

Incident Response Part #1

By Gregory S. Miles, Ph.D.

This article is the first of a six part series in Incident Response (IR). IR professionals have adopted a basic core set of activities that encompass the IR discipline, which includes IR preparation, identification, containment, eradication, recovery, and follow-up. Professional organizations that provide advice in the IR arena include but are not limited to the Carnegie Mellon Software Engineering Institute CERT® Coordination Center (www.cert.org), the SANS Institute (www.sans.org), CanCERT™ in Canada (www.cancert.ca), and the Forum for Incident Response Security Teams (FIRST) (www.first.org). This article focuses on IR preparation.

Preparation is a critical step in any professional environment. Law Enforcement Officers train to use weapons, apprehend suspects, and conduct investigations. Athletes train for months in preparation for their sport seasons. The military trains in preparation for conflict or war. But what

about an organization's computer and network systems?

Many times, an organization's computer and network systems are taken for granted. Assumptions are made that the network will be available whenever it is needed. What does an organization do when the network doesn't work? Why doesn't it work? Who is responsible for making it work again? It is clear in any case, preparation is the key to quickly get the system operational again.

Incident Response is a process devoted to restoring a network or computer system to operation. An incident can be anything from hardware failure to a concentrated attack on the computer system by an unethical hacker. The Computer Incident Response Team (CIRT) provides the 911 response to a computer system emergency.

Preparation is one of the most critical facets of responding to incidents. It is likely that response efforts will be disorganized and confused without it. With this in mind, preparation limits the potential for damage by ensuring response actions are known and coordinated.

“ Incident Response is a process devoted to restoring a network or computer system to operation.”

The following are key steps that need to be accomplished to be prepared for an incident.

Baseline: It is essential to know where you are starting from with your computer/network systems. It is also critical to assure that only appropriate system and network administrators have access to the control systems of the network. These administrators are responsible for establishing and maintaining the access control mechanisms, operating system updates, configuration changes, and structure of the system. It is imperative that administrative access is well controlled by a trusted individual within your organization.

Warning Banners: The warning banner is a critical first defense against an attack. The warning banner gives the organization, when properly worded, the authority to monitor their network activity and defend against an attack. Be sure there are warning banners on every system that are worded in a way to best protect the resources contained within. Be sure to see your legal personnel on the wording.

Written Procedures: Written incident response procedures are critical for responding to incidents. With procedures being written, there is less of a chance of missing a critical consideration or missing a critical contact within the organization. Widely

distributing the procedures helps to ensure that a critical complement of personnel, with the necessary knowledge, will be available when an incident occurs. Written procedures should include checklists that clearly identify the actions that need to be taken when different types of incidents occur. Well written procedures allow a better understanding of the incident response process and requirements.

Communications: Communications are critical during an incident. Assure there is an appropriate amount of communication means available for the CIRT. This includes voice, data, and facsimile. Consider as part of your process, a mechanism to secure your communications through encryption or other means. Contact lists with work, home, facsimile, and cell phone numbers of key personnel should be recorded and kept close by for CIRT use and widely distributed. Issue pagers to key personnel to assure they can be contacted.

Recall: Recall procedures provide operational continuity when there is a significant risk of prolonged failure or disruption. System and network administrators may not be available during a critical incident involving one or more of the systems. It is a good idea to ensure passwords used to obtain super-user access to every system and LAN within your organization are recorded on a sheet of paper, sealed in

a signed envelope, and placed in a locked container in case super-user access is needed by someone other than the assigned system administrator. Recall procedures must include provisions for verifying the identity of the person who needs a password during an emergency.

Backup and Recovery: Regular backups are critical to ensure system and data operational continuity. These backups also enable personnel to check the integrity of systems and data by determining if unauthorized changes have occurred. Since recovery can be a very complicated process, it is also critical to establish and follow recovery procedures. Standardization of these procedures will make it easier for anyone to perform them if required. You may find it necessary to call on someone not assigned to a particular system or network to perform recovery procedures.

Tools: Assure appropriate tools are available for your CIRT. These tools include virus detection and eradication software, tools to restore systems, and incident detection tools. Assure you have identified the tools you project to be critical to incident handling efforts ahead of time as the procurement process can be time-consuming.

Training, Education, and Awareness: Workshops on responding to incidents can be valuable ways to help personnel

learn how to handle incidents. Awareness training is also a good opportunity to get non-CIRT personnel to contribute to the incident response process by knowing what to look for, how to report it, and what to do.

Points of Contact: Assure personnel know where to call in case of an incident. Within your organization, you can place contact information on phone rosters, on stickers attached to a phone, bulletin boards, etc. Also reinforce the contact numbers at training sessions and organizational meetings. There is a greater chance an incident will be reported, and with less delay, when personnel know whom to call.

Practice, Practice, Practice: Even the best plans can fall apart if personnel have not been given the opportunity to experience them in a controlled environment. It is highly recommended the CIRT team practice scenarios that will put the incident response process through a test on a least a quarterly basis.

Preparation is critical to the Incident Response Process. Organizations with the appropriate documentation, tools, and experience will be able to deal with Computer Security Incidents in a professional, composed manner. This will help in restoring systems to operation in a faster, more secure manner.

SECURITY HORIZON



Next IR article, we will be discussing **Incident Response Part 2: Identification.**

© Security Horizon Inc. 2001

Dr. Miles is the COO/CFO for Security Horizon Inc and the Director of CyberCrime Response for JAWZ Inc. You can contact him at gmiles@securityhorizon.com.