Journal of International Technology and Information Management

Volume 15 | Issue 3 Article 7

2006

Computer Security Checklist for Non-Security Technology Professionals

Chlotia P. Garrison
Winthrop University

Roderick B. Posey
University of Southern Mississippi

Computer Security Checklist for Non-Security Technology Professionals

Chlotia P. Garrison
Winthrop University

Roderick B. Posey
University of Southern Mississippi

ABSTRACT

Networked computers and electronic data storage make computer security a fundamental component of a company's survival. Security incidents can cause reputation damage, loss customers, or even liability. Companies that are unable or unwilling to hire certified security professionals often rely on non-security IT professionals for assistance. This paper provides a checklist the non-security professional can use to assist the company in the critical areas of conducting risk analysis, performing vulnerability assessments, educating employees and developing computer security policies and procedures

INTRODUCTION

Many companies have insufficient or non-existent security measures. For example, the Internet Security Alliance estimates that businesses lose several *billions* of dollars *each week* to various forms of cyber attacks (2004). Carnegie Mellon University's Computer Emergency Response Team's Coordination Center, CERT® /CC (2006), received 5,990 vulnerability reports in 2005. Forty-three percent (43%) of 500 respondents to the 2004 E-Crime Watch Survey report an increase in e-crimes and intrusions over the previous year and 70% report at least one e-crime or intrusion against their organization (U.S. Secret Service & CERT Coordination Center, 2004). Computer security is an area that businesses of every size should take seriously.

Becoming a certified security professional requires extensive training and years of experience. This extensive training hurdle can make locating qualified security professionals difficult. In addition, many companies have not placed sufficient emphasis in this area. For example, only 20% of respondents to an annual survey by Ernest and Young that included some of the largest companies in 51 countries strongly agree that their organizations perceive information security as a CEO level priority. Moreover, 47% of respondents with revenues in excess of $1 billion did not have a chief information security officer, CISO, in place (Ernst & Young, 2004). However respondents to the 2004 E-Crime Watch Survey considered hiring a CISO the second most effective policy or procedure in their organization in preventing or reducing electronic crimes (U.S. Secret Service & CERT Coordination Center, 2004).

The general public does not necessarily recognize specialties in the Information Technology (IT) area. Software professionals are asked to troubleshoot hardware problems, network professionals are asked to provide software recommendations, and database professionals are consulted on computer purchasing recommendations. No distinction is made between implementing security features in software and security procedures for a business. Employers often expect employees to expand their area of expertise to meet company needs. For these reasons, it would be beneficial for the non-security IT professional to become familiar with fundamental computer security requirements for businesses. This is especially true for those working or consulting for businesses that are unable or unwilling to hire dedicated security professionals. Computer security knowledge would increase the general IT professional's value to the company, allow them to make recommendations, and help protect companies from the potentially great damage that can result from security incidents. This paper provides a checklist for non-security IT professionals. The checklist will be address three areas - risk analysis, vulnerability assessments, and education, procedures, and policy.

LITERATURE REVIEW

The financial loss caused by computer incidents can be significant. Internet fraud losses alone totaled $1.5 million in a single month in 2005 (Communications of the ACM, 2006). Individual incidents can cost companies thousands of dollars. The mean cost of a security attack by companies surveyed by CompTIA was $35,000 (Wagner, 2006). These costs may be low because as noted by Mercuri (2003) losses of use and loss productivity are harder to measure. The financial effects may also be long term. Campbell et. Al., (2003) verified a negative stock market reaction for companies that experience a computer security breach that involves confidential information.

The costs of security incidents, the rising number of incidents, and the many incident types which according to Bidgoli (2003) can be intentional and unintentional indicate the need for companies to focus on prevention. However, available personnel may be just as much of an issue. Summerfield (2006) and Mitchell (2005) assert that fewer students are pursuing IT careers due to the highly visible dot-com failures, the fear of offshore outsourcing, and the image of IT professionals as geeks. The need for specialized training in computer security only deepens the problem. The federal government formed a program in 1998 that allows universities to apply for designation as a National Center of Academic Excellence in Information Assurance Education. According to Streff and Zhou (2005), the program intent was to encourage universities to develop the capability to produce enough graduates to meet the growing need of securing information. However, as of July 2006 the National Security Agency's website lists only 75 institutions as Centers of Academic Excellence (2006). LeBlanc and Stiller (2004) state that many computer science curricula do not have room for multiple courses dedicated to computer security, and many small colleges do not have faculty members who specialize in computer security. The special training and experience required to obtain security certifications reduces the number even more. Added to this is the need for certified individuals to receive continuing education. According to Kavanagh (2006), Certified Information Systems Security Professionals are expected to commit to an average of 40 hours of continuing professional development a year. An inadequate number of qualified security personnel, increases the salary they can demand.

The great potential to experience financial loss due to a computer security incident highlights the need to focus on security. However great demand and the high salaries available to certified security specialists makes it likely that smaller companies and larger unenlightened companies will not have certified security specialists on staff. The following checklist will aid the non-security IT professional in being a company's first line of defense.

PERFORM RISK ANALYSIS

A risk analysis will help determine the potential risk or loss from a computer incident. As part of the risk analysis, ask the following questions to help assess the risk of a computer incident:

- How important is company data?
- What would be the consequences of destroyed or stolen company data?
- Could propriety information be used to cause harm or gain competitive edge?
- Could the business be liable if information stored on its computers about employees or customers was stolen?
- Could that information be used to cause customers or employees harm? For example, access to social security numbers, bank account routing numbers, or credit card numbers of clients and employees could be used to steal a person's entire bank account or to obtain new charge accounts and run up huge debts before the business even knows the information is compromised.
- Would not having access to computers mean loss revenue or idle employees?

CONDUCT VULNERABILITY ASSESSMENTS

Vulnerabilities may exist in systems, software, and people. For example, the media has reported multiple incidents of stolen laptop computers and improper access to account information that made hundreds or thousands of people vulnerable to identity theft.

Vulnerability assessments should include how easy (or hopefully difficult) it is to gain unauthorized access to the system. The following is a list of inexpensive internal checks to perform:

- Check to see if computer accounts and access codes of former employers have been deleted.

- Periodically check offices and computers to see if passwords can be easily located. It is too easy to gain access to passwords written on sticky notes or in unencrypted files.
- Verify that unattended computers have password protected screen savers activated.
- Check employees' gullibility. Call and send e-mail to determine if employees will provide company, client, or personal information.

The security audit results will identify training needs and areas that require attention.

EDUCATION, PROCEDURES, AND POLICY

Conduct Security Education

Educate employees of their potential to increase the company's vulnerability to a security incident. One employee who gives away username and account information, loads a virus from a disk, opens an infected e-mail, or downloads an infected file can corrupt an entire network. Every employee needs to understand not only the potential loss but also his or her potential to perpetrate that loss through negligence.

Reduce user negligence by emphasizing the importance of following company security policies and procedures. Educate users to be cautious when opening e-mail and downloading software, to follow recommended guidelines for selecting and safeguarding passwords, to activate password protected screen savers whenever the computer is on and unattended, and to backup any file that would be difficult or time consuming to recreate.

Keep Software Patched and Updated

Attackers take advantage of vulnerabilities in software to attack systems. When security vulnerabilities are identified, software vendors will often provide patches (a fix to a software defect) or updates (a newer version of existing software) to remove the vulnerability. Patch management involves identifying what needs patching, installing and testing the patch and identifying any new vulnerabilities the patch may have caused (Fratto, 2003).

Systems need to be patched as quickly as possible following the publication of a new vulnerability before attackers have time to take advantage of the vulnerability. Know what software is on company machines, sign up for alert notifications, and monitor vendor sites for needed updates.

Use Good Passwords

Networked and some stand-alone machines should have individual accounts with usernames and passwords. Educate users and enforce good password guidelines:

- do not use dictionary words or acronyms in any language, slang, or dialect
- do not use personal information
- passwords should be 6-8 characters long with a combination of numbers, letters, maybe upper and lower case, and a special character
- do not write down passwords
- periodically change passwords
- do not reveal passwords
- use different passwords on different systems

Install Firewall and Antivirus Software

A firewall helps prevent attackers from examining a machine and using existing vulnerabilities to facilitate their attacks. Antivirus software attempts to detect and remove computer viruses. Firewall and antivirus software should be loaded on server machines, employee machines, remote machines, and even home computers. Update antivirus definitions at least weekly or have the software updated automatically.

Perform Backups

No matter how many procedures are in place, the potential to lose data exists. Regularly perform central and automatic backups. Backup important files whenever they are changed. Periodically test backup and restore procedures for accuracy and reliability.

Remove Old Accounts and Change Access Codes

Remove the accounts of anyone that leaves the company. If the person's files are needed, transfer them to a new user and delete the old account. When employees leave the company, change not only office keys but also any access codes known to the employee. One of the largest identify theft rings in US history was perpetrated by an employee who continued to use company codes for a year after he had left the company (Sullivan, 2002). In addition, remove or overwrite hard drives before retiring a computer.

Prepare and Distribute Written Policies

Written policies help ensure that everyone knows what is expected. Provide policies whenever a new computer account is established or requested. At a minimum, a company should develop and maintain an acceptable use policy, user responsibility policy, and response procedures to security incidents.

An acceptable use policy should include guidelines for personal use of company resources. The user responsibility policy should identify the user's responsibility concerning computer security. For example, who is responsible for updating software on a personal computer? If separate password guidelines do not exist, include these in the user responsibility policy. Incident response procedures for a suspected computer incident include: guidelines for administrators and users, detailed instructions about what to do, and who to contact. Be specific when writing policies; vague instructions are easier to ignore.

Hire Certified Security Professionals When Needed

Certain measures should be put in place at the network or company level. Many of these require a higher level of expertise. Company level measures include a hardware firewall, blocks at the e-mail server, a systematic method of warning users of new threats, access controls, encryption, secure communication, intrusion detection, and need to know access limitations.

CONCLUSION

Networked computers and electronic data storage make computer security a fundamental component of a company's survival. The lack of consistent and easily implemented security procedures can cause significant damage to companies of every size. Access to personal data stored on a computer can lead to identity thief for customers and employees. The loss of sensitive data can cause a company to lose its competitive edge. Destroyed data can be time consuming or impossible to reproduce. Security incidents can cause reputation damage, loss customers, or even liability. Companies that are unable or unwilling to hire certified security professionals often rely on non-security IT professionals for assistance. Using this checklist the non-security professional can assist the company in the critical areas of conducting risk analysis, performing vulnerability assessments, educating employees and developing computer security policies and procedures.

REFERENCES

Bidgolia, H. (2003). An Integrated Model For Improving Security Management In the E-Commerce Environment, *Journal of International Technology and Information Management, 12* (2), 119-134.

Campbell, K., Gordon, L., Loeb, M. & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market**,** *Journal of Computer Security, 11*, 431–448.

CERT® /CC Statistics. (2006). *Vulnerability Reports.* Retrieved June 8, 2006 from http://www.cert.org/stats/cert_stats.html.

Communications of the ACM. (2006). *The Year of Breaches*, *49* (3), 10.

Ernst & Young. (2004). *Global Information Security Survey 2004.* Retrieved June 8, 2006 from http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf.

Fratto, M. (2003). Security-- Suffering from security marketing overload? Remember: Securing your network from the core to the perimeter involves finding just the right combination of products. *Network Computing*, *Dec 16*, 33.

Internet Security Alliance. (2004). *Common Sense Guide to Cyber Security for Small Businesses, Recommended Actions for Information Security (1st Edition).* Retrieved June 8, 2006 from http://www.isalliance.org/.

Kavanagh, J. (2006). Study can unlock door to IT security riches. *Computer Weekly*, *May 2*, 40.

LeBlanc**,** C. & Stiller, E. (2004). Teaching computer security at a small college**.** *Technical Symposium on Computer Science Education, Proceedings of the 35th SIGCSE technical symposium on Computer science education. Computer Security Session, 36* (1), 407–411.

Mercuri, R. (2003). Analyzing Security Costs. *Communications of the ACM*, *46* (6), 15-18.

Mitchell, R. (2006). Why Good Technologists Are Hard to Find**.** Computerworld, *40* (12), 32-32.

National Security Agency. (2006). Centers of Academic Excellence. Retrieved July 11, 2006 from http://www.nsa.gov/ia/academia/CAE.pdf.

Streff, K. & Zhou, Z. (2006). Developing and enhancing a computer and network security curriculum. *Journal of Computing Sciences in Colleges***,** *21* (3), 4–18.

Sullivan, B. (2002, November 25). Huge identity theft ring busted. MSNBC. Retrieved June 8, 2006 from http://msnbc.msn.com/id/3078518/ .

Summerfield, B. (2005). Marketing IT Careers to Youth. *Certification Magazine*, *7* (9), 42-42.

U.S. Secret Service & CERT Coordination Center. (2004). *2004 E-Crime Watch – Survey Results*. *CSO*. Retrieved June 8, 2006 from http://www.csoonline.com/releases/ecrimewatch04.pdf.

Wagner, C. (2006). Information Security's Biggest Enemy. *Futurist, 40* (4), 11.