerned with information security management or IT related risks. As with all management processes, an ISMS must remain effective and efficient in the long term, adapting to changes in the internal organization and external environment. The objective of ISO/IEC is to provide management direction and support for information security (11). Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization (3). The ISO/IEC framework provides guidance for information security in accordance with the standard, and organizations should create their own additional guidance as necessary. There are several steps in establishing an adequate security plan for an organization. The first step is risk analysis, which requires that all resources and assets including all hardware and software such as server routers, switches and communication lines be identified (22). Next, the potential loss incurred by threats to those assets is identified and examined. The second step is to establish a security plan that creates policies and defines the organization's issues.

Management needs to think about risks and develop plans and establish strategies and policies for computer security. Organizations using new technologies such as Microsoft Sharepoint and cloud technology need to be aware of added complications to security threats of their networks. Introducing new technologies require that management be aware that the proper training/education, collaboration barriers, clear security oversight, and ongoing scanning for viruses would be in place. According to a survey conducted by security vendor Cryptzone in November 2011 (18), 92% of the employees involved agreed that removing information from Microsoft SharePoint made it less secure, but 30% were willing to take that risk. Obviously, there's a disconnect between security and productivity at many businesses.

This highlights the need for businesses to put clear policies in place regarding how information can be shared, and then to monitor access and enforce policy compliance.

According to the literature, organizations need to address several computer security issues such as formal training for employees, maintaining expertise, management commitment and support, allocating sufficient budget for information security, and establishing policy for installing security patches. A survey conducted by the Information Technology Association of America showed that 46 percent of the corporations do not have formal training in information security practices (20). And many of their system administrators don't install all the security patches issued because they don't know how, do not have the resources, do not maintain all of the computers or have computer users who will not let them. Companies can't afford to ignore their most important security threats policies at every level of the corporation. Another security issue is allocating sufficient budget for information security, which is an important management decision. A survey of small firms with revenues between $5 million and $150 million (12) revealed that forty-six percent of them have been victims of security breaches. Contrary to the expectations, these organizations were not planning to allocate sufficient money for their computer security budget to protect their information resources. There is a trade-off between security and the budget allocation. There is no "one-size-fits-all" solution. Management needs to determine how valuable information resources are for organization and act accordingly.

RESEARCH METHODOLOGY

To obtain information about organizations' existing computer security situations, an instrument that was developed in a similar study a decade ago (1) was used to collect data. The instrument is composed of five parts and used for data collection. The first two parts of the questionnaire involves general information about the organizations. The following three parts included some questions that required interviewees (network administrators) to give a rating on a Likert scale (1=very low, 5=very high) and others called for a 'yes/no' answer to the computer security situation. In an attempt to obtain accurate information about computer security issues, the network administrators of organizations in the Upper Midwest area of the U.S. were interviewed face-to-face. Sixteen small to midsize organizations were involved in the study.

ANALYSIS OF THE RESULTS

The information based on interviewing sixteen organizations' network administrators was analyzed. As mentioned earlier, the focus of this study was to obtain information about organizations' computer security plans and policies in place. In a 2002 study (1) the same survey was used for the same region. The following discussion presents the results of the research conducted and compared with the results of the same survey that was conducted in 2002.

An overwhelming one hundred percent of the network administrators interviewed said that they have a formal computer security policy in place and actually enforced the policies, such as installing update program patches and antivirus updating (Table 1). This finding is contrary to the CERT report that states many system administrators don't install all the security patches issued (20). However, according to the findings of this 2012 survey, the computer security situation of organizations has improved. All network administrator, 100 percent of them, stated that they periodically review the policies and security issues (Table 1). This result is similar to that of 2002. As a part of organizational computer security policy, regular antivirus software updates is very important. One hundred percent of the companies involved enforce this policy indicating another improvement in organizational network security (Table 1, 100% vs. 92%; for 2012 and 2002 respectively.) Contrary to our results, the literature shows that it is doubtful that all users in organizations install anti-virus software and keep it updated (20). As mentioned earlier, the majority of network intrusions using malicious software are through email attachments (2); therefore, installing and updating the antivirus software is very important and could cause a major security threat to a firm's information resources. The issue becomes even more disturbing when considering that some organizations don't enforce the security policies. This security threat was clearly shown when many companies were hit by the SQL Slammer and Blaster worms despite having defenses such as network firewalls, gateway antivirus devices, and patches in place. Further investigation showed that this happened because the remote workers logged on to company networks

without proper patches and updated antivirus software and infected internal desktops and servers that were unsecured (10).

Another related finding is the ongoing assessment of the effectiveness of existing security policies. Only 63 percent of the organizations surveyed stated that such an assessment program is in place on an ongoing basis (almost unchanged results from 2002, Table 1). This is a disturbing observation considering the dynamic business environment and ever-changing technology.

Table 1. Percentage of positive responses (based on Yes/No answer to questions)

Survey item	%Yes	
	2002	2012
Periodically review and redefine the security issues	100	100
Formal computer security policies	93	100
Enforcing CAUP	93	100
Policy for updating antivirus software	86	88
Established computer acceptable use policy (CAUP)	71	100
On-going evaluation of effectiveness of security policies	62	63
National computer security policies contribute to organization's security	57	75
Policy for enforcing installing released patches & updating antivirus software	92	100
The 9/11 event has changed the organization's approach to security	36	19

Many organizations have established a formal 'Computer Acceptable Use Policy' (CAUP) for their employees. This policy guides the employees/users on what type of conduct or behavior is acceptable by the organization in using the information resources. One of the findings of the study was that 100 percent of the firms have established CAUP, and all of them enforce the policy. This is a major improvement for organizational computer security policy since in the study conducted a decade ago [Astani & Elhindi, 2004] only 71 percent of the organizations had CAUP in place and 93 percent of them admitted enforcing the policy.

Table 2. Percentage of responses based on 5-point scale (1=very low, 5=very high)

Survey item	%High Ratings	
	2002	2012
Lack of appropriate hardware and/or software	86	94
Top management support and commitment	79	94
Importance of computer security to management	71	75
Computer security training for employees and network administrators	64	69
Formal security policies and strategies	69	87
Communication with the users	64	87
Formal security plan	57	94
Success of organization's computer security	57	81
Tying computer security to firm's goals	50	69
Company-wide support and involvement	50	94
High frequency of attempt to breach security	43	43
User satisfaction with computer security	43	63
Assessment of cost of typical security breach	36	56
Sufficient budget for computer security	21	50

The 9/11 event had a major impact on the national and international security policies. As a result of this event, the national computer security policy has been changed. One of the interview questions was about the impact of the 9/11 event on companies' computer security policy. Only 19 percent of the network administrators stated a change in their approach to security. This result is inconsistent with the finding of a decade ago, in which 75 percent said they follow national computer security policy (Table 1).

Table 3. T-test results for comparison of the survey responses between 2002 – 2012

Survey item	Probability of t
Formal computer security policies	0.02
Enforcing CAUP	0.55
Lack of appropriate hardware and/or software	0.52
Top management support and commitment	0.21
Importance of computer security to management	0.34
Computer security training for employees and network administrators	0.89
Formal security policies and strategies	0.02
Communication with the users	0.09
Formal security plan	0.04
Success of organization's computer security	0.38
Tying computer security to firm's goals	0.04
Company-wide support and involvement	0.00
High frequency of attempt to breach security	0.76
User satisfaction with computer security	0.61
Assessment of cost of typical security breach	0.57
Sufficient budget for computer security	0.11

Another interesting finding is that network administrators have become more confident about their organizations' network security. Eighty-one percent thought that they are successful in securing companies' network (Table 2). This is surprising since there are a number of articles in the literature pointing out that there is a high rate of intrusion attempts on organizations' networks. According to a 2011 Cisco report (5), the rate of unique instances of web malware more than doubled in the second quarter of 2011, from 105,536 in March to 287,298 in June. In an earlier report, CERT stated that the rate of cyber attacks on company systems were 30 times per week (20). But interestingly, when network administrators were asked directly about the frequency of network intrusion attempts, only 43 percent stated that they have high frequency of intrusion attempts. This denial is consistent with findings in the literature (20). Furthermore, the same article reported that only 47 percent of the security executives could quantify the losses incurred as a result of security breach. In the present research, fifty-six percent of network administrators stated that the cost of security breach was low (56 percent, Table 2). This raises the question whether they were really aware of the extent of losses.

One of the major concerns in computer security issues is training. In the literature it was suggested that organization should have ongoing training programs for the users and network administrators (13). Sixty-nine percent (compared to 64% in 2002) of the respondents in the study stated that training is not an issue in their organizations. Eighty-seven percent (sixty-nine percent in 2002) of interviewees said that there is good communication with the users. But when asked about user satisfaction with the company's computer security, only sixty-three percent (less than half, 43 percent in 2002, Table 2) rated this item high. This low rating of user satisfaction with computer security in the organization cannot be justified when the rating for company-wide involvement in computer security is considered (94 vs. 50 percent for 2012 and 2002 respectively, Table 2).

For each individual item we can see some differences in ratings from 2002 to 2012. The question is whether these differences are significant. To answer this question a t-test was performed on the two sets of the survey ratings. The results (in terms of p-values) are presented in Table 3. As shown in the table, organizations have made significant improvements in the areas (small p-value is indicative of significant difference). More organizations have established "Formal computer security policy," "Formal security plan," and "Formal security policies and strategies" to prevent security risks. This indicates that more and more organization management realizes that they need to take all measures to secure their information resources. Another major improvement is seen in the area of aligning company's goals with policies and strategies. Significantly more organizations aligned their computer security with their goals in 2012 compared to that of 2002 (Table 3). This presents more supporting evidence that company

management understands the importance of organization computer security. Finally, significantly more organizations have "Company-wide support and involvement" for computer security policies in 2012.

CONCLUSION

For most parts, the findings presented in this study are consistent with what were reviewed in the literature, although, the sample size for this research was small (sixteen organizations) and the answers from network administrators were self-claimed. Future research on the subject should be based on a larger sample and verification of the answers for more reliability.

System administrators or computer security personnel play a major role in keeping the companies' assets secure. But top management support for computer security is the key. Although there is a significant improvement in the company-wide support and involvement for computer security policies form 2002 vs. 2012, the insufficient top management support is still evident (71 percent of the respondents stated that computer security is important to management in 2002 vs. 75 percent in 2012). A major point that needs to be made based on the results of the two survey research of 2002 and 2012 is that more support and involvement for computer security need to be provided by top management. The insufficient management support and involvement was apparent in low ratings of organizational computer security training, tying computer security to firm's goals, user satisfaction with computer security, and allocation of sufficient budget for computer security. These are indicative of insufficient management understanding of the importance of computer security for organization.

The results showed that all of the organizations involved in this study have computer security policies in place, but it is evident in survey results of 2002 and 2012 that ongoing evaluation of effectiveness of these policies seem to be a major issue. Setting up security policy and not following up to ensure their effectiveness does no help the organization. Another management related issue is the budget allocation for computer security. Top management need to be more involved in the computer security process and allocate sufficient budget to secure organization's information resources.

REFERENCES

1. Astani, M, Elhindi, M. (2004). An Empirical Study of Computer Security Issues. IIS, Volume V, No.1, pp. 15-21.
2. Bhattacharyya, M. Hershkop, S. and Eskin, E. (2002). MET: An Experimental System for Malicious Email Tracking, New Security Paradigms Workshop. September 02, 23-26.
3. Brykczynski, B. Small, B. (2003). Securing Your Organization's Information Assets, The Journal of Defense Software Engineering, http://www.stsc.hill.af.mil/crosstalk.
4. Chen, P., Kataria, G. and Kirshman, R. (2011). Correlated failures, Diversification, and Information Security Risk Management. MIS Quarterly, vol. 35, No.2, pp. 397-422.
5. Cisco Systems, Inc. (2011). Global Threat Report. Network World Networking Alert. nwonline@online.networkworld.com, Accessed February 20, 2012.
6. Daniels, T. Spafford, E. "Network Traffic Tracking Systems: Folly in the Large?" ACM Communications, 2001, pp 119-124.
7. De Albuquerque, J. P., Krumm, H., de Geus, P. L. (2010). Formal validation of Automated Policy Refinement in the Management of Network Security Systems. International Journal of Information Security, vol.9, pp 99-125.
8. Gurpreet, D. Backhouse, J. (2000). Information Systems Security management in the New Millennium. Communications of the ACM, 43, 7.
9. Hogan, J., Montague, P., Purvis, M. and Steketee, C. (2004). Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation, ACM International Conference Proceeding Series, Dunedin, New Zealand, 37 – 42.

10. Hulme, George V. (2003). Enforcing Security At The End Point, InternetWeek, http://www.internetweek.com, retrieved 24 November, 2011.
11. International Standards organization. (2007). Using and referencing ISO and IEC standards for technical regulations http://www.iso.org/iso/standards_for_technical_regulations.pdf.
12. Keizer, Gregg. (2003). Half of Companies Surveyed Suffered Security Breaches, TechEwb News, InternetWeek, http://www.internetweek.com, retrieved 24 November, 2011.
13. Kennedy, Susan. (2003). Best Practices for Wireless Network Security, Computerworld, http://www.computerworld.com, retrieved 8 December, 2011.
14. National Institute of Standards and Technology. (2002) Risk Management Guide for Information Technology Systems, http://csrc.nist.gov/publications/nistbul/b-11-03.pdf, retrieve 29 April, 2011.
15. O'Harrow, Robert Jr. (2005). In Age of Security, Firm Mines Wealth Of Personal Data . *Washington Post*, 19 January 2005, retrieved 17 February, 2012.
16. Pfleeger, C. (1997). Security in Computing, Prentice Hall, Upper Saddle River, NJ.
17. Phillips, C. Teng, T. and Demurijan, S. "Information Sharing and Security in Dynamic Coalitions." ACM Communications, June 2002, pp 87-96.
18. Schwartz, Mathew. 10 SharePoints Security Mistakes You Probably Make. http://www.InformationWeek.com, 31 January, retrived February 12, 2012.
19. Stanniford, S. Hoagland, J. and MaAlerney, J. (2002). Practical Automated Detection of Stealthy Portscans, Journal of Computer Security, 25-36.
20. Stepannek, Marcia. (2004). Re-engineering Security, CIO Insight, http://www.cioinsight.com, retrieved 12 January, 2011.
21. Tom, Jacqueline May. (2010). A simple Compromise: The Need for a Federal Data Breach Notification Law. St. John's Law Review, Vol. 84, pp. 15691603.
22. Toyoizuni, H. Kara, A. (2002). Predators: Good Will Mobile Codes Combat Against Computer Viruses, ACM Communications, 11-17.
23. Viega, J. & McGraw, G. (2002) Building Secure Software, Addison-Wesley.
24. Whitman, Michael and Mattord, Herbert. (2012). Principles of Information Security, Fourth Edition. Course Technology/Cengage Learning.