

# AN EMPIRICAL STUDY OF COMPUTER SECURITY ISSUES

**Marzie Astani, Winona State University, mastani@winona.edu**  
**Mohamed Elhindi, Minnesota State College- Southeast Technical,**  
**melhindi@Southeastmn.edu**

## ABSTRACT

*The number of information security breaches has been on the rise during the past several years. Computer systems have been under attack by hackers through using several techniques including malicious software attached to email. According to the literature, malicious software attached to email accounts for the majority of computer breaches. There are various estimates about the cost of damage, but the most recent statistics is stated to be in the range of billions of dollars for 2002 alone. 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. Yet, 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 difficult times 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 reveal some of the issues that organizations are faced with in securing their information resources. The focus of this study is to show companies' existing security situation in protecting their information resources. The objective is to help organizations to realize where the security weaknesses are and attempt to deal with security deficiencies.*

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

## INTRODUCTION

Throughout the years, since the initiation of electronic information sharing there have been many well-publicized 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. At that time, users were already heavily reliant on the computer's ability to store knowledge and execute business transactions. Recently, a survey released in 2003 showed that nearly half of the nation's fastest-growing companies suffered from a recent information security breach (6). With each new security breach, our awareness of computing technology continues to increase. 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 (9).

According to the 2003 Computer Security Institute and the Federal Bureau of Investigation Computer Crime and Security Survey, security breaches resulted in over \$200 billion in lost revenue last year. Approximately 85 % of companies in the USA experienced internal and external security breaches which weakened the financial strength and confidence of the victimized companies (8). In a small survey conducted by the American Bar Association, 40 percent of the 100 respondents detected and verified incidents of computer crime within their organizations. Respondents of the survey calculated their loss in a single year to 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 (9).

The four most common network security threats that can be caused by intentional or unintentional actions are interruption, interception, modification, and fabrication (9). 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. The outside party can be a person, a program, or a computing system. 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 (8). According to NUA Research (1), e-mail attachments account for 80 percent of computer virus infections. Also, worm activity (intrusion attempts on port 80) was detected to be between 20-60 percent of all intrusion attempts, with worm signatures from Code Red and Nimda remaining prominent after more than a year since they were launched.

This research is an attempt to reveal some of the issues that organizations are faced with in securing their information resources. The focus of this study is to show companies' existing security situation in protecting their information resources from the experts' perspectives, network administrators. The objective is to help organizations realize where the security weaknesses are and attempt to deal with their security deficiencies.

### **Current Security Plans and Limitations**

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.

Information sharing in a secure environment that is constantly changing is a major challenge for organizations. In 2000, the ISO adopted the British Standard (BS) 7799-1 (Part 1) as ISO 17799, "Code of Practice for Information Security Management." This is a best practices framework for information security management standards (ISMS), which includes 10 sections in the areas of security policy, organizational security, asset classification, personal security, physical and environmental security, communications and operations management, access control, systems development and maintenance, business continuity planning, and compliance. Within these control areas, there are a number of control objectives. The following shows a control objective: Objective: To provide management direction and support for information security. 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 (2).

The framework provides guidance, and organizations that implement ISMS in accordance with the standard 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. 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 (12). Management needs to think about risks and develop plans and establish strategies and policies for computer security. In a 2003 survey, it was revealed that 46 percent of small firms with revenues between \$5 million to \$150 millions have been victim of recent security breaches. Contrary to the expectations, these organizations have not allocated more money for their computer security budget to protect their information resources. According to the survey, these companies were spending 1.9 percent of their operating budget on information security for 2003, only a slight increase over the previous year (6). 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 protecting the bottom line is and act accordingly.

Today, competitive pressure may lead to the adoption of IT without careful planning and understanding of security issues by many organizations (3). In light of growing competition, the situation is expected to get worse. The role of security managers is getting increasingly more important. The focus of these managers will be shifting to consider the wholeness and soundness of information systems and the organization.

## **RESEARCH METHODOLOGY**

To obtain information about organizations' existing computer security situation, an instrument needed to be developed. A questionnaire containing five parts was designed to obtain information from firms. The first two parts of the questionnaire involved 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 order to

develop relevant and precise questions, the authors reviewed literature and consulted with a few network administrators. In an attempt to obtain accurate information about computer security issues, the network administrators of organizations were interviewed face-to-face. A combination of fourteen profit and non-profit were involved in the research. These organizations employed between one hundred to three thousand employees. The following section presents the analysis of collected data.

## ANALYSIS OF THE RESULTS

The information based on interviewing fourteen 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. The purpose was to explore the possible strengths and weaknesses in computer security. The following discussion presents the results of the research conducted.

An overwhelming ninety-three percent of the network administrators interviewed said that they have a formal computer security policy in place, but only fifty percent of the firms actually enforced the policies, such as installing update program patches and antivirus updating (Table 1). This finding is consistent with the recent CERT report that states many system administrators don't install all the security patches issued (9). It appears that firms establish policies but don't follow up to make sure they are implemented. This is happening in spite of all network administrators, 100 percent, stating that they periodically review the policies and security issues (Table 1). As a part of organizational computer security policy, regular updating of antivirus software is very important. Although, the majority of organizations stated that they have such a policy in place, 14 percent of the firms lack this program. A similar result was found in the literature showing that it is doubtful that all users install anti-virus software and keep it updated (11).

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

Question	Yes
Periodically review and redefine the security issues	100%
Formal computer security policies	93%
Enforcing CAUP	93%
Policy for updating antivirus software	86%
Established computer acceptable use policy (CAUP)	71%
On-going evaluation of effectiveness of security policies	57%
National computer security policies contribute to organization's security	57%
Policy for enforcing installing released patches & updating antivirus software	50%
The 9/11 event has changed the organization's approach to security	36%

As mentioned earlier, the majority of network intrusions using malicious software are through email attachments (1); 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 only 50 percent of the security policies are enforced.

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 (5). Another related finding is the periodic assessment of the effectiveness of existing security policies. Only 57 percent of the organizations surveyed stated that such an assessment program is in place on an ongoing basis. This is a disturbing observation considering the dynamic business environment and ever-changing technology.

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 only 71 percent of the firms have established CAUP, and of these, 93 percent admitted to actually enforcing this policy. One would wonder that if there is no established CAUP how users would know what the acceptable conduct is when it comes to using technology. Furthermore, even if a company has an established CAUP which is not being enforced, how could it be expected that the users would take it seriously.

The 9/11 event had a major impact in 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 36 percent of the network administrators stated a change in their approach to security. This result is inconsistent with another finding, in which 57 percent said they follow national computer security policy (Table 1).

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

Questions	High Ratings (4 & 5)
Lack of appropriate hardware and/or software	86%
Top management support and commitment	79%
Importance of computer security to management	71%
Computer security training for employees and network administrators	64%
Formal security policies and strategies	64%
Communication with the users	64%
Formal security plan	57%
Success of organization’s computer security	57%
Tying computer security to firm’s goals	50%
Company-wide support and involvement	50%
High frequency of attempt to breach security	43%
User satisfaction with computer security	43%
Assessment of cost of typical security breach	36%
Sufficient budget for computer security	21%

According to the network administrators involved in the study, the majority of top management seemed to understand the importance of computer security and was committed to protecting their information resources (71 percent stated computer security was important to their management and 79 percent said that management is supportive and committed, Table 2). As the result shows, only 57 percent of respondents stated that there is a formal computer security plan in place. Furthermore, only 21 percent of the network administrators thought computer security budget is sufficient. One would question top management's commitment by looking at the budget allocation for computer security and lack of formal security plan. The finding about insufficient computer security budget is consistent with what was found in the literature. A 2003 survey of small companies showed that these firms spent only 1.9 percent of their operating budget for computer security, a slight increase over 2002 (6). A related issue is tying organizations goals to computer security policies. Only fifty percent of the interviewees felt that there is such a connection. One would expect that a committed management who is involved in establishing computer security policy would make sure that the connection exists.

Another interesting finding is that network administrators don't think very highly of their organizations' network security. Only fifty-seven percent thought that they are successful in securing companies' network (Table 2). This is not surprising since there are a number of articles pointing out that there is a high rate of intrusion attempts on organizations' networks. According to a 2003 report, CERT organization tallied cyber attacks on company systems and reported that companies are hacked 30 times a week (11). 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 (11). 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, the cost of security breach was rated low by our network administrators (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 (7). Sixty-four percent of the respondents in the study stated that training is not an issue in their organizations. Sixty-four percent of interviewees said that there is good communication with the users. But, when asked about user satisfaction with the company's computer security, less than half (43 percent, Table 2) rated that high. This low rating of user satisfaction may be justified when the rating for company-wide involvement in security is considered (50 percent).

## **CONCLUSION**

For most parts, the findings presented in this paper are consistent with what were reviewed in the literature, although, the sample size for this research was small 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. In addition, it would be interesting to further explore the possible differences of non-profit organizations and profit firms in security measures and issues.

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. A major point that needs to be made based on the results of this research is that organizations need more support and involvement from top management. The lack of management support and involvement was shown in enforcing computer security, budget allocation, users and network administrators training, and getting employees involved in the computer security.

The results showed that most of the organizations in this study have computer security policies in place, but enforcing these policies seem to be a major issue. Setting up security policy and not following them through 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. Bhattacharyya, M. Hershkop, S. and Eskin, E. (2002). MET: An Experimental System for Malicious Email Tracking, New Security Paradigms Workshop. September 02, 23-26.
2. Brykczynski, B. Small, B. (2003). Securing Your Organization's Information Assets, The Journal of Defense Software Engineering, <http://www.stsc.hill.af.mil/crosstalk>.
3. Gurpreet, D. Backhouse, J. (2000). Information Systems Security Management in the New Millennium, Communications of the ACM, 43, 7.
4. Hogan, J., Montague, P., Purvis, M. & 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.
5. Hulme, George V. (2003). Enforcing Security At The End Point, InternetWeek, <http://www.internetweek.com>, accessed November, 24.
6. Keizer, Gregg. (2003). Half of Companies Surveyed Suffered Security Breaches, TechEwb News, InternetWeek, <http://www.internetweek.com>, accessed November, 24.
7. Kennedy, Susan. (2003). Best Practices for Wireless Network Security, Computerworld, <http://www.computerworld.com>, December 8.
8. National Institute of Standards and Technology. (2002) Risk Management Guide for Information Technology Systems, <http://csrc.nist.gov/publications/nistbul/b-11-03.pdf>, accessed April 29, 2004.
9. Pfleeger, C. (1997). Security in Computing, Prentice Hall, Upper Saddle River, NJ.
10. Stanniford, S. Hoagland, J. and MaAlerney, J. (2002). Practical Automated Detection of Stealthy Portscans, Journal of Computer Security, 25-36.
11. Stepannek, Marcia. (2004). Re-engineering Security, CIO Insight, <http://www.cioinsight.com>, accessed January 12.
12. Toyoizuni, H. Kara, A. (2002). Predators: Good Will Mobile Codes Combat Against Computer Viruses, ACM Communications, 11-17.