4 Threats and Vulnerabilities: A Brief Overview

A vulnerability is a weakness in a system, system security procedure, internal controls, or implementation that could be exploited by a threat source.[6] Vulnerabilities leave systems susceptible to a multitude of activities that can result in significant and sometimes irreversible losses to an individual, group, or organization. These losses can range from a single damaged file on a laptop computer or mobile device to entire databases at an operations center being compromised. With the right tools and knowledge, an adversary can exploit system vulnerabilities and gain access to the information stored on them. The damage inflicted on compromised systems can vary depending on the threat source.

A threat source can be adversarial or non-adversarial. Adversarial threat sources are individuals, groups, organizations, or entities that seek to exploit an organization's dependence on cyber resources. Even employees, privileged users, and trusted users have been known to defraud organizational systems. Non-adversarial threat sources refer to natural disasters or erroneous actions taken by individuals in the course of executing their everyday responsibilities.

If the system is vulnerable, threat sources can lead to threat events. A threat event is an incident or situation that could potentially cause undesirable consequences or impacts. An example of a threat source leading to a threat event is a hacker installing a keystroke monitor on an organizational system. The damage that threat events may cause on systems varies considerably. Some affect the confidentiality and integrity of the information stored in a system while others only affect the availability of the system. For more information on threat sources and threat events, see NIST SP 800-30.

This chapter presents a broad overview of the environment in which systems operate today and may prove valuable to organizations seeking a better understanding of specific threat environment. The list provided herein is not intended to be an all-inclusive list. The scope of the information provided here may be too broad, and threats against specific systems could be quite different from what is discussed in this chapter.

In order to protect a system from risk and to implement the most cost-effective security measures, system owners, managers, and users need to know and understand the vulnerabilities of the system as well as the threat sources and events that may exploit the vulnerabilities. When determining the appropriate response to a discovered vulnerability, care should be taken to minimize the expenditure of resources on vulnerabilities where little or no threat is present. See Chapter 6*, Information Security Risk Management*, for more detailed information on how threats, vulnerabilities, safeguard selection, and risk response are related.

4.1 Examples of Adversarial Threat Sources and Events

The previous section defined threat sources and threat events. This section provides several examples of each followed by a description.

[6] Threat Source – The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.

4.1.1 Fraud and Theft

Systems can be exploited for fraud and theft by "automating" traditional methods of fraud or by utilizing new methods. System fraud and theft can be committed by insiders (i.e. authorized users) and outsiders. Authorized system administrators and users with access to and familiarity with the system (e.g., resources it controls, flaws) are often responsible for fraud. An organization's former employees also pose a threat given their knowledge of the organization's operations particularly if access is not terminated promptly.

Financial gain is one of the chief motivators behind fraud and theft, but financial systems are not the only systems at risk. There are several techniques that an individual can use to gather information they would otherwise not have had access to. Some of these techniques include:

- *Social Media.* The ubiquity of social media (e.g., Facebook, Twitter, LinkedIn) has allowed cyber criminals to exploit the platform to conduct targeted attacks. Using easily-made, fake, and unverified social media accounts, cyber criminals can impersonate co-workers, customer service representatives, or other trusted individuals in order to send links to malicious code that steal personal or sensitive organizational information. Social media exacerbates the ongoing issue of fraud, and organizations should see it as a serious concern when implementing systems. Social media accounts provide a means of gathering contact information, interests, and personal connections of a targeted individual which in turn can be used to conduct a social engineering attack.
- *Social Engineering.* Social engineering, in the context of information security, is a technique that relies heavily on human interaction to influence an individual to violate security protocol and encourages the individual to divulge confidential information. These types of attacks are commonly committed via phone or online. Attacks perpetrated over the phone are the most basic social engineering attacks being committed. For example, an attacker may mislead a company into believing the attacker is an existing customer and have that company divulge information about that customer. Online, this technique is called phishing–an email-based attack intended to trick individuals into performing an action beneficial to the attacker (e.g., clicking a link or divulging personal information). Social engineering online attacks can also be accomplished by using attachments that contain malicious code, which target an individual's address book. The information obtained allows the attacker to send malicious code to all the contacts in the victim's address book, propagating the damage of the initial attack.
- *Advanced Persistent Threat (APT).* An advanced persistent threat is a long-term intrusion that attempts to gain access to specific data and information. Instead of trying to cause damage, APT attacks are designed to harvest information from the network or target. Some APT attacks can be so complicated that to remain undetected by intrusion detection systems (IDSs) in the network, they require around the clock rewriting of the code by an administrator. Once enough information about the network has been gathered, the attacker can create a back door, which is a way of bypassing security mechanisms in systems, and gain undetected access to the network. An external command and control system is then used by the attacker to continuously monitor the system to extract information.

4.1.2 Insider Threat

Employees can represent an insider threat to an organization given their familiarity with the employer's systems and applications as well as what actions may cause the most damage, mischief, or disorder. Employee sabotage—often instigated by knowledge or threat of termination—is a critical issue for organizations and their systems. In an effort to mitigate the potential damage caused by employee sabotage, the terminated employee's access to IT infrastructure should be immediately disabled, and the individual should be escorted off company premises.

Examples of system-related employee sabotage include, but are not limited to:

- Destroying hardware or facilities;
- Planting malicious code that destroys programs or data;
- Entering data incorrectly, holding data, or deleting data;
- Crashing systems; and
- Changing administrative passwords to prevent system access.

4.1.3 Malicious Hacker

Malicious hacker is a term used to describe an individual or group who use an understanding of systems, networking, and programming to illegally access systems, cause damage, or steal information. Understanding the motivation that drives a malicious hacker can help an organization implement the proper security controls to prevent the likelihood of a system breach. Malicious hacker is a broad category of adversarial threats that can be broken out into smaller categories depending on the specific actions or intent of the malicious hacker. Some of the sub-categories adapted from NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security,* include:

- *Attackers.* Attackers break into networks for the thrill and challenge or for bragging rights in the attacker community. While remote hacking once required considerable skills or computer knowledge, attackers can now download attack scripts and protocols from the Internet and launch them against victim sites. These attack tools have become both more sophisticated and easier to use. In some cases, attackers do not have the requisite expertise to threaten difficult targets such as critical government networks. Nevertheless, the worldwide population of attackers poses a relatively high threat of isolated or brief disruptions that could cause serious damage to business or infrastructure.
- *Bot-Network Operators.* Bot-network operators assume control of multiple systems to coordinate attacks and distribute phishing schemes, spam, and malicious code. The services of compromised systems and networks can be found in underground markets online (e.g., purchasing a denial of service attack, using servers to relay spam or phishing attacks).
- *Criminal Groups*. Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups use spam, phishing, and spyware/malicious code to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose threats to the Nation based on their ability to conduct industrial espionage, large-scale monetary theft, and the recruitment of new attackers. Some criminal groups may try to extort money from an organization by threatening a cyber-

attack or by encrypting and disrupting its systems for ransom. Extortion or ransom attacks have disrupted numerous businesses and cost significant resources and planning to mitigate. Without effective backup plans and restoration procedures, many businesses have resorted to paying costly ransoms to restore their encrypted systems.

- *Foreign Intelligence Services*. Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrines, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power – impacts that could affect the daily lives of U.S. citizens.

  In some instances, threats posed by foreign government intelligence services may be present. In addition to possible economic espionage, foreign intelligence services may target unclassified systems to further their intelligence missions. Some unclassified information that may be of interest includes travel plans of senior officials, civil defense and emergency preparedness, manufacturing technologies, satellite data, personnel and payroll data, and law enforcement, investigative, and security files.

- *Phishers*. Phishers are individuals or small groups that execute phishing schemes to steal identities or information for monetary gain. Phishers may also use spam and spyware/malicious code to accomplish their objectives.

- *Spammers*. Spammers are individuals or organizations that distribute unsolicited e-mail with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malicious code, or attack organizations (e.g., DoS).

- *Spyware/Malicious Code Authors*. Individuals or organizations who maliciously carry out attacks against users by producing and distributing spyware and malicious code. Destructive computer viruses and worms that have harmed files and hard drives include the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.

- *Terrorists*. Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malicious code to generate funds or gather sensitive information. They may also attack one target to divert attention or resources from other targets.

- *Industrial Spies*. Industrial espionage seeks to acquire intellectual property and know-how using clandestine methods.

4.1.4 Malicious Code

Malicious code refers to viruses, Trojan horses, worms, logic bombs, and any other software created for the purpose of attacking a platform.

- *Virus*. A code segment that replicates by attaching copies of itself to existing executables. The new copy of the virus is executed when a user executes the new host program. The virus may include an additional "payload" that triggers when specific conditions are met.

- *Trojan Horse*. A program that performs a desired task, but that also includes unexpected and undesirable functions. For example, consider an editing program for a multiuser system. This program could be modified to randomly and unexpectedly delete a user's files each time they perform a useful function (e.g., editing).
- *Worm*. A self-replicating program that is self-contained and does not require a host program or user intervention. Worms commonly use network services to propagate to other host systems.
- *Logic Bomb*. This type of malicious code is a set of instructions secretly and intentionally inserted into a program or software system to carry out a malicious function at a predisposed time and date or when a specific condition is met.
- *Ransomware.* Is a type of malicious code that blocks or limits access to a system by locking the entire screen or by locking down or encrypting specific files until a ransom is paid. There are two different types of ransomware attacks—encryptors and lockers. Encryptors block (encrypt) system files and demand a payment to unblock (or decrypt) those files. Encryptors, or crypto-ransomware, are the most common and most worrisome (e.g., WannaCry). Lockers are designed to lock users out of operating systems. The user still has access to the device and other files, but in order to unlock the infected computer, the user is asked to pay a ransom. To make matters worse, even if the user pays the ransom, there is no guarantee that the attacker will actually provide the decryption key or unlock the infected system.

4.2 Examples of Non-Adversarial Threat Sources and Events

4.2.1 Errors and Omissions

Errors and omissions can be inadvertently caused by system operators who process hundreds of transactions daily or by users who create and edit data on organizational systems. These errors and omissions can degrade data and system integrity. Software applications, regardless of the level of sophistication, are not capable of detecting all types of input errors and omissions. Therefore, it is the responsibility of the organization to establish a sound awareness and training program to reduce the number and severity of errors and omissions.

Errors by users, system operators, or programmers may occur throughout the life cycle of a system and may directly or indirectly contribute to security problems. In some cases, the error is a threat, such as a data entry error or a programming error that crashes a system. In other cases, the errors cause vulnerabilities. Programming and development errors, often referred to as "bugs," can range from benign to catastrophic.

4.2.2 Loss of Physical and Infrastructure Support

The loss of supporting infrastructure includes power failures (e.g., outages, spikes, brownouts), loss of communications, water outages and leaks, sewer malfunctions, disruption of transportation services, fire, flood, civil unrest, and strikes. A loss of supporting infrastructure often results in system downtime in unexpected ways. For example, employees may not be able to get to work during a winter storm, although the systems at the work site may be functioning as normal. Additional information can be found in section 10.11, *Physical and Environmental Protection.*

4.2.3 Impacts to Personal Privacy of Information Sharing

The accumulation of vast amounts of personally identifiable information by government and private organizations has created numerous opportunities for individuals to experience privacy problems as a byproduct or unintended consequence of a breach in security. For example, migrating information to a cloud service provider has become a viable option that many individuals and organizations utilize. The ease of accessing data from the cloud has made it a more attractive solution for long term storage. Everything that is written, uploaded, or posted is stored in a cloud system that individuals do not control. However, unbeknownst to the cloud service user, personal information can be accessed by a stranger with the right tools and technical skill sets.

Individuals' voluntarily sharing PII through social media has also contributed to new threats that allow malicious hackers to use that information for social engineering or to bypass common authentication measures. Linking all this information and technology together, malicious hackers have the ability to create accounts using someone else's information or gain access to networks.

Organizations may share information about cyber threats that includes PII. These disclosures could lead to unanticipated uses of such information, including surveillance or other law enforcement actions.

8 Security Considerations in System Support and Operations

System support and operations refers to all aspects involved in running a system. This includes both system administration and tasks external to the system that support its operation (e.g., maintaining documentation). It does not include system planning or design. The support and operation of any system—from a three-person local area network to a worldwide application serving thousands of users—is critical to maintaining the security of a system. Support and operations are routine activities that enable systems to function correctly. These include fixing software or hardware problems, installing and maintaining software, and helping users resolve problems.

The failure to consider security as part of the support and operations of systems, can be detrimental to the organization. Information security system literature includes examples of how organizations undermined their often-expensive security measures with poor documentation, old user accounts, conflicting software, or poor control of maintenance accounts. An organization's policies and procedures often fail to address many of these important issues. Some major categories include:

- User support;
- Software support;
- Configuration management;
- Backups;
- Media controls;
- Documentation; and
- Maintenance

Even though the goals of system support and operation and information security are closely related, there is a distinction between the two. The primary goal of system support and operations is the continued and correct operation of the system, whereas the information security goals of a system include confidentiality, availability, and integrity.

This chapter addresses the support and operations activities directly related to security. Every control discussed in this publication relies, in one way or another, on system support and operations. However, this chapter focuses on areas not covered in other chapters. For example, operations personnel normally create user accounts on the system. This topic is covered in section 10.7. Similarly, the input from support and operations staff to the security awareness and training program is covered in section 10.2.

8.1 User Support

In many organizations, user support takes place through a service desk. Service desks can support an entire organization, a subunit, a specific system, or a combination of these. For smaller systems, the system administrator typically provides direct user support. Experienced users provide informal user support on most systems. It is not unusual for user support to be closely linked to the organization's ability to handle incident response.

An important security consideration for user support personnel is being able to recognize which problems (brought to their attention by users) are security-related. For example, users' inability to log on to a system may result from the disabling of their accounts due to too many failed

access attempts. This could indicate the presence of malicious users trying to guess a user's password.

In general, system support and operations staff need to be able to identify security problems, respond accordingly, and inform appropriate individuals. A wide range of possible security problems may exist; some will be internal to custom applications, while others apply to off-the-shelf products. Additionally, problems can be software- or hardware-based.

The more responsive and knowledgeable system support and operation staff personnel are, the less user support will be provided informally. The support other users provide can be valuable, but they may not be aware of all the issues across the organization or how they are related.

8.2 Software Support

Software is the heart of an organization's system operations, whatever the size and complexity of the system. Therefore, it is essential that software function correctly and be protected from corruption. There are many elements of software support.

The first element is controlling what software is used on a system. If users or systems personnel can install and execute any software on a system, the system is more vulnerable to viruses, unexpected software interactions, and software that may subvert or bypass security controls. One method of controlling software is to inspect or test software before it is installed (e.g., determine compatibility with custom applications, identify other unforeseen interactions). This can apply to new software packages, upgrades, off-the-shelf products, or to custom software, as deemed appropriate. In addition to controlling the installation and execution of new software, organizations also oversee the configuration and use of powerful system utilities. System utilities can compromise the integrity of operating systems and logical access controls.

The second element in software support can be to ensure that software has not been modified without proper authorization. This involves the protection of software and backup copies and can be done with a combination of logical and physical access controls.

Many organizations also include a program to ensure that software is properly licensed, as required. For example, an organization may audit systems for illegal copies of copyrighted software. This problem is primarily associated with user systems (or devices), but can apply to any type of system.

8.3 Configuration Management

Closely related to software support is configuration management—the process of tracking and approving changes to the system. Configuration management can be formal or informal and normally addresses hardware, software, networking, and other changes. The primary security goal of configuration management is to ensure that changes to the system do not unintentionally or unknowingly diminish security. Some of the methods discussed under software support (e.g., such as inspecting and testing software changes) can be used. Chapter 7 discusses other methods.

Note that the security goal is to know what changes occur, not to prevent security from being changed. There may be circumstances under which reducing security is deemed an acceptable risk due to the need to accomplish the mission. In such cases, the decrease in security is based on a decision by the authorizing official who considered all appropriate factors. Furthermore, the resulting increase in risk is monitored on an ongoing basis.

A second security goal of configuration management is to ensure that changes to the system are reflected in other documentation, such as the contingency plan. If the change is major, it may be necessary to reanalyze some or all of the security of the system. This is discussed in section 10.15.

8.4 Backups

Support and operations personnel and sometimes users back up software and data. This function is critical to contingency planning. The frequency of backups depends on how often data changes and how important those changes are. Consult with system administrators to determine what backup schedule is appropriate. Also, it is important to test that backup copies are actually usable. Finally, store backups securely (discussed below).

8.5 Media Controls

Media controls include a variety of measures to provide physical and environmental protection and accountability for digital and non-digital media. Examples of digital media include diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Examples of non-digital media include paper and microfilm. From a security perspective, media controls are designed to prevent the loss of confidentiality, integrity, or availability of information, including data or software, when stored or disseminated outside of the system. This can include storage of information before it is input into the system and after it is output.

The extent of media control depends on many factors, including the type of data, the quantity of media, and the nature of the user environment. Physical and environmental protection is used to prevent unauthorized individuals from accessing the media and protects against such factors as heat, cold, or harmful magnetic fields. When necessary, logging the use of individual media (e.g., a tape cartridge) provides detailed accountability—so that the organizations may hold authorized individuals responsible for their actions. For more information on media protection, see section 10.10.

8.6 Documentation

Documentation of all aspects of system support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations are performed correctly and efficiently.

The specific security implementation details of a system are also documented. This includes many types of documentation, such as security plans, contingency plans, risk analyses, and security policies and procedures. Much of this information, particularly risk and threat analyses, has to be protected against unauthorized disclosure. Security documentation also needs to be both current and accessible. Accessibility takes special factors into consideration such as the need to find the contingency plan during a disaster.

Some security documentation may need to be designed to fulfill the needs of different system roles. For this reason, many organizations separate documentation into policy and procedures. A security procedures manual may be written to inform system users on how to do their jobs

securely. For systems operations and support staff, a security procedures manual may address a wide variety of technical and operational concerns in considerable detail.

8.7 Maintenance

System maintenance requires either physical or logical access to the system. Support and operations staff, hardware or software vendors, or third-party service providers may maintain a system. Maintenance may be performed on-site or remotely via communications connections. It may also be necessary to move equipment to a repair site for maintenance. If someone who does not typically have access to the system performs maintenance, then a security vulnerability is introduced.

In some circumstances, it may be necessary to take additional precautions (e.g., background investigation of service personnel) to prevent some problems such as "snooping around" the physical area. However, once someone has access to the system, it is very difficult for supervision to prevent damage done through the maintenance process.

Many systems provide maintenance accounts. These special login accounts are normally preconfigured at the factory with pre-set, widely-known passwords. It is critical to change these passwords or otherwise limit access to the accounts. Develop procedures to ensure that only authorized maintenance personnel have access to the preconfigured accounts. If the account is to be used remotely, authentication of the maintenance provider can be performed using call-back confirmation. This helps ensure that remote diagnostic activities actually originate from an established phone number at the vendor's site. Other helpful techniques include encryption and decryption of diagnostic communications, strong identification and authentication techniques such as tokens, and remote disconnect verification.

Manufacturers of larger systems and third-party providers may offer more diagnostic and support services, and larger systems may have diagnostic ports. It is critical to ensure that these ports are only used by authorized personnel, cannot be accessed by malicious users, and are only active when required.

8.8 Interdependencies

There are support and operations components in most of the controls discussed in this publication, such as:

- *Personnel*. Most support and operations staff have special access to the system. Some organizations conduct background checks on individuals in these positions. (See section 10.13);

- *Incident Handling.* Support and operations may include an organization's incident handling staff. Even if they are separate organizations, they need to work together to recognize and respond to incidents. (See section 10.8);

- *Contingency Planning*. Support and operations normally provides technical input to contingency planning and carries out the activities of creating backups, updating documentation, and practicing responses to contingencies. (See section 10.6);

- *Security Awareness, Training, and Education*. Support and operations staff are trained in security procedures and aware of the importance of security. In addition, they provide technical expertise needed to teach users how to secure their systems. (See section 10.2);

- *Physical and Environmental*. Support and operations staff often control the immediate physical area around the system. (See section 10.11);

- *Technical Controls*. The technical controls are installed, maintained, and used by support and operations staff. They create the user accounts, add users to access control lists, review audit logs for unusual activity, control bulk encryption over telecommunications links, and perform the countless operational tasks needed to use technical controls effectively. In addition, support and operations staff provide needed input to the selection of controls based on their knowledge of system capabilities and operational constraints. (See Chapter 10); and

- *Assurance*. Support and operations staff ensure that changes to a system do not introduce security vulnerabilities by using assurance methods to evaluate or test the changes and their effects on the system. Operational assurance is normally performed by support and operations staff. (See Chapter 7).

8.9 Cost Considerations

The cost of ensuring adequate security in day-to-day support and operations is largely dependent upon the size and characteristics of the operating environment and the nature of the processing being performed. It may not be necessary to hire additional support and operations security specialists. If sufficient support personnel are already available, it is important that they be trained in the security aspects of their assigned jobs. Initial and ongoing training is a cost of successfully incorporating security measures into support and operations activities.

Another cost is that associated with creating and updating documentation to ensure that security concerns are appropriately reflected in support and operations policies, procedures, and duties.