



Investigating Cyber Claims

By Mark Greisiger

Corporate networks are vulnerable to a growing number of cyber risk exposures. Until recently, most companies simply absorbed these network-based risks as a cost of doing business. Increasingly, however, many insurance companies are adding cyber insurance to their portfolios to accommodate companies that want to transfer portions of their network risk.

Cyber risks are created by routine computer-based transactions and business activities and can include personal or sensitive information traversing unencrypted

over the Internet; personal account information, credit-card numbers, or passwords sent in non-secure formats over the Internet; and employee e-mail with virus-infected attachments accidentally sent to a company's customer contact lists. Alleged misappropriation of web site content and other intellectual property can result in copyright and trademark infringement lawsuits. Additionally, allegations of privacy policy breaches are beginning to become a familiar trend. All of these events can lead to litigation and costly personal and monetary injuries.

Cyber damage is the loss and damage that results from hacker attacks, employee mistakes, and other types of risks to the information systems of a company. Its extent can range from nuisance damage to devastating damage that seriously erodes data integrity, confidentiality, and system availability. Cyber damage can be caused by direct attacks on the company network or by indirect, upstream attacks on the company's service providers. An example of a direct attack would be a hacker who intentionally penetrates the company's network by



exploiting a server's vulnerability. In contrast, an upstream attack might involve a hacker's disabling a service the company depends upon, such as a domain name server, a provider and ASP service, or an Internet infrastructure provider, such as MCI.

Confirming a Cyber Loss

As part of the process of managing its cyber risks, a company needs to take steps to establish a process for continuously tracking incidents that occur on networks in order to be able to establish the cause of loss or traceable event date, even though for many cyber claims there is no clear cause of loss.

When a company submits a cyber loss claim, the insurer may want to investigate and analyze the facts of the incident. Pertinent questions may include:

- Was there really an occurrence (as defined in the insurance policy)?
- Did the hacker event really cause damage?
- When did this event occur (date, time, place, machine, file)?
- What was the hourly duration of the server outage?
- Who is the culprit and where did the attack originate?
- What loss prevention or compliance process failed?
- Which network security feature was defeated?

The investigation may examine computer hardware and software (including e-mail trails) using legal procedures to obtain evidence that proves or disproves allegations. Part of the investigation is an audit function involving forensic analysis, backward tracing, attack route hypothesis, and possibly attack re-creation.

The scene of the cyber claim or hacker loss event has to be frozen, allowing data evidence to be collected without any contamination. This may involve the cloning or mirror imaging of a hard drive. There must be a chain of custody to account for what has happened to the data since it was originally collected, and the investigation process must be auditable.

Many times, computer data evidence is created transparently by the computer's operating system and without the knowledge of the computer operator. Such information may actually be hidden from view and require special forensic software

Cyber damage is the loss and damage that results from hacker attacks, employee mistakes, and other types of risks to the information systems of a company. Its extent can range from nuisance damage to devastating damage that seriously erodes data integrity, confidentiality, and system availability.

tools and techniques to preserve, identify, extract, and document. The quality and reliability of evidence depends upon how well the evidence has been preserved.

The very use of a computer creates an audit trail that shows what tasks the computer has performed and has accepted into its memory. Forensic software tools and methods can then be used to identify hidden data, passwords, log-ons, and other information that is automatically

dumped from the computer memory as a transparent operation of computer operating systems.

Common computer forensic methods that might be used for a cyber claim investigation include:

- Safe seizure of computer systems and files to avoid contamination and interference.
- Safe collection of data and software (including e-mail).
- Safe and non-contaminating copying of disks and other data media.
- Reviewing of back-up and archived files.
- Recovery or reconstruction of deleted files.
- Recovery of material from "swap" and "cache" files.

Critical Computer Logs

The main purpose of system logs is to capture such data as records of log-ons, changes of privileges, new accounts, and deletion of files. Logs are very critical to any cyber claim investigation. In the near future, many insurance companies may make event logging a condition for coverage. Logs may contain the strongest evidence or proof as to what was damaged or stolen; where the damage occurred; how it happened (were exploit tactic or commands used?); and who did it (password, user ID, or source IP address).

Following an investigation, the insurer must try to present the cyber damage in a logical manner. This may include a step-by-step reconstruction of actions that occurred, with documented dates and times. The report needs to be thorough enough for the company and the insurer to understand what happened and why, in order to determine if there is coverage and to adjust the loss. ▲

Mark Greisiger is VP and co-founder at NetDiligence, and can be contacted at mark.greisiger@privacycouncil.com.