Key Elements of a Threat and Vulnerability Management Program

By John P. Pironti, CISA, CISM, CISSP, ISSAP, ISSMP

With the advent of web-enabled and Internet-connected services, organizations can now provide clients unprecedented access to information that makes it easier to do business and enhances the user experience immeasurably. However, this new level of access has also inadvertently empowered potential adversaries to exploit information without specific knowledge of or physical access to the organization. Enterprises and governments, in effect, are leaving the front and back doors and all those in between unlocked, creating vulnerabilities and exposing themselves to threats they never anticipated—worms, viruses, Trojan horses, "low and slow" information thefts, and many more.

The best way to ensure a fighting chance of discovering and defeating information exploitation and theft is to take a disciplined, programmatic approach to discovering and mitigating threats and vulnerabilities.

Emerging Threats

The adversary community is constantly maturing and refining its capabilities. The traditional, widespread, single-style-attack concept has evolved into a targeted and multifaceted one. Adversaries have more motivation to be successful in their attacks than ever before. Previously, their primary goal was social gain and proof of concept. Adversaries have now come to understand that they can gain financially, socially and politically with minimal risk of capture or prosecution if their efforts are successful. Organizations can no longer protect themselves from these evolving threats by using traditional reactive and technology-focused means. They must constantly evaluate and understand the high-business-impact and high-likelihood threats that exist to their information infrastructure and develop effective controls.

A multifaceted approach to threat and vulnerability analysis and management is critical because of one fundamental rule: adversaries have a distinct and considerable advantage over defenders *because they only need to succeed once* with *one type of attack* to be successful. The defender, on the other hand, must achieve mastery in protecting against *all attacks*. At the same time, defenders are burdened by budgetary, resource and legal constraints with which attackers are not concerned.

To overcome these challenges and constraints, defenders must ensure that they focus their resources on identifying and defending against the threats and vulnerabilities most likely to impact their business. They must empower themselves to adjust and adapt to new attack techniques quickly and easily. Threat and vulnerability management programs provide organizations with that capability—but effective threat and vulnerability management programs cannot exist in a void. They must be aligned with the enterprise's overall strategy for the information infrastructure.

Threat and Vulnerability Management Programs

Properly planned and implemented threat and vulnerability management programs represent a key element in an organization's information security program, providing an approach to risk and threat mitigation that is proactive and business-aligned, not just reactive and technology-focused. These programs provide a way to assess the potential business impact and likelihood of threats and risks to an organization's information infrastructure before those events occur. These programs also facilitate compliance with specific regulations that have key security-related aspects, such as the Gramm-Leach-Bliley Act, which requires financial organizations in the US to have a physical and logical asset inventory of their customer data and the associated threat information (see **figure 1**). Effective threat and vulnerability management programs help enterprises meet and exceed those critical compliance requirements.

Threat and vulnerability management programs include three major elements:

- An asset inventory
- Threat and vulnerability analysis
- Vulnerability management

Each of these elements individually benefits the organization in many ways, but together they form interlocking parts of an integrated, effective threat and vulnerability management program.

Figure 1—Gramm-Leach-Bliley Act, Section III

Development and Implementation of Information Security Program, Section B

- Assess Risk. Each bank shall:
  1. Identify reasonably foreseeable internal and external threats
     that could result in unauthorized disclosure, misuse, alteration,
     or destruction of customer information or customer information systems.
  2. Assess the likelihood and potential damage to these threats, taking into consideration the sensitivity of customer
     information systems.

Asset Inventory

To protect information, it is essential first to know where it resides. The asset inventory must include the physical and logical elements of the information infrastructure. It should include the location, associated business processes, data classification, and identified threats and risks for each data element. This inventory should also include the key characteristics of the information that needs to be protected, such as the type of information being inventoried, sensitivity ratings for the information and any other critical data points the organization has identified for its information.

This asset inventory should be readily available to the organization's information security personnel, as well as to the data owners, internal audit, operations staff and any other individuals who access to that information. The inventory must be accurate and up to date to be effective. An optimal way to achieve this is to integrate maintenance of the asset inventory into the organization's change management process. This will ensure that the inventory is current, and will initiate threat analysis activity if it is based on the characteristics of the data or whether its use, storage or maintenance has fallen short of specified information security criteria.

The physical elements of the asset inventory include the location and disposition of equipment (e.g., servers, routers and storage solutions), paper documents and physical storage devices associated with the organization's data elements. The logical elements of the asset inventory include all of the organization's electronic information assets, such as the data and information, operating systems, and applications.

Threat and Vulnerability Analysis

Threat and vulnerability analysis is an exercise that models a particular solution or business process against attack scenarios and known vulnerabilities to evaluate its resiliency or capability to repel attacks. It utilizes intelligence capabilities such as technical knowledge, behavioral science and business logic to model attack scenarios, the likelihood of such attacks and the potential business impact if the attack were successful.

Threat analysis activities require specific information. First, information must be gathered on the business process or solution to be analyzed, as well as the physical and logical data elements associated with it. Typically, this information is gathered from the business process owner and by utilizing the asset inventory. It is important to define the scope and boundaries of the business process solution; otherwise, the threat analysis can become incomprehensible to the organization and challenging to complete.

Some key additional considerations include the value of the solution or business process to the organization, the regulatory and/or legal constraints, and the impact on third-party activities. This information must be gathered through independent discussions with senior managers, consultations with regulators and interactions with third parties. Additional information can be gathered by examining the organization's business continuity and disaster recovery plans, which should include this type of information for the critical business processes of the organization.

OSI+ Threat and Vulnerability Analysis Methodology

To perform threat analysis effectively, it is important to employ a consistent methodology that examines the business and technical threats to a business process or solution. Skilled adversaries use a combination of skills and techniques to exploit and compromise a business process or solution, so it is necessary to have in place a similarly multipronged approach to defend against them.

The OSI+ threat and vulnerability analysis methodology incorporates business and technology elements to provide a holistic view of threats to information infrastructure. It represents a blending of the six basic questions used in any analytical situation—who, what, when, where, why and how—with an expanded version of the Open Systems Interconnection (OSI) model commonly used in open-standards networking, whose layers roughly parallel the channels adversaries can use for attacks on information infrastructure. The OSI+ methodology enhances that model by adding two new layers to the conventional seven OSI layers: one representing people at the bottom and one representing process, procedures, standards and guidelines at the top.

Who

Who focuses on the type of adversary likely or motivated to attack information infrastructure. The OSI+ threat analysis methodology organizes adversary types into five different groupings, listed in ascending order based on their capabilities and potential impact:

- **Newbies** attempt to use tools and techniques that are well documented through publicly available publications and web sites. They tend to attack a wide array of organizations without a specific motive or intention beyond testing their capabilities and gaining access. They have only basic knowledge of attack techniques and concepts and can typically be defended against by using basic protection techniques.
- **Script kiddies,** similar to newbies, attempt to use tools and techniques that are well documented through publications and public web sites. These adversaries try to expand their knowledge and gain inside information about exploits and vulnerabilities through personal research and hacker community interaction to enhance the existing tools and create their own basic tools.
- **Coders/advanced knowledge attackers** have advanced programming skills and capabilities. They attempt to fingerprint the information infrastructure of an organization and then craft attacks based on those profiles. They are highly likely to utilize blended attack methods that incorporate multiple tools and techniques.
- **Motivated professionals** have advanced knowledge and computing skills. They pose a very high risk to an organization because they also have motivations (political, financial and personal) that drive their behaviors. These adversaries study all public domain information about an organization and conduct reconnaissance studies when possible. Because they are motivated and targeted in their attacks, they continue attempting to penetrate an

organization's information infrastructure until they have successfully achieved their goals.
- **Spooks/government agents/terrorists** have extensive technology capabilities and intelligence resources. These attackers have significant financial and technology resources to draw from, as well as in-depth knowledge of an organization's information infrastructure. They most likely use blended attack methods, including physical and technological means for attack and reconnaissance activities.

Because they are among the least sophisticated adversaries, newbies, script kiddies and coders often advertise their activities to others via chat rooms and web sites. These sites and rooms can be monitored to understand what access those types of adversaries have gained to information infrastructure. The majority of their attacks can be thwarted through defensive strategies and adherence to patch and control guidance from vendors. The tools they tend to use are readily available and can be studied and modeled to allow an organization's information security staff to know when they are being used.

Professionals and spooks are extremely dangerous because they do not advertise their attacks or stray from their attacks until they have some degree of success. They tend to have a specific goal in mind and act on either their own behalf or on behalf of others.

An organization seeking to defend itself should create and maintain competency models of adversaries and the techniques and skills they require to be successful. One way to thwart them is to study the materials publicly available to them about the organization and its information infrastructure. Those materials can be found by using the same tools the adversaries use—search engines and intelligence services.

What

The *what* element of the OSI+ methodology focuses on the areas within the information infrastructure of the organization that an adversary is most likely to attack. Adversaries tend to attack the areas they believe are most vulnerable or have the highest value. The Internet-facing web environments that provide customer self-service capabilities or access to private information about individuals are examples of this.

When

The *when* element of the OSI+ methodology addresses the time during which an adversary is most likely to attack an organization. Unfortunately, adversaries tend not to attack during normal business hours, when defenses are at their highest capabilities. They typically attempt to take advantage of the times when they perceive an organization's defenses to be at their weakest. Skilled adversaries may even attempt to distract security staff with a diversionary attack before carrying out their primary assault. For example, an adversary could launch a virus attack to attempt to initiate the organization's business continuance plan. Once the organization's information security resources are focused on the remediation of the virus attack, the adversary can then launch another attack directed against the primary target.

Where

The *where* element identifies the most likely points of attack in a business process or solution. Skilled adversaries attempt to compromise a solution through the points they feel are most vulnerable, including remote access points, third-party vendors with secure connections, and web environments. A skilled adversary often tries to compromise information infrastructure elements that do not have effective security controls in place because they were perceived by the company to be low in value. For example, backup and print servers, which tend to have high levels of unrestricted access to systems and networks, are often overlooked in protection schemes.

Why

The *why* element of the OSI+ threat analysis methodology addresses an adversary's motivation. Motives can include financial, political, personal and status-seeking activities. Once it understands adversaries' motivations, an organization can determine the warning signs of potential attacks.

How

The *how* element of the methodology uses the expanded version of the OSI+ model to evaluate the potential threats to a business process or solution from a technical perspective. Besides being the location of the two new layers mentioned previously, it also mirrors the structure of the OSI stack and uses the same naming for its constituent layers:

- **People**—The people layer of the OSI+ methodology focuses on social engineering attacks, which continue to be among the most successful against information infrastructure. The ability of an adversary to exploit the trust of an individual or group of individuals often leads to unauthorized access to critical information infrastructure.

  For example, an adversary purporting to be someone trusted within an organization could gain access to PCs or physical areas where strong security does not exist or authorized users have already disabled security features. This would most likely be carried out by an adversary presenting credentials that authorize him/her to have access to the facility for tasks such as maintenance or delivery—or, it could be someone calling an employee and masquerading as a colleague to obtain authorization codes or confidential information.
- **Physical**—The physical layer focuses on the physical information infrastructure elements. These include facilities such as data centers, conference rooms and office areas, as well as documentation and equipment. Documentation and printouts of sensitive information are often discarded and disposed of improperly. An adversary often peruses disposal facilities and containers for this documentation. Sometimes, it can be distributed inadvertently. In a recent incident, printouts with personal information about subscribers were used to wrap bundles of newspapers ready for circulation.
- **Data**—Data attacks relate to the data elements of an organization's information infrastructure. They can include the inappropriate deletion, copying, modification and manipulation of data, or disruption of their movement or access to them. For example, an adversary could gain access

to a financial database and insert an application that uses a pseudo random generator to change data in an irregular pattern and, thus, invalidate the integrity of the database.

- **Network**—The network layer focuses on how an adversary can attack and compromise an organization's network resources, whether conventional wired facilities or mobile/wireless. For example, an adversary can use a network sniffer to capture traffic between the organization and one of its customers, capturing confidential data such as user names and passwords that could provide access to sensitive information.
- **Transport**—Transport relates to the way information moves within an organization's information infrastructure, such as via paper, electronic means or personnel. For instance, if an organization employs a third-party transport service to transfer unencrypted backup tapes offsite for disaster recovery purposes, an adversary can intercept the backup tapes in transit and gain access to confidential information about clients' identities and business transactions.
- **Session**—The session layer relates to all interactions among users and systems within an organization's information infrastructure, such as authentication capabilities, terminal access points and interconnection points. For example, an adversary can set up a false web site that mimics the actual web site for a customer self-service environment within the organization. The adversary can then collect user IDs and passwords from unsuspecting people and use those credentials to access user accounts and compromise sensitive data.
- **Presentation**—The presentation layer relates to all information presented to the internal or external user in either physical or electronic form. It also includes any publicly available information that can be used against the organization. For instance, an adversary can obtain the logo of an organization and a signature of a corporate officer by obtaining a copy of the annual report (if it is a publicly traded company). Adversaries can then use these to create false correspondence to customers to try and obtain sensitive information about them or create false company checks that allow them to withdraw funds from company accounts.
- **Application**—The application layer relates to all application vulnerabilities open to attacks, including operating systems and applications. The applications can be vendor-produced and supported, or they can be proprietary systems. Application attacks are the most common attacks facing information infrastructure. Application attacks include buffer overflows, spyware, key loggers and patch exploits.
- **Policies, Processes, Procedures, Guidelines and Standards**—This layer refers to nontechnical elements of information infrastructure. It focuses on how an adversary can take advantage of weaknesses in current operating activities that an organization has defined, but for which it has not provided the security controls necessary to prevent exploitation by an adversary. For example, an adversary can take advantage of the procedures that an organization employs for password reset activities. If the help desk uses an individual's phone number and digital identifier as the authentication mechanism for password resets, the adversary can gain access to the public broadcast exchange or the user's telephone and call the help desk, asking for a password reset that will enable the adversary to substitute a password, which he/she then can use to access sensitive information.

Threat Level Assignment

One of the key outputs of a threat and vulnerability analysis using the OSI+ methodology should be a threat-level designation (**figure 2**) for the business process or solution that has been analyzed. It should be a visual and/or numeric representation of the current threat level. The level should be easy to understand and interpret. For example, the "traffic light" model, where red represents the highest threat and green represents the least threat, is an ideal depiction. The colors can be assigned numerical values as well, so that they can be interpreted by binary systems, such as a computer. This creates a "dashboard," providing a current status on key vulnerabilities.

Figure 2—Threat Level Assignment

SEVERE (5) (RED) Attack in progress or eminent. Incident response team should be activated.
HIGH (4) (ORANGE) Attack behaviors and activities identified in information infrastructure. Vulnerability management countermeasure plans should be initiated.
ELEVATED (3) (YELLOW) Evidence of attack capabilities and motivated adversaries identified. Controls should be reviewed for effectiveness.
GUARDED (2) (BLUE) Attack possible but not likely. Information infrastructure monitors should be tuned to possible attacks.
LOW (1) (GREEN) No current evidence of attack capabilities or motivated adversaries. Vulnerability management plans should be reviewed and updated.

Vulnerability Management

Vulnerability management uses the input from the threat and vulnerability analysis to mitigate the risk that has been posed by the identified threats and vulnerabilities. A vulnerability management program consists of four key elements:

- **Countermeasure plans**—Countermeasure plans are essentially cookbooks that include prescriptive guidance on how an organization can repel an attack by an adversary on an identified vulnerability. If the plan has been developed properly, the operations staff—the first line of defense in an active attack—should be able to use this guidance to eliminate, or greatly reduce, the impact of an active attack. A primary benefit of an effective countermeasure plan is the way it enables the organization to properly identify the appropriate level of resources and capabilities required to mitigate an attack. In response to an attack, an organization will too often overdeploy resources and capabilities in an attempt to repel it as quickly as possible. That purely reactive approach is extremely inefficient and can have significant financial consequences. A sound countermeasure plan can prevent expensive overreaction.

- **Controls**—Once vulnerabilities have been identified, it is important to put controls in place to mitigate the risks those vulnerabilities create. Controls can be either business or technical, and can be considered normal or key. Key controls provide significant risk mitigation or have other controls that depend upon their being in place to function properly.
- **Metrics and measures**—Metrics and measures provide empirical and statistical data to help an organization understand whether the threat and vulnerability management analysis performed and the controls put in place are effective and capable. Those metrics can be tracked and measured, providing input to statistical analysis activities that not only yields valuable trending information but also provides input points to business risk management activities.

  Metrics and measures also provide an important input into the governance model that oversees the threat and vulnerability management function within an organization. Key performance indicators (KPIs) associated with this process allow the chief information security officer (CISO) and the information security oversight committee to ensure that the function is furthering the business goals of the organization and its capabilities are maturing as the business matures. Vulnerabilities should also be rated based on standard quantitative criteria, not unlike threats.
- **Intelligence**—Within information security, intelligence is a key success factor in the threat and vulnerability management program. Intelligence is the collection and interpretation of data to help determine reality vs. fear, uncertainty and doubt.

  Intelligence gathered and processed appropriately can greatly enhance the organization's ability to be more accurate in threat analysis and vulnerability management activities. Therefore, it is important to explore all possible scenarios in which an adversary can take advantage of a business process or a solution. It is even more important to decide which scenarios are possible and plausible in the current state.

An organization should categorize, catalog and track intelligence in alignment with the OSI+ threat and vulnerability analysis methodology. That way, the organization can build an intelligence database that can be cross-referenced against both the asset inventory and threat and vulnerability management analysis databases. It can then use this intelligence database to monitor trends in activities and common concepts, allowing for more accurate assessment of the likelihood of the attack scenarios identified for particular threats.

This information can be used to adjust the protection posture and control framework of the organization to defend itself more effectively against the most likely attack scenarios with a high degree of confidence. It can also help in assessing whether the controls already in place are capable and effective.

KPIs

To ensure business alignment and continued maturity of the threat and vulnerability management program, an organization must establish KPIs to monitor the activities and effectiveness of the threat and vulnerability management program. There are many KPIs, and those used will differ based on organizational goals. The following represent a sample set of KPIs:

- Accuracy of asset inventory data
- Accuracy of threat and vulnerability analysis
  - Likelihood and impact projections
  - Threat level designations
  - Threat identification characteristics for vulnerability management
- Responsiveness to emerging threats
- Ability to communicate appropriately and effectively to the organization
- Number of information security-related events or incidents
- Time required to remediate business-debilitating information security events
- Number of identified vulnerabilities
- Effectiveness of remediation plans and controls for identified vulnerabilities

An organization should monitor the KPIs it has identified on a continual basis and report the results to the CISO, information security oversight board and management of the organization. Those responsible for presenting the data points should do so in graphical and numeric formats to ensure that the outcomes are easy to understand and can be effectively utilized by the organization.

Conclusion

Information security will continue to be a growing challenge to organizations. To be proactive in their approach to it, organizations must adopt a programmatic approach to information infrastructure risk management. Threat and vulnerability management programs, when part of a larger information security program, provide a significant advantage in addressing this challenge. The first step to solving a problem lies in understanding its scope. Threat and vulnerability management programs provide that critical first step. They afford the organization the capability to understand the problem, evaluate the potential business impact and likelihood of compromise, and implement appropriate levels of risk mitigation. By being proactive, an organization can significantly reduce the risk posed by threats to its information infrastructure and reap economic benefits by avoiding or minimizing the actual costs and the opportunity costs that inaction on security can entail.

John P. Pironti, CISA, CISM, CISSP, ISSAP, ISSMP
is a principal enterprise solutions architect and principal security consultant at Unisys Corporation. He has designed and implemented enterprisewide electronic business solutions, information security programs, and threat and vulnerability management solutions for key customers in a range of industries, including financial services, government, hospitality, aerospace and information technology. He is a published author and writer, and a frequent speaker on electronic business and information security topics at domestic and international industry conferences.