4

Forming and Managing an Incident Response Team

FROM TIME TO TIME, WE'VE MENTIONED THE word "team" in the process of covering various topics related to incident response. This chapter delves into forming and managing an incident response team—what a response team is, the rationale for forming an incident response team, major issues that must be addressed, and special management considerations. These topics are particularly important. Many incident response efforts fail or flounder because of mistakes made in forming and/or managing a response team. This chapter again presents the authors' perspectives and real-life experiences in dealing with the many issues related to this area. We will begin by considering the most fundamental part of an "incident response team"—the meaning of the term itself.

What Is an Incident Response Team?

In many contexts, you will see "incident response" equated with "incident response team." Equating these two constructs might superficially appear logical, but doing so often constitutes a departure from reality. Why? People who know little or nothing about the process of incident response often become involved in dealing with security-related incidents. Users are a classic example.

Suppose a worm infects numerous systems. Users might collaborate to analyze what has happened and to combat the worm, yet they can hardly be called an incident response team. The reason is that an incident response team is a capability responsible for dealing with potential or real information security incidents. A team is assigned a set of duties related to bringing each security-related incident to a conclusion, ideally in accordance with the goals of the organization it serves. *The difference, therefore, between individuals who are dealing with an incident and an incident response team is the mission—in terms of job-related responsibilities—assigned to each.* Individuals might sometimes become involved in dealing with incidents, but an incident response team is assigned the responsibility of dealing with incidents as part or all of the job descriptions of the individuals involved.

How many individuals must be involved in an incident response effort for them to collectively be considered a team? A team consists of one or more individuals. You might ask how a team can consist of one individual when one person is not, in most situations, sufficient to deal adequately with most incidents. The answer is that one individual can effectively serve as the coordinator of efforts by a number of people. When incident handling efforts are finished, the others involved in the incident are released from any responsibilities they might have had in dealing with incident. But the team member has the ongoing, day-to-day responsibility of handling incidents and will have to deal with the next incident that occurs.

Many incident response teams have many team members, each with a specialized role. Consider, for example, the Computer Emergency Response Team Coordination Center (CERT/CC). Some of the many members of this team are engaged in daily operations, receiving reports of incidents and attempting to identify the type, source, impact, and other facets of security-related incidents that are reported. Others attempt to deal with vendors to close known vulnerabilities in operating systems, applications, and so forth. Still others examine data to identify and project incident trends, something that is more related to research.

Outsourcing Incident Response Efforts

Should an organization have its own incident response effort, or should it contract with a consultancy or contractor to provide incident response support? The answer in most cases is that it depends on a number of basic factors. Let's consider the alternatives.

Hiring a Contractor or Consultancy. One of the many advantages of contracting with a commercial incident response team is that the overall cost of dealing with security-related incidents is likely to be lower. Why? Incident response personnel—contractors or consultants—need to deal only with incidents that occur. Unless there is a plethora of incidents, there is no need to keep regular personnel around to wait for incidents to occur. Additionally, contractors or consultancies usually offer special kinds of expertise that are often not available within any particular organization. Be careful, however. Many consultancies and service providers offer incident response services, some of which are far superior to others. Be sure to ask for references, preferably from current and ex-customers, before signing any contract for incident response services with any consultancy or service provider.

Using In-House Capability. The major rationale for developing an in-house incident response capability is to handle incidents in accordance with the policy and cultural/political needs of an organization. Security-related incidents are potentially very sensitive and political; an in-house capability is likely to deal with them in a manner that is most advantageous to the organization (provided, of course, that the individuals within this capability understand the culture and politics of the organization).

Why Form an Incident Response Team?

Why might some organizations want to form an incident response team? This section focuses on some possible reasons.

Ability to Coordinate

In general, it is easier to coordinate the efforts of individuals who are on an incident response team because they generally report to the team leader, who can direct them to become involved in one particular activity or another.

Expertise

Information security incidents are becoming increasingly complex; *incident handling experts* are thus becoming increasingly necessary. Technical gurus always come in handy when incidents occur, but pure technical expertise is not enough when it comes to many incidents. Having helped with many previous incidents, knowing what policies to consider and procedures to follow, and so forth are just as critical, if not more critical, than pure technical skills. One of the best ways to build expertise is to serve on a dedicated incident response function.

Efficiency

A team builds a collective knowledge that often leads to increased efficiency. An isolated individual can easily go astray in dealing with an incident, but collective wisdom accrued within a team can help incident response efforts get back on track. Additionally, a team (as opposed to any individual or a few independent individuals) is more likely to develop and follow procedures for incident response, something that boosts efficiency.

Ability to Work Proactively

Being proactive (that is, adopting measures that address incident response needs before incidents actually occur) is one of the keys to a successful incident response effort. Training users and system administrators to recognize the symptoms of incidents and what to do (as well as what *not* to do) is a good example of a proactive effort. Although it is possible for any number of individuals to engage in proactive efforts, having a team increases the likelihood that proactive efforts will occur. Having a team allows the luxury of having different persons specialize in different functions, especially in proactive activity. Additionally, successful proactive efforts are often the byproduct of successful collaboration by teams; individuals are not as likely to think of and carry out successful proactive activity.

Ability to Meet Agency or Corporate Requirements

Another advantage of having an incident response team is that a team is generally better suited to meeting agency or corporate requirements. The main reason is that a team has individuals who are geared toward the same mission. Note that some government agencies and corporations go one step further in that they *require* (through a management directive or a policy statement) that an incident response team be formed.

Serving a Liaison Function

Response teams are better suited to serving a liaison function than are individuals because outside entities are not likely to learn of and/or be motivated to deal with individuals. Having a team identity provides extra external visibility as well as credibility, both of which are more suited to the liaison function. Furthermore, a "team," in many respects, commands a certain degree of legitimacy within internal and external organizations.

Ability to Deal with Institutional Barriers

Institutional politics invariably affect virtually any effort that occurs within an institution. Incident response teams (or at least incident response teams sanctioned by senior management), however, provide at least some degree of immunity from politics that provide barriers to incident response efforts. The main reason is that these teams are likely to have more authority to take action—such as shutting down systems that have been compromised at the superuser level—than individuals. Additionally, teams often involve individuals from a cross-section of organizations and groups, making them more politically palatable within a range of an organization's divisions and groups.

Issues in Forming a Response Team

Forming an incident response team generally is not as easy as it superficially might appear. The individual(s) charged with this responsibility must deal with many key issues, including policy, whether or not a team is really necessary, defining and communicating with a constituency, defining functional requirements, defining the role of the incident response team, staffing the team appropriately, and creating and updating operational procedures. This section discusses these issues.

Policy

The most important issue in forming and managing an incident response team, all things considered, is policy. Any incident response team must always operate within the constraints of the policy of the organization to which it belongs or that it serves. Suppose, for example, an organization requires that no employee make contact with or answer questions from the press unless that person obtains written approval from the head of the public relations department. Another organizational policy provision might be that no system being attacked can stay connected to the network if it holds extremely valuable resources (such as proprietary data, proprietary source code, and so forth).

Additionally, an incident response team might impose its own policy provisions on its own operations. A policy provision of this nature might be that no team member can spread information about any incident outside of the immediate team without the direct permission of the team leader. Failure to conform to existing policy spells catastrophe for an incident response team; consequences can range from embarrassment to termination of employment or even to dissolution of the team itself.

Is a Team Really Necessary?

Another extremely important issue is whether an incident response team is really necessary. Some of the advantages of forming a response team have been presented earlier in this chapter, but it is not always advantageous to create such a team. An alternative is to have individuals who are not part of an incident response team but who are available (usually on the basis of a matrix agreement[1] between organizations) when incidents occur. Here are some possible advantages of adopting this alternative approach:

- **Smaller organizations generally do not need a team.** A smaller organization, such as a small startup company, does not usually need an incident response team per se. This kind of company is not likely to have very much internal structure; creating policy and procedures, in many cases, is something that must be placed on the proverbial backburner while more immediately pressing issues (survival of the business) are addressed. Forming an incident response team would constitute overkill.
- **Few resources might be available.** One of the major reasons for *not* forming an incident response team is lack of resources, particularly personnel resources. Although not a particularly good reason from a security viewpoint, lack of resources is too often a problem for information security efforts in general.

[1] An agreement of this nature typically specifies, at a minimum, how many hours per time period (week, month, or year) an individual from one organization is available to incident response activities. It also guarantees that the individual devoted to these activities will be paid by a cognizant manager, often the designated incident manager. An agreement of this nature might take the form of a service-level agreement.

- **Incident response might work better as a distributed effort.** In some organizations, incident response works better as a distributed effort. Different individuals from different divisions or groups can be called in whenever an incident of sufficient magnitude or impact occurs. Having this kind of arrangement can make these divisions or groups feel that they have some kind of direct control over the incident response process; some of their own staff members will be involved in handling their own incidents. Additionally, a distributed effort can help ensure that people who know and understand how individual units work, how the systems and networks are configured and maintained, how the applications work, and so forth will be involved in handling incidents. This can lead to better insight into what should and should not be done to resolve each incident satisfactorily.

What if You Don't Have a Response Team Per Se?

The authors of this book feel that, all things considered, it is better to have a response team to deal with security-related incidents than to call on individuals when incidents occur. Many readers of this book will never be part of an incident response team, however. If it is not possible to have such a team, you can adopt measures that will increase the likelihood of success in your efforts to handle incidents. Consider the following suggestions:

- Identify key personnel (especially technical personnel), people you feel are qualified to deal with incidents and obtain contact and other information.
- Establish some kind of ground rules or agreements concerning the availability of people who are likely to be needed in dealing with incidents. Try to get a commitment from management that guarantees a minimum number of hours of participation (per week, month, or year) from each individual who might be involved. Try to obtain assurance that even more hours of support will be available in the case of a severe incident.
- Be wise in your dealings with organizations that provide individuals who are available for incident response support. In many cases, having these individuals participate in incident handling detracts from their own mainstream missions. Avoid being overly demanding and be prepared for a "no" answer. Sometimes an organization might refuse to allow someone from that organization to deal with an incident due to a pressing need such as meeting a major project milestone. Having a long list of potential incident support personnel—so that if one person is not available, you can turn to another—is thus essential.
- Provide some kind of training and orientation to everyone who is likely to help in dealing with incidents. Ensure that everyone has at least a minimum level of knowledge about responding to incidents and that everyone understands the importance of cooperation and teamwork.
- To the maximum possible extent, solve leadership and authority issues in advance. In many (if not most) incidents, having someone in charge is essential to success. Conversely, having several people think they are in charge is extremely counterproductive.

- Do not call on the individuals who are available for incident response support unless they are genuinely needed. You are disrupting some other business unit or group's work each time you call on such individuals. You will wear out your welcome if you call on these individuals too much or if you call them into too many false alarms.
- Organize a committee or board that oversees incident response activities. Have this entity analyze critical aspects such as difficulty in obtaining support personnel, efficiency of incident response activity, and others. This entity might be instrumental in pointing out to management things that need to be improved (such as resource levels) and might prove to be instrumental in helping you form a team in time.

What Are the Functional Requirements and Roles?

If you have ever taken a course in software engineering, you have learned that defining requirements right up front is crucial to the success of the project. Incident response teams are no exception to this principle; functional requirements and the role for this team need to be defined as early in the life of the team as possible.

Basic Requirements

The most fundamental requirement for an incident response team is providing incident response support to a constituency. In providing incident response support, a response team can serve several potential roles:

- A team can assume full control over an incident and any computing and data resources involved. The extreme version of this role is to go to a site or area within a facility and take over all incident response efforts.[2] In most settings, however, this approach does not work too well in that it alienates others, particularly the owners of the computing resources and data, causing territory wars. If mandated by senior management, however, this approach can be viable in that it establishes a clear line of authority during incidents.
- Another, less extreme approach is control sharing—both the incident response team and operations or business unit staff. This generally causes less friction, but questions concerning who is in charge at any time are likely to arise.
- Still another possibility is providing direct (hands-on) incident response support but limiting this support to a purely advisory role. This means that an incident response team will do something only when its constituency requests that it do so. This role ruffles fewer feathers but typically also greatly limits the role and effectiveness of the people who serve on the incident response team.

[2] A good example of a successful use of this approach comes from the well-known Citibank incident in 1994. Two Russians were breaking into several Citibank computers and initiating bogus money transfers. Citibank personnel promptly noticed what was happening and assigned an incident manager, who was given a high level of authority in dealing with the incident.

- A final potential role for a response team is providing indirect rather than direct support in the form of advice but nothing more. This role is the most limiting for team members. However, it also tends to alienate others the least of any role.

Additional Requirements

In many circumstances, simply providing incident response support is not sufficient to keep management happy. Management too often views an incident response team as individuals who sometimes are busy but at other times have absolutely nothing to do. Management might, therefore, demand more of the team. In other cases, the individuals who attempt to create a response team can see the need for the team to perform other activities related to incident response support. Here are some additional potential types of requirements for a response team:

- **Interagency/corporation coordination/liaison.** The response team might, for example, provide a liaison function with other response teams, an organization's business continuity organization, law enforcement agencies, or some other entity.
- **Serving as a clearinghouse.** A clearinghouse serves as a central repository for information, patches, tools, and so forth. Although almost every response team in some way serves as a clearinghouse for information about incidents and vulnerabilities, serving as a clearinghouse for patches and tools has quite a few additional risks. What if the team provides the wrong patch, resulting in an unexpected incident or system failure? The same applies to tools. The point here is that serving as a clearinghouse for patches and tools often (but not always) poses more risk than potential benefit.
- **Contingency planning and business continuity services.** In some organizations, an incident response team also engages in contingency planning and business continuity functions. This is potentially a good idea in that incident response personnel generally become very proficient in recognizing and dealing with emergencies. All things considered, however, the best way to meet this kind of requirement is to have one or more individuals from a business continuity team closely work with or even join an incident response team. Business continuity staff members generally know things that incident response people need to know, such as what to do to protect business interests in the case of a prolonged outage. This kind of knowledge can be well applied to security-related incidents such as massive distributed denial-of-service attacks.
- **Information security tool development.** Another possible requirement is for the incident response staff to develop information security tools in their spare time. This kind of requirement can result in the availability of useful tools for a team's constituency. The downside is that tool development sidetracks team members from the team's main focus, namely handling incidents. A division within the team—incident handlers versus developers—might even develop.

- **Incident response planning and analysis.** A few teams have a requirement to analyze trends and plan for incident response and security needs of the future. Although most teams are not funded sufficiently to engage in efforts of this nature, incident response planning and analysis is one of the most proactive and potentially valuable activities in which a response team can engage.
- **Training and awareness.** We will discuss training and awareness in more detail later in this chapter. Suffice it to say, at this point, that training and awareness is one of the most proactive activities in which a response team can engage. Response team members will learn about many developments and trends—such as new types of malicious programs, new types of attacks, new countermeasures, and so forth—that are potentially of great value to the team's constituency. Training and awareness activities are a good outlet for disseminating this kind of information.

Who is the Constituency?

An essential issue in incident response is determining exactly whom you are supporting. In other words, you need to find out who your constituency is. The reason this is so important is that an incident response effort that does not meet the needs of those it serves is doomed to failure. If you can determine whom your constituency is, you can communicate with that constituency to learn the needs that exist. You also will know how to better focus your efforts.

If, for example, you discover that your constituency consists largely of system administrators, your approach to providing incident response support will be substantially different than if you have mostly users as customers. In the first case, you will probably need to be more technical in your approach. Your communications with system administrators will, in all likelihood, be of a technical nature. In the second case, you will almost certainly take a much less technical approach, emphasizing instead things that users need and can understand. Motivating users to engage in sound computing practices—such as updating antivirus software on desktop systems and helping users whose systems have virus or worm infections by advising them to avoid dealing with these incidents directly[3]—would in this case be more appropriate.

A response team's relationship with its constituency will make or break an incident response effort. Providing quality help to the right people will eventually result in positive feedback to both the team and its management or sponsor. Many teams (some of which are still in existence, others of which are not), however, have failed primarily because they have neither understood who their constituency is nor served their constituency's needs very well. The following sidebar describes some of the many mistakes that some incident response teams have made.

[3] As stated in Chapter 2, "Risk Analysis," human error causes far more loss than do sources of security-related issues (such as crackers). Damage inflicted by panicked users is right at the top of the list of reasons for loss.

Case Studies: Failing to Adequately Serve a Constituency

Several incident response teams have lost most or all credibility within their constituent communities for a variety of reasons. Consider the following mistakes that these teams have made:

- **Failing to get back to someone who contacts a response team to report an incident or new vulnerability.** Some incident response teams send an automated reply containing an incident number but do nothing more. In the perception of a constituency, this is as bad as not replying at all. Several teams have thus deservedly earned the reputation of being a black hole. People who can be an excellent source of information about new incidents and vulnerabilities often quit contacting their incident response team after just one case of failing to follow up a report of an incident.
- **Spreading misinformation.** Recently an incident response team informed someone at the site at which the senior author of this book works that multiple systems at the site were infected by a worm. After hours of investigation, no evidence of any worm could be found in any of the four allegedly infected machines. The individuals who performed the investigation developed negative feelings toward the response team for not getting its facts straight and for wasting their time.
- **Becoming too intrusive.** One incident response team for a government agency became intensely disliked within its constituency because it initiated a project to monitor network traffic at the external gateways at each site without the consent of management at each site. People at the sites felt that the incident response team was eavesdropping on them.
- **Causing embarrassment or leaking information without authorization.** Another incident response team was hired to perform a security evaluation at one of its constituent sites. After finishing the evaluation (in which a considerable number of vulnerabilities were found), the response team reported the results to the head of security within the government agency that oversaw both the site and the response team. Management at that site had expected that the results would be confidential.
- **Betrayal.** Under the edict of Congress, a certain U.S. government contractor launched a set of network attacks against several U.S. government sites. The attacks were very vigorous; the attackers not surprisingly achieved more than a minimal level of success. Not knowing the source of the attacks, those who noticed the resulting security breaches in victim systems frequently turned to their agency's response team.

  As the attacks progressed, people at some of the sites within one government agency noticed a strange phenomenon: After the identity of a victim system had been reported to the agency's response team, that system was never attacked again. After several weeks, the attacks ceased entirely. Soon afterward, the nature of the "white hat" penetration tests started to become common knowledge. Along with the news of the nature and purpose of the tests came the news that one response team was working in full cooperation with those who were launching the attacks. When a site detected an intrusion into a system and reported it to the response team, that response team forwarded the information to the attackers, who quit accessing the system in favor of launching new attacks against others. Since all this happened, virtually no one at any site has wanted to deal with this response team any more.

Communicating with a Constituency

After a response team's constituency is defined, establishing communication channels is essential. One-way communication, in which the response team keeps sending information to its constituency without communication being initiated by the constituency, generally does not work. An effective response team needs to obtain information about what is actually occurring within its constituency. It is possible, for example, for a response team to be unaware that a worm is circulating within part of its constituency's networks. Learning that this is happening would enable the response team to be able to better serve its constituency.

The bottom line here is that an effective incident response team establishes two-way communication. It shares information about vulnerabilities and types of incidents that are occurring within its constituency. As the saying goes, "You have to give information to get information." If the response team's constituency does not share information with the response team, the response team is not likely to have much worthwhile information to share with its constituency.

A response team can use any or all of the following avenues of communication:

- **Telephone.** One of the most simple and direct avenues of communication is the telephone. Calling someone can inject a personal touch into communications with a constituency. The fact that telephone conversations are in real time is also an important advantage of this means of communication. The downside is that people do not always speak and/or listen as well as they should; misunderstandings and miscommunication can occur. Another downside is that telephone communications are subject to eavesdropping, especially with cordless telephones based on radio frequency transmission and wireless telephones.[4]

  Secure telephones solve the eavesdropping threat in that they encrypt voice transmissions from one secure telephone to another. An example of an encrypting telephone is an STU-4—something that the U.S. government uses for transmitting classified information via telephone. A limitation is that not everyone can have access to a secure telephone when it is needed. Additionally, secure telephones can prove financially costly.

- **Email.** Email is another potentially advantageous means of communicating with a constituency because of its efficiency. You can send a message to someone else in another part of the world in only a few seconds. Furthermore, the person to whom you send the message does not have to be monitoring email at that particular moment in time. Additionally, you can create mail *exploders* to which you send a message that is subsequently sent to an entire distribution list of email addresses. As pointed out in Chapter 3, "A Methodology for Incident Response," however, email is extremely prone to eavesdropping. Email can also easily be spoofed, and incident response team members are also sometimes spammed by attackers.

[4] Protocols that secure wireless communications currently exist, but they are not widely used because they tend to interfere with performance.

A better solution is secure email, which encrypts email messages sent from one system to another. Various freeware and commercial packages that deliver email encryption are available. They provide a good solution for the eavesdropping problem but tend to be plagued with problems related to using encryption—particularly key distribution and key recovery.

- **Fax.** Sending faxes is an often overlooked but potentially effective means of communicating with a constituency. A nice feature of faxes is that they generally result in an easy-to-read hard copy. Additionally, faxes can be sent when one's network or mail server is down. Some types of fax machines can even explode a single fax message to hundreds of fax numbers in only a few minutes.

  Faxes, like anything else, are hardly a panacea, however. One of the greatest limitations is that they do not work when the destination fax number is busy or out of order. Faxing messages can also be unduly labor intensive because it takes a while to set up a fax transmission, undo any paper clogs at both ends of the transmission, replace empty paper bins, and so forth. Additionally, fax transmissions are potentially subject to eavesdropping. Secure faxes solve this eavesdropping problem, but they tend to be more expensive. Because of all the potential complications associated with fax communications, our recommendation is to use this method of communication as a *backup* rather than as a primary method.

- **Bulletins/notices.** Bulletins and notices provide an excellent way not only to communicate important information to a constituency but also to gain credibility. CERT/CC, vendors, and others already publish more than enough bulletins; ensuring that there is added value is thus an important consideration. An incident response team might, for example, publish alerts describing only the vulnerabilities currently being exploited most frequently. Alternatively, bulletins might describe new types of countermeasures.

  One of the keys to using bulletins and notices effectively is creating, and then constantly updating, an accurate distribution list. Doing so, however, is likely to be more labor intensive than one might imagine. Additionally, there are many potential pitfalls. Neglecting to add the email address of a key person from within one's constituency (or worse yet, accidentally or intentionally deleting that person's address) is a potentially major mistake. If bulletins are sensitive or proprietary but continue to be sent to employees who leave a company or organization, trouble can also occur.

To Pay or Not to Pay, That Is the Question

In the spring of 2001, CERT/CC announced that its advisories would no longer be available for free and that organizations would have to pay a yearly fee of up to $70,000 to obtain these advisories. A negative reaction within part of the Internet community resulted. Critics pointed out that CERT/CC's capabilities were developed at U.S. taxpayers' expense and that to start charging for CERT/CC advisories was unfair. Since CERT/CC made this announcement, other organizations that create bulletins describing new vulnerabilities have announced that they, too, are considering charging a fee for their bulletins. Even if CERT/CC does charge a fee for its bulletins, there is no need for panic. Many other teams and organizations produce bulletins of such high quality that there will be no shortage of information about vulnerabilities and incident trends.

- **A web site.** One of the most effective ways to share information with a constituency is to create and maintain a web site. Given the current popularity of the World Wide Web, it is now virtually mandatory for an incident response team to have its own web site. The web site should disseminate a variety of useful information, including bulletins and notices, how to contact the response team, and so forth. A response team might even use its web site to distribute patches and/or software tools if it chooses to perform this clearinghouse function.

  A key consideration related to running a web site is the security of the site. A break-in or defacement can cause all kinds of trouble, not only in terms of loss of face for the response team but also for that team's constituency. Without sufficient web site security, users might obtain bogus information or might download malicious programs. Another possibility is that the web site might not be available due to a prolonged outage because of a denial-of-service attack. The distributed denial-of-service (DDoS) attack on CERT/CC in the spring of 2001 is one of the best-known attacks of this nature.

- **Conferences.** Participating in a conference or actually holding a special conference can provide an effective way to communicate with a response team's constituents. Talks and panel presentations can disseminate useful information to a team's constituents. Additionally, having response team members participate as speakers and panelists can enhance the reputation of the team and help it gain more visibility within its constituency.

- **Courses and workshops.** Courses and workshops provide still another potentially useful way to communicate with a constituency. If of sufficient quality, courses and workshops can impart a considerable amount of information to those who need it. They can also enhance the reputation and credibility of team members who teach a course or workshop. Best yet, courses and workshops represent proactive efforts at their best. No incident response team will ever be able to help everyone within a constituency when incidents occur, but courses and workshops can teach users, system and network administrators, and managers enough to be able to deal adequately with most incidents that occur.

  A word of caution is appropriate here. Note that the preceding paragraph included the phrase: "If of sufficient quality . . . " If a course or workshop is not of sufficient quality, the team that develops and presents it can quickly become despised within its own constituency. The availability of so many outstanding security-related courses nowadays has raised the proverbial bar for security training. Getting help from training specialists, possibly from a consultancy, is often a wise move.

- **Media interviews.** Media interviews can also help in the process of communicating with a constituency. If done correctly, these interviews can enhance a response team's reputation and visibility. The following sidebar describes some basic principles in dealing with the media.

Dealing with the Media

Dealing with the media is often an important part of responding to incidents. Much of the damage from many incidents is in terms of loss of reputation or confidence in an organization due to one or more catastrophic incidents. Your organization should have a policy dictating that all contacts with the media be approved in advance by management. In fact, in the ideal scenario, a public relations department should handle all contacts with the media. (You might, in turn, be called upon to furnish technical information.) The following are time-proven methods for dealing with the media:

- Learn as much about the interview in which you are going to participate as early as possible and prepare accordingly.
- Outline the major points you want to get across.
- Anticipate a wide range of difficult questions and prepare answers in advance.
- Establish rapport with your interviewer as soon as possible.
- Use brief sentences.
- Provide simple explanations of each technical point you make.
- Every time you speak, steer your communication to some *point you want to get across* (take the initiative to do this!).
- Don't get intimidated.
- Turn negatives into positives.
- Be diplomatic, but always tell the truth.
- When you don't know the answer, admit you don't know (and perhaps offer to find out).
- Be liberal in giving credit but stingy in assigning blame.
- Dress appropriately.
- Avoid image-damaging nonverbal communication, such as avoiding eye contact or slouching as you sit.
- After the interview, ask to review any written materials for inaccuracies.
- You, the interviewee, have rights. Feel free to terminate the interview at any time if your rights are not respected!

The following are some questions you are most likely to be asked:

- What happened?
- What was the result/damage?

- What was the cause?
- What did you do about it?
- Is what happened likely to reoccur?
- What can people do to avoid what happened?
- There are, of course, no guarantees of success when you deal with the media, but following these principles listed can go a long way toward achieving a desirable outcome.

- **Videotapes.** A final method of communicating with a response team's constituency is videotapes. Videotapes can convey important information such as why having a response team is important, how to contact the response team, the kinds of incidents that are mostly likely to occur, and what to do if an incident actually occurs. If produced professionally, a videotape can have great impact on those who watch it. A videotape can also be shown multiple times with what usually amounts to little effort on a response team's part.

  The security group in one organization developed a very short but effective videotape titled "30 Seconds for Handling Security Incidents." This videotape presented a few major types of incidents and what to do about each if any should occur. The video played continuously in the organization's cafeteria; employees going in and out of the cafeteria were likely to catch at least some of the videotape as they were hanging their coats up or putting them back on.

  Like anything else, videotapes have limitations. Producing them through an in-house effort can be frustrating, time consuming, and financially costly. Yet a videotape produced by the team itself will almost certainly at least be tailored to the specific needs of the organization.

Requirements for Communicating with a Constituency

Because communications with a constituency are so critical to an incident response team's success, trying to meet all of the following goals is extremely important:

- **Relevance.** A response team must provide information that is relevant to whomever it serves. If the constituency has mostly UNIX and Linux systems, providing bulletins about the latest vulnerabilities in mainframes will, if anything, antagonize individuals from within the constituency.
- **Timeliness.** The information that a response team provides must be current. This means that if a new vulnerability that is being widely exploited by freely available cracking tools has been discovered, an effective response team will get this information to its constituency soon afterward. Additionally, this means that if other response teams have written and distributed bulletins about a new vulnerability, a response team cannot afford to lose face within its own constituency by waiting several days after the others have issued their bulletins to issue its own bulletin.

continues

continued

- **Accuracy.** Information provided by a response team must be accurate. Few things destroy a response team's credibility as quickly as disseminating inaccurate information. At a minimum, every sentence of every bulletin or notice should be reviewed (preferably by experts outside the team) for accuracy before the bulletin or notice is sent. At the same time, however, it is important to realize that not all the information that will eventually be available might be available at the time one's constituency needs to hear about some new vulnerability or pattern of incidents. What superficially appears to be true might not turn out to be true over time. Being prepared to issue revised bulletins and notices, therefore, is critical. The same basic principles apply to training materials, press interviews, and so forth.
- **Originality.** First-rate response teams write their own bulletins and notices. Copying or appending other teams' bulletins and notices is generally a bad idea. (An exception is when a very small incident response team has too few people to expend the level of effort needed to create original bulletins). Constituencies generally do not hold teams that merely copy other teams' bulletins in very high regard.
- **Understandability.** Information that a response team disseminates must be readily understandable by those who receive it. Given that part of one's constituency is likely to be management and another part will be technical staff, this is a potentially difficult issue. Sometimes writing an executive summary at the start of a bulletin that is primarily technical in nature solves this problem. In other cases, producing two bulletins on each issue—one for management, one for technical personnel—works.
- **Reliable distribution.** The information needs to get to those who need it—without exception.

Developing Out-of-Band Communications

At some time during the life of an incident response team, conventional communications channels will not be available. It is therefore important to develop out-of-band communications capabilities. A few alternative channels are wireless networks, text pagers, fax communications, and email delivery via a postal service. The first two of these alternative channels, in particular, require advance arrangements and coordination within a response team's constituency. It is expedient to analyze current communication channels and then develop out-of-band communications capabilities for plausible primary communications outage scenarios. You should ensure that each communication channel meets some kind of minimum security standards, and you should regularly test each communication channel to ensure that it works as expected. New developments show that HAM radios are becoming a popular mode for emergency communications.

Case Study: A Lesson Learned in Establishing Communication Channels

Early in the existence of the Computer Incident Advisory Capability (CIAC), the incident response team for the U.S. Department of Energy (DOE), the main avenue of communication between this team and its constituent sites was via fax. At this time, the Internet was not like it is today. The ARPAnet, in fact, had been split into the Milnet and the NSFnet (the Internet) less than a year before an interesting development occurred. The CIAC team was based in the East Bay of the San Francisco area. In October 1989, a massive earthquake struck the area, causing widespread power and telephone outages. Although the CIAC team did not experience any power outages, telephone service was interrupted. At the time of the earthquake, a worm called WANK/OILZ was infecting VMS systems around the world, including many systems within DOE sites. Attempts by CIAC team members to warn DOE sites of new developments and countermeasures for this worm were halted while team members attempted to contact individuals at these sites via other means. Numerous individuals at these sites had email, but the earthquake also disrupted CIAC's email services. The stoppage of telephone and email services lasted for approximately two days; during this time, CIAC was virtually unable to communicate with its constituency.

This episode provided important "lessons learned" for this team. Soon afterward, the team worked on developing better out-of-band communications capabilities through use of more cellular telephones and emergency procedures for contacting key individuals at sites.

Staffing Issues

So far, we have described many difficult issues that need to be addressed, but no issue is more difficult than dealing with staffing. Addressing staffing-related considerations such as team size, prerequisite skills, and location of team members is critical. A discussion of these considerations follows.

Team Size

The size of your team will undoubtedly be dictated by available funding. This is particularly true during the early stages of your team's existence. At a minimum, you will initially want to have someone to manage the team and, if funding permits, someone with the technical skills necessary to deal with the problems that are most likely to surface within your constituency.[5] You can then add staff to broaden the range of expertise as funding allows.

[5] Recall the importance of gauging risks, as discussed in Chapter 2.

Team Skills

This section presents the kinds of skills that are generally required in an effective incident response team.

- **Management skills.** Proficiency in management is almost without question the single most important skill. Without effective management, even the most technically proficient team will falter. The manager of an incident response team must be able to ensure that the team has the appropriate skill sets; organize and coordinate the team's activities; keep team members motivated and on track; ensure that the team has sufficient resources and that the resource burn rate is within acceptable limits; ensure that proper priorities, procedures, and policies are in place and are revised as necessary; prepare reports for senior management; monitor how well the team is meeting its requirements; intervene if and when conflict occurs; and play politics well enough to both shield team members from them and keep management supportive of the team.

  The team manager does not have to be technically proficient (and, if fact, probably should not be too technically proficient to avoid the temptation of getting involved in technical issues at the expense of performing critical management responsibilities). At the same time, however, the team manager needs to know enough about technical matters to be able to make good judgments about priorities and to avoid hurting the team's reputation when the manager deals with the constituency, vendors, and others.

- **Technical skills.** Technical skills are extremely essential to a response team's effectiveness. Many incidents require a high degree of technical proficiency in analyzing what is wrong and dealing with the situation. Additionally, unless team members earn a large degree of respect for their technical prowess within a team's constituency, no one will contact them for help, nor will they heed their warnings and advice. Technical skills in operating systems (UNIX, Linux, Windows NT and Windows 2000, NetWare, OS390, and so forth) and network security are particularly critical.

  Programming experience, particularly in system programming, can help considerably when a response team needs to reverse-engineer malicious programs such as worms and back doors. There is no substitute for real-world troubleshooting experience such as dealing with operational outages. Computer crisis coordination capabilities are constantly in crisis mode; previous relevant experience has great payoff.

  Not every team member needs to be a top-notch technical expert, however. Exceptionally strong technical personnel are rare. Furthermore, they generally command top salaries. Funding realities will generally limit how many gurus can be hired. A key to having sufficient technical expertise, therefore, is to hire one technically accomplished staff member to anchor each key technology area in which the team needs to become involved. The guru in each area can then advise and mentor less technically accomplished team members.

- **People skills.** Nowhere are people skills more important than in the incident response arena. Harmony within the team is critical to the team's efficiency and effectiveness. Being able to get along well with individuals within the team's constituency is also very important. Technical gurus often have the reputation of being hard to get along with, so the challenge of hiring team members with good people skills is a difficult one. Periodic training in interpersonal skills can also have a high payoff.
- **Teamwork skills.** Teamwork skills are somewhat different from people skills in that they involve different types of knowledge, abilities, and perspectives. Teamwork skills are related to having a common vision, effectively dividing responsibilities, effectively estimating task completion time, knowing when to start new tasks, knowing how to get out of other team members' way when doing so is appropriate, obtaining feedback concerning each team member's progress, and so forth. Strong management skills are once again the key ingredient; good managers promote and build team skills. We also recommend participating in periodic team skills training.
- **Communication skills.** Communication skills go hand-in-hand with both interpersonal skills and team skills. Special kinds of communication skills, particularly writing and speaking skills, can be exceptionally valuable. Many incident response teams hire a technical writer for the specific purpose of producing accurate, understandable bulletins and notices. Additionally, speaking skills are very useful for conference and workshop presentations, filming videotapes, and so on.

Location of Staff

Where should team members be geographically located? If an organization and its constituency are all within a single geographical area, the answer is obvious. But what if the constituency is spread out among several different locations, possibly even on different continents? Should all team members reside at one location, or should the team be divided so that each part of the team's constituency is served by team members located where they are needed?

The answer to this question depends on a number of factors. Some advantages of having all team members at a single location include a better ability to coordinate the team, greater ease of communication within the team, facilitation of team building among team members, and (generally) a lower financial cost because only one physical facility, one telecommunications provider, one document custodian, and so forth will be necessary. Additionally, separating a team into different parts residing in different geographical locations often results in undesirable divisions and negative politics within the team itself. In this case, it is not unusual to find that each piece of the team develops an "us versus them" mentality.

Advantages of having multiple locations are generally related to providing a higher quality of service to one's constituency. If part of the constituency is in central Europe, for example, and part is in the central United States, the difference in time of seven hours might prove to be an overwhelming obstacle if all members of a response team are in the central United States. If someone in central Europe arrives at work at 8 a.m. Monday morning and discovers an incident, that person would likely have to wait approximately seven hours before being able to talk to someone from the response team. It would probably be better, in this case, to have part of the team reside in central Europe.

Should you have full-time or part-time team members? The answer to this question is simple; in general, it is better to have full-time team members. Having full-time team members means more personnel resources will be available when they are needed. This is particularly important when high-impact incidents occur or when a multiple-points-of-presence attack (in which multiple attacks are launched against sites in different geographical locations) is launched. On the other hand, funding realities might dictate that part-time team members be hired. Alternatively, perhaps some gurus are available only on a part-time basis. In these cases, part-time involvement is better than no involvement at all.

Creating Operating Procedures

The topic of procedures is potentially very complex. Entire books on effective information security–related procedures have been written. Previous chapters of this book have touched on this topic, especially regarding the necessity of having well-written, well-distributed procedures for incident response. Additionally, procedures must constantly be revised if they are to be effective in guiding the incident response team and others to appropriate actions.

You cannot really simply copy some other team's procedures and then use them. You must instead create procedures that are appropriate to your particular team and the requirements that team must fulfill. The following, however, are issues that any set of procedures must address if they are to be effective:

- What the purpose of the procedures is
- To whom or what the procedures apply and under what conditions (if at all)
- Lines of authority within the incident response team and the organization(s) it serves
- Restrictions on the kinds of actions in which team members can and cannot engage (including actions such as counterattacking sites known to launch attacks)
- How information and evidence must be documented
- Who can contact outside entities (such as the media, law enforcement agencies, and so forth) and under what conditions
- Priorities in response efforts (for example, protecting the lives of humans, keeping systems and networks operational, and so forth)

- What to do in case of incidents in highly valuable, sensitive, proprietary, or classified systems and/or networks
- Kinds of information that can and cannot be disseminated outside of the immediate group or division in which the incident response team belongs
- Management's role with respect to the response team and its activities
- When and how the procedures must be changed
- How the procedures are to be distributed

Procedures should in every respect be a living document. Every time your incident response team engages in the follow-up stage of the PDCERF methodology (or whatever methodology your team creates), it should evaluate existing procedures to determine whether they actually worked. You should then revise your procedures as needed.

About Managing an Incident Response Effort

Now that we have covered the many considerations involved in forming an incident response team, let's next turn our attention to how to manage such a team. We will consider management style, coordinating with other entities, how to develop and use metrics of effectiveness, maintaining the desired level of proficiency, preparing reports, and how to gauge where a response team is in terms of the stages of the life cycle for incident response teams to adjust one's management strategy.

Management Style

Incident handling is often a stressful, difficult activity if it is done correctly. It is thus important for the team manager to convey a positive, supportive management style. Failing to do this can seriously undermine the morale of an incident response team. In addition, we offer the following suggestions:

- **Avoid micromanagement.**[6] Unless you see trouble, adopt a hands-off philosophy. Micromanagement can ruin an incident response effort by causing loss of morale, a high turnover rate, conflict, and so forth.
- **Learn to handle visibility.** A manager of an incident response team will almost certainly gain elevated visibility. Conferences and the media are likely to become very interested in getting that manager to participate; the manager, after all, will know about incidents that are likely to fascinate audiences, readers, and viewers. Take this visibility with a proverbial grain of salt; don't let it change your opinion of yourself and how you relate to others (particularly your other team members). Learn to use whatever visibility you gain to the benefit of the team—to give greater recognition to other team members, to obtain more funding and support, and so forth.

[6] *Micromanagement* means managing minute details of subordinates' jobs (that is, telling others exactly what to do at any point in time).

- **Obtain written evaluation/feedback of your managerial performance from team members and adjust your management style accordingly.** Doing this once every three months or so can help you become a better manager and be better accepted by fellow team members.
- **Take feedback in the form of "flames" seriously.** Consider revising your procedures, attitudes, and so forth accordingly.
- **Help keep team members' efforts on track.** Team members might become confused about a next course of action or might be so burned out after dealing with a complex incident that all they want to do for the next few days is web loafing. Dealing with web loafing is particularly challenging. Intervening and telling that person to quit web loafing usually amounts only to micromanagement, something that usually results only in resentment on that person's part. Ultimately, the answer lies in assigning a reasonable set of tasks with reasonable deliverables and unambiguous due dates for each. If a team member wants to web loaf, that's fine, but whatever is due will nevertheless be due by the assigned date. If that person does not get the job done on time, it is time for that person to deal with the consequences.
- **Be decisive about dealing with baggage and loose cannons on your response team.** In general, weed them out. Incident response generally is as much political as it is technical. It has been said that "loose lips sink ships." Similarly, one or two loose cannons on an incident response team can completely undermine the credibility of that team.

Coordinating with Others

"No team is an island." You need to develop channels of communication and cooperation accordingly. Focus your attention on groups such as business units within your organization; your human relations, legal, and public relations offices; other incident response teams; vendors; law enforcement agencies (if your management so directs); and others. You will also need to develop relationships with other departments and divisions within your organization that have experts whom you might need from time to time. Expertise needed might include information security, information technology, business continuity, and law.

Suggested Action Items for Incident Response Team Managers

- Ensure that your team's existing policies and procedures are current and appropriate. Update and expand them as necessary.
- Perform, review, or update the risk analysis for your team.
- Have an objective evaluation of your incident response team's charter, efforts, and procedures performed by someone outside of your team.
- Have your policies and procedures reviewed by legal and human relations professionals.

- Evaluate your team's expertise and capabilities; bring in new team members (or reassign some existing team members) as appropriate.
- Evaluate your team's communications capabilities and make changes as appropriate.
- Participate in FIRST (Forum of Incident Response and Security Teams; see www.first.org). FIRST works only if teams participate and contribute.

Success Metrics

As far as information security goes, success in many respects means having no incidents whatsoever. Having no incidents, however, will almost certainly spell doom for an incident response team. It makes it even more difficult to rationalize spending resources on your incident response effort. In an odd sense, therefore, success in incident handling requires that incidents transpire. Most significantly, however, actions taken to deal with incidents must be successful. This is where the difficulty begins—what constitutes success in incident response activity?

One of the best ways in information security to communicate results to management is to develop and use metrics. A number of possible metrics for incident response exist:

- How many incidents the incident response team has dealt with in a given time period[7]
- Whether the number and/or percentage of incidents handled in which the estimated financial loss is below a criterion value
- Self-evaluation measures[8] such as questionnaires
- Written or verbal reports of success or failure with people within a response team's constituency
- Average time and manpower needed to resolve each incident plotted against the apparent complexity of each incident
- Documentation by team members of the actions taken to deal with each incident
- Awards presented by organizations and other forms of external recognition[9]

Unfortunately, none of these measures is all that adequate, nor is any combination of them very satisfactory. You should thus view these potential metrics as a start, a proverbial "straw man" for developing your own set of metrics.

[7] This metric is not particularly good, however, in that someone might contact an incident response team without the team ever bothering to respond. Some response teams even proudly count (and report to their sponsors) the number of vulnerability scans reported to them as if they were incidents handled, even though the team took no action.

[8] Be careful here, too. This measure smacks of a fox guarding the hen house!

[9] Also be wary of this measure. Some agencies and organizations have been known to bestow some form of recognition on their own response team to bolster a sagging incident response effort in the eyes of the user community.

Maintaining Proficiency Levels

Forming a response team is not the only major challenge associated with an incident response team. When expertise within the team is established, it is also a formidable challenge to maintain this expertise. Both the credibility and proficiency of an incident response team are directly related to the managerial and technical expertise within the team. Turnover of team members—managers and technical staff—is a constant problem. Additionally, the technical staff needs to expand its skill base and learn of new technology developments. How then can an incident response team maintain its current level of proficiency?

- Ensure that there is ample funding for training of all team members, managers, and technical staff. They should be able to attend several training sessions every year.
- Make sure that relevant books, journals, and papers that expand the managerial and technical skills and perspectives of team managers are freely available to them.
- Ensure that junior team members are paired with your team's experts to help the junior team members in their effort to master the learning curve.
- Every once in a while, have a member of your team visit another response team[10] or organization that excels in areas that you value to learn what they do and how they do it.
- Invite outside experts to visit your team, give presentations, and so forth.
- Encourage team members to take university courses in operating systems, networking, cryptography, information security, and other areas related to incident response.

Preparing Reports and Management Updates

Any effort, such as an incident response team effort, is accountable for its activities to management. Traditionally, an effort will prepare reports to management to relate the activities in which the team has been involved, successes (and possibly failures), the resource burn rate, and other matters of interest to management. In the incident response arena, preparing such reports is particularly important. Remember that incident response is generally an overhead activity, something of which management tends to be suspicious in the first place. Providing carefully prepared reports to management can be potentially advantageous to a response team in that they can provide evidence that the team is on track with expectations.

[10] Ensure first, however, that the other response team is an effective one. Participating in the activities of a deficient response team could actually lower the proficiency level of your team members.

How often should the team manager prepare such reports? The answer depends on the particular organization. Some organizations require monthly reports. Others require quarterly reports, and still others require yearly reports. Regardless of the required frequency of reporting, an incident response team manager would do well to submit frequent reports to management to update them as to the team's efforts and accomplishments. The downside is that sometimes incident response activity becomes so intense that finding time to prepare reports becomes impossible.

Reports should contain the types of information that management expects. If management expects metrics of incident response success, the team manager (or whoever prepares the report) must engage in best-effort attempts to create and use metrics. Be aware that technical jargon turns management off; write in the language that management uses and understands. Be sure to include an executive summary and always remember that these reports comprise an outstanding effort to sell what you are doing to management, thus possibly enabling your response team to obtain greater levels of funding and support. Finally, be sure to properly archive the reports. They can be used as another source of lessons learned as well as analyzing trends and the growth of your incident response effort.

Life Cycle Stages of an Incident Response Team

At the time this book was written, information security incident response teams had been in existence for nearly 15 years. Some incident response teams have flourished. Others have fared poorly. In more than a few cases, an organization or government agency has replaced every member of an existing response team, often turning to a completely different source of manpower (such as a different contractor). One thing we have noticed is that incident response teams seem to go through a cycle of stages as they grow from their initial inception to a certain point in their existence (see Figure 4.1). The following is a model to represent these stages.

The Stages

- **Initial.** The initial stage is what the name implies—the incident response team is just getting started. Normally, someone has submitted a proposal to form an incident response team; management or a sponsoring agency or organization has approved this proposal. Someone (usually the person who will eventually serve as the team manager) tries to get the initial aspects of the response team in existence, perhaps by starting to define the constituency and getting some level of funding in place. At this stage, the effort is by no means even close to being operational (that is, of use to any constituency). Most people have not heard of the emerging team.

- **Critical.** The critical stage is the one in which the incident response team is being formed. It is during this stage that requirements are formalized and then approved by management, a team infrastructure is established, initial procedures are written, communications methods are implemented, and reporting methods and procedures are put in place. If sufficient funding exists, new staff members are added to the team. Additionally, the constituency that the team is to serve is usually finalized at this point. Most people still have not heard of the fledgling team, but someone, usually the team manager, begins actively promoting the team to the constituency. The team becomes capable of limited operations, handling inquiries from users and perhaps giving advice or directly intervening in incidents that the team is qualified to handle.

  This stage is called the critical stage because many things have to be done correctly at this stage if an incident response team is going to experience at least some measure of success. The future of the team is still uncertain. Failing to correctly define requirements, failing to get management's full approval of the requirements, writing deficient procedures (or failing to follow them), being unable to adequately staff the team, or something else can cause the team to falter. Conversely, successfully resolving the many issues that must be addressed during this stage can effectively move the effort to the next stage.

- **Established.** During the established stage, the incident response team achieves a stable level of existence. The team establishes effective operations and fulfills its charter by efficiently dealing with incidents that occur. Management (or possibly a sponsoring agency or client organization) appreciates the job that the response team does. Other agencies and groups recognize the team as the legitimate body for dealing with incidents.

  The team's constituency turns to the response team when it needs help, or if the response team has the authority to assume control when incidents occur, the response team comes to a site and effectively deals with the incident and then returns to its normal location. Other response teams look up to the established team as a model of effective incident response. During the established stage, it becomes clear that the response team's existence is indefinite, that the team will in all likelihood exist in its present form for years to come.

- **Postestablished.** During the postestablished stage, a response team expands its operations to include requirements and operations that were not part of any of the previous stages. Activities are increasingly proactive and now include an increasing amount of analysis and research efforts. Usually, the basis for this expansion is success at the previous stages. Additional team members are added; this in turn expands the range of expertise within the team.

An example of a team in the postestablished stage is CERT/CC. CERT/CC is now engaged in many activities other than incident response operations per se. Part of this team analyzes trends; CERT/CC also has a large and successful research capability. Additionally, CERT/CC was able to obtain funding for a systems survivability center. Finally, virtually the entire Internet community is aware of CERT/CC's existence, and CERT/CC bulletins have had a very positive impact on this community in that these bulletins have enabled system administrators and others to become aware of, and then fix, known vulnerabilities that are related to security incidents.

The Value of This Model

This model incorporates elements that characterize the status and sophistication of an incident response team. This model enables incident response team managers (as well as managers who oversee incident response efforts) to monitor the progress of their teams on the basis of the characteristics of each stage of what amounts to a maturity model. The goal, of course, is to bring the teams to the highest possible stage of maturity. This model provides a benchmark against which the activities and progress of each team can be measured. A team that is still in the initial stage after one year, for example, desperately needs to progress to subsequent stages. Ultimately, a team needs to progress at least to the established stage if it is to be viable.

The progression from one stage to the next is not necessarily in a forward direction, however. It is possible, for example, for a team that has progressed to the established stage to fall backward to the critical stage due to a number of factors such as massive changes in management and technical staff. A team that in the past has functioned well and that was well accepted by its constituency can deteriorate to the point that it is dysfunctional and no longer is well accepted by its constituency.

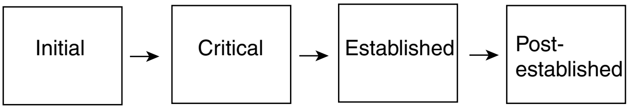

Figure 4.1 The stages of a response team's life cycle.

Summary

This chapter began with a definition of the term "incident response team." An incident response team is one or more individuals with the mission of dealing with security-related incidents. Why should one form an incident response team? Major reasons include expertise, efficiency, having a proactive emphasis, meeting requirements, establishing a liaison with other teams and organizations, and others.

Forming a response team is not always necessary; in some situations, a response team can actually be detrimental to an organization. Above all else, you have to figure out what role you need to perform and what your basic requirements are. Then you have to identify your constituency and determine how to communicate with them. Staffing, procedures, and other considerations are other critical issues that need to be resolved.

Managing an incident response team presents a set of extremely difficult challenges. Issues such as exuding a positive management style, setting up communications with others, developing and using a reasonable set of metrics, and establishing suitable reporting methods are all critical to response teams. Response team maturity can be characterized in terms of four stages: initial, critical, established, and postestablished. Getting a response team to the established stage or further is an important goal of incident response team managers and their management.