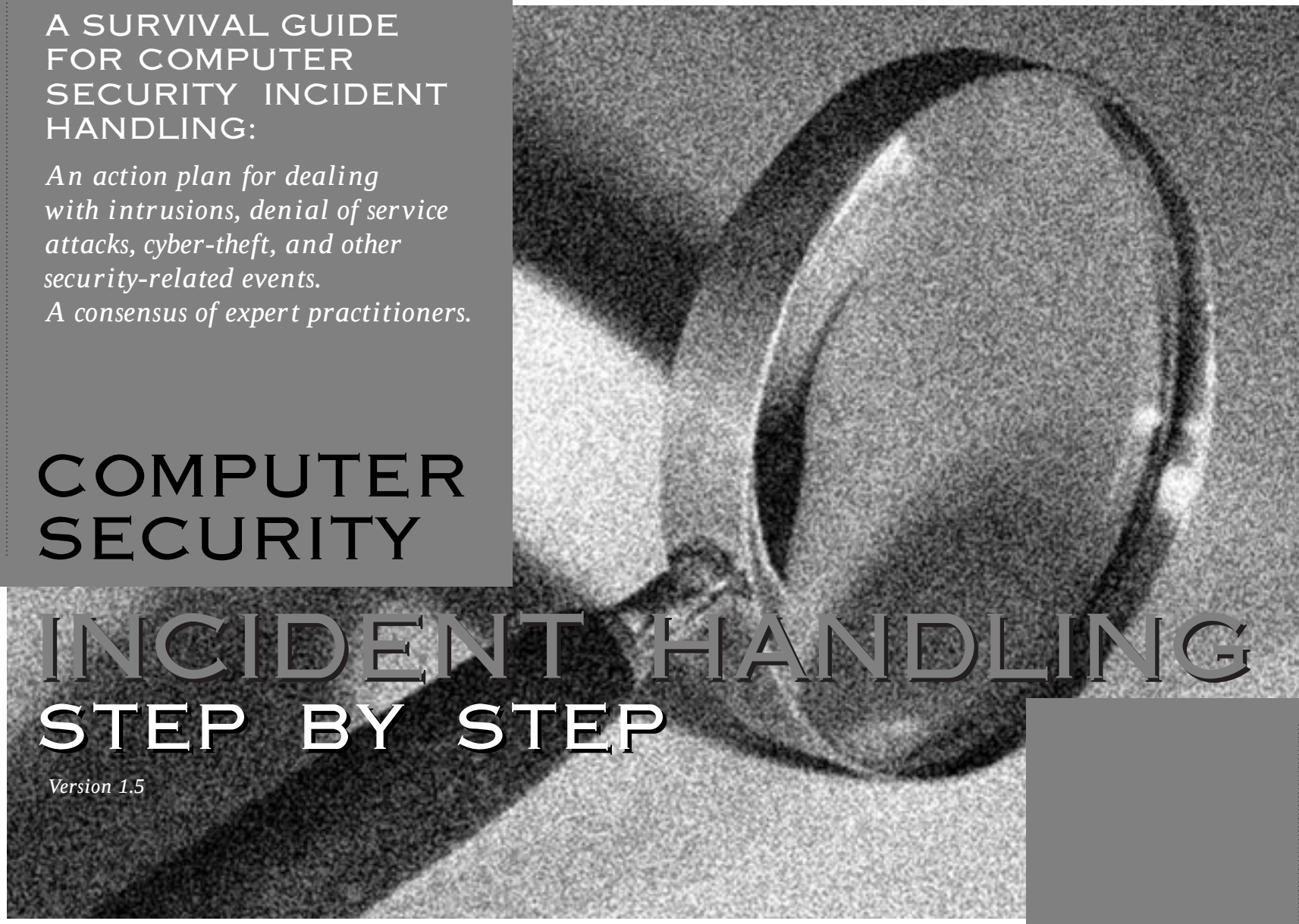
A SURVIVAL GUIDE FOR COMPUTER SECURITY INCIDENT HANDLING:

*An action plan for dealing with intrusions, denial of service attacks, cyber-theft, and other security-related events.*
*A consensus of expert practitioners.*

# COMPUTER SECURITY INCIDENT HANDLING STEP BY STEP

*Version 1.5*



THE SANS INSTITUTE

THE SANS INSTITUTE

# COMPUTER SECURITY INCIDENT HANDLING STEP BY STEP

Version 1.5
May 1998



## A SURVIVAL GUIDE FOR COMPUTER SECURITY INCIDENT HANDLING:

***An action plan for dealing with intrusions, denial of service attacks, cyber-theft, and other security-related events. A consensus of expert practitioners.***

Stephen Northcutt
Naval Surface Warfare Center and Director of the
SANS Incident Handling Research Program

*This document is the joint product of computer security professionals from corporations, government agencies, and educational institutions. They carry battle scars from more incident handling experiences than many would like to remember.*

*The SANS Institute enthusiastically applauds the work of these professionals and their willingness to share the lessons they have learned and the techniques they use.*

AusCERT, The Australian Computer Emergency Response Team
Bryce Alexander, The Vanguard Group
S. Dirk Anderson, Frontier ConferTech
Connie Balodimos, BankBoston
Larry Bassett, FORE Systems Inc.
Sean Boran, Boran Consulting
Peter Brantley, University of California, San Francisco
John J. Brassil, Vanderbilt University
Chris Calabrese, BFR Systems
Rob Marchand, Array Systems Computing
Randy Marchany, Virginia Tech University
Brian Martin, RepSec
John Mason, Hughes Aircraft Employees Federal Credit Union
Chris Mc Donald, White Sands Missile Range
James H. Moore, Xerox Corporation
Kathleen M. Moriarty, FactSet Research Systems
Stephen Northcutt, Naval Surface Warface Center
Kathleen M. Padgett, Los Alamos National Laboratory

Laura Carriere, Raytheon STX
Jeff Davis, Lucent Technologies
George Dimitoglou, Space Applications Corporation
Dennis J. Duval, Epic USA
Nicki A. Eger, US Department of Defense
Andy Feldt, University of Oklahoma
Robert G. Ferrell, US Geological Survey
David Goldberg, The MITRE Corporation
Michael Gregorio, The Coca-Cola Company
David Grisham, University of Arizona
Tom Gutnick, Data General Corporation
Theresa Ho, Lucent Technologies
Kent Landfield, Network Flight Recorder
James Kane III, Information Network of Arkansas
Yaron Keshet, P.S. Publishing
William J. Maciura, Tec Voc High School
Eric Maiwald, Fortrex Technologies
Jeffrey E. Man, Nichols Research Corporation
A. Padgett Peterson, Lockheed-Martin Corporation
Dennis Poindexter, US Ballistic Missile Defense Organization
Ralph A. Rodriguez, Treacy & Company
Ben Schmitz, Fastparts
Dr. Eugene Schultz, Intergity Solutions International
Michael T Shinn, Cisco Systems
Andres J. Silva III, Ameritech
Donald J. Smith, General Dynamics
John C. Smith, Prevention and Recovery Solutions
Sandy Sparks, CIAC, The Computer Incident Advisory Capability of the US Department of Energy
Aurobindo Sundaram, Schlumberger
Saul Tannenbaum, Tufts University
Aron Thomas, Pacific Gas & Electric
Scott A. West, American Express
Paul G. Williams, United States Air Force
Nigel Willson, Disney Online
Laurie Zirkle, Virginia Tech

*Many of the ideas of this document are based on Navy Staff Office Publication 5239-19 Computer Incident Response Guidebook*

# PREFACE

One of the great sources of productivity and effectiveness in the community of computer professionals is the willingness of active practitioners to take time from their busy days and evenings to share some of the lessons they have learned and the techniques they have perfected. Much of the sharing takes place through online news groups, through web postings, and through presentations at technical meetings. Those who are able to take the time to scan the newsgroups, surf the web, and attend the meetings often gain measurably from those interactions.

SANS' Step-by-Step series raises information sharing to a new level in which experts share techniques they have found to be effective. They integrate the techniques into a step-by-step plan and then subject the plan, in detail, to the close scrutiny of other experts. The process continues until consensus is reached. This is a difficult undertaking. A large number of people spend a great deal of time making sure the information is useful and correct.

Computer Security Incident Handling: Step-by-Step is our second SANS consensus research report. We hope you find it of value in your work, and we look forward to your suggestions for improvements.

## A WORD FROM THE PROGRAM DIRECTOR

Incident Handling is similar to first aid.

The caregiver tends to be under pressure and mistakes can be very costly. A simple, well-understood approach is best. This is why even the most experienced incident handling experts follow well-defined and systematic procedures for responding to security-related incidents. They keep the six stages, (preparation, detection, containment, eradication, recovery, and follow-up) in mind; they use pre-designed forms, and they call on others for help.

Few individuals have sufficient incident handling experience to provide guidance for all types of incidents and for all types of organizations. That is why I am so pleased to have helped make this guide possible. The guide reflects the experience of incident handlers from more than fifty organizations: commercial, government, and educational. In addition, two of the most respected incident handling organizations (AusCERT and CIAC), brought their cumulative experience to the effort.

Please use this guide as a starting point to create a set of incident handling procedures tailored to your corporate environment. As you work through the preparation tasks, ask yourself, "If an incident occurred, would I be really thankful if I had done that?" and in the response sections ask, "Would I be really sorry if I hadn't done that?"

If you are in a very small organization, implement the parts of this guide that are feasible for your staff level. Whatever size organization you are in, please let us know of errors or omissions. We'll be updating and reissuing the guide periodically. Email us at ih@sans.org with any suggestions.

When an incident occurs, don't hurry!

I still remember responding to my first alert after earning my Emergency Medical Technician (EMT) certification. My pager went off and I was flying. I zoomed right by this old geezer, who happened to be an assistant fire chief and paramedic with decades of experience. He reached out with a meaty hand and stopped me in my tracks. "Slow down", he said in a gruff voice. "Even if you don't hurt yourself or someone else running like that, when you get there you won't be any good to anyone panting and wheezing". A decade and a half later, I am the old geezer and I want to pass the same advice on to you. Especially with your first few incidents, slow down. Take time to take notes. Take notice of every person in the room. Be as kind as you can under difficult circumstances.

Finally, if your corporate policy will allow it, share what you have learned with other incident handlers and CIRT (computer incident response team) teams. Attacks against computers are happening everywhere, all the time. Even world-class response is of little value if conducted in isolation. Coordinating your efforts with those of other teams is a critical facet of incident response. Do as they told you to do in kindergarten: Share.

*Stephen Northcutt, Naval Surface Warfare Center Dahlgren Division*

COMPUTER SECURITY

# INCIDENT HANDLING

S T E P B Y S T E P

## CONTENTS

# THE EMERGENCY ACTION CARD

## EMERGENCY STEPS

When a computer security incident occurs,
and you are not prepared, follow these ten steps:

Emergency Step 1. Remain calm. Even a fairly mild incident tends to raise everyone's stress level. Communication and coordination become difficult. Your calm can help others avoid making critical errors. Besides, a lot of apparent incidents may not be what they appear to be.

Emergency Step 2. Take good notes. Use the forms in the back of this guide. Start with the one titled "Incident Identification." Then work your way through the others that are relevant. As you complete the forms, keep in mind that your notes may become evidence in court. Make sure you answer the four W's: Who, What, When, Where, and, for extra credit, How and Why. You may find a small hand-held tape recorder to be a valuable tool.

Emergency Step 3. Notify the right people and get help. Begin by notifying your security coordinator and your manager. Ask that a co-worker be assigned to help coordinate the incident handling process. Get a copy of the corporate phonebook and keep it with you. Ask your helper to keep careful notes on each person with whom he or she has spoken and what was said. Make sure you do the same.

Emergency Step 4. Enforce a "need to know" policy. Tell the details of the incident to the minimum number of people possible. Remind them, where appropriate, that they are trusted individuals and that your organization is counting on their discretion. Avoid speculation except when it is required to decide what to do. Too often, the initial information in an incident is misinterpreted and the "working theory" has to be scrapped.

Emergency Step 5. Use out-of-band communications. If the computers have been compromised, avoid using them for incident handling discussions. Use telephones and faxes instead. Do not send information about the incident by electronic mail, talk, chat, or news; the information may be intercepted by the attacker and used to worsen the situation. When computers are being used, encrypt all incident handling e-mail.

Emergency Step 6. Contain the problem. Take the necessary steps to keep the problem from getting worse. Usually that means removing the system from the network, though management may decide to keep the connections open in an effort to catch an intruder.

Emergency Step 7. Make a backup of the affected system(s) as soon as you think an incident has occurred. Use new, unused media. If possible, make a binary, or bit-by-bit backup.

Emergency Step 8. Get rid of the problem. Identify what went wrong if you can. Take steps to correct the deficiencies that allowed the problem to occur.

Emergency Step 9. Get back in business. After checking your backups to ensure they are not compromised, restore your system from backups and monitor the system closely to determine whether it can resume its tasks. Learn from this experience, so you won't get caught unprepared the next time an incident occurs. This guide, "Incident Handling: Step-by-Step," is designed to help you by providing a systematic approach to incident handling.



Version 1.5 Latest updates: ih@sans.org

# PHASE 1
## PREPARATION

*Experienced incident handling professionals divide the process into six phases: preparation, identification, containment, eradication, recovery and follow-up. Understanding these stages, and what can go wrong in each, facilitates responding more methodically and avoids duplication of effort.*

### STEP 1.1.

Establish policy and post warning banners

*Problem:* *In the heat of the moment, when an incident has been discovered, decision-making may be haphazard. By establishing policies, procedures, and agreements in advance, you minimize the chance of making catastrophic mistakes.*

■ Action 1.1.1 Post warning banners.

From a legal perspective this is one of the most important steps you can take to prepare for an incident. Every corporate system should display an approved warning banner visible to all users who attempt to login to the system. The banner should state that the system is the property of your organization, is subject to monitoring, that users should not have an expectation of privacy, and that unauthorized use or access is prohibited. Your corporate legal counsel should review your banner. The banner should not reveal either the operating system or the purpose of the machine.

■ Action 1.1.2 Use proactive techniques to prevent incidents.

The best way to "handle" an incident is to stop it from happening in the first place. To do that, you'll need to establish a security policy, monitor and analyze the network traffic, assess vulnerabilities, configure your systems wisely, install updates regularly, and establish training programs. All these actions are designed to make it difficult for intruders to access or harm your systems. The SANS Institute publishes and updates Step-by-Step guides for proactive security for various operating systems. The "Windows NT Security: Step-by-Step" guide was published in March of 1998 (see www.sans.org for information on ordering this guide.)

■ Action 1.1.3 Establish a policy on presumption of privacy.

Your organization needs to decide on a policy of presumption of privacy and be willing to enforce that policy. The policy should answer questions such as whether the electronic mail stored on a corporate file server is the property of the organization, or of each individual user of the system. The policy should also establish when encryption is allowed and under what circumstances it is required. The encryption section should tell who keeps the keys so that disgruntled employees cannot easily encrypt information and then leave.

# PHASE 1
## PREPARATION
### STEP 1.3.

■ Action 1.1.4 Establish an organizational approach to incident handling.

When an incident is discovered, you will choose between two approaches to incident handling. The first, and generally simplest, is to "contain, clean and deny access." The focus in this approach is to eradicate the problem as quickly as possible and get back into business. The second, requiring more technical skill and planning, is to "monitor and gather information." Here you allow the intruder to continue the attack, perhaps with subtle restrictions that minimize further damage. Often, the decision between the two approaches rests on whether you intend to prosecute the intruder. The simpler "contain, clean, and deny access" may not provide evidence needed to identify and prosecute the criminal.

When the "contain, clean and deny access" approach is selected, an organization will use a range of techniques, such as denying access to "bad IP addresses," further restricting services using a firewall or router filter, or just disconnecting the target system(s) from the network. Both approaches have advantages and disadvantages. It is best to determine your policy in advance of a serious incident.

■ Action 1.1.5 Establish a policy for outside "peer" notification.

A rapidly growing class of computer security incidents involves network-based denial-of-service attacks that spoof (impersonate) addresses in such a way that a person outside your organization can cause your computers to attack another organization. Your organization should develop a policy stating whom to inform, when to inform, and how to inform outside organizations that your computing resources are being used to assault these outside agencies.

It is good practice to be at least as responsive to incidents in which your organization is the source of the problem as you are when you are attacked. In these modern incidents, your organization can be made to appear to be the source of an attack when it is not. Write procedures that incorporate communication with the originating sites and the target sites.

■ Action 1.1.6 Establish a policy for dealing with incidents involving remote computers belonging to you or to your employees and those involving contractors and other non full-time employees.

As more employees routinely work at home or on the road, more security incidents will affect the remote systems or be initiated by remote systems. Establish a policy concerning search and seizure of such systems. Include consultants, temporary employees, and sub contractors. Be sure your organization's Acceptable Use Policies include home computers and portable computers. Establish a system through which you routinely record every outside person, such as a consultant, who is given access to systems and information. The records should detail the access that was granted. And as part of that policy, establish guidelines and mechanisms to remove their access when required. Where possible, make security guidelines mandatory in contracts with all outside vendors, contractors and consultants.

■ Action 1.1.7 Establish extranet (partnernet) agreements and monitoring.

Where feasible, establish agreements with all outside organizations connected to your network. These agreements should give your organization the right to disconnect and monitor as needed.

## FOR SMALL ORGANIZATIONS:

Few small organizations can afford to implement all of the suggestions in this booklet. If you must choose, implement the most common recommendations from incident handlers who reviewed this document. These recommendations are listed below:

- Warning Banners: make sure you have them.
- Have employees, consultants, contractors, sign an acceptable use policy yearly.
- Ensure systems are properly secured. If connected to the internet, ensure you have network monitoring.
- Use free internet resources such as those listed in the Resources Section (page 36) at the end of this guide.
- Back up systems regularly.
- When recovering using backups, be careful not to reintroduce the problem.
- Write a summary of what happened, what you did, and what you learned, so the lessons may be passed on.



## STEP 1.2.

Develop management support for an incident handling capability

*Problem:* *Until you have management buy-in, you'll find it hard to get time, money, and political support for your incident handling activities.*

■ Action 1.2.1 Collect news articles and other publications describing computer break-ins, weather incidents and other events that affected a group's ability to compete, especially in organizations similar to yours.

Keep relevant articles in a folder. Add printed copies of some of the famous break-ins such as the one at the Department of Justice. The CIO Institute (www.cio.org) produced a particularly effective description of this incident. It tells the story of Dr. Mark Boster, the Deputy Assistant Attorney General for Information Systems, who was responsible for the Justice Department systems that were attacked, and the lessons he and his team learned. One useful lesson was that he needed to increase the number of people assigned to monitor and manage security.

Articles and management-level booklets can help you get management's attention. Whenever you attend an in-house meeting related to the incident handling team, carry the folder with you. Then you have the relevant articles right at hand.

■ Action 1.2.2 Graphically illustrate an incident.

Take the time to illustrate one or two of the incidents in your folder. Create a chart showing where the attackers came from, the vulnerabilities they used to get in, and what they were able to access. Help your organization's decision makers understand the consequences if the incident had not been detected. This action can empower your management because once they understand an incident, and can explain it to their peers, they often become supporters.

■ Action 1.2.3 Collect historical support.

Keep the Executive Summaries from previous incidents in the folder. Include information related to the cost of incidents (reputation, downtime, paying people to wait while systems are recovered), or the money that was saved by rapid and professional response.

# PHASE 1
## PREPARATION

### STEP 1.3.

Select incident handling team members and organize the team

*Problem:* *Incident handling isn't a one-person job. Having the right people in the right place with the right preparation can make all the difference.*

■ Action 1.3.1 Identify qualified people to join the team.

Write down the names that occur to you with their contact information. Talk to your co-workers and management about forming a local incident handling capability. Select a team that includes more than system administrators with security responsibilities. Include trained management personnel from your organization to help get the hard decisions made about whether to shut down core business systems in order to preserve your organization from even greater harm.

■ Action 1.3.2 Choose local, centralized, or combination teams.

Your team will have two parts: a Command Decision Team to coordinate activities, and an On Site Incident Handling Team. In some cases these may be the same people; in others they are different.

The On Site Team goes to the location(s) of the incident. They secure the area, survey the situation and begin containment, eradication and recovery.

The Command Decision Team translates the technically oriented assessments of the On Site Team into the recovery steps management directs the organization to take. They work with the organization's public affairs and legal staff if information needs to be provided to outside organizations or the public. They are also responsible for keeping senior corporate management advised of the status of the incident, as appropriate.

Quick action requires that you decide, in advance, what organizations and functions will be represented on both of those teams. Start the planning process by considering what would happen if your organization needed to handle multiple concurrent incidents. In a multiple incident situation, the experienced handlers need to triage the situation and assign less trained personnel to some of the incidents. In such situation, reliance on local support is often required. One corporation uses a staged response and responds from the corporate level only if multiple corporate sites are being affected or if the incident involves a new type of attack. Alternatively, for organizations with multiple sites, the team could be drawn from representatives from each site. Very large organizations that try to handle all incidents with a core team at a single facility sometimes find that travel time lowers their ability to respond quickly.

PHASE 1
PREPARATION

STEP 1.3.

■ Action 1.3.3 Identify the correct individuals in your organization's Public Affairs Office (PAO).

The PAO team is responsible for answering questions from the public regarding corporate activities. When a security-related incident occurs, it is also the PAO's responsibility to disseminate appropriate information to the public. Your public affairs team may also be valuable support for incident handling. They usually have very good access to senior management and can help coordinate communications between the team and senior executives.
NOTE: Dealing directly with the press can be hazardous to your career. There is always a risk of being misquoted, taken out of context, or of releasing information that is sensitive or even harmful to your organization. All press interaction should take place through the PAO with the help of management and the Incident Response team.

■ Action 1.3.4 Update your organization's disaster recovery plan to include computer incident handling.

Certain critical business systems may have requirements for hot spare systems and / or back-up sites. Ensure your organization's disaster recovery plan includes 24-hour contact information for the team for large-scale incidents.

■ Action 1.3.5 Establish visibility and a compensation plan for the team.

Incident handlers and the system administrators they count on for support often have to put in extraordinary time and effort in responding to an incident. Negotiate with management, in advance, to provide mechanisms for recognition and compensation.

■ Action 1.3.6 Provide checklists.

Checklists for incident handling procedures help every member of the team avoid errors and take the right steps toward resolution.

# PHASE 1
## PREPARATION

### STEP 1.4.

Develop an emergency communications plan

*Problem:* *Maintaining communications and keeping the right people informed are well understood, essential tasks. However, when facing new, unexpected events, that are likely to occur during incidents, natural communication channels break down.*

■ Action 1.4.1 Create a call list and establish methods for informing people quickly.

Use the communications form in the back of this guide to record as many contacts and phone numbers as you can. Establish a locator for all system administrators and have contact information for every corporate system administrator and network person. Record work and home numbers for employees and numbers where they may be likely to be found if not at home when an emergency occurs. Record pager numbers and, if the pager can be reached via the web or email, record relevant broadcast information. Many organizations send out a short message (such as 911) letting people know to call a voice mailbox where they can receive a message detailing the status of the incident. This way incident handling resources are not wasted repeating the same message as people are getting up to speed.

■ Action 1.4.2 Create an incident notification call tree.

After an incident has been identified and the On Site Incident Handling Team has been dispatched to the location, a call tree can be used to contact many people in your organization. A call tree allows one call to a department in your organization to initiate calls to the rest of the key people in that department. You may already have such a tree as part of your organization's disaster recovery plan. If not, your organizational chart makes an excellent starting point. Test the call tree and call list at least once a year. Note: Direction to use the call tree should come from the Command Decision Team.

■ Action 1.4.3 Use offsite backup for call lists and call trees.

Keep copies of the call list and call tree at an offsite location, and make sure the incident team members know the location of this information. Experienced incident response professionals carry contact information with them at all times.

## STEP 1.4.

■ Action 1.4.4 Ensure passwords and encryption keys are up-to-date and accessible.

No matter how good your call lists are, some system administrators may not be available during a critical incident. Ensure that the passwords used to obtain superuser or administrator access to every system and LAN within your organization are recorded on paper, sealed in signed, well-labeled, envelopes which are kept in a large sealed envelope, and placed in locked containers that can be accessed by the handling team. Usually, this is done at a local, or department level. Establish procedures to ensure these passwords stay current. The same process is useful for storing encryption keys for critical information. Make sure your procedures include provisions for verifying the identity of the person who needs a password or encryption key during an emergency.

■ Action 1.4.5 Establish a primary point of contact and an incident command and communications center.

Effective coordination requires a single point of contact (POC). Otherwise no one knows who is in charge. For larger incidents, that person should be the leader of a Command Decision Team that establishes a communication and response center. The center should be a place with plenty of phone lines, voice mail boxes and fax machines. Some of these phone and fax lines should be outside lines, rather than lines routed through your organization's PBX. One reviewer, who worked on the response following the Northridge earthquake, suggests a portable generator, cellular phones, cellular modem jacks and lots of spare batteries to supplement land lines. The facility should also have hard copies of all incident procedures and contact information.

■ Action 1.4.6 (In highly critical sites) Establish secured communications.

In a major incident, it is possible that both the computer systems and the PBX might be penetrated. In such a situation, encrypted telephones (including encrypted cell phones) and fax systems might be the only way the team can maintain communications without the attacker knowing their every move. Available tools include PGP, secure web pages, and secure news groups for all team-to-team communications.

■ Action 1.4.7 Set up resource acquisition plans for the teams.

Both teams should have procedures for ordering food, lodging, software and other necessary resources for use during an incident. The On Site Team should maintain a response kit with backup software and hardware, boot diskettes for common operating systems, OS distribution media for common operating systems, blank floppies and portable printers.

# PHASE 1
## PREPARATION

### STEP 1.5.

Provide easy reporting facilities

*Problem:* *When users do not know whom to contact or what to say, they delay reporting information about possible security incidents. Most buildings have fire alarm systems that enable employees to report quickly and conveniently. Reporting computer security incidents should be nearly as easy as reporting a fire.*

■ Action 1.5.1 Educate users early.

New employee briefings and orientation provide an ideal opportunity to inform employees about the organization's incident handling procedures and contact process.

■ Action 1.5.2 Publish a list of indicators of an incident.

A list of indicators can assist your team and others in recognizing an incident when they see it. Examples of indicators to include: activity in previously idle accounts, unusual offsite access, new setuid root scripts, transfer of /etc/passwd in ftp and web logs, system crashes, unexplained filling of file systems, gaps in accounting logs, new or unfamiliar file names and similar anomalies. Work with your system administrators to establish a list of indicators that are suited to the mix of operating systems that your organization uses.

■ Action 1.5.3 Use the web.

Develop and maintain an Intranet Incident Web Page to help users locate your corporate computer incident handling team. Each department should have a printed copy of this information in case the network or web server is unavailable during the incident. You can also use the web page to help keep your organization informed of changes.

■ Action 1.5.4 Encourage email and/or phone reporting.

Establish a simple, easy-to-remember mail alias, such as incident@(yourcompany).com for users to report incidents. Several organizations have established toll free hotlines so users can report security incidents anonymously.

■ Action 1.5.5 Reward reporting.

One organization recognizes employees who identify incidents or odd events with a NAATS Award (Not Asleep At the Switch). Another organization publishes the picture of alert employees with a short description of how they detected the incident and how their alertness aided the organization. Still another organization uses a cash reward as an incentive to encourage reporting.

■ Action 1.5.6 Continually update management.

Keep management informed about threats, cost of incidents, security requirements, and similar information.

PHASE 1
PREPARATION

## STEP 1.6.

### Conduct training for team members

*Problem:* *When an incident handling team is not properly trained, the probability of making mistakes is fairly high. Also, the team learns to work together during training.*

■ Action 1.6.1 Set up a planning / training meeting on scenarios.

Plan and conduct a session for the incident handling team to discuss how to handle basic scenarios. Examples might include a virus epidemic, failed computer penetration attempt, successful computer penetration or the discovery of a significant volume of child pornography on a corporate computer. Determine how these would be handled. Decide whether resources outside the organization need to be involved? Follow up the mock scenarios with the lessons learned process (see the lessons learned materials on pages 24 and 35 for further information).

■ Action 1.6.2 Set up tools and techniques training.

Establish training for incident handling team members covering tools and techniques for backup, evidence collection, and analysis. Teach members how to use the tools to protect evidence. It is useful to ensure that the legal team reviews these tools in advance if you plan to use their output as evidence.

■ Action 1.6.3 Stock some high capacity drives

Because backups are one of the most important activities you will undertake, be prepared by having high-capacity disks, their instruction manuals, and a variety of cables and terminators ready. Practice using them on a variety of hardware configurations before you need to try this under pressure.

▲ Action 1.6.4 (Advanced) Conduct War Games

Run simulation sessions for system administrators and incident handling team members, where some of the members act as attackers and others as defenders. Don't restrict the war games to senior personnel. An entry-level system administrator is as likely to be involved in a large incident as a senior level administrator.

# PHASE 1
## PREPARATION

### STEP 1.7.

Establish guidelines for inter-departmental cooperation

*Problem:* *When an incident occurs, there is no shortage of people who want to help. If organizational roles and responsibilities are not worked out in advance, some of the helpers may make the problem worse.*

■ Action 1.7.1 Encourage local handling of minor incidents—but with care.

The organization's incident policy should define what incidents users and system administrators may handle and what reporting they should do. Technically adept users and local system administrators should be encouraged to handle minor incidents such as virus infections. However, most other users should be warned to call in technical help so they don't make a virus problem worse.

■ Action 1.7.2 Coordinate closely with help desks.

The first indication of a problem may be a user report to a help desk. Help desks can be an excellent early warning system and first line of defense for minor incidents such as virus infections affecting multiple machines. Many help desks have extended hours of service. Consider making the help desk part of the incident handling team, using them as your point of contact to report incidents.

Help desks are also a primary target for social engineering attacks. The classic attack is the phone call saying, "I have a very hot deadline to deliver the frammitz reports to the V.P. of OPS and well, durn, I forgot my password. Could you please give me a new one." If help desk staff are a part of your incident handling process, they will be aware of the types of attacks that are directed against your organization, and will be less likely to be vulnerable to social engineering.

■ Action 1.7.3 Report and record.

If a user suspects a serious incident, after reporting, policy should be to record what they have seen.

STEP 1.8.

## Pay particular attention to relationships with system administrators and network managers

*Problem:* *The system administrator is the individual most often responsible for operational security for a subset of machines at a site or facility. They have their fingers on the pulse of the computer systems. Alert system administrators have detected many incidents by noticing some event that is strange, and by reviewing a system's log files. On the other hand, system administrators have the potential to do great harm in an incident. With privileged accounts they can alert intruders that they have been detected, destroy evidence or even destroy system files in a frantic attempt to stop an intrusion.*

■ Action 1.8.1 Involve system administrators.

Invite system administrators from different sections to consult in the incident handling process. A fresh set of eyes brings the perspective needed to solve the problem in the most efficient manner.

■ Action 1.8.2 Conduct proactive training.

Offer workshops for system administrators on available software packages to help detect attacks and accomplish effective system monitoring. The most effective instructors are usually people who can relate first-hand experience in handling incidents and in using the tools.



■ Action 1.8.3 Recognize "power" log file reading.

The indicators of many never-detected incidents are buried in log files. It is not enough to collect system logs, it is important to also read them. System administrators who detect incidents should be recognized.

■ Action 1.8.4 Encourage regular system backups.

Inadequate backups have been the cause of many catastrophes in recovering from security incidents. Up-to-date, clean, bombproof backups are essential. Strongly encourage system administrators to keep their backups current and to verify that their tape drives are working correctly by testing the backups. In order to encourage backups of systems that may have fallen through the cracks, one organization sends a note to all employees during the first week of December suggesting that if they haven't ensured their systems were backed up that year now might be a good time.

■ Action 1.8.5 Involve network managers early.

Routers are the primary tools of network managers. Routers are also powerful resources to use while detecting, containing and reacting to an attack. Router logs can provide quick corroboration of system log entries. Router filter rules can be used to isolate subnets during the containment phase and to continue to log repeated attempts to access the subnet. The network management group that manages the routers should be involved in your incident handling activities from the beginning. Their roles will be especially important when attacks involve the all-too-frequent IP spoofing and forgery.

## PHASE 1
### PREPARATION

STEP 1.9.

**Develop interfaces to law enforcement agencies and other Computer Incident Response Teams (CIRTs)**

*Problem:* *When you need help in a hurry, you'll get it far more easily if you have established relationships in advance. Multiple law enforcement agencies may have overlapping responsibilities for computer incident handling. The challenge is determining how to find and contact the people who are knowledgeable about computer incidents?*

■ Action 1.9.1 Know the types of cases law enforcement will be interested in.

Law enforcement is primarily concerned with apprehending and prosecuting criminals. Law enforcement agencies care about the following areas: computer trespasses, theft, espionage, child pornography, hate crimes, threats, and stalking. On the other hand, these agencies may not be able to assist in the response. They may provide no more than a cursory investigation if the evidence has not been preserved, or if the case does not appear to be worth the investment in prosecution, (e.g., because the incident is extremely minor or the economic damage associated with it is too low.).

■ Action 1.9.2 Contact local law enforcement before there is an incident.

Now is the time to get to know your local law enforcement computer crime officers. They are often willing to provide computer crime awareness education to your organization and to meet with your management. They can also help you determine local, state, and national requirements for handling evidence. Get all the contact information you can: phone numbers, pager numbers, e-mail addresses and so forth. Include law enforcement contact information in your organization's site-specific incident handling guidelines. Relationships of any sort are an investment; in an incident these people could prove to be your organization's best friends. Some sites strongly recommend that a single person be named as the law-enforcement liaison.

■ Action 1.9.3 Arrange a law enforcement briefing on evidence collection.

Because computer logs are typically the only evidence of an attack, safekeeping these logs is critical if you decide to prosecute the offender. To educate sysadmins and network managers, ask your legal staff or local law enforcement agency to send someone to brief the staff on proper evidence collection. The sysadmin will usually know of an attack before the police are notified; proper training will prevent evidence collection mistakes.

■ Action 1.9.4 Join or create a CIRT or FIRST team.

If a Computer Incident Response Team, or coordinating entity for organizations like yours, exists, get to know the members and establish mechanisms for getting help when you need it. If you use PGP (Pretty Good Privacy) include your CIRT's public key on your key ring. Additional contact information may be found on page 36.

## A FEW WORDS ON PHASES TWO THROUGH SIX

*Nearly half of this guide has been devoted to Phase 1, the Preparation Phase. This makes sense because a team that is well prepared is in position to act quickly and effectively when a computer security incident occurs. The remaining steps are divided into five additional phases: Identification (Phase 2), Containment (Phase 3), Eradication (Phase 4), Recovery (Phase 5), and Follow-up (Phase 6).*

# PHASE 2
## IDENTIFICATION

*Identification involves determining whether or not an incident has occurred, and if one has occurred, determining the nature of the incident. Identification normally begins after someone has noticed an anomaly in a system or network. This phase also includes informing and soliciting help from the people who can help you understand and solve the problem.*

**!** Some experts believe that less than one percent of incidents are both detected and reported. To increase the chance of finding and responding to attacks, most organizations are turning to intrusion detection tools that identify and report potential attacks.

### STEP 2.1.

Assign a person to be responsible for the incident

*Problem:* *Without a central point of control too many people may be working at cross-purposes.*

■ Action 2.1.1 Select a person to handle or coordinate identification and assessment.

This person can be more effective if he or she has an enterprise-wide perspective.

### STEP 2.2.

Determine whether or not an event is actually an incident

*Problem:* *Apparent evidences of security incidents often turn out to indicate something less. If a situation is misdiagnosed it is often easy to make the data "fit" the misdiagnosis. It takes expertise to make an informed diagnosis. The analogy is that anyone can pull the red handle if they think there is a fire, but only the fire team can make the determination that the fire is contained and it is safe to re-enter the building, or to call for more fire-fighting equipment.*

■ Action 2.2.1 Check for simple mistakes.

Examples of simple mistakes include errors in system configuration or an application program, hardware failures, and, most commonly, user or system administrator errors. A seasoned incident handling professional, who has seen many cases, can often make the determination with just a few questions of the local system administration staff.

■ Action 2.2.2 Assess the evidence in detail.

Use the list of indicators developed in Phase 1, Step 1.5 to quickly assess the possible type of incident.

# PHASE 2
## IDENTIFICATION

### STEP 2.3.

Be careful to maintain a provable chain of custody

*Problem:* *The events that you see and the evidence you collect may be excellent. But they won't be worth much in a courtroom unless you can prove six months later that these are the exact events that happened and the same evidence you collected during the incident.*

■ Action 2.3.1 Get your lawyers involved.
Your lawyers can help ensure evidence is handled correctly. The lawyers may recommend an increasingly common practice of videotaping the archival of evidence such as log files from victims' systems.

■ Action 2.3.2 Identify every piece of evidence.
Number, date and sign notes and printouts. Seal disks with original, unaltered, complete logs in an envelope or other container; then number, date and sign the container. When you turn evidence over to the appropriate person in your organization have the recipient sign for each item. If evidence is turned over to law enforcement ensure every item turned over is detailed and signed for.

■ Action 2.3.3 Control access to evidence.
Ensure that you can prove who has access to the secure container used to store the evidence and that this is a very small group of people. If there is a key lock, each key should be stamped *do not duplicate*. Make sure, by policy and practice, that each person with access understands they are required to control access to these items.

### STEP 2.4.

Coordinate with the people who provide your network services

*Problem:* *Many incidents are caused by intruders installing sniffer software on a computer system and collecting passwords and login Ids from the network. If the sniffer is installed on one of your ISP's systems you will continue to have problems.*

■ Action 2.4.1 Coordinate closely with your Internet Service Provider.
Inform your ISP of your initial evidence or opinion and ask the ISP to assist in the investigation.

### STEP 2.5.

Notify appropriate officials

*Problem:* *Computer incidents, fires, and medical emergencies are usually a lot easier to handle when reported promptly. If you saw a co-worker in the cafeteria collapse, you probably wouldn't wait until the next day to alert the emergency medical system.*

■ Action 2.5.1 Notify your manager and security officer.

■ Action 2.5.2 Notify your local or organizational incident handling team. However, be extremely careful and discrete—especially in commercial organizations where public relations damage may be the greatest cost of a successful attack.

■ Action 2.5.2

# PHASE 3
## CONTAINMENT

*The goal of the containment phase is to limit the scope and magnitude of an incident, to keep the incident from getting worse.*

### STEP 3.1.

Deploy the on-site team to survey the situation

*Problem:* *If data is not gathered quickly and accurately, it may never be gathered.*

- Action 3.1.1 Deploy a small team.

  Four or five people are the limit for an On Site Team at one location. If this incident should ever go to court everyone who stays in the area is a potential witness.

- Action 3.1.2 Secure the area if possible.

- Action 3.1.3 Use the survey forms provided in this guide, or answer the same questions in your notebook.

- Action 3.1.4 Review the information that was provided to you from the identification phase.

  Be very careful to check any conclusions others have reached.

- Action 3.1.5 Keep the system(s) pristine.

  Do not allow the system to be altered in any way until the backup is completed.

### STEP 3.2.

Keep a low profile

*Problem:* *If a network based attack is determined, be careful not to tip off the attacker.*

- Action 3.2.1 Avoid looking for the attacker with obvious methods.

  A classic rookie error is to ping, nslookup, finger, telnet to, or in some other way, make contact with the suspected source of the attack (hours later). If your adversaries detect you trying to locate them, they may delete your file systems and break off the connection (for a while anyway) in an effort to cover their tracks.

- Action 3.2.2 Maintain standard procedures.

  If your site is protected by active intrusion detection systems that break connections and block attacking IP addresses, do not disable these systems to try to gather more data. This would create a change in your profile that might warn the attacker.

- Action 3.2.3 Consider planting “treasures” or “honey pots.”

  Some experts recommend planting valuable information that may lure an attacker to take actions that will lead to apprehension.

# PHASE 3
## CONTAINMENT

### STEP 3.3.

Avoid, if possible, potentially compromised code

*Problem:* *Intruders may install trojan horses and similar malicious code in system binaries.*

■ Action 3.3.1 Be wary of compromised system binaries.

It is not advisable to log in to a system, suspected of being compromised, as "root" or "administrator" and then start typing commands. For example, avoid using ftp to download tools from another site. If possible, record the fingerprint of critical binaries for the organization's core operating systems. Some experienced incident handlers recommend building disks with core binaries. In any case, one binary you want to be particularly concerned about at this moment in an incident is the system's backup program.

### STEP 3.4.

Backup the system

*Problem:* *Perpetrators of computer crime are becoming increasingly proficient in destroying evidence of illegal activity. Therefore it is extremely important to obtain a full backup of the system in which suspicious events have been observed.*

■ Action 3.4.1 Backup to new (unused) media.

Do your backup as soon as there are indications that a security-related incident has occurred. And use new media because juries may be convinced that the "evidence is faulty" if it is written over old information. Making a full backup immediately captures evidence that may be destroyed before you and others have a chance to look at it. If possible make two backups, one to keep sealed as evidence and one to use as a source of additional backups. The backup will, in addition, provide a basis for comparison later in case you need to determine if any additional unauthorized activity has occurred. Disk to disk backup is often the fastest method.

■ Action 3.4.2 Safely store any backup tapes so that they will not be lost or stolen.

Tape protection is an important part of the chain of custody of critical information. If tapes are unprotected, the entire legal case could be damaged.

STEP 3.5.

Determine the risk of continuing operations

*Problem:* *One of the most difficult decisions, and one subject to extreme pressure by end-users and senior management, is what to do about the compromised system. Here you will decide whether a system should be shut down entirely, disconnected from the network, or be allowed to continue to run in its normal operational status so that any activity on the system can be monitored.*

■ Action 3.5.1 Acquire router and systyem logs and other sources of information.

Many log files turn over fairly quickly so it is important to acquire network and computer logs immediately. Use the logs to determine whether an attack is external or internal. If external, consider isolating the organization's network from the internet by breaking the connection at the firewall. If the attack is internal, consider isolating the affected subnet at the router level.

■ Action 3.5.2 Review logs from neighboring systems.

Review logs and file signature databases from other systems on the same subnet and from other systems that regularly connect to the affected system(s), especially if there is a trust relationship.

■ Action 3.5.3 Make a recommendation about when and whether to restart operations.

The On Site Team provides a recommendation to the Command Post Team who will make the decision on what to do.

PHASE 3
CONTAINMENT

STEP 3.6.

Continue to consult with system owners

*Problem:* *System owners stress levels can be very high, because their business may stop during the review process, and very large amounts of money may be lost.*

■ Action 3.6.1 Keep system owners and administrators briefed on progress.

The users of the affected system almost invariably really need the system, usually for an important project that is due that day. There is also a tendency for the system administrator, or manager responsible for the system to internalize the incident. They sometimes feel that since they operate the affected computer, the situation is their fault and they become defensive. Keeping them informed and aware of progress can help lower the stress level.

■ Action 3.6.2 Never allow fault to be an issue during incident handling.

As you work to contain an incident, try to take time to give your co-workers a smile, a pat on the back, mention the things that are being done right.

# PHASE 3
## CONTAINMENT

### STEP 3.7.

Change passwords

*Problem:* *A common target of intruders is root or administrator account names and passwords.*

- Action 3.7.1 Change the password on the affected systems.

  Passwords should be changed on compromised systems and on all systems that regularly interact with the compromised systems.

- Action 3.7.2 If a sniffer is detected or suspected, expand the password change order.

  If a sniffer attack is expected, passwords may have been compromised on all systems on the affected LAN or subnet. If a large system such as a POP mail server is compromised and the organization wants to keep rumors and questions to a minimum, it may be advisable to explain the password change as part of a system upgrade or as the routine recommendation of an external security auditor. Be clear that it is important that users change to a unique password that is not being used on any other computer system.

*The goal of the eradication phase is to make sure the problem is eliminated and the avenue of entry is closed off. When a system is compromised or put out of service, the compromise is usually seen as a problem of the system owner. If the problem comes back, the responsibility falls on the incident handling team.*

# PHASE 4
## ERADICATION

### STEP 4.1.

Determine cause and symptoms of the incident

*Problem:* *You cannot fix a problem if you don't know what happened.*

■ Action 4.1.1 Try to isolate the attack and determine how it was executed

This process uses information gathered during the survey phase and may require collecting additional information. Sometimes due to insufficient evidence, the exact mechanism used in the attack can not be determined. If you cannot find a single attack method, list and rank the possibilities.

### STEP 4.2.

Improve defenses

*Problem:* *After a system is compromised, its password file and identity may get advertised so that for weeks following the incident the system may be subjected to repeated attacks or probes.*

■ Action 4.2.1 Implement appropriate protection techniques such as firewalls and / or router filters, moving the system to a new name / IP address, or in extreme cases, porting the machine's function to a more secure operating system.

### STEP 4.3.

Perform vulnerability analysis

*Problem:* *Though prudence dictates that all sites that care about security perform regular vulnerability analyses of their systems and networks, many do not. When the latter experience a security incident, however, they usually act quickly to look for additional vulnerabilities.*

■ Action 4.3.1 Perform system vulnerability analysis.

Use a system vulnerability tool to determine whether configuration and software versions at your site need to be updated. Either acquire a vulnerability analysis tool or hire a security consultant who brings one along.

■ Action 4.3.2 Perform network vulnerability analysis.

Use a network vulnerability analysis tool to scan for vulnerable systems that are connected to your system. Again, either acquire a vulnerability analysis tool or hire a security consultant who brings one along.

■ Action 4.3.3 Search for related vulnerabilities.

If a particular operating system vulnerability is being exploited, check all other systems in your organization to see whether they also have that vulnerability.

# PHASE 4
## ERADICATION

### STEP 4.4.

Remove the cause of the incident

*Problem:* *Deciding what to do to remove the cause of an incident is often a great challenge. The actions below provide high-level guidance. Additional guidance for each of the common types of attack is offered in the section entitled Special Actions for Responding to Various Types of Incidents, beginning on page 25.*

- Action 4.4.1 For virus infestations:

  Virus eradication simply requires removing the virus from all systems and media, (e.g., floppy disks), usually with virus eradication software.

- Action 4.4.2 For network intrusion:

  Network intrusion eradication is more difficult. Many attacks over a network are in two parts. First there is an initial phase where system vulnerability is exploited and the system is accessed. Once in, the intruder often installs a tool (back door) to provide continued access. The intruder may also set up shop on the compromised system to use it for further intrusions. For instance, intruders may launch an exploit script against other computers from your organization's compromised computer. Intruders also often install sniffers to collect additional passwords and user ID's. Your team's job—often it's most difficult job—is to search for all such programs and remove them.

- Action 4.4.3 If the attacker discovers your efforts:

  Sometimes the attackers will detect your eradication efforts and attempt to maintain control of your system. This is an ideal situation in which to call in law enforcement support. Continue in your efforts to remove the attacker code from your system. Do everything possible to get network/phone logs of the attack. Trace the attack back one hop and, if corporate policy allows, contact that organization and try to get their logs as well.

### STEP 4.5.

Locate the most recent clean backup

*Problem:* *In the next phase you'll restore the system to operation al status. First, however, you must locate a backup that is not infected and that is current.*

- Action 4.5.1 Search for a very recent backup before an intrusion.

- Action 4.5.2 In case of a root-kit style attack, don't use back ups.

  If there is evidence of a root-kit style attack, it may be better to avoid the backups. Instead, reformat the disk, rebuild the operating system, (without the vulnerability), and reload the applications and data.

*In the Recovery Phase, your task is to return the system to a fully operational status.*

# PHASE 5
## RECOVERY

### STEP 5.1.

Restore the system

- Action 5.1.1 Restore from backups if required.
  Some incidents, such as malicious code, may require a complete restoration of operation from backups. In this case, it is essential to first determine the integrity of the backup itself. In general, the idea is to restore from the most recent backup made before the system was compromised.
- Action 5.1.2 Make every effort to ensure you are not restoring compromised code.
- Action 5.1.3 If no backups have been made prior to compromise, you may have to reload the system and apply patches, or to obtain and use a backup from a similar system that has not been compromised.

### STEP 5.2.

Validate the system

*Problem:* *Management and users want to know whether the problem has actually been eradicated and that their system has been fully restored.*

- Action 5.2.1 Once the system has been restored, verify that the operation was successful and the system is back to its normal condition.

  Ideally there is a system test plan to evaluate the system against. More commonly, the system is run through its normal tasks while being closely monitored by a combination of techniques such as network loggers and system log files. Sometimes the patches, or techniques used to prevent a vulnerability will cause the system to function differently than it did, before the event.

### STEP 5.3.

Decide when to restore operations

*Problem:* *Uncertainty about whether all malicious code has been removed can cause long delays.*

- Action 5.3.1 Put the final decision in the hands of the system owners.

  We suggest that the management of an affected system and their system administrators make these decisions. Quite often, they may wish to leave the system offline for a couple days to do an operating system upgrade or even to install patches!

### STEP 5.4.

Monitor the systems

*Problem:* *Back doors and other malicious code can be very well hidden.*

- Action 5.4.1 Once the system is back on line continue to monitor for back doors that escaped detection.

# PHASE 6
## FOLLOW-UP

*In Phase 6, the goal is to identify lessons that will help you do a better job in the future. Some incidents require considerable time and effort. Stress levels rise and relationships may become strained. Afterwards, the folks who were at the center of the storm tend to want to forget it and get on with their lives. Performing follow-up activity is, however, one of the most critical activities in responding to incidents. This procedure, only slightly more popular than wisdom tooth removal, is known as "lessons learned". Organizations that follow up soon after any problems are contained improve their incident handling capability. Quick follow up will also support any efforts to prosecute those who have broken the law.*

### STEP 6.1.

Develop a Follow-Up Report

*Problem:* *Experience must be captured quickly. A Follow-up report, including lessons learned, is the accepted method of protecting the knowledge so it can be used in the future.*

- Action 6.1.1 Start as soon as possible.
  Folks who wait until weeks after the dust has settled learn that human memory, unlike fine wine, does not improve with the passage of time.
- Action 6.1.2 Assign the task to the On Site Team.
  In order to make the lessons learned section as positive and effective as possible, most sites require the incident handling team to draft the lessons learned report as an integral part of their handling of the incident. The job's not finished until the paperwork is done.
- Action 6.1.3 Include forms from this guide.
  The incident report is generally an electronic version of the identification, survey, containment and eradication forms. Ask the people preparing the report to focus especially on answering the questions on the Lessons Learned questions list on page 36.
- Action 6.1.4 Encourage all affected parties to review the draft
  Submit the Lessons Learned along with the draft incident report for review by all affected parties.
- Action 6.1.5 Attempt to reach consensus.
  Gather responses, disagreements, additions, and suggestions from all the interested parties. Encourage them to submit their responses electronically so they will do so quickly. Retain their comments as part of the record.
- Action 6.1.6 Conduct a Lessons Learned meeting.
  Because you have collected comments from all parties, and distributed them in advance, you can generally plan for a one hour Lessons Learned meeting. Focus the meeting on recounting the incident and ratifying any process changes.
- Action 6.1.7 Create an Executive Summary.
  Summarize the incident including cost and impacts for management. Include the costs of time and money spent dealing with the incident. Submit the summary to management with a promise that recommended changes will follow.
- Action 6.1.8 Send recommended changes to management.
  Provide management with a set of recommended changes derived from the lessons learned process. Include a cost estimate, schedule, and impacts of doing or not doing the actions.
- Action 6.1.9 Implement approved actions.
  For those changes which get management approval, ensure the changes are made.

# SPECIAL ACTIONS

## FOR RESPONDING TO VARIOUS TYPES OF INCIDENTS

*In the previous sections we outlined actions that are applicable to a wide variety of computer security incidents. In this section we define common types of incidents and suggest specific actions appropriate for dealing with each type.*

### TYPE 1.

Malicious Code Attacks.

*Malicious code is the name given to programs such as viruses, trojan horses, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and to modify audit logs to hide unauthorized activity. Malicious code is usually designed to be difficult to detect and trace. Certain viruses can even modify their signature. NOTE: Even when your firewalls and other defenses stop adversaries, those attackers may be able to accomplish the same objective with trojan horse code pre-installed on computers you purchase.*

- Special Action 1.1 Virus checkers. The most common malicious code it still the virus. Ensure anti-virus software is widely available and that the signature files are kept up to date.

- Special Action 1.2 Monitor for abnormal outgoing traffic (Advanced). Focus network monitoring systems to detect inexplicable packets originating from your organization bound for the Internet. This occurs most frequently at boot up, especially initial bootup.

- Special Action 1.3 Protect the software load process by doing it yourself. (Advanced). Develop processes to install all operating system software and applications locally, from tested configurations.

# SPECIAL ACTIONS FOR RESPONDING TO VARIOUS TYPES OF INCIDENTS

## TYPE 2.

Probes and Network Mapping.

*Probes are a special case of (often-)failed unauthorized access attempts. One class of probe occurs when a potential intruder uses an exploit script against your corporate information systems, or firewall, and the script fails. The failure occurs because the exploit script does not find the expected vulnerability. The probe then attempts to map your network using SNMP or broadcast ICMP "ping" packets to determine the architecture of your network. Another class of probes is used simply for information gathering. In this case, the attacker tests a variety of ports, (a behavior often called a port scan) or host addresses (called a host scan), attempting to map your facility. Some attackers "war dial" your organization's telephones looking for modems.*

■ Special Action 2.1 Report probes to your CIRT. Even of your facility isn't vulnerable, your customers and suppliers may be. If they have access to your systems, your facility could still suffer. There is some controversy as to whether one should "bother" CIRTs by reporting probes. AusCERT's guidance on this follows: "A reason for reporting probes to your CIRT is that they act as a central reporting agency. We have seen cases of probes that were not considered significant by individual sites being part of significantly larger attacks against many sites."

■ Special Action 2.2 Assess the damage. It is great if the intruders do not actually get inside and do damage, but ask whether they learned information about your operating systems and network architecture that they can use in the future. Examine logs carefully. If the exploit script or technique is available, consider running it against yourself to determine what information it can reveal.

## TYPE 3.

Denial of service.

*Users rely on services provided by networks and computers. Attackers use many tools to cause your network and/or computer to cease operating effectively: erasing a critical program; "mail spamming and mail bombing" (flooding a user account with electronic mail), and altering system functionality.*

▲ Special Action 3.1 (Advanced) Employ backup facilities for core services. Denial of service attacks are a difficult problem because they are hard to trace, they are easy to execute, and they are effective. The most likely targets in your organization for a network attack are DNS, web and mail servers. If your organization conducts a lot of business over the Internet, it may pay to establish backup facilities.

## SPECIAL ACTIONS FOR RESPONDING TO VARIOUS TYPES OF INCIDENTS

TYPE 4.

Espionage.

*Espionage is stealing information to subvert the interests of an organization or government. Many cases of unauthorized access to corporate systems are for espionage purposes*

■ Special Action 4.1 Maintain a very small core team. Espionage and insider criminal cases do not benefit from many helpers. The risk of an information leak or evidence contamination continues to rise as additional workers are added to the investigation. A senior member of management such as the CIO, or Chief Security Officer must be advised as well as the incident handling team member on the legal staff. The technical lead should be one of the more seasoned members of the incident handling team, someone who has already proven capable in previous sensitive situations. One issue that often arises is whether to include the system administrator. If you are reasonably sure the sysadmin is not involved in the espionage, the answer is probably yes.

■ Special Action 4.2 Maximize data collection. Ensure that access records of the affected facility are collected and protected. These may include records from badge access systems, phone records from your organization's PBX, log books, system logs, network logs and surveillance videos. Collect as much back data as possible.

■ Special Action 4.3. If an outsider is performing espionage, you may be able to provide erroneous information and actually benefit from the incident. If you suspect the information is being collected and distributed by an insider, this is less likely to work.

■ Special Action 4.4 Target analysis. Review the lead, or leads that tipped off your organization that it might be dealing with espionage. Ask what are the most probable targets of the activity. For each probable target ask what the information is worth? Who (outside the organization) might benefit from having the information? What are all the possible ways to acquire these targets? What are the two or three most likely ways to acquire these targets? This process leads to a fairly simple, but important question: are monitoring capabilities in place for the most likely ways to acquire the most probable targets? If the answer is yes, begin reviewing the monitoring data immediately. If the answer is no, determine what is required to monitor the most likely ways to acquire the probable targets? Make it so.

▲ Special Action 4.5 (Advanced) Establish a war room. A war room is a secure room with *copies* of evidence in the case. The purpose of a war room is to facilitate displaying the data in a meaningful way to help solve high risk or difficult cases. The walls of the room can be decorated with evidence, lines of investigation, charts from the target analysis process, maps of the area and blue prints of the facility. A tape player and TV/VCR should be available; it is often a good idea to record and play back interviews, or access tapes.

# SPECIAL ACTIONS FOR RESPONDING TO VARIOUS TYPES OF INCIDENTS

## TYPE 5.

Hoaxes


*An Example: If you receive a mail message entitled 'Here it is doodz' don't open it! If you do it will delete all the files on your hard disk, stop your pacemaker, and cause your dog to mess on the floor."*

| | |
|---|---|
| NOTE! | In early 1995, hundreds of thousands of users with Internet access distributed information about a virus called the Good Times Virus, even though the virus did not exist. Hoaxes are valid incidents, (remember, our definition of an incident includes the threat of an adverse event). They tie up incident response resources as system administrators and incident handlers try to sort things out. Hoaxes also serve to make users uncomfortable with computing resources by spreading fear, uncertainty and doubt. |

■ Special Action 5.1 Use the Hoaxes page at CIAC (see Resources on p. 36) to validate or debunk possible hoaxes.

## TYPE 6.

Unauthorized access

*Unauthorized access ranges from improperly logging into a user's account, (e.g., when a hacker logs into a legitimate user's account), to unauthorized access to files and directories stored on a system or storage media by obtaining superuser privileges. Unauthorized access could also entail access to additional computer systems by planting an unauthorized "sniffer" program or device to capture all packets traversing the network at a particular point. Another common method used to gain unauthorized access is to exploit a vulnerability in your corporate information systems, routers, or even firewalls. Exploit scripts for gaining unauthorized access are widely available on hacker web sites.*

■ Special Action 6.1: Examine firewall or filtering router protections. The single most likely avenue of attack from an outsider is through an organization's network connections, especially the Internet connection. If possible do not allow people to run the following services: "r-utilities", sunrpc, xwindows, or NetBIOS/IP. Telnet and FTP should be allowed only to systems that absolutely need to provide these services to the internet. DNS servers and mail relay systems are always popular targets with attackers, run as few services on these systems as possible and ensure they are well protected.

■ Special Action 6.2 Regularly examine access services. It is not absolutely necessary to access another user's account to perpetrate an attack on a system or network. An intruder can access information, plant Trojan horse programs, and so forth, by misusing available services. One example is outsiders using the network file system, (NFS), or the file access mechanisms in Windows NT to reach files and directories in another of your organization's domains.

## INCIDENT RECORD KEEPING

*Record keeping is crucial for each of the six phases of incident handling above. Use a log book to record the nature of suspicious events immediately after they've been observed. Include the name of the system, time and other details related to the observations, even details that may not seem to be very relevant at the time they're recorded. Also record the names of those with whom you discussed the incident or possible incident. Careful recording of these details can assist efforts to identify the nature of an incident, develop effective solutions, and prosecute those who commit computer crime.*

*Common practice among incident handlers is to use a new bound blank book such as those commonly available at "dollar stores". Other folks prefer spiral bound notebooks. Either option is fine. Just be sure that you take notes that you would be proud to see displayed in a courtroom six months later. That means never doodle or write sarcastic remarks in your notebook! Some organizations use dictation devices rather than notebooks for convenience and speed.*

*Video and audio recordings of the event provide an excellent record and may be very useful in court. However, they may collect more information about your corporate structure and proprietary information than you wish to reveal. If you do use these tools, you may be forced to turn them all over in a legal situation. Discuss the use of these tools with your attorney before you actually use them in an incident.*

*Experienced incident handlers rarely need more than three or four pages to record most of the essential information. However, the pace of incident handling is very fast, so remembering what to record may become difficult.*

*In this Step-by-Step guide, we provide forms you may use as an option to notebooks. Or you may use them as aids to help you remember what to record in the notebooks. The forms may prompt you to record information that might be useful to you as your memory begins to dim. Feel free to reproduce them and give them a try during a mock incident to see what works well for you. Whether you use the forms, notebooks, or a combination, remember to sign, date, and number the pages you use, and store them in an "evidence worthy" container.*

*The Command Decision Team members should make sure that they keep an accurate record of the information that they receive from the On Site Team, as well as any communications to individuals outside the CIRT team, such as executives or local law enforcement officials. If the managers on the Command Team have an excellent working relationship with their secretaries or administrative assistants, your organization may benefit by having these administrative employees on the Command Decision Team.*

### DEFINITIONS OF INCIDENTS AND EVENTS

Incident:
The term "incident" refers to an adverse event in an information system, and/or network, or the threat of the occurrence of such an event. Examples of incidents include: unauthorized use of another user's account; unauthorized use of system privileges; and execution of malicious code that destroys data. Incident implies harm, or the attempt to harm.

Event:
An "event" is any observable occurrence in a system and/or network. Examples of events include: the system boot sequence; a system crash; and packet flooding within a network. These observable events recorded in the incident-handling notebook, along with the evidence you are able to collect, provide the bulk of your organization's case if the perpetrator of an incident is caught and prosecuted.

*You may make additional copies of this form as needed.*

## INCIDENT CONTACT LIST

Date Updated: _____ Page _____

INCIDENT #:_____

**Local Law Enforcement Official for Computer Crime:**

Name:_____

Phone: _____

Pager: _____

Fax:_____

E-mail: _____

**Local FBI:**

Name:_____

Phone: _____

Pager: _____

Fax:_____

E-mail: _____

**Outside CIRT, or FIRST Team:**

Name:_____

Phone: _____

Pager: _____

Fax:_____

E-mail: _____

**Onsite Team Member:**

Name:_____

Phone: _____

Pager: _____

Fax:_____

E-mail: _____

**Onsite Team Member:**

Name:_____

Phone: _____

Pager: _____

Fax:_____

E-mail: _____

**Onsite Team Member:**

Name:_____

Phone: _____

Pager: _____

Fax:_____

E-mail: _____

**Command Decision Team Member:**

Name:_____

Phone: _____

Pager: _____

Fax:_____

E-mail: _____

**Command Decision Team Member:**

Name:_____

Phone: _____

Pager: _____

Fax:_____

E-mail: _____

**Command Decision Team Member:**

Name:_____

Phone: _____

Pager: _____

Fax:_____

E-mail: _____

*You may make additional copies of this form as needed.*

## INCIDENT IDENTIFICATION

Date Updated: _____ Page _____ of _____ INCIDENT #:_____

Your contact information:

Name: _____

Phone / Alt Phone: _____

Fax / Alt Fax: _____

E-mail: _____

Type of incident: (Denial of Service, Espionage, Hoax, Malicious code, Probe, Unauthorized access, Unauthorized use.)

_____

Location of incident:

Address: _____

Building: _____ Room: _____

Additional Information: _____

How was the incident detected:

_____

Who detected the incident: _____

Signature: _____

When was it detected: _____

*You may make additional copies of this form as needed.*

## INCIDENT SURVEY

Date Updated: _____ Page _____ of _____ INCIDENT #:_____

Location(s) of affected system(s):

Date / Time incident handlers arrived at site: _____

Describe affected information systems: *(one form per system is recommended)*

_____

_____

Hardware Manufacturer:_____

Serial Number of CPU:_____

Corporate Property Number if applicable:_____

Operating System type / version:_____

Disk capacity (if known):_____

Is affected system connected to a network?

System name: _____

System address:_____

MAC address: _____

Is affected system connected to a modem? _____ Phone number: _____

Describe physical security of location of affected information system *(locks, alarm systems, building access etc.):*

_____

_____

_____

_____

*You may make additional copies of this form as needed.*

## INCIDENT CONTAINMENT

Date Updated: _____ Page _____ of _____ INCIDENT #:_____

Isolate affected systems:

Command Decision Team approved removal from network?

☐ YES ☐ NO

If NO what was the reason:

_____

_____

_____

If YES time systems were disconnected. _____

Backup affected systems:

System backup successful for all systems? _____

Name of persons who did backup(s): _____

Time backups started: _____ complete: _____

Backup tapes sealed? ☐ YES ☐ NO

Backup tapes turned over to: _____

Signature:_____

Location tapes will be stored:_____

*You may make additional copies of this form as needed.*

## INCIDENT ERADICATION

Date Updated: _____ Page _____ of _____

INCIDENT #:_____

Names of all persons performing forensics on affected system(s):

_____

_____

_____

_____

Was the vulnerability identified? Describe:

_____

_____

_____

_____

What was the validation procedure used to ensure problem was eradicated?

_____

_____

_____

_____

# INCIDENT FOLLOW-UP AND LESSONS LEARNED

*Below you will find some suggested questions for the Lessons Learned meeting.*

The primary purpose of the meeting is to improve your corporate incident handling process, not to play politics! In almost every incident some things are done well, some things aren't. People have a tendency to remember the screw-ups. Accentuate the positive.

The questions below are to be answered by the incident handling team. All affected parties are welcome to comment.

Briefly describe what has transpired and what was done to intervene. Was there sufficient preparation for the incident? What preparation wasn't done that should have been done?

Did detection occur promptly or, if not, why not? What additional tools could have helped the detection and eradication process? Was the incident sufficiently contained?

What practical difficulties were encountered? Was communication adequate, or could it have been better? We have never been involved in a serious incident where anyone could honestly claim that "communication was great". The phone lines are overtaxed; the On Site Team has trouble reaching the Command Decision Team to provide them needed tactical information. As stress goes up, communication degrades. (The point of this question is to find ways to improve communication. An organization might not wish to approve three extra phone lines into the facility that will be used by the Command Decision Team. After the lessons learned phase of an incident in which the team was unable to stay in communication with critical parts of the organization, extra phone lines are often installed without further review).

Analyze the cost of the incident. Work within your chain of command to determine personnel time that was invested in dealing with the incident, including time necessary to restore systems. Convert those hours into monetary cost. Ask how much the incident disrupted ongoing operations. Were any data irrecoverably lost, and, if so, what was the value of the data? Was any hardware damaged? Generate an executive summary that includes cost and schedule impacts. If possible, post the results of the incident investigation on the incident handling intranet web page.

# RESOURCES SUGGESTED BY THE CONTRIBUTORS

## WEB SITES

*AusCERT posts advisories and also has information about security tools.*
http://www.auscert.org.au/

*The Computer Emergency Response Center posts advisories and also has information on recovering from an intrusion.*
http://www.cert.org/
ftp://ftp.cert.org/pub/incident_reporting_form

*The Computer Incident Advisory Capability posts advisories, has sections on hoaxes, chain letters, viruses and other security resources.*
http://ciac.llnl.gov

*The Forum of Incident Response and Security Teams web site can help you locate the outside CIRT team most relevant to your organization.*
http://www.first.org

*The High Tech Crime Investigation Association has regional sub groups that may be beneficial.*
http://htcia.org

*IETF Security Incident Processing Charter*
http://www.ietf.cnri.reston.va.us/html.charters/grip-charter.html

*Kumite has a section on virus myths and hoaxes.*
http://www.kumite.com

*Rootshell and sabotage have collections of exploits.*
http://www.rootshell.com
http://www.sabotage.org/rootshell/

*Site Security Handbook, RFC 2196*
ftp://ftp.isi.edu/in-notes/rfc2196.txt

## MAILING LIST

The bugtraq mailing list is a good source of vulnerability information that is often posted long before traditional advisories. To subscribe send mail to listserv@netspace.org with the following in the body of the message:

SUBSCRIBE BUGTRAQ yourfirstname yourlastname

## DIGEST

*The SANS Network Security Digest*, edited by Michele Crabb with the assistance of the dozen top security experts in the US, summarizes new threats that have been uncovered and provides pointers to the sources of further information and patches where available. It is provided eight times a year, via email, at no cost to system administration and security professionals in eligible organizations. Email digest@sans.org with the subject subscribe.

# ADDITIONAL OFFERINGS FROM THE SANS INSTITUTE

## ELECTRONIC DIGESTS

**The SANS Network Security Digest**
Published every six weeks, and distributed via email, the SANS Network Security Digest reports on the most important new security threats and provides guidance on where to find the latest patches or additional information on the threats. Each issue can be read in about eight minutes. The SANS Digest is written by Michele Crabb with assistance from Matt Bishop, Dan Geer, Gene Spafford, Steve Bellovin, Bill Cheswick, Gene Schultz, Marcus Ranum, Rob Kolstad, Hal Pomeranz, Dorothy Denning, and several other leading experts.

**The NT Digest**
This digest provides updates to NT Security: Step-by-Step plus up-to-date guidance on new Hotfixes and Service Packs that should and should not be implemented. It also summarizes new threats and new bugs found in NT and its services.

## ROADMAP TO NETWORK SECURITY POSTER

**The SANS Roadmap To Network Security Wall Poster and Web Security Roadmap Poster**
Updated twice a year, these posters present "top ten" lists of answers to common questions: the best security books, the best security web sites, the biggest threats, the vendor contacts, and more. They are mailed automatically to all Network Security Digest subscribers and people who attend the Institute conferences.

## COOPERATIVE RESEARCH REPORTS

**CIDER: The Cooperative Intrusion Detection, Evaluation and Response Project**
A cooperative program to develop low-cost, open source software for network monitoring and intrusion detection.

**The SANS Salary Survey**
Published annually, the survey reports salaries of sysadmin, networking, and security professionals based on their primary operating environment (UNIX, NT, Netware, or combination) where they live, the type and size of employer, the machines they manage, whether they are employees or consultants, and other characteristics. It also reports the size of their raises, by salary level, and the principal reasons reported for above-average raises. More than 1,600 people participated in the 1997 survey.

**Windows NT Security: Step-by-Step**
A consensus of security professionals from seventy-seven large user organizations - who worked together to develop a list of 93 actions in eight phases that should be done to secure an NT server. 36 pages.

**Computer Security Incident Handling: Step-by-Step**
A consensus of the leading incident handling agencies and experts plus fifty other experienced incident handling professionals. 44 pages.

*Other consensus guides under development*
Virtual Private Networks: Step-by-Step
Firewall Troubleshooting: Step-by-Step
Solaris Security: Step-by-Step
Windows NT PowerTools: Administrators' Consensus.

## SELECTED TOPICS COURSES

In addition to its two major conferences, in the spring and the fall, SANS schedules a few full-day and two-day courses in cities around the US and around the world. Topics include Intrusion Detection, UNIX Security, Windows NT Optimization, Windows NT Security and other advanced technical subjects. These courses feature the top-rated speakers from SANS conferences. Because we run them very rarely, the SANS Selected Topics courses always fill up within a few days of being announced. If you would like advance notice of courses in your city, send email to info@sans.org with the subject Selected Topics Courses and in the body tell us your name, company, address, preferred email address, and which topics you wish to learn about: Windows NT, UNIX, or Intrusion Detection.

## ABOUT THE SANS INSTITUTE

The SANS Institute is a cooperative research and education organization through which system administrators, security professionals, and network administrators share the lessons they are learning. It offers educational conferences and in-depth courses, cooperative research reports, and electronic digests of authoritative answers to current questions.

## INFORMATION ON UPCOMING EVENTS

# SANS Network Security 98 Conference

*including the New* INTRUSION DETECTION CONFERENCE

Orlando, Florida
October 24-31, 1998

www.sans.org or email info@sans.org for details

*"The most concentrated source of security information that I know of."*
— Del Armstrong, Frontier Communications

*"More technical and less commercial than the other security conferences"*
— Alan Morewood, Bell Canada

Those comments from attendees in Monterey just about sum up SANS conferences. And the SANS Network Security program in Orlando will be even better! Never before have so many of the leading security gurus come together to teach the state of the art of network and UNIX and Windows NT security.

Please join us in Orlando and share in this feast of learning opportunities. Starting early in the morning with our exclusive "How Things Work" briefings, SANS Network Security '98 offers you learning opportunities every minute of every day you are there:

Twenty-five great full-day courses
Eleven intensive half-day courses
Ten two-hour short courses on emerging technologies
A whole raft of invited and peer-reviewed presentations
Evening courses
Evening grad-school sessions
Evening birds-of-a-feather sessions
The guru-is-in sessions
And even lunch time, "brown bag" sessions on professional development topics.

MAJOR TOPIC AREAS:

- Intrusion Detection
- Active Auditing
- New Firewall Technology
- Network Forensics
- Windows NT Security
- VPNs
- Extranets and Partnernets
- Incident Handling
- Selecting Intrusion Detection Tools
- UNIX Security Tools and Their Uses
- Security Policy and Management

***The quality of these programs is extraordinary!!***

*"SANS brought together an astounding number of experts in a wide variety of areas. The speaker quality is really exceptional."*
— Stephen Jones, US Army Corps of Engineers Waterway Experiment Station

And this year we've added a parallel conference on How To Implement Effective Intrusion Detection Systems—a program designed to help you launch a new intrusion detection program or perfect the one you've been running all year. And you'll be able to attend any combination of the Intrusion Detection sessions and the regular NS98 sessions.

If staying current with technology matters to you, then it makes sense that you should attend this unique program.

*"Fantastic! Tons of information! My brain is now Jell-o®— I'll be back next year"*
— Kurt Danielson, National Marrow Donor Program

COMPUTER SECURITY
INCIDENT HANDLING
STEP BY STEP
THE SANS INSTITUTE