Global Information Assurance Certification Paper

In this age of information gathering, computer users are faced with the influx of computer fraud and computer crime. This ranges from personal computer users to system administrators who work in the office or at home. Computers without any means of security are vulnerable to attacks from viruses, worms, and illegal computer hackers. If the proper steps are not taken, safe computing may become a thing of the past. Devices such as routers and firewalls can be used to defend the perimeter of a companies network infrastructure. An intrusion detection system can also be put in place. An intrusion detection system is the art of detecting inappropriate, incorrect, or anomalous activity. ID systems that operate on a host to detect malicious activity on that host are called host-based ID systems, and ID systems that operate on network data flows are called network-based ID systems. Consider the following:

• This past February, Egghead Software began to move its operations from storefront retail to cyberspace—a big move. Over time, Egghead closed many of its U.S. stores and constructed a "virtual store" Web site, on which you could browse, select and purchase a wide variety of items. On a pre-selected day, the company closed its remaining stores, making it the first major retailer to complete a total transition from real space to cyberspace. Then, its Web site went down and stayed down for more than 24 hours, costing Egghead thousands in lost revenue.

• Omega Engineering Corp., a New Jersey-based manufacturer of high-tech measurement and control instruments, fired its chief network program designer and administrator in July 1996. Less than a month later, the administrator allegedly stole $50,000 in computer equipment, which he used to set off a logic bomb (hidden code that performs an action when a particular event occurs). When the smoke finally cleared, Omega had suffered between $10 million and $20 million in lost contracts.

• In February and March of this year, Department of Defense (DoD) Web sites experienced a series of hacks. Deputy Defense Secretary John Hamre said the attacks were a major "wake-up call" on the vulnerability of sensitive information in government and corporate computers.

These and many others who are victims of a cyber attack shared a high cost of doing business. Many are faced with the question of how to prepare themselves and how to recover when they are hit. Although creating layers of protection is part of the steps needed to protect the network and the company's assets, this paper will only attempt to answer the question of how to report an incident. Also, because this report does not specify a governing reporting agency (government or private), I will refer to this governing body as the 'chosen authority'.

Let us begin by analyzing what is an incident and how that incident

impacts a company's ability to perform it's normal business practice. The incident response team must differentiate what is authorized or unauthorized activity. The following are some activities recognized as being illegal.

-attempts (failed or successful) to gain unauthorized access to a system or it's data.
-unwanted disruption or denial of service (DoS)
-unauthorized use of a system for the transmission, processing, or storage of data
-changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

Keep in mind that if a machine is compromised, anything on that system could have been modified, including the kernel, binaries, data files, running processes, and memory. In general, the only way to trust that a machine is free from backdoors and intruder modifications is to reinstall the operating system from the distribution media and install all of the security patches before connecting back to the network. Merely determining and fixing the vulnerability that was used to initially compromise this machine may not be enough.
It is highly encouraged you restore your system using known clean binaries. In order to put the machine into a known state, you should re-install the operating system using the original distribution media. In order to protect the entire information infrastructure, you must be able to collect data that describes the malicious activity. You can create a baseline to be analyzed later.

Before reporting an incident, you must first adopt a formal plan. This plan details the steps you must take to bring resources together in an organized manner. This plan should include:

1. What type of activity should be reported
2. Why should the activity be reported
3. To whom should the report be sent
4. What to include in the report
5. How to report an incident
6. When should the incident be reported

Your security plan should be included in the company's policies and procedures and should detail what type of activity to report and to whom it should be reported to.
In addition, because incidents may grow in large numbers, reporting them should be prioritized based on their impact or severity. An incident classified as low usually is listed as incidents where the impact is minimal. Examples are email spam, isolated Virus infections, etc. Incidents where the impact is significant may be classified as Medium. Delayed ability to order or manufacture a product, or delayed delivery of critical email are some examples.

Those of a more serious nature should be classified as high. These are proprietary or confidential information being compromised, a virus or worm becoming wide spread and affecting a high percentage of the employees.

Why report an incident? Reporting an incident helps security awareness and improves overall information assurance practices. Procedures should outline who is to be contacted. Identify who your site security coordinator is. This person would receive and track all reported potential threats. The incident response process should list a criterion defining the characteristics of an incident before escalating the response to a higher level. The following is an example of such a criteria:

-how wide spread is the incident
-what is the impact to business operations?
-how difficult is it to contain
-how fast is the incident propagating
-what is the estimated financial impact to the company?

When reporting an incident, you should include in the report contact information, demographic information, hosts/networks involved, attack description, and damage assessment. A name is necessary to ensure a point of contact once additional information is obtained. Identifying whether your organization is government or private in nature is helpful in categorizing the report. While providing host names and IP numbers are not required to provide assistance to sites, they help the chosen authority to determine how widespread the activity is and to understand other technical issues relating to the attack, which might have been observed at other sites. Also, you may include a chronological log and any system logs you deem pertinent. A description of the attack provides the chosen authority with the information needed to help the site determine what has happened and how to recover from it.

Reporting an incident can be done by electronic mail or telephone hotline. Electronic mail allows for rapid prioritization for response actions and enables the chosen authority (government or private) to reply to those messages quickly and efficiently. Electronic mail also provides an accurate medium for exchanging information that might be too complex to discuss over the telephone wire such as packet dumps, or large files.

The quick response of an incident helps in mitigating damages if any might occur. The rule of thumb is to report all suspicious activity. Reporting an incident helps the awareness across government and private environments and contributes to the overall protection of the information infrastructure. For an example of a real incident reported, take a look at http://www.incident-response.org/incident.doc

Remember that system administrators have three weapons against computer crime. The first defense is protecting the peripheral network with the many layers of defense such as host system security, auditing, router security, firewalls, Intrusion detections systems, and incident response plans. Its' second

defense is computer law. Since the early 1980's, there were no clear definitions of what constituted as illegal activity in cyber space. Prosecutors are still changing the language to make clear the playing field, but they have made great strides. The Third defense is teaching computer ethics. This is an area that expert's hope will deter people from becoming illegal hackers. If it is made clear to the new employee that honesty is valued in the company, the employee might think twice about committing a crime against the company.

Reference:

Forensic Techniques in Incident Response Short Course
http://www.incident-response.org/incidentresponse.ppt

Handbook for Security Incident Response Teams
http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf

Information Security Magazine
http://www.infosecuritymag.com/articles/1998/mayspringing.shtml

Incident Response -- Investigating Computer Crime
by Kevin Mandia & Chris Prosise