University of Illinois at Urbana-Champaign

BADM 557
Enterprise IT Governance

Guide to Vulnerability Management for Small Companies

Andrew Tan

Table of Contents

List of Appendices

Abstract

Vulnerability management is a risk management discipline that addresses the dangers of IT systems. It can be defined as the regular auditing of hardware and software components in IT systems to discover and remediate weaknesses. Keeping the systems safe from rapidly evolving malicious intent is critical. A security breach on a company's IT systems can be devastating, causing unrecoverable financial and information loss as well as damage to the company's reputation, all of which are extremely difficult to recover from. While large companies have specialized IT teams and sophisticated tools dedicated to IT vulnerability management, small companies, with their limited resources, can ill-afford such luxuries. As a result, many small companies do not have any vulnerability management program in place. This guide seeks to enable small companies to establish and maintain a simple vulnerability management program.

1. Introduction

Motivation

Vulnerabilities can be introduced into a company's IT systems when it acquires products with known and unknown bugs and/or insecure default settings. Many vulnerabilities also occur because of misconfigurations by system administrators. Attacks on these weaknesses are increasing and can cause unrecoverable financial and information loss as well as severely damage a company's reputation. Managing the security of their IT systems has thus become a key concern for companies. Vulnerability management is a discipline that addresses the dangers of IT systems and can be defined as the regular auditing of IT hardware and software to discover and remediate weaknesses. While large companies have specialized teams and tools dedicated to vulnerability management, small companies, with their limited resources, are usually unable to do so. As a result, many small companies do not have even a basic vulnerability management program in place, thus putting their IT systems at extreme risks to attacks.

Purpose and Audience

This guide seeks to enable small companies to develop and implement a simple vulnerability management program and is intended for IT security managers who want to do so but do not know how to start.

Overview of the Vulnerability Management Program

The vulnerability management program consists of the following three phases:

1. *Risk Assessment:* The program starts with the Risk Assessment phase, where you will identify and prioritize the IT security risks present in your company.

2. *Risk Remediation:* Next, evaluate potential measures and implement the most appropriate measures to remediate the risks, starting with assets with the highest risk level first.

3. *Continual Prevention:* The program does not end with the implementation of the remediation measures. You need to put in place policies to ensure that the measures are adhered to and conduct the program regularly to ensure that your company's systems stay protected.

The following sections describe the steps you need to do to accomplish each phase successfully.

2. Risk Assessment

You cannot address all the IT risks that your company faces at the same time due to limited resources. You need to prioritize the risks so that you know which to focus on first. Use the following qualitative method to work out the prioritized list of risks your company faces.

Step 1 – Identify and Classify all IT Assets

You must first identify all the IT assets in your company. As a starting point, you can use the list in Appendix A, which lists the IT assets typically found in companies. Next, assign the assets to one of the following three classes – high business impact (HBI), moderate business impact (MBI) and low business impact (LBI).

High Business Impact (Rating 3): Impact on the confidentiality, integrity, or availability of these assets causes severe loss to the company. Confidentiality refers to being secure from unauthorized access, integrity refers to data accuracy and completeness, while availability is the state of the systems and data being ready for use at all times. Examples within the HBI class are highly sensitive business material (such as financial data and intellectual property), financial transaction data (such as credit card data), and authentication credentials (such as passwords).

Moderate Business Impact (Rating 2): Impact on the confidentiality, integrity, or availability of these assets causes moderate loss to the company. The loss does not constitute a severe impact but does disrupt normal functions to the extent that proactive measures are needed to minimize impact. Examples include internal business data, purchase order data and network designs.

Low Business Impact (Rating 1): Assets not falling into either the HBI or MBI are classified as LBI and have no special protection needs. These assets are usually public information where unauthorized disclosure would not result in financial loss or operational disruptions, such as materials on the company's Internet website and published press releases.

Step 2 – Identify Vulnerabilities

For each asset, work out its vulnerabilities by asking yourself "What are you afraid of or are trying to avoid, and how may it happen?" For example, a common vulnerability of financial data is theft by hackers breaking into financial systems because of the absence of protective firewalls. If you can, invest in a vulnerability scanner. Vulnerability scanners are the easiest and most popular tools for identifying known system vulnerabilities and the machines that contain the vulnerabilities. However, it is important to note that vulnerability scanning only uncovers technical vulnerabilities and hence should be used as a supplement to this step.

Step 3 – Estimate Asset Exposure and Exploitation Likelihood

For each vulnerability, estimate the asset exposure, which is defined as the extent of the potential damage to the asset if the vulnerability is exploited successfully. For simplicity, you can use the following three levels:

- *High exposure (Rating 3)*: Severe or complete loss of the asset
- *Moderate exposure (Rating 2)*: Limited or moderate loss
- *Low exposure (Rating 1)*: Minor or no loss

Next, estimate the likelihood of the vulnerability being exploited. Again, for simplicity, we consider three levels:

- *High likelihood (Rating 3)*: Likely, one or more expected within one year
- *Medium likelihood (Rating 2)*: Probable, expected within two to three years
- *Low likelihood (Rating 1)*: Not probable, not expected to occur within three years

Multiply all three ratings to obtain the risk level of the vulnerability. An example is given below:

Asset name	**Asset Class**	**Vulnerabilities (What are you afraid of or are trying to avoid, and how it may happen)**	**Asset Exposure**	**Exploitation Likelihood**	**Risk Level**
Financial data	3 HBI	Theft by hackers breaking into financial systems because of the absence of protective firewalls	3	3	3 x 3 x 3 = 27
		Theft by malicious employees downloading data into flash drives	3	2	3 x 3 x 2 = 18

Repeating the above steps for all vulnerabilities produces a list that you can rank in order of risk level. Note that you need not restrict yourself to just three levels of ratings each for the asset class, asset exposure and exploitation likelihood. You can have, say, four levels of ratings (1, 2, 3 and 4) for the exploitation likelihood if you wish. Nonetheless, the final risk level remains the product of all three ratings.

Clearly, you should focus on the risks with the highest risk level, and if resources permitting, risks in the lower levels. Within the highest risk level, you might want to further prioritize the risks to have a better idea on which are the ones you should handle first. If you want to do so, you need to estimate the potential cost of each risk.

Estimation of Potential Costs of Risks

Step 1 – Estimate Asset Worth. For each asset, estimate its worth by estimating its value (such as its physical value and annual revenue generated) and subtracting the costs associated with it from the value. Examples of the costs are its purchase cost, implementation cost and maintenance cost.

Step 2 – Estimate Exposure Factor (EF) and Annual Rate of Occurrence (ARO). The EF is the percentage of loss that a successfully exploited vulnerability could have on the asset, while the ARO is the number of times you expect the risk to occur in one year. If you feel that a risk may occur twice in a year, the ARO is two. If a risk may occur once every two years, the ARO is 0.5.

Step 3 – Calculate Annual Loss Expectancy (ALE) and Rank Risks According to the ALE. The ALE is the amount of money your company will lose in one year if nothing is done to mitigate the risk and is calculated by multiplying the asset worth with the EF and ARO.

Example: An asset is worth $10,000 and a fire results in damages worth about 25 percent of its value (EF = 0.25). If the probability of a fire happening is once in ten years (ARO = 0.1), then the ALE would be $10,000 x 0.25 x 0.1 = $250.

Note that the ALE is only a rough estimate due to the difficulties in estimating the asset worth, EF and ARO. Nonetheless, it does give you a qualitative figure that you can use to rank the risks within each risk level. By putting a value to how much damage a threat might cause, the ALE also provides a value that you can work with to budget what it will cost to deploy measures to protect against this type of damage. For example, if the ALE is $250, you would not want to spend more than this amount when deploying a measure to mitigate the risk.

3. Risk Remediation

You will now identify possible remediation measures, calculate the costs of the measures, and work with management to determine which measures to implement.

Types of Possible Measures

Measures can be divided into two types – operational and technological – and further divided into those that provide prevention and detection and recovery. Preventative measures keep a risk from being realized, while detection and recovery measures help a company to determine when a security breach has occurred and to resume normal operations thereafter.

Operational Measures

Operational measures define how people in the company should perform their duties and handle the company's IT assets. Preventative measures in this category include:

- *Clear responsibilities*. To ensure everyone understand their part in maintaining IT security.
- *Access and least privileges*. To ensure that everyone has only enough access to systems and data to effectively perform their duties and no more.
- *Incident response and business continuity plans*. To enable your company to quickly react to and recover from security breaches while minimizing their impact.
- *Documented plans*. To explain how the measures are implemented and to be maintained.
- *Disposal procedures*. To ensure that media used for storing sensitive data is degaussed before disposal.
- *Security training*. For everyone to know how to protect the company's IT assets.

- *De-provisioning procedures*. To ensure leaving personnel lose access immediately upon departure, and employees who transfer within the company have their access levels reviewed and changed if necessary.
- *Physical protection of assets*. Using physical means such as locks and biometric locks.
- *Emergency backup power*. To save systems from harm during power brownouts and blackouts, and ensure that systems are properly shut down to preserve data and transactions.

Detection and recovery measures in this category include:

- *Regular vulnerability management*. To continually assess and measure risks to your company's IT assets, and to verify the measures' effectiveness and efficacy.
- *Background investigations*. To check potential recruits and employees being considered for promotions to positions with a higher level of access to IT assets.
- *Rotation of duties*. To uncover and minimize malicious activities by employees with access to sensitive information.

Technological Measures

Technological measures include system architecture design, engineering, hardware and software. Preventative measures in this category include:

- *Authentication*. The process of validating the credentials of an employee, which requires that the employee making a transaction proves his or her identity. Common forms of credentials are smart cards, biometric data, and a combination of user names and passwords.
- *Nonrepudiation*. The need for undeniable proof that a user took a specific action such as transferring money or sending a message, so that the user cannot falsely deny that he or she performed that action.

- *Access measures*. The mechanism for limiting access to certain information based on a user's roles and responsibilities in the company.
- *Protected storage and communications*. The use of encryption to protect the integrity and confidentiality of information stored in storage media and transmitted over networks.
- *Removal of unwanted software*. Removing or uninstalling unwanted software eliminates the threats and vulnerabilities associated with the software.
- *Security Patch Installation*. Applying a security patch that modifies the software to remediate its vulnerabilities. Patching, when available, provides the simplest way to reduce risks.

Detection and recovery measures in this category include:

- *Audit systems*. To monitor and track system behavior that deviates from norms.
- *Antivirus programs*. To detect and respond to malicious software such as viruses and worms.
- *Integrity tools*. To determine whether unauthorized changes have been made to systems.

Selection and Implementation of Appropriate Measures

Once you have identified the potential measures, estimate their cost. This is important because some measures might be too costly to implement, or the cost is higher than the ALE and thus not cost effective. The main cost is the acquisition cost. Some measures have no acquisition cost. For example, deploying a new measure may merely involve enabling a previously unused feature on hardware that your company is already using. Other costs include the costs of deploying and maintaining the measure. Management must then review the proposed measures and select those with costs deemed acceptable. Once done, you need to implement the measures and thereafter verify that the measures have indeed mitigated the risks.

4. Continual Prevention

The vulnerability management program does not end with the implementation of measures to mitigate the risks. You need to establish and put in place a security policy to ensure that the measures are adhered to. The program is also not a once-off project. You have to conduct the program regularly to ensure that your company's systems stay protected.

Establishing an IT Security Policy

You need to establish an IT security policy to be endorsed by management and communicated to every employee in the company. The policy should specify in detail the measures that must be implemented and adhered to by everyone. You can use the sample given in Appendix B to develop the appropriate IT security policy for your company. Note that the sample security policy in Appendix B can also be modified into an IT security checklist for your company.

Reassessment of Assets and Risks

To be effective, vulnerability management must be an ongoing. You need to regularly verify that the implemented measures are providing the expected degree of protection. You should update the lists of assets, vulnerabilities and measures developed during the start of the program and focus only on the changes to your operational environment. If there has been no change to an asset since it was last reviewed, there is no point reviewing it again. Events that should draw close scrutiny include installation of new software or hardware. You should also stay alert for relevant changes that take place outside of your company by constantly reviewing vendor

websites for new security updates and monitoring third-party websites for information about new security research and announcements regarding security vulnerabilities. These types of changes may require you to take prompt action to protect your company from new or changing risks.

Conclusion

This guide has presented a simple approach that can assist you in your response to IT security risks that may challenge the success of your company's business. Now that you have read the guide, you are ready to start the process. If you would like to learn more about vulnerability management, two excellent references are given in Appendix C.

Appendix A: Common Information Systems Assets

This appendix lists IT assets commonly found in companies. It is provided as a reference list and a starting point to help you get underway. It is not comprehensive and will not represent all the assets present in your company. Thus, it is important that you customize the list accordingly.

Asset	Asset
Servers	Human resources data
Desktop computers	Financial data
Mobile computers	Marketing data
PDAs	Employee passwords
Server application software	Employee private cryptographic keys
End-user application software	Employee biometric identifiers
Development tools	Employee personal contact data
Routers	Supplier contract data
Network switches	Supplier financial data
Fax machines	Supplier contact data
PBXs	Supplier cryptographic keys
Removable media (DVDs, portable drives etc.)	Supplier purchase order data
Uninterruptible power supplies	Customer credit card data
Source code	Customer contact data
Network infrastructure design	Customer purchase order data
Computer system cryptographic keys	Published press releases
Smart cards	Training materials
IT Intellectual property	Internet website materials
IT Strategic plans	Annual reports

Appendix B: Sample IT Security Policy

This appendix provides a sample that you can use to develop your company's IT security policies. It is provided as a reference to help you get underway. It is not comprehensive and thus it is important that you customize it according to your company's unique environment.

Section 1 – IT Security Policies

1.1 IT security policies must be formally documented, disseminated to all users and reviewed at least once a year and updated as needed.

1.2 The roles and responsibilities for IT security must be clearly defined within the company.

1.3 IT security awareness and training programs must be in place for all users.

1.4 Employees must sign an agreement verifying they have read and understood the security policies and procedures

1.5 Background investigations must be performed on all new recruits and employees with access to sensitive data.

Section 2 – Systems and Network Security

2.1 Default vendor security settings, accounts and passwords must be changed on systems before putting the systems into production.

2.2 Production systems must be hardened by removing all unnecessary services and protocols installed by the default vendor configuration.

2.3 Secure, encrypted communications must be used for remote administration of production systems and applications.

2.4 All router, switches, wireless access points, and firewall configurations must be secured and conform to documented security standards.

2.5 All computers must have anti-virus software installed.

2.6 Web servers located on a publicly reachable network segment must be separated from the internal network by a firewall.

2.7 Customer financial data (such as credit card information) stored in a database must be located on the internal network and protected by a firewall.

2.8 A firewall must be used to protect the network and limit traffic to only that which is required to conduct business.

2.9 Changes to the firewall must require authorization and are the changes must be logged.

Section 3 – Data Storage and Security

3.1 All sensitive data must be stored securely encrypted.

3.2 Access to sensitive data must be restricted to users on a need-to-know basis

3.3 Sensitive data must be securely disposed of when no longer needed (for example, by shredding and/or burning, or by degaussing the storage media).

3.4 All but the last four digits of the account number must be masked when displaying customers' credit card account information.

3.5 Encryption must be used in the transmission of sensitive data via e-mail.

3.6 Equipment (such as servers, workstations and hard drives) and media containing sensitive data must be properly inventoried, securely stored and physically protected against unauthorized access.

3.7 Procedures must be in place to handle the secure distribution and disposal of backup media and other media containing sensitive data.

Section 4 – Access Measures

4.1 All users must be required to authenticate using, at a minimum, a unique username and password.

4.2 If employees, administrators, or third parties access the network remotely, remote access software (such as PCAnywhere) must be configured with a unique username and password and encryption and other security features must be turned on.

4.3 When an employee leaves the company, that employee's user accounts and passwords must be revoked immediately.

4.4 All user accounts must be reviewed on a regular basis to ensure that malicious, out-of-date or unknown accounts do not exist.

4.5 Non-consumer accounts that are not used for a lengthy amount of time (inactive accounts) must be automatically disabled in the system after a pre-defined period.

4.6 Users must change their passwords on a pre-defined regular basis.

4.7 There must be a password policy that enforces the use of strong passwords and prevents the resubmission of previously used passwords.

4.8 There must be an account-lockout mechanism that blocks a malicious user from obtaining access to an account by multiple password retries or brute force.

4.9 All access to cardholder data, including root/administration access must be logged.

4.10 Access measure logs must contain information on successful and unsuccessful login attempts and access to audit logs.

4.11 All critical system clocks and times must be synchronized, and logs must include date and time stamp.

4.12 The firewall, router, wireless access points, and authentication server logs must be regularly reviewed for unauthorized traffic.

4.13 Audit logs must be regularly backed up, secured, and retained for at least three months online and one-year offline for all critical systems.

Appendix C: Further References

The following two guides are excellent references in helping you know more about the vulnerability management process.

1. "Security Risk Management Guide" by Microsoft

http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/default.mspx

Microsoft's 129-page Security Risk Management Guide explains in detail how to conduct a successful security risk management project. It references many industry accepted standards for managing security risks, incorporates real-world experiences from Microsoft IT and also includes input from Microsoft customers and partners. The process offers a combination of various approaches including pure quantitative analysis, return on security investment (ROSI) analysis, qualitative analysis, and best practice approaches.

2. "Risk Management Guide for Information Technology Systems" by the National Institute of Standards and Technology (NIST)

http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

This 55-guide from the NIST provides a foundation for the development of an effective risk management program. It contains both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems and provides information on the selection of cost-effective security measures.