

DATA SECURITY MANAGEMENT

ESTABLISHING A COMPUTER INCIDENT RESPONSE PLAN

David Adler and Kenneth L. Grossman

INSIDE

The Constituency; The Computer Incident Response Team (CIRT); Incident Reporting Procedures; Incident Handling Procedures; The "Protect and Forget" Philosophy; The "Apprehend and Prosecute" Philosophy

INTRODUCTION

A truly effective information technology (IT) security program requires a computer incident response plan. This plan is composed of three sections. The first details whom and what the plan will cover (i.e., the plan's constituency); the second entails establishing a Computer Incident Response Team (CIRT), also known as a computer security incident response capability; and the final section is a formalized set of procedures for reporting and handling IT security incidents.

THE CONSTITUENCY

Before starting to develop the plan, the organization must determine the personnel responsibilities and scope because the plan's coverage will affect the procedures and processes used to handle a computer security incident. For example, the plan might cover only headquarters personnel and systems, or it might include regional offices. The plan must also consider any external connections, determining how an incident might affect a trading partner, contractor, or client that is connected in some way to the affected system or network.

The plan should also state how the organization works with its IT and security staff, and the types of systems the plan will cover. This will help determine which job positions the incident response team needs

PAYOFF IDEA

A truly effective information technology (IT) security program requires a computer incident response plan. This plan is composed of three sections. The first details whom and what the plan will cover; the second entails establishing a Computer Incident Response Team (CIRT), also known as a computer security incident response capability; and the final section is a formalized set of procedures for reporting and handling IT security incidents, including whether to "protect and forget" or "apprehend and prosecute."

filled. For example, if the organization has legacy mainframes, UNIX servers, and a Microsoft Windows NT LAN, but the plan only covers the LAN, there is no need for the team to include mainframe or UNIX administrators. Therefore, knowing the plan's constituency assists in forming the team.

THE COMPUTER INCIDENT RESPONSE TEAM (CIRT)

The organization's procedures identify who will be performing them, so the plan must describe the makeup and duties of the CIRT. If the plan covers regional offices, there must be a central CIRT, along with regional teams. The latter are subordinate to the central team, handling only those incidents that are specific to that region. The central office team handles any incident that affects multiple regions or the entire organization, assisted by the regional teams.

All teams should have the same membership criteria. If the plan does not cover the regional offices, the team makeup and organization must reflect this. The team is composed of a core group who will be involved in all incidents, and a group of platform and system specialists who will participate as the incident requires. Of course, the latter will depend on which platforms or systems the plan covers.

The Core Group

The core group members include the IT security program manager (or the IS security manager); representatives from the legal department, public relations, and human resources or personnel; as well as someone with an investigative or forensics background. The organization can add personnel to the core group as needed.

IT Security Program Manager. This person is the overall head of the organization's IT security program, and should be the CIRT leader. In most cases, he or she will appoint someone to be the IS security manager, who will run the day-to-day incident response team operations. This leaves the security program manager free to manage the organization's overall IT security. In the case of a multi-regional or multi-country organization, an IS security manager should be appointed for each regional office, who will lead the regional incident response team. As the team leader, the IT security program manager or IS security manager will be the director of each incident investigation. He or she will decide if additional personnel are required for the investigation, as well as ensuring that all procedures are followed, and deciding if outside assistance is required, as approved by upper management. The IT security program manager also authorizes the release of any information about the incident, again with upper management consent. However, he or she is not the organization's media spokesperson.

Legal Department. The CIRT requires a representative from the legal department who is knowledgeable about the various laws that deal with IT security and privacy. This person's function is to ensure that the team does not violate the law while investigating the incident, especially when the organization deals with incidents using the "apprehend and prosecute" philosophy. The legal representative must also know whom to contact at the local, state/province, and national levels (e.g., in the United States, it is the FBI/National Infrastructure Protection Center), as well as at international law enforcement agencies. This person will be the contact with the law enforcement agencies.

Public Relations. Only the central office team will have a public relations representative on the team. The regional teams will forward all media requests for information to this person, who will be the sole point of contact to the media for the organization when it releases information, as authorized by the IT security program manager.

Human Resources or Personnel. There must be a human resources/personnel representative on the team for various reasons. This person will ensure that the team does not violate employees' rights during the investigation (e.g., privacy). Also, this representative will make sure that appropriate disciplinary methods are used if an employee is found to be the source of the incident. The organization's appropriate punishment can go as far as firing the individual.

IT Investigative/Forensics Expert. This person will ensure that the investigation is performed in a methodical manner, seeing that evidence is collected and stored properly. Not only will this assist in the overall handling of the incident, but it will be especially helpful if the organization wishes to prosecute the individual responsible for the incident. If so, the evidence must be collected and handled so that it can be used in the criminal case. This includes keeping the "chain of evidence" clean, secure, and verifiable.

Incident-Specific Team Members

The CIRT will also require other personnel on an as-needed basis. While these individuals will depend on the specific incident to be handled, all must be knowledgeable about the system under attack. Key personnel include the IS security officer, as well as system administrators, communication specialists, system developers, database administrators, and the system owner. Others may also be included.

IS Security Officer. Each system or application must be assigned an IS security officer who ensures that the system is in line with the organiza-

tion's IT security policy and guidelines. This officer assists the core group in handling an intrusion by stating how the entire system is supposed to be set up and configured.

System Administrators. Those who administer the hardware on which the system runs are critical in incident handling, due to their intimate knowledge of the hardware and operating system configuration and the services that run on the system.

Communication Specialists. These specialists are necessary in handling the incident, due to their intimate knowledge of the network and its configuration, including the firewall configuration if a firewall is used. They know where the compromised system is connected to the network, and if it has any other connections to the Internet that are not protected by the firewall. They also know how the routers, bridges, and gateways are configured, and where they are located within the network. In most cases, they also monitor the intrusion-detection system, if the organization uses one.

System Developers. The developers know the intricacies of the system or application. Therefore, they know if the compromised system or application is not running properly, and if it has been modified.

Database Administrators. If the compromised system uses a database, the database administrators must evaluate if changes have been made to the database structure or configuration. They can also tell if any database-specific programs (e.g., stored procedures or queries) have been modified.

System Owner. It is important that the system owner be a part of the incident handling team for several reasons. First, because the owner knows exactly how critical the system is to the organization's mission, he or she can say how soon an intrusion session is to be terminated, and if the system should be taken off the production server. The owner also knows if a backup system must be put into production immediately, or if the system can be kept down until the main system is validated and any system vulnerabilities corrected. Second, the system owner knows the proper data format, and can tell if the data makes sense and provides the proper output.

Response Team Duties

The function of the CIRT is to handle information security incidents as they occur, using the procedures in the IT security program. The team members ensure that the incident is handled as quickly as possible, and

that it does not affect the security of other systems and applications. If there is an incident, they must know who should be contacted, even if only for informational purposes.

Many countries have a centralized incident response capability in which government agencies report such incidents. In the United States, for example, federal civilian agencies are required to report all incidents to the Federal Computer Incident Response Capability, while the Department of Defense has its own hierarchy for this capability.

The response team must also have procedures for controlling the release of information within the organization. This is to control fear, uncertainty, and disturbance, from which the organization might otherwise suffer.

INCIDENT REPORTING PROCEDURES

A standard process for reporting incidents should be developed as part of the formalized procedures. This should include a standardized form that can assist personnel in reporting a suspected computer-related incident. The form should provide the following information:

- *Date of the report*: the date that the alleged incident was noticed
- *Time and duration of the incident*: the time that the incident was noticed (including time zone data), and approximately how long it appeared to last
- *System name*: the name of the system being attacked
- *Location of the alleged incident*: the location of the system that was the focus of the incident
- *Contact information of the person reporting the incident*: the name, office, phone number, fax number, cell phone or pager number, and e-mail address of the person reporting the incident
- *Contact information of the information systems security officer*: the name, office, phone number, fax number, cell phone or pager number, and e-mail address of the information systems (IS) security officer for the system at issue, if known
- *Contact information of the IS security manager*: the name, office, phone number, fax number, cell phone or pager number, and e-mail address of the company's IS security manager
- *Type of system under attack*: the type of system being attacked (e.g., a Web server, database server, e-mail server, network, or application), if known
- *Operating system and IP address of the system being attacked*, if known
- *Description of the incident*: as detailed a description of the incident as possible
- *Implications of the incident*: the adverse effects on the company as a result of the attack

The incident reporting procedures should stipulate to whom the reporter should send the completed incident reporting form. This standardized form should be the basis for creating a Web-based incident response function, located on the company's IT security home page, which should be housed, in turn, on the company's intranet. The form should serve as the front end of a security incident database and help track and handle security incidents. Other useful fields might be assessment of the damage caused by the incident, response actions for handling the incident, and final recommendations.

INCIDENT HANDLING PROCEDURES

Once an incident has been reported, the procedures should stipulate how it should be investigated and handled. The procedures will vary, based on upper management attitudes regarding incidents. Thus, upper management must decide which of the two major philosophies for incident response to use: "protect and forget" or "apprehend and prosecute." The latter requires that certain regular processes be established to assist the team in handling incidents. These processes might include setting up warning banners indicating that system activity is logged and monitored, setting up the system and other logs to collect the activity, and having someone review the logs on a daily basis. Everyone must be aware of the procedure whereby those taking part in incident response are not to discuss the incident outside their particular incident response subteam. Upper management decides who is informed of the incident and how much information is released.

The "Protect and Forget" Philosophy

If upper management decides to follow the "protect and forget" philosophy, the response team should follow these procedures (see also [Exhibit 1](#)):

1. *Determine if the event is a real incident.* This is one of the most important aspects of handling any incident. The team must know if this is truly a computer security incident, as opposed to a user error or a system configuration error.
2. *If the event is indeed an incident, terminate the current intrusion.* This is the key part of "protect and forget." The team must stop any further damage from being done to the system, or to information that the attacker takes off the system. Because it does not matter if the intruder knows that he or she was discovered, the team can just kill the session.
9. *Discover how access was obtained and how many systems were compromised.* The team needs to know how the person gained access to the system, as well as where they went while they had access. This

EXHIBIT 1 — Incident Handling Using “Protect and Forget” Philosophy

1. Determine if event is a real incident.
2. If so, terminate the current intrusion.
3. Discover how access was obtained and how many systems were compromised.
4. Restore compromised systems back to the pre-incident configuration.
5. Secure the method of unauthorized access by the intruder on all systems.
6. Document steps taken to deal with the incident.
7. Develop lessons learned.
8. Brief upper management on the aftermath of the incident.

reveals the vulnerabilities that need fixing and how many systems must be restored back to their pre-incident configuration. The team must also determine approximately when the first intrusion was made, to determine how far back to go, in order to obtain an uncompromised system backup.

10. *Restore the compromised systems back to the pre-incident configuration.* This can be done from an uncompromised backup tape. However, all transactions that were performed after that backup was performed will be lost, and will need to be redone.
11. *Secure the method of unauthorized access by the intruder on all systems.* This means fixing the system vulnerability that was used to gain access. The corrections and fixes might entail turning off services that are not required by the system to operate and function, installing necessary software patches, or changing user passwords and enforcing good password practices.
12. *Document steps taken to deal with the incident.* Someone should take notes during the entire incident, documenting every step taken to combat it. The notes should include what was done, the exact time that it was done (including time zone information), who performed each step, and who witnessed the step. At the end of the incident, these notes should be collected and formalized into an after-action report.
13. *Develop lessons learned.* The after-action report should be reviewed by both the CIRT and the IT security program manager, giving rise to ideas for improvement such as modifying system security and configuration guidelines, improving user security awareness, modifying IT security policies and procedures, or modifying security incident response procedures.
14. *Brief upper management on the incident's aftermath.* In the military, this is called an after-mission debriefing. Here, the IT security program manager and the IS security manager should discuss the incident with upper management, in terms of what occurred, what was done to combat the incident, the results of the incident, and what

EXHIBIT 2 — Incident Handling Using “Apprehend and Prosecute” Philosophy

1. Determine if the event is a real incident.
2. If the event is an incident, contact law enforcement.
3. Document each action taken, including the date and time that the action was taken and who was present.
4. Isolate the compromised systems from the network.
5. If the organization has the capability, it should entice the intruder into a safe system (i.e., a honey pot) that seemingly contains valuable data.
6. Discover the identity of the intruder while documenting his or her activity.
7. Discover how the intruder gained access to the compromised systems, and secure these access points on all uncompromised systems.
8. Terminate the current intrusion as soon as sufficient evidence has been collected, or when vital information or systems are endangered.
9. Document the current state of compromised systems.
10. Restore the compromised systems back to the pre-incident configuration.
11. Secure the method of unauthorized access by the intruder on all compromised systems.
12. Document the cost of handling the incident, and the time in man-hours.
13. Secure all logs, audits, notes, documentation, and any other evidence that was gathered during the incident, with appropriate identification marks, securing the “chain of custody” for future prosecution.
14. Develop lessons learned.
15. Brief upper management on the aftermath of the incident.

must be done to prevent similar events from re-occurring. Although upper management must be kept informed of what is happening during the entire incident, it is at the end that they must be told the entire story.

The “Apprehend and Prosecute” Philosophy

If upper management decides to follow the “apprehend and prosecute” philosophy, the CIRT should follow these procedures (see also [Exhibit 2](#)):

1. *Determine if the event is a real incident.* This, again, is one of the most important portions of handling any incident. The team must know if this is truly a computer security incident, as opposed to a user or system configuration error.
2. *If the event is an incident, contact law enforcement.* If management has decided that it wants to pursue and prosecute the attacker, the local police or the Federal Bureau of Investigation (FBI) must be notified as soon as it is verified that the incident is real. In most cases, law enforcement agencies will not step in and take over the incident. However, they will work with the team, ensuring that its actions stay within the law and do not violate any individual rights. They will as-

- sist the team in properly documenting and storing evidence to protect the chain of custody that is necessary for evidence to be used in court.
3. *Document each action taken, including the date and time, as well as who was present when the action was taken.* In cases where the organization wishes to prosecute the attacker, it is absolutely necessary to be extremely precise in recording what action was performed, when it was performed, and who saw it being performed. The reason is that these notes can be used as evidence at the trial, if it goes that far. All notes must be protected using the rules of evidence that the courts have stipulated.
 4. *Isolate the compromised systems from the network.* This is done to protect the remainder of the network. The organization must try to remove the system from the main part of the network without killing the attacker's session, because the team is still trying to track down the individual and obtain additional evidence against him or her.
 5. *If the organization has the capability, it should entice the intruder into a safe system that seemingly contains valuable data.* This is generally known as a "honey pot." By providing the attacker with an area to play in that appears to have extremely vital information, he or she remains in this system for a while, giving the team time to trace the individual back home. There has been much discussion in security-focused mail lists¹ regarding honey pots. The general consensus is that they are too dangerous in most cases because they are difficult to configure in a secure manner. However, if the organization wishes to use one, it must be in place prior to the intrusion. Also, the login banner must indicate that people who access the site consent to monitoring.
 6. *Discover the identity of the intruder while documenting his or her activity.* This is one of the reasons to bring in law enforcement early on. In most cases, attackers will not be attacking the system from their personal PCs or workstations. Instead, they will have compromised multiple sites and will use them as the conduit for their attack against the system. Some of these sites may be in a different country, requiring the assistance of a federal law enforcement agency to perform some of the tracing, such as the FBI in the United States, Scotland Yard in the United Kingdom, or Interpol. To be able to trace back through the various legs, the organization will also need the assistance of the various Internet service providers (ISPs) and telephone companies. Most ISPs and telephone companies will only provide assistance if are they served with a warrant for their records, and it is the law enforcement agencies that must usually obtain the warrants to perform searches. The international angle can make things even more difficult. In the meanwhile, the organization can document that the attack against the system is coming from "IP address A," which

would be owned by such IP address providers as ARIN, Network Solutions, RIPE, or APNIC, for example.

7. *Discover how the intruder gained access to the compromised systems, and secure these access points on all uncompromised systems.* The organization must know which vulnerability point the intruder used to gain access to the system. Once the vulnerability is known, it can be removed from the systems that have not been compromised but remain susceptible to that particular vulnerability. This prevents those systems from being compromised in the future by intruders using that hole in the system.
8. *As soon as sufficient evidence has been collected, or when vital information or vital systems are endangered, terminate the current intrusion.* The intruder's session must be severed when the organization has collected sufficient evidence to use against him or her, or if the intruder is about to compromise a vital system or vital data.
9. *Document the current state of compromised systems.* The team must state whether the system was left in production, was taken offline and is being analyzed, is offline and ready to be restored to production, or is to be replaced by another system.
10. *Restore the compromised systems back to the pre-incident configuration.* The team must make sure that the systems' operating systems and application software are restored to the same condition they were in prior to the intrusion.
11. *Secure the method of unauthorized access by the intruder on all compromised systems.* The team must correct the vulnerability that was used to gain access to the systems. This could include installing the latest required patches for the system, upgrading to the latest version of the application software, changing user and system passwords, or some combination of these. When changing passwords, the new passwords must meet the password requirements stated in the organization's IT security policies, procedures, and guidelines. If these requirements are not strong enough, they should be modified.
12. *Document the time in man-hours, as well as the cost of handling the incident, providing itemization.* The cost can be used as part of the intruder's prosecution. If the intruder is convicted, it can then be used to help in sentencing.
13. *Secure all logs, audits, notes, documentation, and any other evidence that was gathered during the incident, with appropriate identification marks, securing the "chain of custody" for future prosecution.* Logs, audits, notes, and other documentation that is in paper form must be placed in thick envelopes that are securely taped. The envelopes must then be clearly marked, detailing what the envelope contains; who placed the items into the envelope, with the date and time this occurred; and the names of each person who then touched the

envelopes, including the date and time. All logs, audits, notes, and other documentation stored on electronic media must be marked in a similar fashion. These markings must be permanent so that there is no question about the “chain of evidence.” Also, at this time, a copy of these notes should be collected and formalized into an after-action report, and a copy of the latter should be placed with the rest of the evidence.

14. *Develop lessons learned.* The CIRT and the IT security program manager should review the after-action report, resulting in improvement ideas. These might include modifying system security and configuration guidelines, improving user security awareness, modifying IT security policies and procedures, or modifying security incident response procedures.
15. *Brief upper management on the incident's aftermath.* The military calls this an after-mission debriefing. The IT security program manager and the IS security manager hereby discuss the incident with upper management, in terms of what occurred, what was done to combat the incident, the results of the incident, and what must be done to prevent similar events from occurring. While upper management must be informed of what is going on during the entire incident, they must also be told the entire story at the end.

SUMMARY

This article highlights several factors that are required for an effective computer incident response plan. They include the constituency of the plan; the makeup and duties of the team that handles the incident; the procedures for reporting suspected incidents; and the different procedures to follow, depending on management's position regarding the perpetrators.

The success of the plan depends on how well it is understood and accepted by both upper management and the system users. They must all be comfortable with the plan and trust it if they are to support it and follow the procedures. This plan must be part of a comprehensive IT security program. The latter must include IT security awareness training, incorporating the plan with the rest of the training.

Note

1. Security Focus mail lists, URL <http://www.securityfocus.com>, founded by Elias Levy (aka aleph) as Bugtraq.

David Adler and Kenneth L. Grossman, CISSP, are Information Security Specialists for the Federal Computer Incident Response Capability (FedCIRC), part of the Office of Information Assurance and Critical Infrastructure Protection, GSA/FTS. They can be reached at dadler@fedcirc.gov and kgrossman@fedcirc.gov, respectively.