

Eric Elgar, Private Consultant

To prepare for a break-in, an organization must determine its security goals, the scope of security it needs and the procedures to implement. When a break-in occurs, the organization identifies the problem, notifies the right people, contains the problem, documents the event, and initiates recovery procedures.

To determine security goals, scope and procedures, an organization must first know the value of its own data. Scope must address both staff expectations regarding privacy and access and management's need for security (accountability, authentication, etc.). Procedures should cover auditing, reporting, notification, investigation, and enhancement. Recovery plans must be tested under real-life conditions.

System monitoring requires logging tools such as Netlog and Pinglogger, administrative tools such as Dig and Fping, and Host scanning tools such as COPS, CRACK and SATAN. To analyze networks, network security personnel might use Argus, Arpwatch, Klaxon, etc. Finally, the organization must keep up to date with CERT advisories and vendor information. System monitoring must be done by human operators to be successful.

When a security incident does occur, the organization implements the following steps:

1. **Identification.** Identify the problem. Make sure all activity is being logged. Determine the extent and severity of the attack, then figure out the impact on system resources.
2. **Notification.** Notify the right people, from technical and administrative personnel to users to the public. Have a defined response team to ensure that investigative and legal action starts immediately.
3. **Containment.** Contain the problem. Human safety is the first priority. After that, protect classified and sensitive data, prevent exploitation of other systems, prevent damage to system files, and minimize disruption of the system.
4. **Documentation.** Document all events and evidence on a secure, removable medium. It should be a medium that can be signed and witnessed.
5. **Recovery.** Eradicate the problem. First verify that all possible data about the problem has been collected. After eradicating the problem, audit all facilities, conduct risk analysis, determine enhancements to the system to prevent reoccurrence, and, if possible, start legal prosecution.