Vulnerability Management – A Guide to Managing Internal and External Threats

By: Johnny Leung

Professor Mike Shaw

Spring 2008 BADM 458

Abstract: As the information technology becomes easier use and implement for business, it becomes easier for intruders, both within and outside the firm, to steal and use that information for personal gain. Firms should have a vulnerability management program so that they can avoid various losses due to a breach in security. This paper will give an overview of the NIST Special Publication 800-40 v2 framework and gives several recommendations as to how to manage internal and external threats.

Introduction

As technology improves, firms are using IT as an essential part of their business. IT can help business be more efficient internally with various applications and infrastructure. It can also help the business externally by making it easier to conduct business through various methods such as the ability for clients to order products online. With these advances in IT, people's lives are made easier and firms are able to tap into markets that weren't available before. This convenience does come at a price though. Hackers and other cyber criminals look for weaknesses in a company's IT infrastructure and attack it in various ways. The effects of these attacks could be harmless if the person does not do anything with the findings; however, if the criminal uses the information that was obtained, the losses to the company could be tremendous. There can be internal threats as well. For example, a careless employee could accidentally leak company information to people who should not have access to the data. Much like external threats, internal ones could cause tremendous damage as well. That is why it is important to secure a company's IT infrastructure from threats, both internal and external. The process of identifying and remediation of IT risks based on the costs and benefits associated with it is called vulnerability management.

The Importance of Vulnerability Management

It is very important for companies to manage their vulnerabilities. Government

regulations, risk of financial repercussions as well as a damaged reputation create a need for companies to try to monitor their IT activities for weaknesses and remedy them. The amount of government regulations that a firm is subjected to varies by industry. For example, the healthcare industry is subjected to the Health Insurance Portability and Accountability Act[1] (HIPPA) which requires healthcare firms to protect personal health information such as health status, payment for healthcare, and provisions of healthcare of a patient. Health firms found in violation of HIPPA could be fined for each record lost. Another popular example would be the Family Educational Rights and Privacy Act (FERPA)[2] which protects the privacy of a student's education records. Institutions that violate this could lose federal funding.

The most important government regulation that public firms face today is the Sarbanes-Oxley Act of 2002. The Sarbanes-Oxley Act was a reaction to the multitude of accounting scandals that plagued the United States in the early 21st century. This new act required stricter accountability of the various executive positions in stating the financial status of the firm. Penalties for misrepresenting data could results in both jail time and hefty fines.[3] Section 404 in particular deals with the assessment of internal controls. Since many firms use IT in order to generate their financial statements, adequate care is needed so that these statements

[1] More information concerning HIPPA can be found at http://www.hhs.gov/ocr/hipaa/
[2] More information concerning FERPA can be found at http://www.ed.gov/policy/gen/guid/fpco/index.html
[3]

are generated in an accurate manner. If these systems are vulnerable to unauthorized changes or are used improperly, the statements generated will be inaccurate which could lead to jail time and fines. The desire for the chief officers to avoid the negative effects implemented by Sarbanes-Oxley is one reason firms would want to make sure their firm's vulnerabilities are managed and addressed accordingly.

Reputation and financial losses is another reason firms would want to make sure their firm's IT is secure. Firms that have their customer information leaked faces lost of customer trust, lost sales, and other fees associated with recovering such an incident (i.e. mailings to clients saying their personal information is compromised.) According to the 12th annual computer crime and security survey sponsored by CSI and the FBI[4], the average losses per respondent (194) were 345 thousand dollars. However, the losses could be a lot higher; TJX Companies had to pay over $40.9 million to Visa issuing banks because of a security breach in its transaction processing network. This breach compromised 45.6 million credit and debit card records and those cards had to be replaced by the banks. In sum, TJX estimates that the cost of the breach will total $156 million dollars through fiscal year 2009. This large sum, although not typical, represents the financial harm that a security breach could cause to a company that did not take proper precautions in managing their vulnerabilities.

[4] Full report can be found at http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

Aside from enormous financial losses, damage to a firm's reputation is also one of the negative consequences if customer or employee data is lost. According to the CSI study, 26% of the 196 respondents do not report intrusions to law enforcement because they believe that the negative publicity created would be bad for the firm's image[5] and ultimately their bottom line. Employees would probably not feel as secure working in a firm if their data is insecure. For example, a laptop was stolen from a Forrester Research employee. Within this laptop were names, addresses, and social security of an unknown number of past and present employees.[6] Although the hard disk is password protected, it was not encrypted. If this theft was a selected attack, the criminal could use one of many methods to bypass this password protection and steal the data for personal gain. Even though Forrester is providing a full year of credit monitoring (which appears to be standard compensation for stolen company records) and $25,000 identity theft insurance, it can only partially heal the loss of trust between employer and employee.

Cases like the ones mentioned for Forrester and TJX are not uncommon in the United States. According to the CSI report, 46% of the 487 respondents reported that their firm experienced a security incident in the past 12 months[7]. That is why it is important for management to monitor and remediate any sort of vulnerabilities and other IT threats that might face the company either

[5] Richardson, Robert. CSI Survey 2007. Computer Security Institute. 2007. 20 Apr. 2008 <http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf>. 23

[6] Vaas, Lisa. "Forrester Loses Laptop Containing Personnel Data." EWeek. 05 Dec. 2007. Ziff Davis. 28 Apr. 2008 <http://www.eweek.com/c/a/Security/Forrester-Loses-Laptop-Containing-Personnel-Data>

[7]

now or in the future in order to avoid Government probes, loss of profits, and damaged reputations.

Framework for Vulnerability Management

It is important to manage vulnerabilities, but every firm has a different method as to how to manage it. There are several frameworks that CIOs and other top managers can take in order to manage their vulnerabilities. This section will give an overview of the NIST – Special Publication 800-40 v2 framework.

NIST is the National Institute of Standards and Technology; it is a non-regulatory agency under the U.S. Department of Commerce. NIST has several divisions that try to set standards in various fields. One of the divisions is the Computer Security Division. In November of 2005, they wrote a 75 page guide titled "Creating a Patch and Vulnerability Management Program.[8]" It seeks to "inform the reader about the technical solutions that are available for vulnerability remediation[9]" The paper is divided into three major sections: Patch and Vulnerability Management Process, Security Metrics for Patch and Vulnerability Management and Patch and Vulnerability Management Issues. It also gives out resources that readers can reference for further reading.

[8] More information concerning the NIST publication can be found at http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

[9] Mell, Peter, Tiffany Bergerson, and David Henning. Creating a Patch and Vulnerability Management Program. National Institute of Standards and Technology (NIST). Gaithersburg, MD: U.S. Department of Commerce, 2005. 18 Apr. 2008 <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>. Section 1-1

The Patch and Vulnerability Management outlines a 10 step process in order to create a solid management program.

Step 1: Create a patch and vulnerability group. – The organization should have a specific group devoted to the conduction of the steps outlined in this process. Members of this group should know about the firm's IT infrastructure as well as technical IT know-how such as firewall management and intrusion detection.

Step 2: Create an inventory of all information technology assets. – By creating an inventory of the hardware, operating systems, software and IT resources that are used within a firm, the patch and vulnerability group (PVG) can more effectively identify the scope of their activities. For example, they don't have to monitor patches or vulnerabilities that exist for programs that they don't have.

Step 3: Continuously monitor for vulnerabilities, remediations, and threats. – The PVG should continuously monitor the organization's IT systems for vulnerabilities, remediations to those vulnerabilities, and threats. Threats include viruses, Trojans, and exploit scripts – methods in which people could exploit vulnerabilities of a network. This is important because as time goes by, new threats arise and system administrators must patch their systems from those threats.

Step 4: Prioritize patch application and use phased developments as appropriate. – After

scanning for threats and vulnerabilities, the PVG must check how these will affect the firm. This is important as not every firm is the same. Some firms may need to leave some vulnerability un-patched due to the nature of business. Whereas another firm might fine it very important to patch the same vulnerability mentioned above. A company should also prioritize which machines to patch first to make sure the more important services are protected before less important ones.

Step 5: Test patches before deployment. – Before implementing a patch on a system, the PVG should test the effects of the patch. This is because a variety of things can go wrong with a new patch. This includes: New patch opens up new exploits; new patch might not work with current system configurations, and new patch might cause poor system performance.

Step 6: Deploy enterprise-wide automated patching solutions. – By automating these patches, systems can be patched faster and more efficient than manual application. It is also important that it is enterprise-wide since it ensures that there can be a uniform policy for easier administration. However, this might not be practical in organizations with large scopes since every division might have different needs.

Step 7: Create a remediation database. – The NIST suggests that the PVG group should create a database (usually included in enterprise patch management tools) so that administrators can see which patches remediate which vulnerabilities. Ideally, this database should also host these fixes as a backup source should internet be unavailable.

Step 8: Use automatically updating applications as appropriate. – Although it is important to apply patches only after it has been tested, non-crucial systems could be updated automatically. One example would be using windows' automated updated to update regular employee desktops.

Step 9: Verify that vulnerabilities have been remediated. – The PVG team should verify that the vulnerabilities are in fact remedied and the threats mitigated. They can do this by scanning the system for the vulnerability that was supposed to be patched. Another way they can check for this is by checking the documentation for the patch, making sure what is supposed to happen did happen.

Step 10: Train applicable staff on vulnerability monitoring and remediation techniques. – Although the main vulnerability management process will be handled by the AVG team, it is also important to train users of the machines to make sure they aren't exposed to threats through everyday usage.

These ten steps outlined in the article are summarized by Deron Grzetich of Sidley Austin into a cycle of four steps: Asset inventory, Scan/validate, Remediate, and report. Even though every firm is unique, these four steps should be common in its vulnerability management. Other than the NIST framework, ISO-17799 is another framework managers could use to implement their vulnerability management program. That standard advocates the four steps in the vulnerability management cycle as well.

Managing Internal Threats

While the NIST framework provides a guideline to manage vulnerabilities, it does not go into specifics as to how to manage various threats. So this section will provide some ways in which companies can manage internal threats; how to prevent company information from leaving because of an insider.

System administrators can setup access controls for various applications and systems in general. In the Ernst and Young presentation, Rich Castle described changes that can be made to the master data on Oracle so that the correct internal controls are in place. These controls ensure that only the relevant people can make changes as well as put controls on what kind of data could go into the fields. Required entries would also ensure that the numbers are calculated correctly. By having these controls in place, the chief officers can lower their financial risk – avoiding inaccurate reporting of financial reports.

Another control layer would be through access controls. By having access controls, an organization can ensure that only the proper people would have access to certain data. For example, payroll personnel should have access to employees' bank account numbers; whereas sales team should not. By having these controls in place, chances of information leak is lowered since fewer people "hold the key" to see that information.

Proper logging and authorization of events can also help in preventing losses due to an

insider. It can also help track who was responsible for an event should an abnormality show up. For the SPSS presentation, CIO Ron Markham remarks that access to their data has to be scheduled, authorized by him, granted access by security personnel, and person granted access must sign in and out. These visit logs are then checked once a month to ensure the accuracy of these logs. By having strict and vigorous controls that are policy based, well-documented and communicated, companies can protect themselves from unauthorized access. These logs can also enhance accountability of personnel in the event of a security breach.

The blockage of external resources is another method in which companies can restrict the outflow of information to outsiders. For example, with the popularity and convenience of instant messaging, people can easily message coworkers in order to collaborate without actually meeting. However, just as easy as they can communicate with insiders, they can communicate with outsiders. Monsanto CIO Mark Showers says that they have an internal IM system so that employees could communicate to each other worldwide with just a few steps and keeps outside conversations that might contain company information out of these instant messages.

Proper monitoring of IT use could help prevent the spread of viruses and other malicious attacks before they get to be a major problem. It can also ensure that no company secrets are leaked through email or other means. John Heller, Caterpillar's CIO says that their IT department monitors packets to look for abnormalities in their vast network of IT systems.

Should these anomalies arise, they can redress and prevent its spread more efficiently than if no monitoring takes place. Also by monitoring resources, you can make sure employees are not abusing network resources by using services such as Peer to Peer or Bit torrent; thus, encouraging work time productivity while keeping bandwidth costs low. According to the CSI survey, 59% of the 436 respondents reported inside abuse of net access were detected in 2007[10].

There are many other methods that exist for managing internal threats to the company, each company should assess the costs of the options and how it would benefit or undermine the company's overall strategy before choosing to implement these options.

Managing External Threats

Although internal threats are more dangerous since employees are more trusted and theoretically assess resources more readily than mere strangers. External threats should not be ignored. There are much more outsiders than insiders in terms of numbers and they can hinder operation just as insiders can. Therefore, it is very important for organizations to manage external threats so they can avoid the losses associated with compromised records.

One of the best ways to manage external threats is through education. There are a variety of threats that can be reduced with just mere education. Phishing[11] attacks and e-mail spoofs

[10] Richardson, Robert. CSI Survey 2007. Computer Security Institute. 2007. 20 Apr. 2008 <http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf>. 13 – Figure 14

[11] An email or website that looks to be from an authenticate source but is in fact created by a scammer in order to obtain personal information such as usernames and passwords to various accouts.

[12]are popular e-mail based threats. By educating users to check the headers for e-mail spoofs and verify the URL of the website before sending any personal or company information, a firm can prevent leaking information to scammers. This education is especially important for people who hold important information but do not need to be tech savvy to do their job; recruiting personnel for example might fall under this category. Employers could test their effectiveness of awareness training via several methods such as a mandatory test or conduct a social engineering test to see how many employees fall into the trap.

Aside from education, installing various standard applications could help reduce the chance and exposure to various threats. Anti-virus programs and firewalls have almost become requirements in a business - with 98 and 97 percents of the 486 respondents reporting they have those applications in place respectively[13]. Even so, 52% of 436 respondents reported to have been affected by viruses[14]. This could be because although an application is in place, it is not updated. This makes a case for the patch and vulnerability management group, who makes sure that these applications are up to date. More sophisticated applications could be used to further reduce the risks, such as implementing an intrusion detection system. Once again, depending on the organization and its needs, such measures might not be practical or possible to implement.

---

[12] Much like phishing attempts, spoofed emails attempt to obtain a user's information by faking a reliable source's email address.

[13] Richardson, Robert. CSI Survey 2007. Computer Security Institute. 2007. 20 Apr. 2008 <http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf>. 18 – Figure 19

[14] See footnote 10.

As outlined in the previous section, having a patch and vulnerability management group to perform the four steps in the vulnerability management cycle would also reduce the risk. This is because one of the first things an attacker would do is attempt to exploit threats that are well known. These well known vulnerabilities are often patched, without any sort of patch and vulnerability personnel, attackers could exploit these weaknesses that could've easily been avoided. The CSI survey mentions that 63% of the 484 respondents have a vulnerability management program. This number is small given the benefits such a group can provide.

Other solutions to reduce external threats can be done by are security audits by internal staff. By having these internal audits, the team can hopefully discover and remediate threats and vulnerabilities before hackers and cyber criminals can carry out those threats. One such method is through penetration testing. Penetration testing simulates an attack on an organization's systems and network; it checks if there are any system flaws, improperly configured systems, or otherwise weak systems. The types of penetration testing include "white box[15]" and "black box.[16]" Various methods that could be used for penetration testing could be through: DNS zone transfers[17], port scans[18], ping sweeps[19], SQL injections[20], and default password checks[21].

[15] White box penetration testing simulates an attack from an insider. This insider might know the network infrastructure, maybe some passwords and possibly the functions of the machines.
[16] Black box penetration testing simulates an attack from an outsider. This means that the testers would have no knowledge of the network's infrastructure and would have to try various methods.
[17] DNS zone transfers allow an intruder to check which machine are registered with the DNS and allows the intruder to have an easier time to hack into resources since all active machines will be listed. Organizations should configure their DNS servers to only relay this information to machines/systems that need it within the organization.
[18] Port scans is a scan of a machine's ports to see if it is opened/closed/filtered. Open ports allow a hacker to

Penetration programs such as Nessus[22] and eEye Retina[23] allows PVG teams to find these vulnerabilities without spending a large amount of resource by automating the process.

Conclusion

As the information age progresses and people are starting to use technology more and more in various ways, businesses are susceptible to an increasing amount of threats. These threats could cause significant financial losses and damaged reputations. Government regulations also gave an incentive for firms to enforce vigorous controls in order to make sure that their data is reliable and secure. They can manage these threats by outsiders by implementing a patch and vulnerability management framework such as the NIST special publication 800-40 v2. They can manage a large number of threats by educating their employees and implementing software such as virus scanners and firewalls. Also, by implementing various policy based, well-documented and communicated controls, firms can reduce chances of leakages due to employees.

---

execute various commands and possible gain access to restricted resources.

[19] Ping sweeps allow an intruder to identify which machines are active. Active machines can then be further examined for vulnerabilities to exploit. This can be remedied by turning off ping replies.

[20] SQL injections are exploits that can be very dangerous if entered data is not cleaned of escape characters and such. SQL injections can allow hackers to execute various code within the SQL server and allow further access into company data

[21] Hackers will often try default passwords for programs and routers first in order to gain access into an organization's system. These organizations can easily change the password when they implement certain hardware or services in order to guard against such actions.

[22] Nessus is free a vulnerability testing program developed by Tenable Network Security. It is considered one of the best programs to scan for vulnerabilities. Further information can be found at http://www.nessus.org/nessus/

[23] Retina is a pay to use vulnerability testing program developed by eEye Digital Security. Further information can be found at http://www.eeye.com/html/products/retina/index.html