Appendix C
Best Practices for Victim Response and Reporting

A quick and effective response by a company is critical for stopping an ongoing attack and preventing future attacks. Moreover, the use of established procedures—including preservation of evidence—and notification to incident-reporting organizations and/or to law enforcement will help to secure systems of other victims or potential victims. Use of the practices discussed below by companies may help to minimize damage to computer networks from attacks and maximize opportunities to find the attacker.

Because victims play an important role in providing computer logs and factual testimony regarding the intrusion, we also suggest some "best practices" for companies to consider when responding to a network crime, including reporting incidents to law enforcement and to data subjects. Companies, universities, and other organizations should consider these practices as part of their contingency planning before they are attacked, so they are prepared to respond appropriately when attacked.

While these practices are designed to assist network operators and system administrators, it is important for investigators and prosecutors to be familiar with these practices as well. For first-time victims, law enforcement can offer advice on prudent steps the victim should take. Law enforcement also may have opportunities for outreach to organizations that are considering contingency planning for future network attacks or to organizations that are considering remedial steps (e.g., changes to company procedures) after they have responded to a network crime.

A. Steps Before Confronting an Intrusion

1. Be Familiar with Procedures, Practices, and Contacts

Organizations should have procedures in place to handle computer incidents. These procedures should be reviewed periodically and made available to all personnel who have system security responsibilities. The procedures should

provide specific guidance to follow in the event of a computer incident. Ideally, those procedures should specify: who in the organization has lead responsibility for internal incident response; who are the points-of-contact inside and outside the organization; what criteria will be used to ascertain whether data owners or subjects of any data taken by the attackers must be notified; and at what point law enforcement and a computer incident-reporting organization should be notified.

2. Consider Using Banners

Real-time monitoring of attacks is usually lawful, if prior notice of this monitoring is given to all users. For this reason, organizations should consider deploying written warnings, or "banners," on the ports through which an intruder is likely to access the organization's system and on which the organization may attempt to monitor an intruder's communications and traffic. If a banner is already in place, it should be reviewed periodically to ensure that it is appropriate for the type of potential monitoring that could be used in response to a cyberattack. More information on this topic can be found on CCIPS' website at http://www.cybercrime.gov.

B. Responding to a Computer Incident

1. Make an Initial Identification and Assessment

A first step for an organizations is to make an initial identification of the type of incident that has occurred or is occurring, and to confirm that it is, in fact, an incident. The network administrator should determine the nature and scope of the problem—i.e., which specific systems were affected and in what ways they were affected. Indicators that an intrusion or other incident has occurred will typically include evidence that files or logs were accessed, created, modified, deleted or copied, or that user accounts or permissions have been added or altered. In the case of a root-level intrusion, attention should be paid to any signs that the intruder has gained access to multiple areas of the system—some of which may remain undetected. Using network log information, the system administrator should determine (a) the immediate

origin of the attack; (b) the identity of servers to which the data were sent (if information was transferred); and (c) the identity of any other victims. Care should be taken to ensure that such initial actions do not unintentionally modify system operations or stored data in a way that could compromise the incident response—including a subsequent investigation.

2. Take Steps to Minimize Continuing Damage

After the scope of the incident has been determined, an organizations may need to take certain steps to stop continuing damage from an ongoing assault on its network. Such steps may include installing filters to block a denial of service attack or isolating all or parts of the system. In the case of unauthorized access or access that exceeds user authorization, a system administrator may decide either to block further illegal access or to watch the illegal activity in order to identify the source of the attack and/or learn the scope of the compromise.

Initial response should include at a minimum documenting: users currently logged on, current connections, processes running, all listening sockets and their associated applications.

Image the RAM of the attacked systems.

As described below, detailed records should be kept of whatever steps are taken to mitigate the damage flowing from an attack and any associated costs incurred as a result. Such information may be important for recovery of damages from responsible parties and for any subsequent criminal investigation.

3. Notify Law Enforcement

If at any point during the organization's response or investigation it suspects that the incident constitutes criminal activity, law enforcement should be contacted immediately. To the extent permitted by law, information already gathered should be shared with law enforcement. As noted above, certain state laws may allow a company that reports an intrusion to law enforcement to delay providing notice to data-subjects if such notice would impede a law enforcement investigation.

Companies should note that law enforcement has legal tools that are typically unavailable to victims of attack; these tools can greatly increase the chances of identifying and apprehending the attacker. When law enforcement arrests and successfully prosecutes an intruder, that intruder is deterred from

future assaults on the victim. This is a result that technical fixes to the network cannot duplicate with the same effectiveness.

Intrusion victims may believe that they can block out an intruder by fixing the exploited vulnerability. However, it is not uncommon for an intruder to install a "back door" through which he can continue to access the system after the initial point of compromise is repaired. Catching and prosecuting the intruder may be the only method to truly secure the organization's system from future attacks by the culprit.

In addition, by using the criminal justice system to punish the intruder, other would-be intruders may be deterred from attacking the organization's networks. Criminal law enforcement can thus play a significant and long-term role in network security.

4. Do Not Hack into or Damage the Source Computer

Although it may be tempting to do so (especially if the attack is ongoing), the company should not take any offensive measures on its own, such as "hacking back" into the attacker's computer—even if such measures could in theory be characterized as "defensive." Doing so may be illegal, regardless of the motive. Further, as most attacks are launched from compromised systems of unwitting third parties, "hacking back" can damage the system of another innocent party. If appropriate, however, the company's system administrator can contact the system administrator from the attacking computer to request assistance in stopping the attack or in determining its true point of origin.

5. Record and Collect Information

Mirror Image

A system administrator for the company should consider making an immediate identical copy of the affected system, which will preserve a record of the system at the time of the incident for later analysis. This copy should be a "system level" or "zero level" copy and not just a copy of user files. In addition, any previously-generated backup files should be located. New or sanitized media should be used to store copies of any data which is retrieved and stored. Once such copies are made, the media should be write-protected to guard it from alteration. In addition, access to this media should be controlled to maintain the integrity of the copy's authenticity, to keep undetected insiders away from it, and to establish a simple chain of custody. These steps will enhance the value

of any backups as evidence in any later internal investigations, civil suits, or criminal prosecutions.

Notes, Records, and Data

As the investigation progresses, information that was collected by the company contemporaneous to the events may take on great significance. Immediate steps should be taken to preserve relevant logs that already exist. In addition, those persons participating in the incident response should be directed to keep an ongoing, written record of all steps undertaken. If this is done at or near the time of the events, the participants can minimize the need to rely on their memories or the memories of others to reconstruct the order of events.

The types of information that should be recorded by the company include:

- description of all incident-related events, including dates and times
- information about incident-related phone calls, emails and other contacts
- the identity of persons working on tasks related to the intrusion, including a description, the amount of time spent, and the approximate hourly rate for those persons' work
- identity of the systems, accounts, services, data, and networks affected by the incident, and a description of how these network components were affected
- information relating to the amount and type of damage inflicted by the incident, which can be important in civil actions by the company and in criminal cases.

Ideally, a single person should be provided copies of all such records. This will help to ensure that the records are properly preserved and capable of being produced later on. It is often crucial to the success of a legal proceeding to defeat any claim that records or other evidence may have been altered subsequent to their creation. This is best accomplished by establishing a continuous "chain of custody" from the time that records were made until the time they were brought into the court.

6. Record and Log Continuing Attacks

When an attack is ongoing or when a system has been infected by a virus or worm, this continuing activity should be recorded or logged by the victim. *If logging is not underway, it should begin immediately.* Increase default log file size to prevent losing data. A system administrator may be able to use a "sniffer" or other monitoring device to record communications between the intruder and any server that is under attack. Such monitoring is usually permissible, provided that it is done to protect the rights and property of the system under attack, the user specifically consented to such monitoring, or implied consent was obtained from the intruder—e.g., by means of notice or a "banner." More guidance on banners can be found in our manual *Searching and Seizing computers and Obtaining Electronic Evidence in Criminal Investigations* (2d ed. 2002).

A banner should notify users or intruders as they access or log into a system that their continued use of the system constitutes their consent to being monitored and that the results of such monitoring may be disclosed to law enforcement and others. Legal counsel at the company should be consulted to make sure such monitoring is consistent with employment agreements, privacy policies, and legal authorities and obligations.

7. Do Not Use the Compromised System to Communicate

The company should avoid, to the extent reasonably possible, using a system suspected of being compromised to communicate about an incident or to discuss incident response. If the compromised system must be used to communicate, all relevant communications should be encrypted. To avoid being the victim of social engineering and risking further damage to the organization's network, employees of the company should not disclose incident-specific information to callers who are not known points-of-contact, unless the employee can verify the identity and authority of those persons. Suspicious calls, emails, or other requests for information should be treated as part of the incident investigation.

8. Notify

People Within the Organization

Appropriate people in the organization should be notified immediately about the incident and provided with the results of any preliminary investigation.

This may include security coordinators, managers, and legal counsel. (A written policy for incident response should set out points-of-contact within the organization and the circumstances for contacting them.) When making these contacts, only protected or reliable channels of communication should be used. If the company suspects that the perpetrator of an attack is an insider, or may have insider information, the company may wish to strictly limit incident information to a need-to-know basis.

Computer Incident-reporting Organization

Whenever possible, the company should notify an incident-reporting organization, such as a Computer Emergency Response Team (CERT). Reporting the incident and the means of attack may help to hamper the attacker's ability to replicate the intrusion against other target systems.

The United States Computer Emergency Response Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT is charged with protecting our nation's Internet infrastructure by coordinating defense against and response to cyber attacks. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public. US-CERT also provides a way for citizens, businesses, and other institutions to communicate and coordinate directly with the United States government about cyber security. Reporting intrusions may not only help protect the company's system from further damage, it could also help to alert other actual or potential victims who otherwise might not be aware of the suspicious activity. They can be contacted on the Internet at http://www.us-cert.gov.

Other Potential Victims

If there is another organization, or a vulnerability in a vendor's product that is being exploited, it may be prudent for the company to notify the victim or vendor—or request that an incident-reporting organization or CERT alert the victim or vendor. The third-party victim or vendor may be able to provide new and previously unknown information about the incident (e.g., hidden code, ongoing investigations in other areas, or network configuration techniques). Such notification may prevent further damage to other systems.

Note also that state laws may require companies to notify people whose data is compromised during an intrusion. For example, California law requires that:

> [a]ny person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Cal. Civil Code § 1798.82(a). As of July 2006, thirty-four states have passed database breach notification laws.[1] Some of the state laws allow for notice to be delayed if it would impede a criminal investigation.[2]

At least one state law allows the database owner to elect against providing notice to data subjects if the database owner consults with law enforcement and thereafter determines that the breach "will not likely result in harm to the individuals whose personal information has been acquired and accessed."[3] A number of federal bills are currently pending, many of which would preempt existing state laws.

C. After a Computer Incident

A critical action after an intrusion and its associated investigation are complete is to take steps to prevent similar attacks from happening again. In order to keep similar incidents from occurring, victims should do conduct a post-incident review of the organization's response to the attack and assessment of the strengths and weaknesses of this response. Part of the assessment should include ascertaining whether each of the steps outlined above occurred.

---

[1] State PIRG Summary of State Security Freeze and Security Breach Notification Laws, *available at*: http://www.pirg.org/consumer/credit/statelaws.htm (visited October 12, 2006).

[2] Fla. Stat. § 817.5681(3) (2005); Conn. S.B. 650 § 3(d).

[3] Conn. S.B. 650 § 3(b).