https://doi.org/10.48009/2_iis_2005_231-237

PROTECTING INFORMATION RESOURCES AND MANAGING THE RISK

Robert Behling, Arrowrock Technologies, rbehling@hotmail
Susan Haugen, University of Wisconsin – Eau Claire, shaugen@uwec.edu
Wallace Wood, Bryant College, wwood@bryant.edu

ABSTRACT

This paper addresses some of the problems in protecting information resources in organizations and in particular implementing data security measures. A survey was conducted of employees of organizations in southern New England and in Wisconsin to measure user awareness of a group of ten widely known data security concerns. While the ranking of the recognition and addressing of the concerns was consistent for the two samples, it was found that user awareness of data security procedures was far from comprehensive and further work needs to be done by management in this area.

Keywords: Data Security, User Awareness

INTRODUCTION

The dramatic growth of computer technologies and the Internet has resulted in new and exciting ways for people to communicate, process and transfer information, engage in commerce, and extend their educational opportunities [14]. The organizational advantages of information technology have been described as: 1) reduced waste; 2) increased productivity; 3) less workforce; 4) higher profits; and 5) advanced communications [5]. To effectively achieve these advantages requires a set of supporting physical, technological and social resources [12].

At the same time that organizations are gaining effectiveness through deployment of information and communications technologies, the combination of increased security risks and expanded connectivity vulnerabilities has made it possible for relatively unsophisticated cyber criminals to breach systems controls and gain access to confidential and sensitive data stored on networked computer systems [3]. The increase in cyber attacks, along with increasing regulatory requirements, has caused organizations to evaluate how much risk is acceptable, and to put in place policies and procedures to control or reduce unacceptable information technology risks.

Simply increasing hardware and software security resources is not always an effective strategy for controlling risk and combating cyber crime in computerized organizations [4]. The threats from viruses and worms, as well as hackers, spammers and incidents of identity and information theft, will continue to be a problem for all modern organizations [13]. While there are tools to provide some basic protection from these risks, the human element is a critical component of any effective security procedure. A recent survey of the public and private sector found that human error, not technology, is the most significant cause of security breaches [8].

A cultural clash may also put cyber security at risk [7]. Effective security requires a successful convergence of the areas of physical security (the “cops”), IT security (the “geeks”), and financial risk management (the “bean counters”). This is often difficult because of problems with jargon, personalities, turf and stereotypes. There is no magic bullet to get them to work together, even though it is imperative to do so if the organization is to have any hope of maintaining effective data security.

A well planned audit program is essential to evaluate risk management activities, internal control systems, and compliance with organizational policies and procedures designed to protect information resources. [2]. The audit may become the glue that holds the various areas together in striving for organizational information security. Security plans implementing software, hardware, policies and procedures to control risk is not a one-time activity, and needs continual review and evaluation, which can be supported through the audit function.

Protecting organizational information resources usually involves protecting against cyber crime which presents the most fundamental challenge to law enforcement because there are no geographic or political borders to restrict the flow of information, there are easy methods of concealment that provide the cyber criminal with anonymity, and the problem of Internet crime has grown at such a rapid pace that laws have lagged behind the technology [16]. There are efforts underway by law enforcement and government agencies to provide assistance in protecting information systems and resources, including the establishment of the Critical Infrastructure Protection Board, Office of Homeland Security. Their mission is to convince the private sector to cooperate with federal government agencies by reporting information security attacks [15]. The United States Computer Emergency Readiness Team provides a listing of publicly known security vulnerabilities and exposures, produces security advisories, and issues cyber alerts to the international community [1].

Balancing Security Needs with Business Goals

Computer and information security is a dynamic process which is constantly at odds with business goals and consumer demands for speed and functionality [3]. Possible vulnerabilities are to the network, the information resources, and to the bandwidth available to the organization [6]. There is no universal approach to data security that will protect all organizations from all risks, but any approach is best accomplished by following a three step approach [17] of

(1) Business Assessment. Management begins by describing and defining the high level security objectives for an organization and what is at stake if information resources are compromised. The outcome of the business assessment is to determine what information assets have to be protected.

(2) Risk Analysis. This step of the analysis looks to create a risk profile for critical assets by identifying likely threats and estimating potential losses. A cost/benefit assessment will reveal if the cost to protect the information outweighs the potential loss which is not an efficient investment of company resources. The outcome of the risk analysis is a prioritized listing of security functions that are required.

(3) Risk Mitigation. This step applies the risk profiles that have been created to standards, policies, procedures and security architecture required to deliver the desired level of security and information protection. The outcome of the risk mitigation activities will be a determination of

the right combination of security safeguards, and a description as to how the security measures will be implemented.

Security Awareness

While performing the aforementioned three steps is vital, organizations need to recognize that employees are the stewards of corporate data; therefore they should be the first line of defense when securing company information. In reality, security awareness and training is the most overlooked component of security management programs and people may be the weakest link in security plans. Some analysts believe that the vast majority of resources have been dedicated to the technical aspects of security and that many security plans will fail due to the lack of effective strategies for user data security education [11]. This is reinforced by a survey on the threats of e-mail and spyware where the 400 business technology officials indicated that user education and awareness must be a priority in addressing these threats [10].

RESEARCH METHODOLOGY

A survey was designed to measure employee awareness of security measures currently being used in their organizations. The Top 10 enterprise security risks described by esecujrityplanet. com were used as the foundation for the items developed for the questionnaire. This listing of security risks was selected because it focuses on the human issues rather than the technological component of the information security plan. The authors recognize that the list is not all inclusive, and the literature supports numerous listings of critical, most important or relevant security risks. The survey assumes that protection of information resources begins with recognition of the risk, followed by development of policies, and then procedures to mitigate the risk.

The survey was administered to graduate students in a Masters of Business Administration program who were employed full-time in businesses and organizations in southern New England. A second sample consisted of MBA graduate students who were employed full-time in Wisconsin. After removing responses from duplicated companies in each region, the resulting sample sizes were 42 and 26 respectively.

SURVEY RESULTS AND DISCUSSION

Table 1 provides the summarized results for organizations in southern New England and Table 2 presents the results for organizations in Wisconsin.

For each of the 10 security areas, the number of responses (and percentages) for the four possible responses are presented. For example, the first row of Table 1 shows that 7 respondents (16.7 %) indicated that their company recognized the risk of e-mail attachments; 4 respondents (9.5 %) stated that their company recognized the risk of e-mail attachments and had developed policies; 29 respondents (69.0 %) reported that their company recognized the risk, had put policies in place and had also developed procedures; and 2 respondents (4.8 %) indicated that they did not know the status of this security area in their organization.

The fourth column (4) in both Table 1 and Table 2 was considered the most important because it indicates that the organization has not only recognized the risk, it has developed policies, and put appropriate procedures in place to address the given security problem. For comparison purposes, the rows of the tables were sorted in descending order by percentages for column four. A Spearman rank order correlation was calculated for the rankings of the 10 security concerns by the southern New England and Wisconsin samples. The resultant value of 0.78 indicates that the rankings are consistent for the two samples.

Table 1
Number of Responses (percentages) by Risk
Southern New England Organizations (n = 42)

(1)	Risk Recognized by Organization (2)	Risk Recognized and Policies in Place (3)	Risk Recognized, Policies in Place, and Procedures in Place (4)	Do Not Know (5)
E-Mail Attachments. Workers opening attachments could unleash a worm or virus.	**7 (16.7)**	**4 (9.5)**	**29 (69.0)**	**2 (4.8)**
Web Downloads. Bringing unwanted web misuse of company resources for personal use.	**5 (11.9)**	**11 (26.2)**	**25 (59.5)**	**1 (2.3)**
Instant Messaging. Message is exposed to interception, copying or modification as it passes through various systems to final recipient.	**9 (21.4)**	**7 (17)**	**22 (52.4)**	**4 (9.5)**
Virtual Private Network Compromised. VPNs are vulnerable to hackers giving them easy access to the entire organization's resources	**8 (19.0)**	**2 (4.8)**	**20 (47.6)**	**12 (28.6)**
Blended attacks. Worms and viruses attacking more than one platform.	**5 (11.9)**	**3 (7.1)**	**20 (47.6)**	**14 (33.3)**
Music and Video Browsers. Browsing uses valuable resources and bandwidth.	**12 (28.6)**	**8 (19.0)**	**17 (40.5)**	**5(11.9)**
Network Partners. Partners can introduce vulnerabilities by utilizing a less secure system.	**5 (11.9)**	**3 (7.1)**	**15 (35.7)**	**19 (45.2)**
Server to Server Access. Access given to hackers and rogue employees to infiltrate multiple systems.	**5 (11.9)**	**5 (11.9)**	**14 (33.3)**	**18 (42.9)**
Diversionary Tactics. Hack one target to divert security attention, and then attack another part of the system.	**4 (9.5)**	**2 (4.8)**	**12 (28.6)**	**24 (57.1)**
Renaming Documents. Critical information renamed and sent to others, bypassing monitoring software.	**8 (19.0)**	**6 (14.3)**	**6 (14.3)**	**22 (52.4)**

The first item of note is that the security concern of E-mail Attachments was the first ranked concern for southern New England companies and was tied for first for Wisconsin companies, but that it was addressed by twice as many (69% to 34.6%) southern New England companies as Wisconsin companies. Similarly, Instant Messaging was ranked third for southern New England companies at 52.4% and fourth by Wisconsin companies at 30.8% continuing the large difference in percentages despite the comparable rankings.

It is also interesting that Server to Server Access, Diversionary Tactics, and Renaming Documents were the bottom ranked concerns for both samples. This low ranking is probably due to the fact that approximately 50 percent of the respondents in both samples indicated Do Not Know for these three security concerns.

Table 2. Number of Responses (percentages) by Risk; Wisconsin Organizations (n = 26)

(1)	Risk Recognized by Organization (2)	Risk Recognized and Policies in Place (3)	Risk Recognized, Policies in Place, and Procedures in Place (4)	Do Not Know (5)
E-Mail Attachments. Workers opening attachments could unleash a worm or virus.	10 (38.5)	5 (19.2)	9 (34.6)	2 (7.8)
Music and Video Browsers. Browsing uses valuable resources and bandwidth.	6 (23.1)	9 (34.6)	9 (34.6)	2 (7.8)
Blended attacks. Worms and viruses attacking more than one platform.	8 (30.8)	2(7.8)	8 (30.8)	8 (30.8)
Instant Messaging. Message is exposed to interception, copying or modification as it passes through various systems to final recipient.	5 (19.2)	7 (26.9)	8 (30.8)	6 (23.1)
Web Downloads. Bringing unwanted web misuse of company resources for personal use.	5 (19.2)	10 (38.4)	7 (26.9)	4 (15.4)
Virtual Private Network Compromised. VPNs are vulnerable to hackers giving them easy access to the entire organization’s resources	8 (30.8)	2 (7.8)	7 (26.9)	9(34.6)
Network Partners. Partners can introduce vulnerabilities by utilizing a less secure system.	5 (19.2)	3 (11.5)	6 (23.1)	12 (46.2)
Diversionary Tactics. Hack one target to divert security attention, and then attack another part of the system.	5 (19.2)	2(7.8)	5 (19.2)	14 (53.8)
Renaming Documents. Critical information renamed and sent to others, bypassing monitoring software.	3 (11.5)	4 (15.4)	5 (19.2)	14 (53.8)
Server to Server Access. Access given to hackers and rogue employees to infiltrate multiple systems.	2 (7.8)	4 (15.4)	5 (19.2)	15 (57.7)

The average percentage of Do Not Know responses for the southern New England sample was 29 and for the Wisconsin sample it was 33 which is interesting in light of an InformationWeek survey [9] which indicated that 74% of the 2956 respondent sites had taken steps to raise employee awareness of security policies and procedures. The results of the survey in this paper would indicate that the 74% figure has not changed much since 2002.

The overall large percentage of Do Not Know responses is probably the most interesting fact from the tables. While it is recognized that a Do Not Know response does not necessarily imply that the respondent’s organization failed to recognize that security concern as a problem, it, at the very least, points out a lack of user awareness to a given security concern. Thus, even if the organization recognizes the concern and has developed policies and procedures to address it, the fact that an employee is not aware of it, is not a good situation. Of course, the alternative where the employee does not know because the organization failed to recognize the security problem is worse. It is not a desirable situation in either case.

Table 3. Web Downloads

Number of Employees in Organization	Risk Recognized by Organization	Risk Recognized and Policies in Place	Risk Recognized, Policies in Place, and Procedures in Place	Do Not Know
1-50	3	0	1	0
51-500	1	2	10	0
501-2000	0	4	2	0
2001-10000	1	3	5	0
Over 10000	0	2	7	0
Chi Sq = 28.164	p = 0.005			

Table 4. Music and Video Browsers

Number of Employees in Organization	Risk Recognized by Organization	Risk Recognized and Policies in Place	Risk Recognized, Policies in Place, and Procedures in Place	Do Not Know
1-50	5	0	0	0
51-500	4	4	2	13
501-2000	2	1	1	2
2001-10000	2	2	4	1
Over 10000	0	1	8	0
Chi Sq = 26.596	p = 0.009			

Tables 3 shows the results of the survey by company size for the Web Download security concern for the southern New England sample, while Table 4 displays the results for the Music and Video Browser security concern. A Chi Square test was performed on each table to determine if there was a significant relationship between company size and responses to the security concern. The Chi Square value in both cases was significant indicating that a relationship does exist.

Similar tests were performed on the remaining eight security concerns, but none were significant at the 0.05 level indicating that for the most part user awareness of data security issues is not dependent on the size of the organization of the user.

CONCLUSIONS

Samples of employees from southern New England and Wisconsin were consistent in their ranking of how ten security issues were being handled by their respective organizations. At the same time, though, the survey results indicated that large numbers of the employees in the samples did not know whether several security concerns were being addressed by their organizations. These results reinforce the idea that data security in organizations is more than a technical problem and data security user awareness must be better addressed by organizations concerned with data security.

REFERENCES

1. "Common Vulnerabilities and Exposures: United States Computer Emergency Readiness Team," (2004) Retrieved February 10, 2004 from http://www.uscert.gov/cve/.
2. "FFIEC Information Technology Examination Handbook," Retrieved February 10, 2004 from http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.
3. "Hackers: A Canadian Police Perspective," (2004) Retrieved February 9, 2004 from http://www.rcmp.ca/crimint/hackers_a_e.htm#.
4. "ICC Cybercrime Unit," (2004) Retrieved February 9, 2004 from http://www.icc-ccs.org/main/index.php.
5. "The Advantages of New Technology in Your Business," Retrieved February 9, 2004 from http://www.bizhelp24.com/it/working_without_new_technology_pros_cons.shtml.
6. Gaudin, S. (2002), "Top 10 Enterprise Security Risks," Retrieved February 9, 2004 from http:// http://www.esecurityplanet.com/trends/article.php/1384081.
7. Gaudin, S. (2004). "Is a Culture Clash Risking Your Security?," Retrieved February 17, 2004 from http:// http://www.esecurityplanet.com/prevention/article.php/3425021.
8. Gross, G. (2003). "Human Error Is Greatest Security Risk," *PC World*, March 18, Retrieved February 17, 2004 from http:// http://www.pcworld.com/news/article/0,aid,109872,00.asp
9. Hulme, G. V. (2002), "Security Training Still a Business Afterthought," Retrieved February 17, 2004 from http://www.informationweek.com/shared/printableArticleSrc.jhtml?articleID-6503747.
10. Hulme, G. V. (2005). "Raising Awareness Key to Thwarting Spyware," Retrieved February 13, 2004 from http:///www.informationweek.com/shared/printableArticleSrc. jhtml?articleID=57700433
11. "Information Security Moves Front and Center," (2002). *Electronic Commerce News*, Retrieved February 16, 2004 from http://proquest.umi.com/pqdweb?index=0&did= 121825905&SrchMode=1&Fmt=3
12. Kling, R. and T. Jewett. (1994). "The Social Design of Worklife With Computers and Networks: An Open Natural Systems Perspective," Retrieved February 9, 2004 from http://www.slis.indiana.edu/faculty/kling/pubs/worknt.html.
13. Roberts, P. 2004. "Security Worries for 2004," *PC World*, Retrieved February 10, 2004 from http:// http://www.pcworld.com/news/article/0,aid,114058,00.asp.
14. Robinson, J. K. (2000). "Cybercrime and the Internet Integrity and Critical Infrastructure Act," Retrieved February 9, 2004 from http://www.usdoj.gov/criminal/cybercrime/ robtest.htm
15. Scarlett, S. (2002). "They Want You for a Safer Infrastructure," *CIO Magazine*, June 15, Retrieved February 10, 2004 from http://www.cio.com/archive/061502/safer.html.
16. Vatis, M. (2000). "Statement on Cybercrime Before the Senate Judiciary Committee, Criminal Justice Oversight Committee and House Judiciary Committee, Crime Subcommittee," Retrieved February 10, 2004 from http://www.usdoj.gov/criminal/ cybercrime/vatis.htm.
17. Wilson, J. (2003). "Managing Your Security Risk," Retrieved February 10, 2004 from http:// http://computercops.biz/article2942.html.