The Information Security Process
Prevention, Detection and Response

By James LaPiedra

Information security is a process that moves through phases building and strengthening itself along the way. Security is a journey not a destination. Although the Information Security process has many strategies and activities, we can group them all into three distinct phases - prevention, detection, and response.

Each phase requiring strategies and activities that will move the process to the next phase. The dynamic growth of new threats attacking vulnerabilities requires timely adjustments to the methodologies in the prevention, detection, and response cycle. A change in one phase affects the entire process in some form. A proactive strategy adjustment in the prevention phase will adjust the detection and response activities. Lessons learned during the response phase will be addressed in the planning of prevention measures and detection configurations. As I have indicated the Information Security process is a journey, it is a living cycle that is under constant change due to the threat and vulnerability environment. For successful stewardship of the process, strategies must be one step ahead of the advisories or at least in step with them. To accomplish this, each phase must be designed with adequate capabilities and management oversight to ensure the maturity of these capabilities.

The ultimate goal of the information security process is to protect three unique attributes of information. They are:

- **Confidentiality** – Information should only be seen by those persons authorized to see it. Information could be confidential because it is proprietary information that is created and owned by the organization or it may be customers' personal information that must be kept confidential due to legal responsibilities.
- **Integrity** – Information must not be corrupted, degraded, or modified. Measures must be taken to insulate information from accidental and deliberate change.
- **Availability** – Information must be kept available to authorized persons when they need it.

Attacks compromise systems in a number of ways that affect one if not all of these attributes. An attack on confidentiality would be unauthorized disclosure of information. An attack on integrity would be the destruction or corruption of information and an attack on availability would be a disruption or denial of services. Information security protects these attributes by:

- *Protecting* confidentiality
- *Ensuring* integrity
- *Maintaining* availability

An organization succeeds in protecting these attributes by proper planning. Proper planning before an incident will greatly reduce the risks of an attack and greatly increase the capabilities of a timely and effective detection and response if an attack occurs. Lets now examine each phase of the prevent, detect, respond cycle in turn, illustrating the individual process and how they relate with the whole.

Prevention:

There is an age-old advisory that says, "It's too late to sharpen your sword when the drum beats for battle". Make no mistake, we are in a war and we must prepare for the cyber battles by sharpening our skills. Information security professionals must continuously mature their capabilities by working smarter not harder. It is always better to prevent, then to pursue and prosecute. Preventing an incident requires careful analysis and planning.

Information is an asset that requires protection commensurate with its value. Security measures must be taken to protect information from unauthorized modification, destruction, or disclosure whether accidental or intentional. During the prevention phase, security policies, controls and processes should be designed and implemented. Security policies, security awareness programs and access control procedures, are all interrelated and should be developed early on. The information security policy is the cornerstone from which all else is built.

Security Policy:

The first objective in developing a prevention strategy is to determine "what" must be protected and document these "whats" in a formal policy. The policy must define the responsibilities of the organization, the employees and management. It should also fix responsibility for implementation, enforcement, audit and review. Additionally, the policy must be clear, concise, coherent and consistent in order to be understood. Without clear understanding, the policy will be poorly implemented and subsequent enforcement, audit and review will be ineffective. Once management endorses a completed policy, the organization needs to be made aware of its requirements.

Security Awareness:

Security awareness is a process that educates employees on the importance of security, the use of security measures, reporting procedures for security violations, and their responsibilities as outlined in the information security policy. Security awareness programs should be utilized for this purpose. The program should be a continuous process that maintains an awareness level for all employees. The program should be designed to address organization wide issues as well as more focused specialized training needs. The program should stress teamwork and the importance of active participation. To motivate individuals, a recognition process should be adopted to give out awards or rewards for employees that perform good security practices.

Access Controls:

Access is the manner by which the user utilizes the information systems to get information. Naturally all users should not have the ability to access all systems and its information. Access should be restricted and granted on a need to know basis. To manage this access we establish user accounts by issuing identifiers, authentication methods to verify these identifiers and authorization rules that limit access to resources.

- **Identification** – Identification is a unique identifier. It is what a user – (person, client, software application, hardware, or network) uses to differentiate itself from other objects. A user presents identification to show who he/she is. Identifiers that are created for users should not be shared with any other users or groups. Once a user has an identifier the next step taken to access a resource is authentication.

- **Authentication** – Authentication is the process of validating the identity of a user. When a user presents its identifier, prior to gaining access, the identifier (identification) must be authenticated. Authentication verifies identities thereby providing a level of trust. There are three basic factors used to authenticate an identity. They are:

  1. Something you know – The password is the most common form used. However, secret phrases and PIN numbers are also utilized. This is known as one-factor or single authentication. This form is weakened due to poor password selection and storage.
  2. Something you have – This authentication factor is something you have, such as an identification card, smartcard or token. Each requiring the user to possess "something" for authentication. A more reliable authentication process would require two factors such as something you know with something you have. This form is known as the two-factor or multilevel authentication.
  3. Something you are – The strongest authentication factor is something you are. This is a unique physical characteristic such as a fingerprint, retina pattern or DNA. The measuring of these factors is called biometrics. The strongest authentication process would require all three factors. Facilities or applications that are highly secret or sensitive will utilize all three factors to authenticate a user. However, biometrics on the surface appears to be a panacea, its not. There are weaknesses and to work the verifier needs to verify two things. These requirements are outlined in a Counterpane.com article *by Bruce Schneier, titled "Biometrics: Uses and Abuses"*. The author indicates that the verifier needs to verify two things. The first is that the biometric came from the person at the time of verification and secondly, that the biometric matches the master biometric on file. Without these two biometric authentication requirements this factor won't work.

- **Authorization** – Authorization is the process of allowing users who have been identified and authenticated to use certain resources. Limiting access to resources by establishing permission rules provides for better control over users actions. Authorization should be granted on the principle of least privilege. Least privilege is granting no more privilege than is required to perform a task/job, and the privilege should not extend beyond the minimum time required to complete the task. This restrictive process limits access, creates a separation of duties and increases accountability.

Once an organization has adopted a policy, created an awareness program and has established access controls, it must implement detection strategies and response plans. It would behoove an organization to take a more proactive stance in preparing for an attack or disaster rather than a reactive ad hock response to an underestimated threat.

The process of detecting malicious or accidental misuse of resources is much more than sounding an alarm. Also, responding to an incident is much more than just showing up. An organization to be successful must know what to detect and once alerted know how to effectively coordinate resources for a response. With both of these processes time is of the essence.

Detection:

Detection of a system compromise is extremely critical. With the ever-increasing threat environment, no matter what level of protection a system may have, it will get compromised given a greater level of motivation and skill. There is no full proof "silver bullet" security solution. A defense in layers strategy should be deployed so when each layer fails, it fails safely to a known state and sounds an alarm. The most important element of this strategy is timely detection and notification of a compromise. Intrusion detection systems (IDS) are utilized for this purpose.

IDS have the capability of monitoring system activity and notifies responsible persons when activities warrant investigation. The systems can detect attack signatures and also changes in files, configurations and activity. To be protected, the entire system should be monitored. Intrusion detection tools should be strategically placed at the network and application levels. However, monitoring a busy network or host is not a simple task. Intrusion detection tools must have the ability to distinguish normal system activity from malicious activity. This is more of an art than a science. The IDS must be fine-tuned or 'tweaked" in order for the IDS to work in accord with a particular network or host. This tuning process must take into account known threats, as well as intruder types, methods and processes.

As previously indicated, intrusion detection is much more than an alarm. Although it is an alarm, it's an alarm with brains. Imagine a fire alarm that had the capability of detecting a fire, distinguish the type of fire, pinpoint its source and path, alert the building occupants and fire department, and forward intelligence to the firehouse prior to their response. All this and even having the capability of distinguishing normal activity such as bad cooking. A properly configured intrusion detection system is such a device. An alarm with brains.

Once your IDS is properly configured and strategically placed, it's only a matter of time before an alert will sound and notifications sent. Now what? Without a documented response plan you will have total confusion.

Response:

For the detection process to have any value there must be a timely response. The response to an incident should be planned well in advance. Making important decisions or developing policy while under attack is a recipe for disaster. Many organizations spend a tremendous amount of money and time preparing for disasters such as tornados, earthquakes, fires and floods. The fact is, the chances are greater that a computer security incident will occur than any one of these scenarios. Equivalent if not more effort and resources should be expanded on a computer security incident response plan.

The response plan should be written and ratified by appropriate levels of management. It should clearly prioritize different types of events and require a level of notification and/or response suitable for the level of event/threat. A Computer Security Incident Response Team (CSIRT) should be established with specific roles and responsibilities identified. These roles should be assigned to competent members of the organization. A team leader/manager should be appointed and assigned the responsibility of declaring an incident, coordinating the activities of the CSIRT, and communicating status reports to upper management.

There are two philosophies on how an incident should be handled. An organization may wish to cut off the intruder's connection, eradicate the cause of the incident and recover the effected system. This approach would be more feasible when mission critical machines are affected and timely recovery is a priority. Another approach would be to pursue and prosecute the attacker(s). This approach is a riskier endeavor requiring much more exposure. However, due diligence may require an organization to take reasonable investigative measures to identify an attacker or an upstream organization that may have been compromised by their system. Management must review each situation on a case-by-case base and act accordingly. Whichever approach an organization decides, the methodology of the response should be documented in the response plan. Responders will be assigned tasks suited for their skill set. Whether gathering forensic evidence, containing the attack or recovering compromised systems, individuals participating in the response should possess the skills required to successfully accomplish their assignments. Other key responders will be external to the organization. Law enforcement (federal, state, local), prosecutorial agencies and the news media are all interested parties who will be involved with an incident at some point. Relationships with these external parties should be established during the planning phase of the security process and not during a crisis. This point is illustrated in a July 2000 Security Focus article written *by Ben Malisow, titled "Moment's Notice: The Immediate Steps of Incident Handling"*. The author indicates that if you are working in the private sector you need to be aware that law enforcement may be more or less inclined to assist you, depending on the size or breadth of your company. This is why, particularly if you are a small organization, establishing a good relationship with external agencies is very important. People tend to work well when they know one another. You could never have enough friends when things go bad.

After an incident has been declared and the notifications made to responders, the incident must be contained, the damage assessed and the system cleaned and recovered. Each process requiring special skills and having an important role in the response phase. However, the post incident analysis and report is the most important process towards strengthening the information security cycle. This process is extremely important due to the lessons learned. By examining the answers to the who, what, where, why, and when questions and evaluating the results, an organization can incorporate lessons learned in each of the security phases.

The Ever Maturing Cycle:

To successfully defeat the attacker, whether internal or external, an organization must be properly prepared. As I have outlined, the information security process is a journey and not a destination. It is a dynamic process requiring skilled management and flexibility. Disciplined management of the prevention, detection and response cycle is required to ensure continuous improvement. Organization wide support and involvement is paramount in the maturing of the security strategy. It is a team effort requiring unselfish cooperation. Management must buy into the big picture. In a Network Computing article titled, *"The High Price of Vulnerability" by Greg Shipley*, the cost associated with "don't want to know" management could be disastrous. One small organization with fewer than 100 servers was compromised 8 hours into a monitoring project. Management at the organization faced difficult options, all more costly than instituting a plan and following simple preventive maintenance procedures. Everyone in the organization must be committed.

Sources:

Schneier, Bruce. "Biometrics: Uses and Abuses." Counterpane. August 1999. URL: http://www.counterpane.com/insiderrisks1.html

Malisow, Ben. "Moment's Notice: The Immediate Steps of Incident Handling. 7 July 2000. URL: http://www.securityfocus.com/focus/ih/articles/moments.html

Shipley, Greg. "The Price of Vulnerability." 19 February 2001. URL: http://www.nwc.com/1204/1204colshipley.html

Additional sources:

Pipkin, L. Donald, *Information Security: Protecting The Global Enterprise*. (Prentice Hall), May 2000.
Schneier, Bruce, *Secrets & Lies: Digital Security In The Networked World*, (Wiley) August 2000.