

TECH HOUSTON

SECURITY

Using forensic examiners can assist in recovery from cyber crimes

The FBI and local law enforcement continues to receive reports of cyber crimes such as identity theft, corporate and client information theft and computer break-ins. The loss is near catastrophic to those who owned the information or to the consumer whose identity was stolen. However, today's technology and court systems are providing better tools to companies and clients to recover from data loss, employee fraud and computer crimes.

COMPUTER
FORENSICSANGELIQUE
GRADO

MODERN CRIME SCENE

If a thief steals from a safe or a vault, the recovery and investigation process is well known.

But what could happen to a company's competitive advantage if a multimillion-dollar confidential design is e-mailed to a competitor from a trusted insider's computer? What if an employee embezzles funds out of corporate accounts with fake payroll checks or fraudulent purchase orders? Also, what are the profits at stake when computer systems fail or viruses infect the company's network? Thousands of dollars and hundreds of hours of labor could be lost just to recover from the infection.

There are no fingerprints left on an e-mail, an electronic purchase order, or a computer attack. Or are there? What about digital fingerprints or evidence on the computer?

With improved technology, businesses

can increase productivity many times over. However, so can the criminals, hackers or unscrupulous employees. Using newer and better tools to hide digital fingerprints makes it harder to find the offending party and recover the loss. To get help, many companies are turning to computer forensics investigators who have expert witness certification and can represent their cases to judges and attorneys.

For example, vendors of a Houston hospital needed help to clean up after a virus attack and network outage. Although the hospital's information technology staff had already taken the right initial steps after the attack, the proliferation was severe, and they needed help in speedily bringing the hospital back to full service.

While one team of forensic investigators began probing live systems and forensic reports, another worked with the security and information systems groups to clean the network and carefully restore services.

According to the hospital's CEO, the forensics investigators "monitored the hospital network as 6,000 devices were returned to service. Several 'rogue' machines were identified and confiscated during the process, and services were quickly returned to normal." The evidence on critical machines "would have been lost without the guidance and sophisticated forensic techniques and skills provided, and, after services returned to normal at the hospital, changes in network structure and controls were made," based on the investigators' forensic investigation and reports.

DIGITAL WITNESSES

Incidents such as this have increased in recent years. Years ago, there wasn't much need for computer forensics and evidence

collection. In the past, the focus was on physical evidence, fingerprints, photographs, eye witnesses and signatures.

Beginning in the early 1980s, investigators started looking at computers as sources of evidence. These new "digital witnesses" recorded a criminal's every step. The problem the early investigators faced that still exists today is that the courts, judge and jury didn't often understand how computers recorded this critical information. It was difficult then to convince them the evidence proved a person's role in the crime.

Today, forensics specialists are helping educate people on the potential cyber evidence has as a "smoking gun" in crimes. Even if a criminal tries to cover his tracks by deleting incriminating evidence, tools exist to recover the information, document the steps they took to delete the data and detail the person's specific activities.

Forensics specialists are helping both Houston and the nation find the dirty little secrets hidden, and even deleted from, criminals' computers. They also can look for the lack of evidence, helping prove an individual's innocence.

STRUCTURED APPROACH

Computer and information security is like fire fighting. Obviously, when there is a fire, a swift and scientific attack against the problem is paramount. However, today it is known how fires are started and spread, so it makes more sense to prevent the situation that leads to a fire starting to protect from loss and danger.

The digital clues from an incident to prove a case may be found by forensics specialists, but there are many precautions that can be taken to limit a company's risk

of an incident. A structured approach to prevention is advised:

- Identify important company information — company trade secrets.

- Determine the level of risk management and protection necessary to protect the information. Use the company's risk management protocols for physical assets as a baseline.

- Provide a scaled system of protection with checks and balances. Some call this "defense in depth." It extends from publishing security policies to doing background checks on employees granted access to critical information and monitoring the integrity of the network and the data.

- Follow through with enforcement if policies are violated.

- If policies are violated, intrusions are discovered or data is manipulated, immediately preserve both physical and cyber evidence, according to guidelines available from computer forensics professionals.

- Isolate the offending systems and start the company's damage control and forensics process.

- If necessary, call a professional with knowledge of proper forensics and evidence preservation techniques. Even the simplest step like shutting off a machine or unplugging it can contaminate evidence and render it useless as arbitration and court evidence or even as human resources evidence in defense of a wrongful termination lawsuit. ■

ANGELIQUE GRADO is vice president and director of operations at CyberEvidence Inc. (www.cyberevidenc e.com), a computer forensics company based in The Woodlands. **PAUL E. BROWN**, president and CEO, contributed to this commentary.