DATA SECURITY MANAGEMENT

CIRT: Responding to Attack

Chris Hare, CISSP, ACE

INSIDE

History; Who is Attacking Who? The Nature of the Attack; The First CERT; Learning from the Morris Worm; Legal Issues; Threat Analysis; CIRT: Roles and Responses; Defining Incidents; When does the CIRT Respond? Relationship to External Agencies; CIRT: The CIRT Process; Establishing the Process Owner; Establishing the Team; Creating the CIRT Operation Process; Policy and Procedures; Funding; Authority

INTRODUCTION

This article presents a number of topics and issues for today's organization when considering the requirements and impact of establishing a Computer Incident Response Team (CIRT). This article makes no assumptions as to where a CIRT should be positioned from an organizational perspective within an organization, but focuses on why establishing a CIRT is important and what is involved in setting one up.

The term Computer Emergency Response Team, or CERT, is used to identify the government-funded team located at Carnegie Mellon University. The university has trademarked the name CERT (http://www.cert.org). Consequently, incident response teams are known by one of several other names. These include:

- Computer Incident Response Team (CIRT)
- Computer Security Incident Response Team (CSIRT)
- Systems Security Incident Response Team (SSIRT)

Regardless of the nomenclature, the CIRT is typically responsible for the initial evaluation of a computer security incident and providing corrective action recommendations to management. This article explores in detail the prerequisites, roles and re-

PAYOFF IDEA

Incident response using a well-prepared CIRT is insurance that an effective team is ready to answer the call should a computer security incident occur. This proactive approach to computer crime is becoming a baseline security measure. Those organizations not prepared with the equivalent of a CIRT could be considered negligent if a major incident causes major losses.

sponsibilities, and supportive processes necessary for a successful CIRT capability.

HISTORY

Prior to the Morris Internet Worm of 1988, computer security incidents did not really get a lot of attention, as the problem was not well understood. At that time, there was only a fraction of the total network hosts connected today.

The Morris Worm demonstrated to the Internet community, and to the computing world in general, that any determined attacker could cause damage, wreak havoc, and paralyze communication systems by using several commonly known vulnerabilities in UNIX system applications.

The nature of the problem is quite severe. An Internet mailing list known as BUGTRAQ discussed security issues and vulnerabilities in applications and operating systems. This mailing list currently has a volume of more than 1000 messages per quarter, most of which are exploits, bugs, or concerns about commercial applications.

Consider that IBM's mature MVS operating system has 17 million lines of assembly language instructions. Microsoft's Windows NT 5 (Windows 2000) has more than 48 million lines of C and assembly language code. The recognized "bug" factor is one bug for each 1000 lines of code. Windows NT 4 had more than 100,000 validated bugs. This means that there is potential for 48,000 bugs in Windows NT 5.

These bugs provide the perfect opportunity for the attacker to gain access to a system, and either steal, modify, or destroy information or resources from the system owner.

WHO IS ATTACKING WHO?

The nature of the attacker is changing dramatically. Considering the movies of a few years ago, *The Net* and *Sneakers*, computer hackers were portrayed as well-educated adults who knew their way around computer systems. They understood what information they needed, how to get it, and what they had to do once they gained access to a system.

Attacker profiles vary considerably:

- **The Naïve**: These attackers have little real knowledge or experience. They are out to do it for fun, with no understanding of the potential consequences.
- **Brutish** (script kiddies): These attackers also lack little real knowledge, and make heavy use of the various attack tools that exist. This means that they become obvious and visible on attacked systems due to the heavy probing and scanning used.

- **Clueful**: These are more experienced attackers, who use a variety of techniques to gain access to the system. The attacks are generally more subtle and less obvious.
- **Truly Subtle**: These are the computer criminals of the twenty-first century. They know what they want, who will pay for it, how to get access, and how to move around the system once they enter it. These attackers leave few or no traces on a system that they were in fact there.

The Teenage Attacker

The development of more sophisticated tools has lowered the required sophistication level of the attacker. There are reports of attackers who successfully used the tools to gain access to a system, but then did not know what to do once they got in.

Many teenage attackers also make use of the techniques demonstrated by actor Matthew Broderick in the 1980s movie *War Games*. Broderick used a program known as a "war dialer" to locate the modem tones for computer systems. Today's tools provide the naïve or clueful and brutish attackers with the necessary tools to gain access to almost any system. These tools are meant to be stealthy by nature; and while frequently used by the people outside the organization, they are also used from within. Information on common exploits and attacked sites are available at http://www.rootshell.com, among others.

While these tools do provide an easier method to compromise a system and gain access, attackers must still know what to do on the system once they have gained access. Recent attempts, as reported in *Systems Administration and Network Security (SANS)* (http://www.sans.org) bulletins and briefings, show that some successful attacks result in little damage or information loss because the attacker did not know how to interact with the system.

The Insider

Insiders may or may not have malicious intent. Their authorized presence on the network allows them virtually unrestricted access to anything, and may allow them to access information that they would normally not have the authority to access. This makes the distinction between the fact that employees are authorized to access the network and specific information and applications available. It does not imply that an employee has any implicit or explicit authorization to access all of the information available on the network.

Malicious insiders are insidious individuals whose goal is to steal or manipulate information so that the company does not have access to complete and accurate data. They may simply destroy it, provide it to the competition, or attempt to embarrass the company by leaking it to the

media. These people have authorized access to the network, and therefore are difficult to trace and monitor effectively.

Insiders who are experiencing personal difficulties (e.g., as financial problems), are targets for recruitment by competitive intelligence agencies.

Even more important, insiders can make copies of the information and leave the original intact, thereby making it more difficult to detect that a theft took place. Those insiders that do cause damage lead to detection of the event, but those that undertake some planning make detection much more difficult — if not impossible.

The Industrial Spy

Probably the most feared are the industrial spies. These attackers specifically target a particular company as a place from which to obtain information that they have been hired to collect, or that they believe will be considered valuable to others who would buy it. This is known as industrial or economic espionage. The difference between the two is that industrial espionage is conducted by organizations on behalf of companies, while economic espionage is data collection that is authorized and driven by governments.

These criminals are likely well-trained and will use any means at their disposal to discover and steal or destroy information, including social engineering, dumpster diving, coordinated network attacks, even getting a job as a contractor. The FBI (http://www.fbi.org) states that a typical organization can expect that one in every 700 employees is actively working against the company.

THE NATURE OF THE ATTACK

The attackers have a variety of tools and an increasing number of vulnerabilities in today's software from which to choose. The nature of the attack and the tools used will vary for each of the attacker types and their intent.

Attack Tools

A very extensive — and for the most part easily obtained — set of attack tools is available to today's attacker. They range from C language files that must be compiled and run against a system, to complex scanning and analysis tools such as *nmap*. A sample *nmap* run against several different hosts is illustrated in Exhibit 1.

The output of the various attack tools can provide the attacker with a wealth of information regarding the system platform, and as such is used by many attackers and system administrators alike. For example, the output illustrated in Exhibit 1 identifies the network services that are configured and additional information regarding how easy it would be to

EXHIBIT 1 — Sample Output of nmap of a Linux System

LOG OF: ./NMAP -O -V -V -O /TMP/LOG2 192.168.0.4
INTERESTING PORTS ON LINUX (192.168.0.4):

Port	State	Protocol	Service
21	open	tcp	ftp
23	open	tcp	telnet
25	open	tcp	smtp
37	open	tcp	time
79	open	tcp	finger
80	open	tcp	http
110	open	tcp	pop-3
111	open	tcp	sunrpc
113	open	tcp	auth
139	open	tcp	netbios-ssn

TCP Sequence Prediction: Class = random positive increments
Difficulty = 4686058 (Good luck!)
Remote operating system guess: Linux 2.2.0-pre6 - 2.2.2-ac5

launch a particular types of attack against the system. Take special note that it was able to correctly guess the operating system.

Viruses and Mobile Code

A virus is program code that is intended to replicate from system to system and execute a set of instructions that would not normally be executed by the user. The impact of a virus can range from simple replication, to destruction of the information stored on the system, even to destruction of the computer itself.

Viruses are quite common on the Windows platform due to the architecture of the processor and the operating system. It is likely that most computer users today have been "hit" by one virus or another. The attacker no longer has to be able to write the World Wide Web (WWW).

Use of the WWW introduces additional threats through "active code" such as Microsoft's ActiveX and Sun Microsystems' Java languages. These active code sources can be used to collect information from a system, or to introduce code to defeat the security of a system, inject a virus, or modify or destroy information.

THE FIRST CERT

The first incident response team was established by the Defense Applied Research Projects Agency (DARPA) (http://www.darpa.mil) in 1988 after the Morris Worm disabled approximately 10 percent of the computer systems connected to the Internet. This team is called the Computer Emer-

gency Response Team (CERT) and is located at the Software Engineering Institute at Carnegie Mellon University.

LEARNING FROM THE MORRIS WORM

The Morris Worm of 1988 was written by Robert Morris, Jr. to demonstrate the vulnerabilities that exist in today's software. Although Morris had contended since his arrest that his intent was not to cause the resulting damage, experts who have analyzed the program have reported that the Morris Worm operated as expected.

There were a large number of reports written in the aftermath of the incident. The U.S. General Accounting Office (GAO) issued a thorough report of the Morris Worm, its impact and the issues surrounding security on the Internet, and the prosecution of this and similar cases in the future.

The GAO report echoes observations made in other reports on the Morris Worm. These observations include:

- The lack of a focal point in addressing Internet-wide security issues contributed to problems in coordination and communication during security emergencies.
- Security weaknesses exist in some sites.
- Not all system managers have the skills and knowledge to properly secure their systems;
- The success of the Morris Worm was through its method of attack, where it made use of known bugs, trusted hosts, and password guessing.
- Problems exist in vendor patch and fix development and distribution.

While these issues were discussed after the Morris Worm incident, they are, in fact, issues that exist within many organizations today.

LEGAL ISSUES

There are many and inconsistent legal issues to be considered in investigating computer crime. It is worth noting, however, that an incident response team (or corporate investigations unit) typically has considerably more leeway in its operations than law enforcement.

As the property being investigated belongs to the company, the company is free to take any action that it deems appropriate. Once law enforcement is notified of the crime, then the situation becomes a law enforcement issue, and the organization's ability to act is significantly curtailed. This is because once law enforcement is informed, the company's investigators become agents for law enforcement and are then bound by the same constraints.

Among the legal issues that must be addressed are the rules of evidence. These vary from country to country due to differences in legal systems. These rules address how evidence must be collected and handled in order for it to be considered evidence by law enforcement agencies and in a court of law.

The exact actions that the CIRT can perform are governed by the appropriate legislation. The team will be advised by Corporate Counsel, at which point appropriate action will be taken with the intent of not jeopardizing the value of collected evidence or interviews.

THREAT ANALYSIS

Threat — and risk analysis in general — is a major proactive role of the CIRT. The CIRT must evaluate every vulnerability report and, based on an analysis of the situation, recommend the appropriate actions to management and who is responsible for completing these actions.

Most often, risk analysis focuses on new exploits or attack methods to determine if there are associated risks within the organizational environment and how such risks can best be mitigated. This is part of the CIRTs ongoing activity, and can include a variety of methods, including research and penetration testing. From this collected information, the CIRT can make recommendations on how to mitigate these risks by making changes to our computing or security infrastructures.

There is, however, the notion of "acceptable" risk. Acceptable risk is that risk which the company is knowingly prepared to accept. For example, if the company can earn $1 million but in the process has an exposure that could cause the loss of $10,000, the company may choose to accept such risk.

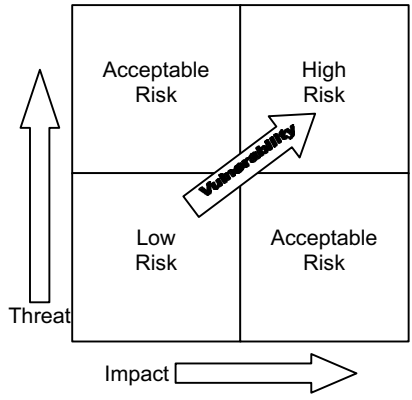
These decisions, however, cannot be made by just anyone in the organization. The exact nature of the vulnerability, the threat, and the resulting impact must be clearly evaluated and understood.

- *Threat* is defined as the potential to cause harm to the corporation — intentional or otherwise. Threats include hackers, industrial espionage, and at times, internal employees.
- *Vulnerability* is a weakness or threat to the asset. If there are no vulnerabilities, then a threat cannot put the organization at risk.
- *Impact* reflects degree of harm and is concerned with how significant the problem is, or how much effect it will have on the company.

The threat graph in Exhibit 2 illustrates threat, impact, and vulnerability. The risk is lowest when threat and impact are both low. Low impact, low threat, and low vulnerability imply that the *risk* is also low.

If the threat is low, the impact is high, and the vulnerability is low, the company may accept the risk of information loss. The same is true if the

EXHIBIT 2 — Threat Graph: Threat, Impact, and Vulnerability



impact is low, the vulnerability low, and the threat high. This may still be an acceptable risk to the organization.

Finally, as the impact, vulnerability, and threat all increase, the issue becomes one of high risk. This is typically the area that most companies choose to address and place their emphasis. This is where the greatest risk is and, consequently, where the greatest return on security investment is found.

CIRT: ROLES AND RESPONSES

Most people think of "Incident Response Teams" as the emergency response unit for computers. The confusing term is "computer." A security incident that involves a computer is only different from a physical security incident in how the event took place. When an unauthorized person gains tactical access to a system or specific information, it should have equivalent importance to unauthorized physical access.

The CIRT must be able to handle a crisis and prevent it from becoming worse than it already is. The CIRT, however, has much more to offer, including a proactive role of vulnerability testing, vulnerability analysis, and awareness.

Obviously, the exact nature of responsibilities that one assigns to a CIRT will depend on the size and nature of the organization, the number of incidents recorded, and how many systems and networks exist. Consequently, some of the suggested activities may not be possible for a CIRT to integrate into its day-to-day tasks.

Incident Response

As mentioned, incident response is the prime reason behind establishing a CIRT. This incident response team puts highly trained people at the forefront of any incident, and allows for a consistently applied approach to resolving the incident. The team handles the investigation from start to finish and makes recommendations to management regarding its findings.

Vulnerability Testing

There are two elements to vulnerability testing. The first is to use automated tools with preconfigured tests to determine if there are vulnerabilities that could be exploited by an attacker. The second element test security implementation is to try it out. A penetration or protection test simulates the various types of attacks — internal and external, blind and informed — against the countermeasures of the network. Essentially, a penetration test attempts to gain access through available vulnerabilities by taking on the mindset of the perpetrator.

As the CIRT is responsible for investigating incidents, over time it will develop a set of skills that can be used to offer penetration or protection testing services to the organization's product developers or IS organization. Vulnerability testing is considered the cornerstone of the effort to improve a security program as it attempts to use vulnerabilities as an attacker would. Protection testing is conducted in a similar manner, but the goal is different.

Types of Penetration Tests. There are essentially three major types of penetration testing, each with its own tools and techniques:

> **Level 1**. Zero-Knowledge Penetration testing: This attempts to penetrate the network from an external source without knowledge of its architecture. However, information that is obtained through publicly accessible information is not excluded.
> **Level 2**. Full-Knowledge Penetration testing: This attempts to penetrate the network from an external source with full knowledge of the network architecture and software levels.
> **Level 3**. Internal Penetration testing: This attempts to compromise network security and hosts from inside one's network.

Penetration testing is interval based, meaning that it is done from time to time and against different target points. Penetration testing is not a real-time activity.

The process consists of collecting information about the network and executing the test. In a level 1 test, the only information available is what is published through open source information. This includes network broadcasts, upstream Internet service providers, domain name

servers, and public registration records. This helps simulate an attack from an unsophisticated intruder who may try various standard approaches. This approach primarily tests one's ability to detect and respond to an attack.

A Level 2 penetration test assumes full knowledge of the hardware and software used on the network. Such information may be available to meticulous and determined intruders using whatever means, including social engineering, to increase their understanding of one's networks. This stage of the test assumes the worst-possible scenario, and calls to light the maximum number of vulnerabilities.

A Level 3 penetration test (or acid test) is an attack from within the network. This is the best judge of the quality of the implementation of the company's security policy. A real attack from within a network can come from various sources, including disgruntled employees, accidental attacks, and brazen intruders who can socially engineer their way physically into a company.

Penetration testing should be considered very carefully in the implementation of an overall detection program, but it can lead to the negative side effects that one is trying to prevent. Therefore, it should be used cautiously, but still be used to attempt to locate vulnerabilities and to assess the overall operation of the protection program.

Studying Security Vulnerabilities

When an incident occurs, it is essential to understand what allowed it to happen. Examining the vulnerability used during the incident allows the organization to improve its Security Infrastructure Program to prevent further exploitation.

In addition, security vulnerabilities that are released to the security community need to be assessed for their impact within the organization, and a course of action recommended. The CIRT, with its enhanced skills and knowledge, is capable of reviewing those vulnerabilities and offering the operating system and product groups a method of addressing them.

Publishing Security Alerts

When new issues are found that impact the organization, the CIRT is responsible for the publication of those bulletins and warnings, along with a set of instructions or recommendations regarding how users and systems administrators should react.

Publishing security alerts within the corporation, or new vulnerabilities found, does not include publishing the details of security incidents. The reporting of security incidents is a role for Corporate Security.

Working from the analysis of incident data, the CIRT is able to make specific recommendations to the systems administrators or applications owners on how to better configure their systems to increase the level of security.

Survivability comes from the application of good administration and consistently applied security techniques to reduce the threat of loss of data from an incident, or the loss of the system. Having to completely rebuild a system is an onerous task that is costly to the business, and one that few people want to repeat frequently.

DEFINING INCIDENTS

An obvious question is, "What is an incident?" Incidents cannot be easily identified without the team. However, an incident can be defined as any unexpected action that has an immediate or potential effect on the organization.

Example incidents include:

- viruses
- unauthorized access, regardless of source
- information theft or loss of confidentiality
- attacks against systems
- denial of service
- information corruption

However, incidents can be further classified based upon the extent to which the incident affects the organization.

The classification of CIRT responses is often based on several factors, including geography, business impact, and the apparent nature of the problem. Business impact includes how many people are affected; how many sites are affected, and will the issue affect stock prices, investor confidence, or damage the organization's reputation.

These classifications are meant to be a guide for discussion purposes — the CIRT may choose to broaden or identify improved characteristics for each.

Class 1: Global. These incidents have the greatest impact on an organization. They have the potential of affecting the entire organization, and they are serious. The uncorrected distribution of a virus can have very significant effects on the organization's ability to function. Other examples include a firewall breach, potential financial loss, customer services, compromise of the corporation's credibility, or the compromise of the organization's external Web site. In these situations, the CIRT is activated immediately, due to the threat to the company.

Class 2: Regional. Regional incidents affect specific areas of the company. They do, however, have the capability of becoming global. Regional threats include logic bombs, and attacks against specific systems in that region. While these can become global in nature, the information systems and security organizations in that region may be able to handle the issue without involvement from the CIRT. In this situation, the CIRT is activated at the request of the region IS or Security Directors.

Class 3: Local. Local incidents are isolated to a specific department and are of low impact. Examples include a virus on a single system, and the building cleaning crew playing solitaire on improperly configured desktop systems. In this situation, the CIRT is not activated unless requested by the department manager.

WHEN DOES THE CIRT RESPOND?

The CIRT responds in one of several situations:

- at the request of a manager when an event is noticed or reported to them
- when the incident requires it, based on sufficient evidence, probability, or due to a pattern of occurrence
- as the result of issues found during vulnerability testing
- on the advice of the help desk personnel who receive problem reports
- on the advice of an external security agency

CIRT response is based on the severity of an issue, as outlined previously. Managers can request CIRT involvement when they suspect unauthorized activity, regardless of whether there has been an incident reported to the CIRT.

If an incident is believed to have occurred based upon evidence (e.g., missing or altered information in a database) or due to alerts from an intrusion detection system, the CIRT is involved to determine the significance, scope, and method of the attack.

It is important to note that help desks can assist in reporting incidents to the CIRT. As employees call their help desks with issues, the help desk may see a pattern emerge that will initiate contacting the CIRT. Consequently, additional training is required for the help-desk staff to inform them of what they should be looking for.

The CIRT then provides a recommendation on how to address the attack and proceed with the investigation of the incident. In some situations, external agencies such as security departments of other organizations may advise of a potential incident and this must be investigated.

RELATIONSHIP TO EXTERNAL AGENCIES

The CIRT operates within the organizational framework and reviews incidents and provides other services as discussed. It is important, however, that the CIRT establish a relationship with external Computer Emergency Response Teams, such as CERT, CANCERT, etc. These teams provide similar services, but focus on incident reporting and advisory capabilities.

In addition, contact with law enforcement and other external teams that may be required must be established early on, so that if an issue arises, the CIRT is not spending valuable time looking for the correct external resource and then contacting them.

CIRT: THE CIRT PROCESS

There is a defined process for creating and establishing the CIRT function. This process is presented in this section. The process consists of six steps. These steps are explained here, but more information on some of the process steps is discussed in other sections.

CIRT is a global process. The team must be available 24 hours a day, 365 days per year. As such, mechanisms to contact the CIRT regardless of where the incident is, must be put into place to allow quick response.

1. Establishing the Process Owner

The *process owner* is responsible for supporting the team, and is the individual to whom the team itself reports. The process owner provides the interface to executive management and ensures that the CIRT is fulfilling its responsibilities effectively.

The process owner is assigned by senior management — not by the reputation or position of a single individual. Many organizations choose the Chief Information Officer (CIO) as the process owner, due to the technical nature of the team. While this is not necessarily incorrect, it is now considered more appropriate to choose either the Chief Financial Officer (CFO) or the Internal Audit Director to avoid any possibility of conflict of interest. The two alternate positions have legally defined fiduciary responsibilities to protect the corporation's assets and their departments often include staff with fraud investigation backgrounds.

2. Establishing the Team

The development of a CIRT is a process that requires full acceptance from the corporation's executives, *and* the groups involved in forming the core team. Specific resources, funding, and authority must be granted for the initiative to be successful and have benefit to the corporation. This section discusses the structure of the CIRT and how it interacts with other internal organizations.

Many organizations consider computer security incidents as an IS problem, while in fact they are a business problem. They are a business problem because any security incident, regardless of how it is caused, has the potential to affect the corporation in many ways, including financial loss, legal or financial liabilities, or customer service.

The very nature of computer involvement means that what is deemed to be an incident may not be when investigated. For example, consider the user who forgets his password and disables it. This may appear like a denial-of-service attack, when in fact it is not. This strains the internal investigative resources, and impacts the company by redirecting resources where they are not needed.

The investigation of an event is a complex process that involves a precise sequence of events and processes to ensure that, should the corporation choose to, it could involve law enforcement and not lose access to the valuable information, or evidence, already collected.

To do this, and for the response to any incident to be effective, people with a wide range of backgrounds and experiences are required. The CIRT ideally would have people from the following areas:

- technical specialists: an understanding of the production aspects of the technology that are relevant to the investigation
- information security specialists: data and systems protection
- auditors and fraud examiners: compliance and fraud
- corporate security: investigations
- human resources: personnel and labor issues
- business continuity specialists: system and data recovery
- legal specialists: protecting the organization's intellectual property
- corporate public relations: press and media interaction
- executive management: the decision-makers
- any other organization- or industry-specific personnel, such as business unit or geographically relevant personnel

The Core Team. For most organizations, it is difficult to rationalize the dedication of such a group of people to the CIRT role and, consequently, it is seen within the industry that the CIRT has two major components: a core team and a support team. The core team is composed of five disciplines, preferably staffed by a single individual from each discipline. These disciplines are:

- corporate security
- internal audit
- information protection
- legal specialists.
- technical specialists, as required

The CIRT core team must:

- determine if the incident is a violation
- determine the cause and advise management on the action required
- if required, establish the appropriately skilled support team
- manage the investigation and report
- call in external agencies as necessary

It is essential that the core team be made up of individuals who have the experience required to determine the nature of the incident and involve the appropriate assistance when required.

Many larger organizations have a corporate security group that provides the investigators who are generally prime for the incident. Smaller organizations may have a need to address their investigative needs with a security generalist. This is because the ultimate recommendation for the CIRT may be to turn the incident over to the corporate security organization for further investigation or to contact law enforcement. Obviously, the correct course of action depends on organization structure, and whether or not to contact law enforcement. In that event, specific rules must have been followed. These rules, while important, are not germane to the discussion here.

Internal Audit Services provide the compliance component. Every organization is required to demonstrate compliance with its policies and general business practices. The internal audit organization brings the compliance component to the team; moreover, it will be able to recommend specific actions that are to be taken to prevent further incidents.

The Information Protection or Information Services security specialist is required because the incident involved the use of a computer. The skills that this person holds will enable rapid determination of the path of the attack from one place to another, or gain rapid access to the information contained on a system.

Legal Specialists are essential to make sure that any actions taken by the CIRT are not in violation of any existing corporate procedures, ofany rights of any individuals within the company or country. This is especially important, as there are different laws and regulations governing the corporation and the rights of the individual in many countries.

While team members have these backgrounds in their respective areas, the core team operates in one of two ways:

- dedicated full-time to the role of the CIRT and its additional responsibilities identified previously
- called as needed to examine the incident

In large, geographically dispersed organizations, the CIRT must be capable of deploying quickly and getting the information such as logs, files,

buffers, etc., while it is still "fresh," There is no "smoking gun" — only the remnants left behind. Quick action on the part of the CIRT may enable collection of incident-related information that would otherwise be rendered useless as evidence minutes or hours or later.

Selecting the Core Team Members. The selection of the core team members is done based on experience within their knowledge area, their ability to work both individually and as part of a team, and their knowledge of the company as a whole. The process owner, who will select a team leader and then work together to choose the other members of the core team, would conduct the selection process. It is recommended that the team leader be a cooperating member of the team, and that the team leader operate as the point of contact for any requests for assistance.

The Support Team. The support team is used to provide additional resources once the core team has determined what the incident really is, and what other experts need to be called in to assess the situation.

The support team is vital to the operational support of the core team. This is because it is impossible for the core team to have all of the knowledge and expertise to handle every possible scenario and situation. For the core team to be effective, it must identify who the support team members are and maintain contact with and backup information for them over time.

The Support team consists of:

- human resources (HR)
- corporate communications
- platform and technology specialists
- fraud specialist
- others as required, such as business unit specialists or those geographically close to the incident.

Human resources (HR) is a requirement because any issue that is caused by an employee will require HR's involvement up front to assist in the collection of relevant information, and discussion of the situation with the employee's manager and the employee, and recommendations of appropriate sanctions.

If the incident is a major one that might gain public attention, it is recommended that the corporate public relations function issue a press release earlier, rather than take "knocks" from the public press. While any bad news can affect a company, by releasing such information on its own, the company can retain control of the incident and report on planned actions. However, it is essential that any press announcements must be cleared through the appropriate departments within the company, including the legal department and senior management. However,

there have been sufficient examples with companies (like Microsoft) that would argue this point both ways.

Additionally, the team must designate an individual who is not actively participating to provide information and feedback to management and employees, as deemed appropriate. By choosing a person who does not have an active part in that particular investigation, that person can focus on the communications aspect and let the rest of the team get the job done.

The platform and technology specialists are used to provide support to the team, as no single individual can be aware of and handle all of the technology-related issues in the company. It is also likely that multiple technical specialists will be required, depending on the nature of the incident.

Fraud specialists provide guidance on the direction and investigation of fraud. In some cases, fraud will be hidden behind other issues to cloud the fraud and throw confusion on the issue.

The core team does the selection of the support team members. The core team must evaluate what types of skills it must have access to and then engage the various units within the organization to locate those skills.

It is essential that the core team conduct this activity to allow establishment of a network of contacts should the identified support team member and his or her backup be unavailable. Support team members are selected based on experience within their knowledge area, their ability to work both individually and as part of a team, and their knowledge of the company as a whole.

A major responsibility of the core team is to maintain this database of support team members to allow for quick response by the team when its involvement is required.

3. Creating the CIRT Operation Process

With the structure of the actual team in mind, it becomes necessary to focus on how the CIRT will operate. This is something that cannot be easily established in advance of core team selection. The process defines the exact steps that are followed each time the team is activated, either by request or due to the nature of the incident.

Aside from some steps that are required to create, establish, and authorize the team, the remaining steps in the process are to be handled by the core team. In addition to training and various other roles, the team must also:

- document its own practices and procedures
- establish and maintain databases of contact names and information
- maintain software and hardware tools required and used during an incident

Several matrices must be developed by the newly formed CIRT. These include an incident matrix and a response matrix. In the incident matrix, the team attempts to discover every possible scenario, and establish the:

- incident type
- personnel required
- financial resources required
- source of resources

With this, the CIRT can establish the broad budget it will need to investigate incidents. The response matrix identifies the incident type, what the team feels is an appropriate response to the incident, what resources it anticipates will be needed, and how it will escalate the incident should that become necessary. Neither of these matrices can be developed without the core team, and even some initial members of the support teams.

With the matrices completed, it is necessary to establish the training and funding requirements for the team.

Training Requirements. With the CIRT formed, it is necessary that the training requirements be determined. At a minimum, all members of the core team will need to be trained in intrusion management techniques, investigations, interviewing, and some level of computer forensics. (There are organizations that can conduct training specifically in these areas.)

Funding Requirements. The CIRT must now establish its requirements for a budget to purchase the needed equipment that will be used on a frequent or daily basis. A contingency budget is also needed to establish spending limits on equipment that is needed in the middle of an incident.

Given the nature and size of the core team, it is easy to establish that personnel budgets within a large organization will include a minimum of $500K for salaries and other employee costs. Training will approximate $50K per year, with an initial training expense of approximately $100K.

4. Policy and Procedures

The operation of the CIRT must be supported through policy. The policy establishes the reasons for establishing a CIRT, its authority, and the limits on its actions. Aside from the issues regarding policy in general, policies that support a CIRT must:

- not violate the law: doing so results in problems should the need for law enforcement result, or if the employee challenges the actions taken by the company as a result

- address privacy: employees must be informed in advance that they have no reasonable expectation of privacy (management has the right to search e-mail, stored files and their on-site workstations during an investigation)
- have corporate counsel review and approve the policy and procedures as being legal and sustainable in the given local areas

The policy itself leaves out the specifics surrounding the CIRT and how it operates. These are written in standards and procedures and describe how the team will react in specific situations, who the team members are, what the organization structure is, etc.

As mentioned, the employee must not have any expectation of privacy. This can only be accomplished effectively by understanding the privacy laws in the different regions, and stating specifically in policy, that this is the case.

CIRT members should operate within a code of ethics specifically designed for them, as they will be in contact and learn information about employees or situations that they would otherwise not know.

5. Funding

Funding is essential to the operation of the CIRT. While it is impossible to know what every investigation will cost, the team will have established a series of matrices identifying possible incidents and the equipment and resources required to handle them. This information is required to establish an operating budget, but contingency funds must be available should an incident cause the team to run over budget, or need a resource that was not planned.

Obviously, not having this information up front affects senior management's decisions to allocate base funding. This means, however, that senior management must believe in the role of the CIRT and the value that it brings to the overall security posture. The CIRT process owner in consultation with the identified CIRT members and external CIRTs, should be able to establish a broad level of required funding and modify it once the matrices are completed.

6. Authority

The CIRT must be granted the authority to act by senior management. This means that during an investigation of an incident, employees — regardless of level in the company — must be directed to cooperate with the CIRT. They must operate with extreme attention to confidentiality of the information they collect. The CIRT's responsibility is to collect evidence and make recommendations — not to determine guilt.

The role of the CIRT, as previously mentioned, is to investigate incidents and recommend appropriate actions to be taken by management

to deal appropriately with the issues. The authority for the creation of the CIRT and its ability to get the job done is conveyed through policy.

SUMMARY

In a previous article this author has discussed intrusion detection.[1] Intrusion detection, regardless of the complexity and accuracy of the system, is not effective without an incident response capability. Consequently, any organization — regardless of size — must bear this in mind when deciding to go ahead with intrusion detection.

But incident response goes well beyond. Incident response is a proactive response to an incident. However, the CIRT can assist in the prevention and detection phases of the security cycle, and thereby create a much stronger, more resilient, and more responsive security infrastructure for today's organization.

Note

1. Intrusion detection is the focus of Chris Hare's article in *Data Security Management*, 84-10-31, April – May 2000.

Chris Hare, CISSP, ACE, teaches information security at Algonquin College (Ottawa, Canada) and sits on the Advisory Council for this program. Chris is currently employed with Nortel Networks as a systems auditor in the Internal Audit Department.

CIRT: References

1. Farrow, Rik, *Intrusion Techniques and Countermeasures*. Computer Security Institute: San Francisco, 1999
2. Icove, David, Seger, Karl, and VonStorch, William, *Computer Crime: A Crime Fighter's Handbook*, O'Reilly & Associates: Sebastopol, CA, 1995.
3. Stephenson, Peter, *How to Form a Skilled Computer Incident Response Team*, Computer Security Institute: San Francisco, 1999.
4. CERT, *Responding to Intrusions*, Carnegie Mellon Software Engineering Institute 1998.
5. Winkler, Ira, *Corporate Espionage*, Prima Publishing: Rocklin, California, 1997.