

Incident Response: The First Step in e-Discovery

by Gregory Fordham

A network intrusion. The theft of confidential or trade secret data. A fraud. An employee complaint or employee misconduct. A malicious attack or destruction of computer data. Each is an example of a computer incident that will require a management response to determine the scope and veracity of the event. And in each case special care is warranted.

Often, the internal technology (IT) support staff is dispatched to remedy the problem or collect the requisite management information. In addition, management may have been advised by its lawyer to use the IT staff as a cost saving measure.

Unfortunately, dispatching the IT staff is usually inadequate and a prescription for trouble. Since IT's mission is to operate and maintain the organization's computer systems, they are not well suited for incident response.

It is like returning to your home and finding a window broken and your belongings disheveled. Who would you call first; a repairman or the Police?

Essentially, there are three problems with using the IT staff to examine the incident rather than a forensic expert to investigate.

First, the IT staff is not usually trained or experienced in the collection and preservation of digital evidence.

Using the same skills that they would use to install a print driver, their investigation will likely, at a minimum, change important date and time stamps, lose volatile memory and change or overwrite free space. Perhaps even the files themselves will be altered.

Even if the consequence of these blunders can be neutralized, they still bring complexity and cost to any subsequent litigation. Even worse, they could raise doubt about the authenticity of significant evidence.

Second, they are not trained or experienced with the very specialized tools that are used for forensically sound incident response. For example the tools that the support staff might use for recovering deleted data produces all the blunders described above.

Third, they lack sufficient forensic analysis experience. As a result, telltale signs of wrongdoing can go unnoticed. Similarly, inappropriate or less effective analysis techniques could be used.

The support staff may not be aware of the additional data resident in many computer system artifacts or even how to interpret them. Without the knowledge of their existence or how they could be used, false conclusions could be reached.

Clearly the lesson to be learned is that special training is required for computer based incident response. If the internal sup-

port staff is not specially trained and proficient in this area, management is best advised to retain an expert.

Other than using the right people as incident responders, there are additional steps that management can take to prepare for incident response. Essentially, these tasks ensure that there is sufficient, reliable data for examination.

The first step is to always practice basic security procedures such as requiring user IDs and passwords for access. Furthermore, passwords should be changed frequently. In addition, adopt a policy prohibiting employees from leaving computers unattended when a user is logged-in.

Second, design and implement a procedure for event logging on servers and client workstations. Windows 2000 and XP include features for system, security and application event logs.

The logs should be captured or retained for at least a year. For servers where a backup system is in place, the backup should include the log files.

On workstations that are not part of a backup plan, increase the log sizes so that they can retain at least one year of data.

The default Windows log size is 512 kilobytes. Increasing the size to 1 or 2 megabytes is usually enough to capture a year of data on a workstation.

Servers only need to retain the activity since the last backup. So, the default size may be adequate, but management should examine their activity volumes and determine the best size.

In addition to default events captured in the event logs, management should identify the key files and folders containing sensitive data. For those files and folders they should also enable auditing.

Auditing will populate the security event log with instances where users accessed the key files and folders. This data can be very helpful when analyzing a computer incident.

§§§

Gregory Fordham has written extensively on this subject and the Georgia Bar has approved his e-discovery presentation for CLE credit. His papers are available for download from the K&F website, www.knfcon.com. He regularly advises clients on how to structure their e-discovery plans in order to minimize cost and maximize return. He also has served as an expert witness in many state and federal cases involving e-discovery and computer forensics. He is also a contributing writer for the 2007 Construction Law Update which was published earlier this year by Aspen Publishers. His e-mail is greg@knfcon.com