NIST

Establishing a Computer Security Incident Response Capability (CSIRC)

John P. Wack
Computer Systems Laboratory
National Institute of Standards and Technology

NIST Special Publication 800-3

November, 1991

Establishing a Computer Security Incident Response Capability (CSIRC)

Abstract

Government agencies and other organizations have begun to augment their computer security efforts because of increased threats to computer security. Incidents involving these threats, including computer viruses, malicious user activity, and vulnerabilities associated with high technology, require a skilled and rapid response before they can cause significant damage. These increased computer security efforts, described here as Computer Security Incident Response Capabilities (CSIRCs), have as a primary focus the goal of reacting quickly and efficiently to computer security incidents. CSIRC efforts provide agencies with a centralized and cost-effective approach to handling computer security incidents so that future problems can be efficiently resolved and prevented.

While the risks to computer security have increased, agencies have also become more dependent on computers. Many systems in widespread use today do not contain safeguards to guarantee protection from these threats. Additionally, as systems become more complex, they are more prone to vulnerabilities that can increase the risk of malicious exploitation. Due to greater availability of computers, users are often de facto system managers, however many have neither the requisite skills nor time to manage their systems effectively. These factors make it clear that agencies need to augment their computer security capabilities before they suffer from serious computer security problems that can harm their missions, result in significant expense, and tarnish their images.

A CSIRC can help agencies resolve computer security problems in a way that is both efficient and cost-effective. Combined with policies for centralized reporting, a CSIRC can reduce waste and duplication while providing a better posture against potentially devastating threats. A CSIRC is a *proactive* approach to computer security, one that combines reactive capabilities with active steps to prevent future incidents from occurring.

Acknowledgments

Many people contributed to versions of this document and provided valuable support. NIST would especially like to recognize the efforts of E. Eugene Schultz of DOE's CIAC and Kenneth R. van Wyk of the CERT/CC, who commented on drafts of this document and provided valuable insight into the many issues involved in incident handling.

Table of Contents

1. Introduction

This guide provides advice for federal agencies and other organizations on establishing a Computer Security Incident Response Capability (CSIRC). A CSIRC provides computer security efforts with the capability to respond to computer security-related incidents such as computer viruses, unauthorized user activity, and serious software vulnerabilities, in an efficient and timely manner. A CSIRC further promotes increased security awareness of computer security-related risks so that agencies are better prepared and protected.

1.1 Purpose

This publication provides guidance for those interested in establishing a CSIRC. It describes why traditional computer security efforts may not be sufficient in light of more recent threats. This guide discusses some of the considerations in establishing a CSIRC as well as the organizational, technical, and legal issues connected with a CSIRC operation.

This guide is a starting point; it does not address all the issues relevant to Computer Security Incident Response (CSIR) for each agency or environment. To establish a CSIRC, each agency must explore many options and make many decisions. References are included in this document to help agencies in this process.

1.2 Audience

This guide is written primarily for federal agencies; however, it is also intended for other governmental, commercial, and academic organizations. Although this guide focuses primarily on establishing a CSIRC, it contains basic information that is useful for readers unfamiliar with the CSIRC concept.

1.3 Basic Terms

A *computer security incident*, for purposes of this guide, is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. The definition of an incident may vary for each agency depending on many factors; however, the following categories and examples are generally applicable [SCHULTZ90]:

- **Compromise of integrity**, such as when a virus infects a program or the discovery of a serious system vulnerability;
- **Denial of service**, such as when an attacker has disabled a system or a network worm has saturated network bandwidth;
- **Misuse**, such as when an intruder (or insider) makes unauthorized use of an account;
- **Damage**, such as when a virus destroys data; and
- **Intrusions**, such as when an intruder penetrates system security.

The acronym *CSIRC* stands for *Computer Security Incident Response Capability*, whereas *CSIR* is used to stand for *Computer Security Incident Response*. Other acronyms exist for CSIR capability, including *CSRC* (Computer Security Response Center) and *CERT* (Computer Emergency Response Team).

This guide uses the term *traditional computer security effort* to describe computer security efforts that are rooted in sound principles of physical security and contingency planning but that do not provide a CSIR capability.

The terms *incident response* and *incident handling* are used synonymously to describe the reactive activities associated with a CSIRC.

1.4 Structure of this Document

This document is structured as follows: Chapter 2 presents an overview of a CSIRC, including reasons for CSIR activity, the CSIRC concept, its goals, components, and interaction with existing agency computer security efforts. Chapter 3 deals with issues and factors associated with establishing an agency CSIRC. Chapter 4 describes some of the issues associated with operating and maintaining a CSIRC. The appendices contain an annotated bibliography for further reading on computer security and incident handling and information on FIRST, the Forum of Incident Response and Security Teams.

2. CSIRC Overview

This section describes the basic aspects of a Computer Security Incident Response Capability: its concept, benefits, components, and relationship to current computer security efforts within an agency. Background sections are included that deal with traditional computer security efforts, current threats to computer security, and justifications for increased CSIRC activity.

2.1 Traditional Agency Computer Security Efforts

A traditional computer security effort typically is *not prepared* to detect and subsequently react in a *timely* and *efficient* manner to computer security threats, such as systems intrusions or serious bugs and vulnerabilities in systems.

Traditional computer security efforts are designed to meet a threat scenario that today is considered incomplete or outdated. Until the early 1980s, problems such as computer viruses and malicious hacking activity were not recognized as problems. Available guidance concentrated on subjects such as disaster recovery, physical security, backup contingency procedures, and data confidentiality. Agencies sometimes combined computer security responsibilities with general security responsibilities, therefore those responsible for computer security often were not highly skilled in computer technology. For many years, this arrangement of resources sufficed.

2.2 The Changing Threat Environment

Computer systems have progressed rapidly in capability and availability. Networks such as the *Internet*[1] link together tens of thousands of systems and cross international boundaries. System costs have decreased so that multi-user systems, personal computers, and local area networks are often widespread throughout agencies.

Along with the growth and spread of computer technology, a similar growth has occurred in the ways in which high technology can be exploited for harmful purposes. Four factors have increased risks of malicious exploitation:

- An emphasis on data confidentiality (and not integrity or availability);
- Increased use of local and wide area networks;

[1]The *Internet* is an interconnected network of many networks all running the TCP/IP protocol suite, connected through gateways. It exists to facilitate sharing of resources at participating organizations, which include government agencies, educational institutions, and private corporations. The *Internet* is very large, covering the United States, Canada, Europe, and Asia. Estimates of numbers of hosts exceeds 500,000; it continues to grow at a fast rate.

- Extensive use of personal computers combined with lack of user training; and
- Increased chances of vulnerabilities due to system complexity.

Due to computer security requirements being driven in the past by concerns primarily with secrecy, most advances in computer security have been oriented towards protection of data confidentiality [RISK91] and not integrity or availability. However, threats such as computer viruses and worms are generally defeated by mechanisms for ensuring integrity and availability. While many vendors' products contain some integrity-enhancing mechanisms, systems are more at risk to threats such as viruses and worms that target integrity and availability.

The growth of networks now provides more freedom of range for malicious activity [QUARTERM90]. A networked system whose manager and users practice poor security poses significant threats to other systems on the network by enabling the spread of malicious software or by use as a springboard for malicious user activity. Interconnected computer networks also provide attackers a high degree of anonymity since connections between networks and countries are often difficult to trace.

As the price and size of systems has decreased, many users of systems have become, in effect, system managers as well. This is particularly true of personal computers, but often users of more complex and powerful systems must combine their other work activities with system management. This arrangement may reduce emphasis on proper system management and security procedures and increase the likelihood that systems are not maintained to be more resistent to computer security threats.

Finally, the complexity of modern systems has increased the risk that software defects remain undetected until the systems are already in operation. Users are at risk from undetected vulnerabilities and system failures that affect system integrity and availability and increase the odds of malicious exploitation.

2.3 The Need for CSIR Capability

The elements of a traditional agency computer security effort continue to be important and useful. As shown in the previous discussion, two trends necessitate the establishment of CSIR capability: first, computers are widespread throughout agencies; agencies rely heavily on computers and cannot afford denial of service, and second, agency computer systems and networks are at much higher risk to threats such as computer viruses, intrusions, and vulnerabilities. The following examples of computer security incidents are now commonplace:

- A computer virus is copied to a LAN server; within minutes hundreds of other computers are infected; recovery takes several people and several days.
- Backups infected with viruses result in reinfected systems, requiring more time and expense.
- Vulnerabilities in software are discovered that permit unauthorized entry; explicit instructions on how to exploit the vulnerability become quickly known.
- System intruders copy password files and distribute them throughout large networks.
- Break-ins through international networks require cooperation of different government agencies.
- Outbreaks of viruses or system penetrations appear in the press, causing embarrassment and possible loss of public confidence.

These situations could cause agencies to face extreme expense in productivity, significant damage to their systems, loss of funds, and damage to their reputations [GAO89]. Clearly, agencies now need to take action prior to suffering the consequences of a serious computer security problem.

2.4 The CSIRC Concept

A Computer Security Incident Response Capability is that part of a computer security effort that provides the capability to respond to computer security threats rapidly and effectively. A CSIRC is a direct extension of the contingency planning process, due to its explicit preparedness to respond to threats as they occur.

A CSIRC should be a central capability for dealing with virtually any computer security problem that occurs. It should provide a means for reporting incidents and for disseminating important incident-related information to management and users. It should concentrate the coordination of incident handling into one effort, thereby eliminating duplication of effort.

One basic aim of a CSIRC is to mitigate the potentially serious effects of a severe computer security-related problem. To effect this aim, a CSIRC effort requires the involvement and cooperation of the entire agency. It requires not only the capability to react to incidents, but the resources to alert and inform the users. It requires the cooperation of all users to ensure that incidents are reported and resolved and that future incidents are prevented.

A CSIRC, viewed as a discrete organization, would be relatively small, perhaps only three or more individuals. In its broadest sense, a CSIRC effort can be viewed as the involvement of the agency as a whole, organized such that its management structures, communications and reporting mechanisms, and users all work together in reporting, responding to, and resolving computer security incidents quickly and efficiently.

2.5 CSIRC Constituency and Technology Focus

Inherent to the purpose of a CSIRC is the existence of a *constituency*: the group of users or organizations served by the CSIRC. The constituency members share specific characteristics, such as a specific agency, its computer network, certain operating systems, or other common factors. The CSIRC's *technology focus* is that area of computer technology in use by the constituency that the CSIRC specializes in, such as microcomputers, or microcomputers of a certain make.

A CSIRC constituency need not be the entire agency or organization. For example, an agency might utilize several types of computer and networked systems, but may decide that a CSIRC is required to serve only its microcomputer users, e.g., computer viruses are viewed as more likely a threat than those threats more common to larger systems. Or, a large agency composed of several sites may decide that current computer security efforts at some sites do not require a CSIRC, whereas other sites do.

2.6 Proactive vs. Reactive Nature of a CSIRC

A CSIRC is not solely a reactive capability; it is also a *proactive* approach to reducing an agency's computer security risks. When not responding to incidents, a CSIRC can take proactive steps to educate its constituency regarding pertinent risks and threats to computer security. These activities can prevent incidents from occurring. They include informing users about vulnerabilities and heightening awareness of other security threats, procedures, and proper maintenance of their systems.

An analogy to this mix of activities is a typical fire department. The reactive activities include fighting fires; however, one could say that the proactive, or fire-prevention, activities result in more injuries prevented. Likewise, a CSIRC may prove more cost-effective because of its incident-prevention activities than its incident-handling efforts.

2.7 CSIRC Relationship to Current Agency Security Efforts

A CSIRC activity complements and improves current computer security efforts. Results of CSIRC activity such as collected statistics and other information on computer security, complement other components of current efforts such as risk analysis, contingency planning, and security audit. The proactive functions of a CSIRC, such as security awareness training, may already exist to some degree in current security programs. The essential requirements for centralized reactive capability may already exist to some degree in the form of help desks, management reporting structures, and policies for centralized reporting.

However, a CSIRC is defined less by its organizational structure than by its centralized, proactive capability to respond to security threats with speed, efficiency, and without duplication of effort and waste of agency resources. To achieve those objectives, current efforts will most likely require some revamping. Policies for centralized reporting and mechanisms for effecting it may need to be put into place. Personnel with the requisite skills and necessary equipment may need to be dedicated to the effort. Other changes in the way in which the agency manages computer security will most likely result.

2.8 Early Agency CSIRC Efforts

Several government agencies have started CSIRC activities or have augmented their computer security efforts with CSIR capabilities. In 1988, the Defense Advanced Research Projects Agency (DARPA) funded the CERT/CC (Computer Emergency Response Team/Coordination Center) to investigate and resolve computer security incidents related to the Internet, concentrating mainly on UNIX[2] operating systems [SCHERLIS88], [SCHERLIS89]. In 1989, the Department of Energy (DOE) funded the CIAC (Computer Incident Advisory Capability) to handle computer security incidents affecting DOE systems [SCHULTZ89]. Both teams have handled and resolved many incidents and regularly issue alerts concerning new vulnerabilities and software defects. Several other government and commercial organizations also created CSIRC efforts [DDN89], [FEDELI91]. In 1990, the National Institute of Standards and Technology (NIST), in conjunction with the CERT/CC, DOE's CIAC, the National Aeronautics and Space Administration (NASA), and other agency response teams, organized a cooperative activity known as the Forum of Incident Response and Security Teams (FIRST). The purpose of the Forum is to share technical information and to foster further participation in incident-handling efforts by government, commercial, and academic institutions [NIST90]. Refer to Appendix B for more information.

[2]UNIX is a registered trademark of AT&T.

3. Issues in Establishing a CSIRC

This section describes some of the initial steps and issues in establishing a Computer Security Incident Response Capability. While each agency has its own specific requirements, the steps and issues listed here should be applicable to most environments. The issues center on determining the initial goals of the CSIR effort, defining the CSIRC constituency, acquiring agency support, effecting policies for centralized reporting, documenting procedures, and staffing.

3.1 Determining CSIR Goals

The first step in establishing an incident response capability is to determine whether the nature of the computer security problem in the agency and how it could better be handled via a CSIRC as opposed to an existing effort. From there, the goals of the CSIRC effort need to be stated. The goals define the scope and boundaries of the effort, including the type of technology to be protected and the constituency served. Establishing clear and realistic goals will help to determine expectations of the management and the funding necessary.

A major objective of a CSIRC is to gain control of the security problem by taking a proactive approach to the agency's security problems and reacting to incidents as necessary. The goals of a CSIRC might include some of the following:

- facilitate centralized reporting of incidents;
- coordinate response to incidents of a certain type or affecting a certain technology;
- provide direct technical assistance as needed;
- perform training and raise security awareness of users and vendors;
- provide a clearinghouse for relevant computer security information;
- provide data and other inputs to the contingency planning effort;
- promote computer security policies within a constituency;
- develop or distribute software tools to the constituency;
- encourage vendors to respond to product-related problems; and
- provide liaisons to legal and criminal investigative groups.

Goals should be simple, unambiguous, and realistic. For example, the ability to perform training might be too expensive for some organizations. Attempting to serve disparate constituencies such as main-frame *and* microcomputer users may be impractical depending on fiscal constraints. Therefore, guard against adopting any overly ambitious or ambiguous goals.

3.2 Defining the CSIRC Constituency

The CSIR goals determine the CSIRC's *constituency*. The constituency is usually aligned along a particular technology focus of the CSIRC, such as a particular type of computer operating system or network. However, if the constituency is defined to be an entire agency, the technology focus results in any computer technology in use by the agency, including mainframes, personal computers, and associated networks. The size of the constituency and the diversity of the technology focus thus determine the size and scope of the CSIRC effort. The more broad the technology focus, the more important and expensive it will be to acquire staff with technical expertise in every area.

3.2.1 Constituency Communications Issues

An important factor in choosing a constituency is whether there exists a means by which the CSIRC and the constituency can communicate efficiently and rapidly, such as a centralized computer network. The constituency will need to be in touch with the CSIRC to effect centralized reporting of incidents, to request assistance, or to request information about relevant aspects of computer security. If some convenient or common means of communication is not available, other means such as facsimile or printed information disseminated via mail could suffice or could be used as a backup measure (however, the CSIRC's ability to respond quickly to incidents would be curtailed). Another issue in constituency communications is whether sensitive or classified information will be communicated; a means for trusted communications might be required such as encryption devices or STU-III telephones.

3.2.2 Formal and Informal Constituency

In certain situations, a CSIRC will serve both a *formal* and an *informal* constituency. The CSIR goals determine the formal constituency, for example, a formal constituency of microcomputer users within a specified agency. However, the CSIRC could find itself serving an informal constituency of multi-user system users from the same agency, microcomputer users from other agencies, agency contractors, or users from the general public. This situation might arise because the CSIRC has become well-known and may be the only such capability within convenient reach of the informal constituency. While the evolution of an informal constituency can be a sign of the CSIRC's success and effectiveness, it can also cause problems. A CSIRC could have difficulty turning down requests from an informal constituency and thus find itself overwhelmed with work. Also, the relations between agencies could be disrupted if, for example, Agency A's users prefer to directly contact Agency B's CSIRC instead of going through Agency A's own computer security channels. Thus, a CSIRC needs to be aware of its requirements to serve its formal constituency, despite pressures from other communities.

3.3 Determining the Structure of the CSIRC Effort

A CSIRC structure can take different forms, depending on agency size, its diversity of technologies, and its geographical locations. When determining a structure, keep in mind the objectives of centralized response and avoiding duplication of effort. From there, much will depend on the size and diversity of the constituency and existing reporting and security practices at the agency. Although there are many suitable structures for a CSIRC, the following paragraphs describe two general approaches.

3.3.1 Centralized, Distinct Organization

Certain environments may find it most practical to utilize a CSIRC that is separate from the agency reporting structure. The CSIRC may operate in conjunction with existing security efforts, but physically may be a separate group that can be contacted directly by agency users. This approach results in a highly centralized CSIRC which is most feasible when the constituency is aligned along a centralized communications network.

Several working models for centralized and distinct CSIRC activities exist [PETHIA90], [SCHULTZ90]. In the case of the CERT/CC and DOE's CIAC, DARPA and DOE respectively have created new organizations as opposed to augmenting existing ones. Although the two organizations are different, they share the same characteristics of being highly centralized, they operate without authority to enforce policies, and they are relatively small in size. Yet by virtue of centralization, they are able to meet the needs of very large constituencies.

This model can be reworked in many ways to fit different circumstances. An agency or site may be able to augment an existing computer security group with CSIR capabilities, such that the group can operate as a discrete unit for the location. For certain environments, this approach is more cost-effective as much duplication of effort is avoided and centralized reporting is rendered less complicated. Additionally, this structure lends itself to a contracted activity if agency expertise is not available.

3.3.2 Decentralized, Distributed Organization

For a variety of reasons, certain environments may find it difficult or impractical to create a CSIRC that is separate from the agency reporting structure or that is centralized into a separate group. For example, the sensitivity of the agency's operations may make it difficult to relinquish any control to one CSIRC activity. Or, the diversity of the technology and resultant constituencies may require a less unified approach. The existence of certain reporting and communications structures may also make it more feasible for the CSIRC activity to be distributed among several locations and levels of the agency.

As an example, an agency could augment existing computer security capabilities, such as help desks or site security offices, with CSIR capability. Each resultant CSIRC would specialize in the needs of its local constituency. However, if the agency is large, many such CSIRCs might be required, all needing to report to a centralized computer security capability. The centralized capability may not require any incident handling expertise, but would minimally log all incidents and facilitate communications among the lower-level CSIRCs; it could also coordinate contacts with investigative agencies and the press. Existing management structures could be used to bubble information up and down throughout the agency [FEDELI91]. This model may work well in certain environments, but could also result in some duplication of effort and prevent incidents from being handled in a timely manner.

In summary, it is difficult to prescribe one best structure, as each agency has different requirements. The objectives and goals of the CSIR effort may have to be adjusted somewhat with existing practices and the nature of the agency; however too much compromise could result in an unwieldy approach that may prove inefficient and too expensive.

3.4 Management Support and Funding

The establishment and operation of a CSIRC requires significant time and resources. Without proper support from management for the CSIRC effort and for policies such as centralized reporting, an effective CSIRC is not possible. Furthermore, a "rogue" CSIRC may cause an agency more harm that good and reduce the likelihood of funding for an approved CSIRC.

3.4.1 Funding and Staffing Issues

A CSIRC requires two types of funding: start-up and continued funding. Start-up funding includes items such as computer equipment, new hires, communications facilities, and offices. Continued funding includes items such as salary growth, inflation, travel, workshop and resource center expenses, and equipment maintenance.

A CSIRC plan might calls for at least one manager and one or more technical staff members. A basic level of staffing is required to accomplish all goals and avoid burn-out. Since it may be difficult to identify all staffing costs at the outset, the following year's funding estimates should account for possible growth in staff.

Management should be presented with several alternative CSIRC configurations, with their respective funding and staffing estimates. For example, a full CSIRC effort could be scaled back and presented as an alternative, with the appropriate trade-offs noted.

3.4.2 Effecting Centralized Reporting of Incidents

Once management support for the CSIRC is established, agency officials need to issue policies to direct the reporting of computer security-related problems to a central point of contact, such as the CSIRC hotline or e-mail address. Centralized reporting is vital to the CSIRC's ability to be effective; if the CSIRC is a single point of contact for its constituency, it is then possible to respond to all incidents and to determine whether incidents are related. With centralized reporting, a CSIRC can also develop accurate statistics on the size, nature, and extent of the security problems within the agency.

3.5 Creating a Charter

Incident response is fraught with many difficulties that arise out of confusion over roles and responsibilities. A charter helps to resolve these conflicts as well as other turf issues that arise. The charter is a statement of the CSIRC's purpose and function. It represents management's acknowledgment and approval of the CSIRC effort. The charter lists the requirements that the CSIRC must satisfy and lays out the boundaries or scope of the CSIRC effort. It should be made available to the agency for use as a reference.

3.5.1 Legal Issues in Determining a Charter

[STEWART89] notes that CSIRC activity raises several legal issues, mostly involving liabilities that may be incurred as a result of intentional, reckless or negligent conduct on the part of the CSIRC that could cause injury to another party.[3] Even though a CSIRC is performing a useful service, it may be liable to software vendors, users, or others if it performs its work negli-

---

[3][STEWART89] is oriented towards those who would establish *Computer Security Response Centers* (CSRCs) for the Internet; it does not purport to provide definitive legal advice. It states that the implementation of a CSRC raises a number of legal issues, including the following:

- What is a CSRC's liability if, having undertaken to assist in the protection of Internet, it fails to do so and someone is harmed as a result?
- What is a CSRC's liability if it reports a software bug to a publisher or to users and the bug does not, in fact, exist?
- How should legal concerns shape a CSRC's planned collection and notification procedures, if at all?

It states that most of the liabilities facing a CSRC are in the nature of torts, i.e., the civil liabilities the law imposes for intentional, reckless, or negligent conduct that causes injury to another. It then suggests that a CSRC could limit its exposure by clearly declaring that (a) its sole purpose is to evaluate and report software defects, (b) it will not be in the business of independently uncovering software defects, (c) it does not purport to displace the obligations software publishers have to computer users, (d) its efforts should be viewed as mere supplements to the efforts of Internet users and beneficiaries to protect the Internet, (e) it encourages users to purchase software maintenance from publishers and remain in contact with publishers and (f) it is undertaking these duties for the purpose of assisting publishers, users and other beneficiaries in protecting the viability of the Internet network and not attempting to protect the security of any particular computer system or user.

gently. A CSIRC might limit its legal exposure by clearly declaring within the charter what the CSIRC is and is not purporting to do, how it will accomplish its goals, and where its boundaries of involvement lay. Appropriate legal advisors need to review the charter and all other procedures in use by a CSIRC.

3.5.2 Components of a CSIRC Charter

A CSIRC charter should include the following (or equivalent) sections to describe the purpose and scope of the effort [STEINBERG89]:

1. Executive Summary
2. Responsibilities
3. Methods
4. Reporting Structure and Staffing

Executive Summary - to quickly acquaint readers with the existence of the CSIRC, its overall scope of responsibilities, and other basic information.

Responsibilities - a description of what the CSIRC is and is not purporting to do. To limit its legal exposure, this section states the express purpose of the CSIRC effort and defines the boundaries of involvement for the CSIRC, such as when dealing with classified matters or matters involving other agencies or contractors.

Methods - defines in a high-level manner how the CSIRC will meet its responsibilities and requirements and the general approach used by the CSIRC for dealing with certain types of threats and for reducing risks in the affected areas.

Reporting and Staffing - identifies how the CSIRC will fit within the organizational structure of the agency and the staffing and funding requirements. This helps to quickly resolve boundary disputes and other potential conflicts over who should handle certain types of computer security problems.

3.6 Creating a CSIRC Operations Handbook

The *Operations Handbook* contains the procedures that the CSIRC will follow and refer to during its daily activities. It provides a single point of reference for outlining the operating procedures as they are developed and implemented. The handbook is an evolving document that will undergo changes and modifications over time and as the CSIRC effort gains experience and benefits from lessons learned. Like the charter, it should be reviewed by legal advisors to avoid unnecessary legal conflicts.

The CSIRC staff members will need to consult the Operations Handbook routinely, thus it should be organized to provide ready access to operational information. The operations handbook should contain the following:

- Staffing Information - contacts, facsimile, pagers
- Hotline Use - numbers, procedures for 24-hour operation, on-call lists
- Constituency Communications - procedures for receiving and sending information
- Incident Reports - types of, content of, reviews of, how verified
- Information Handling - logging, sensitive information, incident summaries
- CSIRC Computer Equipment - administration policies, configurations, procedures
- Administrative Procedures - expense reports, travel, security clearances
- Contacts within investigative agencies
- Dealing With Media - press reports, clearance process
- Vendor Contacts
- Other Contact Information - other individuals to contact for help, reference

The Operations Handbook will need to be revised frequently, especially during the first year of CSIRC operation. An on-line copy helps to facilitate frequent revisions.

3.7 CSIRC Staffing Issues

Although agency requirements differ, a typical CSIRC might have the following full-time staff:

- one or more CSIRC coordinators;
- several technical staff members (probably two or more); and
- support staff as necessary.

It is difficult to prescribe a typical staffing profile, as the profile is directly related to the diversity of the constituency and its size as well as to other factors such as the types of risks to the constituency technology. For example, a CSIRC that handles incidents of computer viruses may be much smaller than a CSIRC that covers several types of systems.

3.7.1 CSIRC Coordinator

The position of *CSIRC coordinator* entails much more than typical management functions. A CSIRC, in the course of handling incidents, may prove to be controversial, especially when the incidents involve dealings with other agencies or with law enforcement groups or the press. In situations where delicate political relationships have to be considered, the manager of a CSIRC will need to be adept at maintaining a positive working relationship between the CSIRC and any affected groups. The CSIRC coordinator might also have to spend a considerable amount of time "selling" the CSIRC efforts to the constituency and vendors to effect a better relationship and raise computer security awareness.

3.7.2 Technical Staff

A CSIRC's *technical staff members* should possess a number of important qualities. Technical expertise in the CSIRC's technology focus is essential; however, a broad range of experience is most desirable. Other important qualities center around good communications skills. A summary of the qualifications a technical staff member ought to possess might be as follows:

- capable of supporting the technology focus;
- work in a group environment and share information with others;
- communicate effectively with different types of users, who will range from system administrators to unskilled users to management to law-enforcement officials;
- be "politically" adept and skilled at dealing with emotional situations;
- be on-call 24 hours as needed; and
- be able to travel on short notice.

3.7.3 Other Support Staff

Other support staff could be utilized to perform functions connected with the daily operation and support of the CSIRC; this could also be performed by technical staff members. Some of the functions performed by other support staff would be as follows:

- maintain CSIRC computer resources;
- coordinate incident logging procedures;
- develop histories and summaries of CSIRC interactions;
- on-line analysis of CSIRC operations;
- capture lessons learned through operation of the CSIRC and post-incident reviews; and
- provide support services to the rest of the CSIRC members.

3.7.4 Requirements for Clearances

CSIRC staff members may require clearances to work with Department of Defense agencies and law enforcement groups in situations where data may be sensitive or classified. While clearances will not be necessary for all environments, information about aspects of incidents can become classified depending on many factors. Finding people who can or wish to undergo the clearance process and who possess the requisite skills may be time-consuming and the clearance process itself may take several months or longer. If there exists a requirement for clearances, paperwork should be submitted at the earliest opportunity.

3.7.5 Avoiding Burn-Out

If a CSIRC performs only incident handling and no other activities, burn-out may become a critical problem affecting the CSIRC staff members. Incident handling on a full-time basis may prove somewhat underchallenging for highly technical individuals, and some alternative tasks may need to be built-in. Some suggestions for these tasks are:

- performing workshops or training sessions for the constituency;
- writing educational material that can be distributed or published;
- writing software tools for system managers to better detect or prevent incidents; and
- conducting research.

4. CSIRC Operational Issues and Activities

This section describes some of the issues and activities involved in operating a CSIRC. Incident response is a process whereby incidents are identified, contained, and resolved. There are many issues and details involved in each of these steps; a detailed discussion is beyond the scope of this guide. Readers are encouraged to examine [HOLBROOK91], [BRAND89], and [SCHULTZ90] for discussion on incident response.

This chapter concentrates on operational activities and issues that are generally involved in incident response, regardless of the type of incidents, computing environments, or organization. Sections deal with constituency communications, logging information, legal issues, the press, and post-incident procedures.

4.1 Communications with the Constituency

A CSIRC needs to be in touch with its constituency on a daily basis to effect centralized reporting and to disseminate information concerning vulnerabilities, alerts, and other awareness information. This section contains information on technical communications issues, i.e., the mechanisms for convenient and effective communications between the constituency and CSIRC. Sections focus on issuing a press release to the constituency and issues on using a hotline and information repository.

4.1.1 Issuing a Press Release

A press release is useful for making the existence of the CSIRC known to the constituency so that misconceptions and misunderstandings about the CSIRC's role and purpose are avoided. A press release should minimally state the purpose of the CSIRC and where its boundaries of involvement lay. It should define the constituency and how the constituency can get in touch with the CSIRC. It may be advisable before commencing CSIRC operations to make other information available to the public affairs office so that they will have appropriate material on-hand when fielding inquiries about the CSIRC.

A CSIRC may find it advantageous to issue press releases for reasons other than initial start-up. During the course of an incident, it may be useful to issue information to ensure that accurate information gets disseminated and damaging misconceptions are prevented. When dealing with the press, always make use of the public affairs office. Working with the press is covered in more detail in section 4.5.

4.1.2 Setting Up a Hotline Capability

The CSIRC needs to advertise how the constituency can contact the CSIRC in case of emergencies and other matters. It may be most practical to publish a "hotline" telephone number that the constituency can call for urgent matters. An e-mail address is useful for constituents to send inquiries or obtain information. Using an e-mail address or telephone voice mailbox permits the CSIRC staff to prioritize calls. An e-mail address offers the further advantage of all members of the CSIRC being able to receive the e-mail, enhancing team communications.

An important detail to setting up a hotline capability is deciding who should answer the calls. A practical arrangement is to designate a technical staff member to be "on-call" for a certain period, one week for example, and then to rotate the assignment to the next staff member, with other staff members available to help out as needed. This arrangement is most practical when the hotline is to be staffed 24 hours a day; the staff member on-call needs to wear a pager when away from the office and stay within a close geographical area during the period of on-call duty.

4.1.3 Setting Up Alert Mechanisms

The CSIRC needs some mechanism for alerting its constituency of important alert and vulnerability-related information. In certain environments, a computer network works well for this purpose; information sent out to the network could rapidly reach users. Users could respond to a central CSIRC e-mail address.

Factors that make a computer network less feasible include lack of uniform access to a network and lack of trust in the network, i.e., if classified or very sensitive information would need to be relayed via a network subject to eavesdropping. If no central, homogeneous network exists, communications are more complicated. A frequent networking situation is that several different types of networks are in use throughout an agency. In this case, gateways between the networks could be investigated, or else the CSIRC may need direct access to each network. Encryption methods should also be explored so that network traffic can be protected from surreptitious tampering and listening. The CSIRC could also issue alerts and information via telephone, management bulletins, facsimile, or phone-mail.

Emergency backup communications should be put in place for contingencies such as equipment failure or malicious activity that could make the primary mechanism unavailable. While a redundant computer network is preferable, a simple but effective backup mechanism could make use of a points-of-contact list to alert management, which could in turn alert users.

4.1.4 Use of an Information Repository

An electronic information repository offers significant advantages in that it can be used to make awareness information available to the constituency in a format that is both convenient and efficient for the CSIRC. Users are able to peruse and download information without requiring assistance from the CSIRC, enabling the CSIRC to concentrate its resources on incident handling and information gathering. An information repository might include the following:

- archived vulnerability or alert information;
- descriptions of the CSIRC and related information;
- agency security policies;
- procedures for reporting suspected problems or incidents;
- self-help information, such as how to use access controls to improve integrity; and
- information about current threats, such as viruses or software vulnerabilities.

If the constituency is aligned along a network, a network server could be made available as an information repository. Otherwise, a bulletin board system (BBS) system reachable via telephone lines may work. Minimally, this information could be made available in hard copy, although the dissemination of hardcopy material may better be handled by a group other than the CSIRC.

4.2 Logging Information

A CSIRC needs to retain a variety of information for its own operational use and for conducting reviews of effectiveness and accountability. Several types of information need to be maintained:

- contact information
- activity logs
- incident logs

4.2.1 Contact Information

The demands of incident handling necessitate that contact information be maintained in a format that can be readily accessed and updated. A contacts database includes such items as vendor contacts, legal and investigative contacts, other individuals with technical expertise, and other CSIRC information. A contacts database record might include the following information fields:

Name
Title

Organization
Address
Regular Phone
Emergency Phone
E-mail Address
Facsimile Address
Comments (could include field of expertise or other information)
Alternative Contact (in case contact is not available)

4.2.2 Activity Logs

Activity logs reflect the course of each day. It is not necessary to describe each activity in detail, but it is useful to keep such a log so that the CSIRC can account for its actions. Noting all contacts, telephone conversations, and so forth ultimately saves time by enabling one to retain information that may prove useful later. Security incidents or other events that are seemingly unrelated may, through examining activity logs, prove to be related or otherwise more important. While it is possible to maintain activity logs on-line, a simple notebook is convenient and flexible.

4.2.3 Incident Logs

Incident logs are generated during the course of handling an incident. While physically similar to activity logs, they are dedicated to incident response and merit more detail. Incident logs are important for accurate recording of events that may need to be relayed to others - if little or no information is logged, the source of information needs to be contacted repeatedly, wasting valuable time. Information in incident logs is helpful for establishing new contacts, piecing together the cause, course, and extent of the incident, and for post-incident analysis and final assessment of damage. Additionally, if the CSIRC will be involved in potential prosecutions, the information might also be used as evidence. An incident log should minimally contain the following information:

- all actions taken, with times noted;
- all conversations, including the person(s) involved, the date and time, and a summary; and
- all system events and other pertinent information such as audit logs.

It is practical to maintain an incident log in a notebook along with the activity log. It may be difficult to pinpoint when an incident first began or when the CSIRC first became aware of it, thus the log of an incident may become intertwined with the activity log.

4.2.4 Information Maintenance

Maintain all contact and other information in a tightly controlled area. Notebooks need to be stored in locked, fireproof areas. All information maintained on-line needs to be backed up daily and secured from unauthorized access. Store the information on a system that is inaccessible to non-CSIRC members, i.e., a system not connected to an agency-wide network.

4.3 Incident Notification Issues

When first notified of an incident, a CSIRC follows an established set of procedures to verify the actual existence of the incident and to notify appropriate contacts within the agency as well as others affected by the incident. If these procedures are not established beforehand, embarrassing and potentially damaging situations could arise that may damage the agency's reputation and expose it to legal problems [STEWART89].

4.3.1 Identifying the Existence of an Incident and its Scope

Upon learning of a possible incident, a CSIRC needs to take steps to verify that the incident actually does exist. If the source of the incident information is unfamiliar or not trusted, verify the source, especially if the source has identified themselves as a representative of a legal or investigative agency. Verify the incident, firsthand if possible, to ensure that the incident is not a harmless misunderstanding or even a hoax. The CSIRC should be aware of false alarms and other activity that may only resemble something more serious.

Once the incident is verified, determine its scope. While the real scope of the incident may not be apparent at this stage, knowing whether it affects other agencies or organizations will determine who should be notified and whether investigative agencies should be contacted.

4.3.2 Notifying Appropriate Agency Personnel

After the incident has been confirmed, the CSIRC may be required to notify a predetermined list of agency personnel. Create this list before incident handling occurs to avoid confusion and prevent situations where agency officials learn of the incident via third parties. While each agency has its own notification requirements, a typical list might include the following:

- agency directors
- computer security personnel
- network managers as appropriate
- data processing sites as appropriate
- legal advisor

- public affairs office
- local or state police
- contacts in investigative agencies

4.3.3 Notifying Affected Users

If the incident affects other users, they may need to be notified so as to take appropriate action. For example, if an intruder is using a system to break into other systems, the system's administrator needs to be contacted so that the intruder's access can be closed or their actions monitored. When apprising users of the existence of an incident, the CSIRC should make every attempt to provide clear and concise information, as those users may need to inform their respective organizations. The CSIRC should avoid any appearance of being an enforcement activity and should be aware that affected users may not take the news of the incident in a positive manner. Good communication skills and the ability to be adaptive to different users and their respective levels of technical experience are all the more important.

4.3.4 Requests for Confidentiality

During the course of incident handling, a CSIRC may find that some individuals wish to remain anonymous, i.e., the CSIRC may be requested to keep its source of incident information confidential. This presents a dilemma if the CSIRC is obligated to report source of information: if the party is not granted anonymity, the party may refuse to cooperate further or may turn to another CSIR effort that respects the party's wishes.

The central issue is that if the CSIRC takes on the appearance of an enforcement aspect and does not respect requests for confidentiality, incidents may not be reported because the affected parties may not want to risk exposure, embarrassment, or penalty. If the parties turn to other CSIR efforts, it may present dilemmas for those efforts, since they may not wish to overstep their boundaries of involvement.

If the CSIRC is to respect requests for confidentiality, CSIRC staff members should advise affected parties that they may still be under other obligations for reporting the incident information, i.e., the CSIRC's decision not to report a source does not remove any other obligations for reporting. Making this clear to the party is important from a legal standpoint and may encourage the party to fulfill its obligations.

4.4 Legal Issues

There are a number of legal issues in operating a CSIRC. Some of these issues have already been covered: Chapter 3 discussed appropriate language in the CSIRC charter to reduce legal exposure by defining the CSIRC's expressed purpose and boundaries of involvement. The guidance given here is not authoritative; always consult appropriate agency legal advisors.

4.4.1 Working With Law-Enforcement and Investigative Agencies

A CSIRC needs to make contacts within the local and state law-enforcement groups and within the investigative agencies, most importantly the FBI and the Secret Service, before assuming an incident response role. There are many reasons for establishing these contacts at the outset, most importantly because the handling of an incident does not leave time to establish the correct contacts. If an incident involving criminal conduct is mishandled, the CSIRC could conceivably cause its agency to be legally liable.

Issues to resolve with law-enforcement and investigative agencies include differences between state and federal law that affect computer security, gathering evidence, monitoring issues, and which agencies will assume jurisdiction in an incident.

4.4.2 Incurred Liabilities

A CSIRC may face a legal obligation of performing its duties with reasonable care in the investigation and reporting of software defects and vulnerabilities. If the CSIRC's Charter states that the CSIRC will accept and investigate reports of software defects or vulnerabilities, the CSIRC must make itself reasonably available to receive reports of software defects. An e-mail address or hotline should be made available for reporting problems, and all problems must be checked thoroughly for accuracy and then logged. The CSIRC must accurately record and report the defects to the proper vendors or, failing that, to user groups. The reports must be held confidential and reported to the proper vendor(s) in a timely manner. It may be useful to solicit the vendor's response and help when writing a report of the defect or vulnerability to the constituency [STEWART89].

The possible consequences of failures to perform the above in a reasonable fashion could involve a lawsuit whereby the plaintiff could argue that the CSIRC, by not properly disclosing knowledge of a software defect or vulnerability, would have a legal liability to a plaintiff that was harmed by the defect. For this reason, a CSIRC must not purport to assume any obligations that other groups already incur, such as a vendor's stated obligation to correct software defects. The CSIRC should also widely disseminate a detailed description of its policies on notifying software vendors, its constituency, and the public about software defects or vulnerabilities to ensure that any misunderstandings or false expectations of its policies are minimized.

4.4.3 Wording of Constituency Communications

When writing alerts or reports to send to the constituency regarding an incident or vulnerability, care should be taken to choose the proper wording. While the agency and the CSIRC may consider that any communication to the constituency are private, the agency should expect that the communications may be disseminated far beyond the constituency. The same care should be taken with the press: be accurate, but do not reveal evidence or technical details that may result in more incidents or further damage.

When writing about software defects or vulnerabilities, a CSIRC should avoid possible copyright, defamation, patent, or trade secret issues with the vendor(s) in question [STEWART89]. Value-neutral words should be chosen to describe the problems, such as "possible software defect" or "potential security vulnerability" as opposed to words that imply vendor negligence or guilt. If the CSIRC possesses source code or has made non-disclosure agreements, care should be taken to avoid revealing any information that is legally protected.

The legal advisor may suggest that a disclaimer be attached to CSIRC communications, especially when vendor products are mentioned. Following is an example of such a disclaimer[4]:

```
Neither the United States Government nor any of its employ-
ees makes any warranty, express or implied, or assumes any
legal liability or responsibility for the accuracy, com-
pleteness, or usefulness of any information, apparatus, pro-
duct, or process disclosed, or represents that its use would
not infringe privately owned rights.  Reference herein to
any specific commercial products, process, or service by
trade name, trademark, manufacturer, or otherwise, does not
necessarily constitute or imply its endorsement, recommen-
dation or favoring by the United States Government.  The
views and opinions of authors expressed herein do not neces-
sarily state or reflect those of the United States Govern-
ment, and shall not be used for advertising or product en-
dorsement purposes.
```

[4]This disclaimer is adapted from a disclaimer used by the Department of Energy's Computer Incident Advisory Capability (CIAC). It is provided here only as an example; agencies should consult their legal advisors for appropriate wording.

4.4.4 Logging and Gathering Evidence

At the outset of an incident, it may not be possible to determine whether the incident will result in a prosecution. Thus, incident logging should be treated much the same as evidence gathering: the incident log should be detailed, accurate, and the proper procedures should be followed so that the incident log could be used as evidence in a court of law. Investigative agencies can provide more detail; at a minimum, use the following procedures:

- at the end of each day, make a photocopy of the incident log;
- sign and date the photocopy and submit it to a document custodian;
- accept and retain the receipt from the custodian; and
- the document custodian must store the photocopy in a secure area.

When logging or monitoring electronic information concerning an incident, always contact the investigative agencies first for advice on legal issues and procedures [HANSEN90], [HOLBROOK91].

4.5 Working With the News Media

Certain types of incidents may generate inquiries from the press or broadcast media, or it may be advisable in certain circumstances to issue information to the media. There are many issues to consider when working with the press, thus an agency's public affairs office (or equivalent) should always be contacted first before any dealings with the press. The public affairs office can act as a single point of contact for the press, which shields the CSIRC staff and leaves them more time to handle the incident. Talk candidly with the public affairs office and ensure that they understand the technical issues, so that they may communicate more effectively and accurately with the press. False or misleading information may ultimately cause more damage to the agency's image than the incident itself [BRAND89]. Some suggestions when working with the press regarding an incident are:

- contact the legal advisor if unsure of legal issues;
- establish a single point of contact to the press so that media inquiries are coordinated and the CSIRC is able to concentrate on resolving the incident;
- keep the level of technical detail low - do not provide attackers with information;
- be as accurate as possible, but do not speculate; and
- ensure that details about the incident that may be used as evidence are first checked with investigative agencies.

4.6 Post-Incident Analysis

After an incident has been resolved, a *post-mortem* should be conducted so that the CSIRC can learn from the experience and, if necessary, update its procedures. The following sorts of incident information should be examined:

- how the incident started: which vulnerabilities were exploited, how access was gained, and other relevant details;
- how the CSIRC became aware of the incident;
- how the incident was resolved;
- whether existing procedures were adequate or require updating;
- whether vulnerabilities still need to be closed; and
- whether new contacts were made.

As a result of a post-incident analysis, a CSIRC may need to issue alerts or warnings to its constituency about certain actions to take to reduce vulnerabilities that were exploited during the incident. The CSIRC may also need to update its Operations Handbook to reflect new procedures. The CSIRC could use a post-incident analysis to ascertain its impact on the agency as a result of handling and resolving the incident. Although this may be difficult to quantify, some measure of its performance and beneficial effect may be useful in determining the future scope and direction of the CSIRC.

4.7 Measuring the Effectiveness of a CSIRC

How does an agency determine whether the investment in a CSIRC has actually *paid off* in terms of increasing security? The answer might not be entirely quantifiable in terms of dollars saved and incidents handled. It may not be possible to satisfactorily quantify the benefits a CSIRC provides within its first year of operation. It could turn out that the initial estimate of the security problems to be handled by the CSIRC has fallen far short of the real problem, making it appear as if the CSIRC is not making rapid progress. A CSIRC will have to recognize the difficulty in measuring the success of its activities and in part, justify those activities to the organization.

One of the ways in which a CSIRC could rate its success is by collecting and analyzing statistics on its activity. For example, a CSIRC could keep statistics on the following items:

- incidents responded to
- vulnerabilities reported
- vulnerabilities fixed

- incidents reported
- tools implemented
- e-mail messages received/sent

By examining these statistics and others, the CSIRC and other management can measure the success of the operation. Statistics such as these will be very helpful in measuring and comparing CSIRC performance in subsequent years.

4.8 Additional Assistance

There are more issues, steps, and concerns involved in establishing a CSIRC than are listed here. Agencies should draw on the experiences of others that have already developed CSIRC efforts as well as examine the references listed in this guide for more information. It is important that these agencies document the lessons learned in this process, so that other agencies and groups can gain from their experiences. Of particular use is [FEDELI91], [SCHULTZ90], and [RFC1244].

5. References

[BRAND89] Brand, Russell L., *Coping With the Threat of Computer Security Incidents: A Primer from Prevention through Recovery*, July, 1989.

[DDN89] DCA DDN Defense Communications System, "DDN Security Bulletin 01," DDN Security Coordination Center, October, 1989.

[FEDELI91] Fedeli, Alan, "Organizing a Corporate Anti-Virus Effort," *Proceedings of the Third Annual Computer VIRUS Clinic*, Nationwide Computer Corp., March, 1990.

[GAO89] *Computer Security - Virus Highlights Need for Improved Internet Management*, United States General Accounting Office, Washington, DC, 1989.

[HANSEN90] Hansen, Steve, "Legal Issues: A Site Manager's Nightmare," *Proceedings of the Second Invitational Workshop on Computer Security Incident Response*, June, 1990.

[HOLBROOK91] Holbrook, P., and Reynolds, J., *Security Policy Handbook*, RFC 1244 prepared for the Internet Engineering Task Force, 1991.

[NIST90] *CERT System Operational Framework*, National Institute of Standards and Technology, 1990.

[PETHIA90] Pethia, Rich, and van Wyk, Kenneth, *Computer Emergency Response - An International Problem*, 1990.

[QUARTERM90] Quarterman, John, *The Matrix - Computer Networks and Conferencing Systems Worldwide*, Digital Press, 1990.

[RISK91] National Research Council, *Computers at Risk*, National Academy Press, 1991.

[SCHERLIS88] Scherlis, William, "DARPA Establishes Computer Emergency Response Team," DARPA Press Release, December 6, 1988.

[SCHERLIS89] Scherlis, William, Squires, Steven, and Pethia, Rich, *Computer Emergency Response*, 1989.

[SCHULTZ89] Schultz, E. Eugene, "The Computer Incident Advisory Capability (CIAC)," *Center for Computer Security News*, Vol. 8, 1989.

[SCHULTZ90] Schultz, E. Eugene, Brown, David, and Longstaff, Thomas, *Responding to Computer Security Incidents: Guidelines for Incident Handling*, University of California Technical Report UCRL-104689, 1990.

[STEINBERG89] Steinberg, Tad, "Developing a Computer Security Charter," *Security, Audit, and Control Review*, Vol. 6 No. 4, ACM SIGSAC, Winter 1989.

[STEWART89] Stewart, Geoffrey, and Sylvester, David, *Potential Liabilities of Computer Security Response Centers Arising from Notification to Publishers and Users of Security Deficiencies in Software*, December, 1989.

[WCSIR91] *Proceedings of the Third Invitational Workshop on Computer Security Incident Response*, August, 1991.

Appendix A. Annotated Bibliography

This section consists of an annotated list of selected works dealing with incident handling. Where noted, some works are available from NIST in electronic form for users with a modem and communications software or for Internet users; refer to the end of this section for details. Some references are from RFC 1244, *Security Policy Handbook*; see [HOLBROOK91].

[BRAND89] Brand, Russell, *Coping With the Threat of Computer Security Incidents: A Primer from Prevention through Recovery*, July, 1989.

Contains a wide range of guidance regarding incident handling, but oriented mostly towards technical issues. Has advice in particular for UNIX and VAX/VMS managers. This guide is recommended for anyone involved in incident handling. In draft form, available via the Internet from *cert.sei.cmu.edu*.

Cheswick, B., "The Design of a Secure Internet Gateway," *Proceedings of the Summer Usenix Conference*, Anaheim, CA, June, 1990.

Brief abstract (slight paraphrase from the original abstract): AT&T maintains a large internal Internet that needs to be protected from outside attacks, while providing useful services between the two. This paper describes AT&T's Internet gateway. This gateway passes mail and many of the common Internet services between AT&T internal machines and the Internet. This is accomplished without IP connectivity using a pair of machines: a trusted internal machine and an untrusted external gateway. This configuration helps protect the internal internet even if the external machine is fully compromised. Available via the Internet from *research.att.com*.

Courtney, Robert, Jr., "Proper Assignment of Responsibility for Data Security," *Computers and Security*, Volume 7 #1, February, 1988.

Brief abstract: "An analysis of the data security responsibilities within an organization is presented. It is proposed that DP management should not have total responsibility, but that this should be shared by staff in the functional areas to ensure cost-effectiveness and viability." The author recommends creation of a Computer Security Competence Center that has some parallels to a CSIRC, especially in administration of security and user awareness.

Curry, David, *Improving the Security of Your UNIX System*, SRI International Report ITSTD-721-FR-90-21, April 1990.

A practical guide to improving UNIX system security that lays out a number of vulnerabilities and methods for improving monitoring and detecting threats. Contains a number of good references to other sources of information. Available on-line from NIST.

Denning, Peter, *Computers Under Attack: Intruders, Worms, and Viruses*, ACM Press, 1990.

A collection of 40 pieces divided into six sections: the emergence of worldwide computer networks, electronic breakins, worms, viruses, counterculture (articles examining the world of the "hacker"), and finally a section discussing social, legal, and ethical considerations.

[FEDELI91] Fedeli, Alan, "Organizing a Corporate Anti-Virus Effort," *Proceedings of the Third Annual Computer VIRUS Clinic*, Nationwide Computer Corp., March, 1990.

Discusses IBM's approach in organizing their computer virus incident handling procedures. Contains mostly management issues involved in establishing the incident handling center, locating it within existing organizational structures, and initial steps in operating the center. This document contains much useful guidance and is highly recommended. Available on-line from NIST.

Fites, M., Kratz, P., and Brebner, A., *Control and Security of Computer Information Systems*, Computer Science Press, 1989.

This book serves as a good guide to the issues encountered in forming computer security policies and procedures. The book is particularly notable for its straight-forward approach to security, emphasizing that common sense is the first consideration in designing a security program. The authors note that there is a tendency to look to more technical solutions to security problems while overlooking organizational controls which are often less expensive and more effective.

[GAO89] U.S. General Accounting Office, *Computer Security - Virus Highlights Need for Improved Internet Management*, United Stated General Accounting Office, Washington, DC, 1989.

This paper, a General Accounting Office Report, contains much useful information regarding the Internet, the Internet worm, common vulnerabilities, and computer viruses. It contains a number of recommendations for improving system management and communications between vendors and system managers as regards bug reports and fixes. Some legal issues regarding prosecution are discussed. Available on-line from NIST.

Garfinkel, Simson, and Spafford, Eugene, *Practical UNIX Security*, O'Reilly & Associates, Inc., 1991.

A comprehensive guide to UNIX security; an important source for UNIX sites that are attached to UUCP networks or the Internet. The book contains some guidance regarding incident handling: detecting signs of unauthorized activity and subsequent steps to take.

Hafner, Katie, and Markoff, John, *Cyperpunk - Outlaws and Hackers on the Computer Frontier*, Simon and Schuster, 1991.

Entertaining and useful reading for insights into computer hacking. The book contains case studies of Kevin Mitnick, a noted telephone hacker, Pengo, a West German who offered his hacking services to the Soviet Government, and Robert Morris Jr.,, a student who wrote the "Internet Worm" program. The book alerts readers as to the extent to which society is dependent on computers and how fragile the computer safeguards are.

[HANSEN90] Hansen, Steve, "Legal Issues: A Site Manager's Nightmare," *Proceedings of the Second Invitational Workshop on Computer Security Incident Response*, June, 1990.

This paper details some of the legal issues involved in incident handling, especially in logging electronic information. The paper focuses on the Federal Electronic Communications Act of 1986 and some of the ambiguities and ethics involved in interpreting the law and monitoring user activity. Available on-line from NIST.

Hoffman, Lance, *Rogue Programs: Viruses, Worms, and Trojan Horses*, Van Nostrand Reinhold, 1990.

A collection of papers and excerpts from publications regarding computer viruses and related threats. Recommended for its thoroughness and broad scope.

[HOLBROOK91] Holbrook, Paul, and Reynolds, Joyce, *Security Policy Handbook*, RFC 1244 prepared for the Internet Engineering Task Force, 1991.

A highly useful paper, prepared as an Internet Request For Comments (RFC). Although this paper is oriented towards sites connected to the Internet, much of the information is equally applicable to other system and network environments. It contains useful information regarding basic security procedures, incident response, and legal issues. A detailed bibliography is included. This paper is highly recommended for its discussion of management and technical issues involved in incident response. Available on-line from NIST.

National Institute of Standards and Technology, *Bibliography of Selected Computer Security Publications January 1980 - October 1989*, NIST Special Publication 800-1, December, 1990.

This bibliography cites selected books and articles on computer security published from January 1980 through October 1989. To have been selected, an article had to be substantial in content and have been published in professional or technical journals, magazines, or conference proceedings. English language from foreign journals were included as available. A category of pre-1980 publications is also provided, as well as an appendix containing address of all journals and magazines referenced. For sale by the U.S. Government Printing Office, Washington, DC 20402, (202) 783-3238, reference #003-003-03060-1. Available on-line from NIST.

[PETHIA90] Pethia, Rich, and van Wyk, Kenneth, *Computer Emergency Response - An International Problem*, 1990.

This paper describes how computer security incidents have begun to become international in scope due to networks. The paper recommends international cooperation in dealing with incidents and suggests methods by which individual computer security response groups can work together internationally to cope with computer security incidents. Available via the Internet from *cert.sei.cmu.edu*.

Pfleeger, Charles, *Security in Computing*, Prentice-Hall, Englewood Cliffs, NJ, 1989.

A general textbook in computer security, this book provides an excellent and very readable introduction to classic computer security problems and solutions, with a particular emphasis on encryption. The encryption coverage serves as a good introduction to the subject. Other topics covered include building secure programs and systems, security of database, personal computer security, network and communications security, physical security, risk analysis and security planning, and legal and ethical issues.

[QUARTERM90] Quarterman, John, *The Matrix - Computer Networks and Conferencing Systems Worldwide*, Digital Press, 1990.

A comprehensive guide to the world's computer networks and their protocols. A useful source of information for sites connected to networks.

[RISK91] National Research Council, *Computers at Risk*, National Academy Press, 1991.

This document presents a comprehensive agenda for developing nationwide polices and practices for computer security. It contains a number of recommendations that address roles of agencies, expansion of current efforts, and cooperation between industry and government.

Russell, Deborah, and Gangemi, G.T. Sr., *Computer Security Basics*, O'Reilly & Associates, Inc., July, 1991.

Provides an introduction to computer security concepts: passwords, access controls, network security, biometrics, TEMPEST, and more. Describes government and industry standards for security, including the "Orange Book." Contains a number of useful references.

[SCHULTZ90] Schultz, E. Eugene, Brown, David, and Longstaff, Thomas, *Responding to Computer Security Incidents: Guidelines for Incident Handling*, University of California Technical Report UCRL-104689, 1990.

Contains general guidance on incident handling and specific procedures for viruses and other related threats. A useful document for organizing incident response procedures. Available from NTIS, 5285 Port Royal Rd., Springfield, VA 22161, (703) 487-4650.

Spafford, Eugene, "The Internet Worm Program: An Analysis," *Computer Communication Review*, Vol. 19, No. 1, ACM SIGCOM, January 1989.

A thorough analysis of the Internet Worm, including information on the vulnerabilities it exploited, how it spread, and analysis of its software routines. A good source of information about how network worms operate. Available on-line from NIST.

Spafford, E., Heaphy, K., and Ferbrache, D., *Computer Viruses: Dealing with Electronic Vandalism and Programmed Threats*, ADAPSO, 1989.

This is a good general reference on computer viruses and related concerns. In addition to describing viruses in some detail, it also covers more general security issues, legal recourse in case of security problems, and includes lists of laws, journals focused on computers security, and other security-related resources. Available from ADAPSO, 1300 N. 17th St, Suite 300, Arlington, VA 22209. (703) 522-5055.

[STEINBERG89] Steinberg, Tad, "Developing a Computer Security Charter," *Security, Audit, and Control Review*, Vol. 6 No. 4, ACM SIGSAC, Winter 1989.

An informative article on developing a computer security charter. Contains useful examples of a charter's contents.

[STEWART89] Stewart, Geoffrey, and Sylvester, David, *Potential Liabilities of Computer Security Response Centers Arising from Notification to Publishers and Users of Security Deficiencies in Software*, December, 1989.

A highly useful paper that concentrates on legal liabilities that a computer security response center might face. It contains some legal advice, although it does not purport to contain authoritative answers to legal questions. Certain incurred liabilities are described along with methods and steps to take for reducing legal exposure. This paper also contains advice for dealing with vendors as regards reporting of software defects and vulnerabilities. Available on-line from NIST.

Stoll, Cliff, *The Cuckoo's Egg*, Doubleday, New York, 1989.

This book describes the author's discovery and subsequent tracking of a series of break-ins to computer sites connected to military and research networks. The book is entertaining and easy to read, as it explains many technical issues in laymen's terms. The book is especially useful to managers of systems connected to networks.

[WCSIR91] *Proceedings of the Third Invitational Workshop on Computer Security Incident Response*, August, 1991.

The proceedings to these conferences are very useful for those interested in establishing incident response capabilities. Information on these proceedings can be obtained from CERT/CC, SEI, Carnegie Mellon U., Pittsburgh, PA 15213-3890

Obtaining Electronic Information from NIST

Works from this section noted as being available on-line from NIST, as well as this document and other general information, can be obtained via the NIST Computer Security Resource Center BBS or via the Internet using ftp:

BBS: (301) 948-5717 (2400 or less),
(301) 948-5140 (9600)

ftp: ftp *csrc.ncsl.nist.gov* (129.6.54.11),
login as user *anonymous*, password *your name*,
works are located in directory *pub*

Appendix B. Forum of Incident Response & Security Teams (FIRST)

The Forum of Incident Response and Security Teams (FIRST) is an organization whose members work together voluntarily to deal with computer security problems and their prevention. The forum is composed of a Secretariat, Steering Committee, Representatives from each participating team, and ad hoc working groups. The forum meets regularly and conducts periodic workshops on incident handling.

There are two types of participation in the forum. **Forum Members** represent organizations who assist an information technology community or other defined constituency in preventing and handling computer security-related incidents, i.e., incident response teams. **Liaisons** are individuals or representatives of organizations other than emergency response teams that have a legitimate interest in and value to the forum.

Information on a prospective participant is circulated among existing Forum Members for possible nomination interest. Information provided by the nominee is reviewed by the Steering Committee, which votes on acceptance of the nominee. Written notification of acceptance is sent by the Secretariat.

Membership information and operational procedures are available on-line from the NIST Computer Security Resource Center BBS or via the Internet using ftp; refer to Appendix A for details. More information about FIRST can be obtained by contacting any participating member or the National Institute of Standards and Technology at the following address:

National Institute of Standards and Technology
Computer Security and Management Group
A-216, Technology
Gaithersburg, MD 20899
Telephone: (301) 975-3359
Facsimile: (301) 590-0932
Internet e-mail: *csrc@csrc.ncsl.nist.gov*