SEA ISLAND™
Summit 2004

Meeting of G8 Justice and Home Affairs Ministers

Washington – May 11, 2004

BEST PRACTICES FOR NETWORK SECURITY, INCIDENT RESPONSE AND REPORTING TO LAW ENFORCEMENT

This Best Practices document was developed by the G8's Subgroup on High-Tech Crime to assist network operators and system administrators when responding to computer incidents.

A quick and effective response is critical for stopping an ongoing attack and preventing future attacks on your system. 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 these Best Practices should minimize damage to computer networks from attacks and maximize opportunities to find the source of the attack, to prevent further attacks, and to hold the responsible parties accountable for their actions.

National resources for network security, incident response and reporting to law enforcement are also available, and such information is appended to this document.

The order in which these Best Practices are presented is not necessarily the order with which they should be considered or implemented at the time of a computer incident, since different circumstances can call for different responses, but they are organized into the following seven topics:

Before confronting a computer incident:

1. Be Familiar with Established Procedures, Practices, and Points of Contact

When responding to a computer incident:

2. Make Initial Identification and Assessment of Incident

3. Take Steps to Minimize Continuing Damage

4. Do Not Attack or Damage Source Computer

5. Record and Collect Information

- **A. Consider Making a Complete Copy of the Affected Systems**
- **B. Make Notes / Keep Records / Preserve Data**
- **C. Make Sure You Record and Log Continuing Attacks**

6. Share Information

> **A. Do Not Use Compromised System(s) to Communicate About Incident**
> **B. Notify Appropriate People in Your Organization.**
> **C. Contact Appropriate Computer Incident-Reporting Organization or CERT**
> **D. Consider Notifying Other Victims or Vendors**
> **E. Report Criminal Activity to Law Enforcement**

After a computer incident:

7. Take Steps to Prevent Similar Attacks from Happening Again

* * * * * * * * * * *

Before confronting a computer incident:

1. <u>Be Familiar With Established Procedures, Practices, and Points of Contact</u>. Your organization should have procedures in place to handle computer incidents. Find these procedures, review them, and make them available to all personnel who have system security responsibilities. The procedures should provide specific guidance for you to follow. Procedures should specify: who in your organization has lead responsibility for internal incident response; who is the point-of-contact for inside and outside contacts; who inside and outside the organization requires immediate notification; and at which point law enforcement should be notified. If your organization does not have such plans, do not wait until an incident to start developing them.

Also, determine and review which logs, if any, your system routinely captures and stores, and the period for which they are stored, and see if this practice is most suitable and appropriate to your needs.

Finally, some legal systems will allow real-time monitoring of attacks if prior notice of this monitoring is given to all users. For this reason, consider deploying written warnings, or "banners," on the ports through which an intruder is likely to access your organization's system and on which you may attempt to monitor a hacker's communications and traffic. If you already have banners in place, review them to ensure that they are appropriate for the type of monitoring you anticipate conducting in response to a cyber-attack.

While responding to a computer incident:

2. <u>Make Initial Identification and Assessment of Incident</u>. Make an initial identification of the type of incident, and take steps to confirm that it is, in fact, an incident. Using network topology and trusted relationships, determine how many and which systems were affected, and in which way(s) they were affected, even if it is not readily apparent that certain systems have been affected. Good indicators will 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, watch carefully for any signs that the intruder is in multiple areas of your system and possibly still undetected.

Using your log information, attempt to 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. Remember, an intruder may have installed several paths into your organization's system, some of which you may not have discovered, some of which you may not be able to discover until you have engaged in painstaking analysis, and some of which you may never discover.

Initial identification and assessment may not be an easy task; a system may have been Trojan-ized in such a way that it is difficult to detect certain file or configuration changes. Since it is likely that you will not know all of the implications of a particular incident when first detected, it is also likely that you will not know the extent to which other systems have been affected. Take care to ensure that any actions you undertake do not modify system operations or stored data in a way that could compromise your response.

3. Take Steps to Minimize Continuing Damage. You may need to take certain steps to stop continuing damage from an ongoing assault on your organization's network, such as installing filters to block a denial-of-service attack, or isolating all or parts of your system. In the case of unauthorized access or access that exceeds user authorization, you 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.

In reviewing your options, consider that (at least in the case of a remote intruder) isolating the network from other networks and cutting off outside access may alert the attacker that you have seen his activity and thereby eliminate any chance of identifying the attacker. Further, if your attempt to cut off access is detected but ineffective, the attacker may inflict damage in retribution or take other steps to destroy evidence or otherwise hide his activities. If you do decide to block access to the intruder, install all appropriate system patches that address known vulnerabilities, look for and remove any back-doors or Trojan-ized programs, and watch your organization's system vigilantly. Alternatively, you may decide to maintain overall outside connectivity but isolate (or segment-off) particularly infected systems from the remaining network and/or the Internet.

Consult with others in your organization to determine if disconnecting the network is feasible and appropriate as a business and legal matter. Also consult to determine the best technical method for proceeding.

Remember to keep detailed records of the costs imposed on your organization as a result of steps taken to mitigate the damage flowing from the attack, and keep records of the specific processes used to mitigate the attack. Such information may be important for recovery of damages from responsible parties and for any subsequent criminal investigation.

4. **Do Not Hack Into or Damage Source Computer.** Although you may be tempted to do so (especially if the attack is ongoing), do not take offensive measures on your own, such as "hacking back" into the attacker's computer. Doing so may be illegal, regardless of the motive. As most attacks are launched from compromised systems of unwitting third parties, "hacking back" can damage the system of an innocent party. If appropriate, however, you can contact the system administrator from the attacking computer to request assistance in stopping the attack or in determining the source of the attack.

5. Record and Collect Information.

A. Consider Making a Complete Copy (a "Mirrored Image") of the Affected Systems. 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 can be particularly helpful if an incident occurs before your organization has procedures in place. In many instances, mirrored backups prove invaluable in later attempts to identify vulnerabilities exploited, data removed, and sniffers installed, as well as to aid efforts to track the attacker. In addition, locate and obtain previously generated backup files.

Bit-by-bit and file-by-file backups both have advantages and disadvantages. Bit-by-bit copies will capture hidden files and directories, swap data, deleted data and information in slack space, all of which may provide critical clues for an investigator. However, bit-by-bit copying may be overly burdensome or otherwise impractical, necessitating more efficient methods of file or system-wide back-up.

New or sanitized media, which is subsequently protected from alteration should be used to store copies of any data which is retrieved and stored, and access to this media should be controlled, in order to maintain the integrity of the copy's authenticity, to keep undetected insiders away from it, and to help establish the chain of custody of any media. These steps will enhance the value of any backups as evidence in any later internal investigations, civil suits or criminal prosecutions.

B. Make Notes / Keep Records / Preserve Data. As the investigation progresses, information that was collected at earlier stages of the investigation may have great significance. You should take immediate steps to preserve relevant logs that already exist and you should keep an ongoing written record of all steps undertaken so that you will not need to rely on your memory and the memory of others. The types of information that you should try to record include:

- A description of all incident-related events;
- Dates and times (and time zone, preferably in GMT) when incident-related events were discovered or occurred;
- Information (names, dates, times) concerning incident-related phone calls, e-mails and other contacts;

- Identity of persons working on incident-related tasks, a description of those tasks and amount of time spent on tasks;

- Identity of the systems, accounts, services, data and networks affected by the incident, and how these network components were affected; and

- Information relating to the amount and type of damage inflicted by the incident, which can be important if your organization decides to take action to recover these costs from responsible parties or if prosecution of responsible parties is undertaken.

Include in these records copies of all audit information (e.g., system log files and root history files), and secure process/status information and suspicious files. Remember that logs may be in several locations (e.g., logs may be stored locally as well as with a centralized syslog host); get as many as possible. Time and date information in logs will be very important in tracing an attacker and, later, in proving his responsibility if he is caught. Therefore, be sure that log entries accurately reflect this information. Because logs may be stored on servers in various time zones, take care to identify the respective time zone for each log.

As mentioned above, keep information you record and collect in a location and on a medium which cannot easily be altered or destroyed by others. For this reason, you may want to keep handwritten notes and print out all logs, instead of keeping them in a digital format.

Designate one person to be responsible for maintaining control and possession of any records, logs, and backup files. It may be important at a later date to establish the chain of custody of these records in order to show that the records have not been altered. ("Chain of custody" refers to the means by which evidence was handled from the time of collection to the time it is used as evidence in a judicial proceeding, and to the identities of all individuals who had access to this evidence.) Usually, it is easier to show a secure chain of custody if only one person is needed to testify about the storage of the data.

C. <u>Make Sure You Record and Log Continuing Attacks</u>. When an attack is on-going or when your system has been infected by a virus or worm, make sure you are recording or logging this continuing activity. *If you were not logging, begin immediately.* Logging can be done both on a system or on an affected server; decide which is better.

You 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 activity usually is permissible if it is done to protect the rights and property of the system under attack, if a user consents to such monitoring, or if you obtain implied consent from the intruder (e.g., by means of notice or a "banner"). Where monitoring is permissible with explicit or implied consent, determine if your system has deployed banners on the ports through which the intruder is accessing your organization's system and on which you intend to monitor the traffic. (Warning banners can be a useful method to obtain implied consent to monitor from authorized and unauthorized users.) A banner should notify users or intruders as they access or log into the system that their use of the system constitutes their consent to monitoring and the results of monitoring may be disclosed to law enforcement and others. (Banner-ing a high-numbered or unusual port through which the intruder is entering the system may be difficult; likewise, a banner may also put the intruder on notice that he is being observed.)

Consult with your organization's legal counsel to make sure such monitoring is consistent with employment agreements, privacy policies, and legal authorities and obligations in your country, and to receive guidance with respect to the deployment of banners.

6. Share Information

A. Do Not Use Compromised System(s) to Communicate About Incident. Do not use a system that you suspect has been compromised to communicate about an incident or to discuss incident response. If the system has been compromised, using the system to discuss incident handling may compromise the investigation and thwart chances to block or catch the culprit. Preferably, use out-of-band modes to communicate, such as telephones and fax machines. If you must use the compromised system to communicate, encrypt all relevant communications. To avoid being the victim of social engineering and risking further damage to your organization's network, do not disclose incident-specific information to callers who are not known points-of-contact, unless you can verify the identity and authority of those persons. Treat suspicious calls, e-mails and other attempts to get information as part of the incident investigation.

B. Notify Appropriate People in Your Organization. Let appropriate people in your organization know immediately about the incident and any results of your preliminary investigation. This may include security coordinators, managers and legal counsel. (Your written policy for incident response should set out points of contact within your organization; thresholds for contacting them will be extremely useful.) When making these contacts, use only protected or reliable channels of communication. If you suspect that the perpetrator of an attack is an insider, or may have insider information, you may wish to strictly limit incident information to a need-to-know basis.

C. Contact Appropriate Computer Incident-Reporting Organization or CERT. Contacting an incident-reporting organization, such as a CERT, to report the incident and identify the means of attack may help to prevent the attack from happening again and may prevent the attacker from finding other targets. This not only helps protect your system from further damage; it also helps to alert other actual or potential victims who otherwise might not be aware of the suspect activity.

D. Consider Notifying Other Victims or Vendors. If you learn of another victim, or you learn of a vulnerability in a vendor's product which is being exploited, you may want to notify the victim or vendor or see that an incident-reporting organization or CERT alerts the victim or vendor. They may be able to provide information about the incident of which you are not aware (e.g., hidden code, ongoing investigations in other areas, network configuration techniques). In addition, you may be able to prevent further damage to other systems.

E. Report Criminal Activity to Law Enforcement. If, at any point during your response or investigation, you suspect that the incident constitutes criminal activity, contact law enforcement immediately. Some indications that the incident involves criminal conduct include:

- An unauthorized user logged into or using the system;
- Abnormal processes running on the system which use abnormally high amounts of system resources;
- A virus or worm infecting the system;
- A user from a remote site trying to penetrate the system through unusual means of access, such as through a high-numbered port or suspicious port scanning; and
- A heavy volume of packets reaching the system in a short period of time (from the same or varied sources).

If you see such activity, follow the procedures you have in place, which may direct you to contact your organization's attorney, local law enforcement, or other criminal investigative entity. To the extent permitted by law, share the information you have gathered with law enforcement. Based on the technical nature of these investigations, many law enforcement agencies have limited capabilities in the area of cybercrime investigations. Therefore, prior contact with the various law enforcement agencies in your area is recommended to identify a technically-proficient point of contact. If you have a prior relationship with law enforcement in your area, the transfer of information can occur more quickly and efficiently. Explain to your law enforcement contact any confidentiality concerns and potential disruptions to business that may occur due to law enforcement activities.

Although, as system administrator, you may take certain steps to protect your organization's system, you should consult with legal counsel to determine what information you may collect and disclose to law enforcement and any other steps you may take to aid in a criminal investigation – both with and in the absence of legal processes.

Law enforcement has legal tools that are typically unavailable to victims of attack, and these tools can greatly increase the chances of identifying and apprehending the attacker. For example, law enforcement often can require upstream and downstream providers to preserve transactional logs and other evidence, can seek court orders or other legal means to require disclosure of those logs and other evidence, can search and seize evidence, and can require electronic surveillance.

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 try to block out an intruder by fixing the exploited vulnerability, only to find that the intruder has built in a back door and is able to continue to access the system. Catching and prosecuting the intruder may be the only method to truly secure your organization's system from future attacks by the culprit. In addition, by using the criminal justice system to punish the intruder, other would-be hackers may be deterred from attacking your organization's networks. Criminal law enforcement can thus play a significant and long-term role in network security.

After a computer incident:

7. <u>Take Steps to Prevent Similar Attacks from Happening Again</u>. In order to keep similar incidents from occurring, do an "after action" report, i.e., a post-incident review of your organization's response to the attack and assessment of the strengths and weaknesses of this response. Also, be familiar with ongoing risk assessments made by your organization and by outside experts.

[END]

Appendix to Best Practices for Network Security, Incident Response, and Reporting to Law Enforcement

Points of Contact for G8 Countries
May 2004

CANADA

CERT:	http://www.ocipep.gc.ca
Law Enforcement:	http://www.rcmp-grc.gc.ca

FRANCE

CERT:	http://www.certa.ssi.gouv.fr
Law Enforcement:	http://interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic

GERMANY

CERT:	http://www.bsi.de and http://www.bmi.bund.de
Law Enforcement:	http://www.bka.de

ITALY

CERT:	http://idea.sec.dsi.unimi.it
Law Enforcement:	http://www.poliziadistato.it/pds/informatica

JAPAN

CERT:	http://www.jpcert.or.jp, http://www.npa.go.jp/cyber and http://www.ipa.go.jp/security
Law Enforcement:	http://www.npa.go.jp/cyber

UNITED KINGDOM

CERT:	http://www.niscc.gov.uk
Law Enforcement:	http://www.nhtcu.org

UNITED STATES

CERT:	http://www.us-cert.gov
Law Enforcement:	http://www.cybercrime.gov/reporting.htm