Computer Forensics in the Global Enterprise

John Patzakis ¹
Scott Mann ²
Melisa LaBancz ³

¹ President and CEO
² Regional Manager Pacific Rim
³ Corporate Writer

Guidance Software
Pasadena, California, U.S.A.
e-mail: john.patzakis@guidancesoftware.com
e-mail: scott.mann@guidancesoftware.com
e-mail: melisa_labancz@yahoo.com

Abstract

The increase in cyber-crime has created the need for security technologies that are always one step ahead of the criminal. Computer forensics and incident response solutions allow a corporation to self-regulate and investigate their infrastructure with a significantly increased level of assurance; identifying the root cause of an incident and verifying the integrity of critical information. Many countries have enacted laws that call for corporations to implement extensive incident response policies and forensic capabilities. These laws are designed to protect both customers and ultimately, corporations. Government regulatory bodies are frequently requesting discovery from corporations in relation to certain investigations or allegations. Corporations are held responsible for conducting forensic-level investigations on their own. If a corporation does not have the adequate resources to perform such an investigation, these regulatory bodies may assign a third-party to conduct the discovery, significantly disrupting business processes and giving the corporation no control over the direction of the inquiry. With round-the-clock access of multi-national business environments, and real-time, anywhere response capabilities, network-enabled computer forensics provides the missing link in the security arsenal of today’s corporations.

Keywords

Computer forensics, incident response, forensics, security, evidence, Sarbanes-Oxley, ISO 1799

COMPUTER FORENSICS IN THE MAINSTREAM

According to PricewaterhouseCoopers’ 2003 Global Economic Survey (2002), on a global scale, Australian enterprises are among those hardest hit by fraud attacks.

An estimated 47 per cent of businesses in Australia experienced some form of economic crime in the last two years. In the Asia-Pacific region the figure was 39 per cent. Sectors most vulnerable in Australia to white-collar crime were companies in the manufacturing and industrial products sectors. As a result, 37 per cent of organizations surveyed in Australia saw cyber crime as a threat in the next five years (Han, 2003).

In the Americas, billions of dollars are lost each year due to white-collar crime that stems from internal fraud and information embezzlement (CSI, 2003).

Staggering amounts of loss are incurred through the use of computers attached to a company’s internal networks. It is essential to understand silent threats and the damage that they pose. More compelling is the ability to respond immediately to computer related incidents and security breaches, regardless of their worldwide origin.

In addition to fending off network intrusions and denial of service attacks, companies must also contend with silent threats to their information infrastructure and assets. Industrial espionage, employee misconduct, and intellectual property theft are among the computer security incidents that increasingly plague corporate organizations. Additionally, the vast majority of information in the workplace is now stored on PCs, laptops and servers, meaning that no internal investigation should ignore the criticality of preserving digital evidence.

Incident response procedures must include proper computer forensics protocol to properly secure, recover, analyze and preserve relevant computer evidence. Computer forensics technology and investigative training are
also of paramount importance when conducting thorough internal corporate audits. Finding the “smoking gun” will not benefit an investigation if the examiner cannot establish that the resulting data was not corrupted or tampered with.

Only 29% of organizations have implemented fraud-related training for the Board of Directors or management (Ernst & Young, 2003).

Computer forensics has made an important transition from a “black art” practiced by a select few experts, to a requisite component of the information security enterprise. Innovative technology allows for the evolution of computer forensics into a broader technical process, incorporating proactive computer investigations and incident response. Current case studies illustrate how computer forensics enable corporations to seek out network intruders and properly handle internal security breaches.

**Not Just For Law Enforcement Anymore**

A previously “super-niche” technology, computer forensics have moved into the collective consciousness of System Administrators, security professionals and CSOs worldwide.

Much has been made of firewalls, VPNs, IDSs and authentication technology. These security mechanisms are important of course, but how is the technology industry investing in protecting their internal security? Threats from within make up a large percentage of identity theft, credit card fraud, embezzlement, proprietary information theft, harassment, and intellectual property violations. Almost 70% of U.S. related businesses have experienced unauthorized use of their computer networks in 2003 (FBI, 2003).

42% of respondent organizations experienced one or more computer attacks, which harmed the confidentiality, integrity, or availability of network data or systems. Of those events, 72% occurred from the outside (AUSCERT, 2003).

In the United States, 12% of respondents to the CSI/FBI survey noted between 11 and 30 incidents had occurred from the inside of their organizations (CSI, 2003).

Worldwide, 85% of the worst frauds were by insiders on the payroll. Over half of the perpetrators were from management with less than a year in their position (Ernst & Young, 2003).

As with New York’s horse racing scandal (Associated Press, 2002), shady insiders are orchestrating theft and misappropriation of funds from within the trusted walls of their employers. With increasing technological savvy and a desire to reap outrageous rewards, employees are increasingly utilizing company networks to conduct their illegal activities.

Corporations have reached a boiling point where the danger from internal sources just about mirrors that of external sources in regards to the loss of information assets. In general, the landscape of threat has changed dramatically. In years’ past, the biggest threats to the corporate network used to revolve around external attacks. The trend is shifting, putting internal attacks on the steady rise.

Insider abuse of Net access has cost U.S. corporations $11,767,200.00 in 2003, while unauthorized use of the network cost $406,300.00 (CSI, 2003). In the best of times, these “self-inflicted” attacks and their losses are staggering.

According to John Smart (2002), an Ernst & Young forensic services partner specializing in fraud, “Transient staff, the growing complexity of organizations and the internet are all fuelling this dramatic increase in risk. As trusted, long-established middle management is downsized around the world, the eyes and ears of the company are becoming blind and deaf to potential misdemeanours. Fraud also tends to increase during an economic downturn so companies across the globe should watch out for their surviving senior management – especially those new to management who pose a particular threat.”

Computer forensics are critical tools for responding to incidents as they are occurring on the worldwide network. The ability to monitor business-critical functions for signs of abuse, policy violations and fraud are of paramount importance to an industry that experienced a total loss of $70,195,900.00 from the theft of proprietary information in the year 2003 (CSI, 2003).

**Computer Forensics in Motion: Large Scale Enterprise-Wide Incident Response**

Proper tools, procedures and training are the foundation for successful infrastructure security. Understanding the methodology and technology behind forensic investigations is of critical importance to those interested in protecting their assets from both internal and external forces. When implementing computer forensics technology throughout your organization, you must decide what is “enough” in terms of shielding your network from intrusion.
There are many determinants in deciding on appropriate investigative tools: What signs of malicious activity or internal abuse will you be looking for? Do you need to monitor critical business functions across a worldwide network? What private or confidential information needs to be monitored to ensure authorized access and update control? Are PCs and laptops forensically archived when employees voluntarily leave your organization or are terminated?

These are questions that warrant consideration. The “threats” to corporate security are ready to be found on a daily basis. It’s information available to the experienced system administrator. Multi-national companies pose an interesting challenge in that there typically thousands of computers networked together, which makes the ability to respond to threats remotely, on-line, increasingly urgent. In the Australian Computer Crime and Security Survey, Asian Pacific businesses surveyed listed many tools for securing their infrastructure such as: anti-virus (98%), firewalls (95%), access controls (93%), and physical security (83%) (AUSCERT, 2003).

However, despite the alarming increase in internal security vulnerabilities, and despite the fact that none of the above-mentioned technologies can prevent and detect the source of internal fraud, only 7% of respondent companies in the Asia Pacific region have implemented a forensic plan (AUSCERT, 2003).

While anti-virus software and physical security are certainly important components of an overall security plan, they rarely identify the ‘root cause’ of an incident. Typically, organizations fail to deal with the underlying cause or fail to sustain the new internal controls. If lessons are not learned, organizations are likely to be defrauded again and again (Ernst & Young, 2003).

Today’s computer forensic technology allows for the location, extraction, and preservation of critical digital evidence, while allowing filters to run on the network constantly auditing the infrastructure. Utilizing forensic technology to secure the enterprise and enacting a consistent incident response policy can strengthen the framework of international business.

**LAW AND POLICY INVOLVING COMPUTER FORENSICS**

Computer Forensics provides critical insight into policy violations and volatile data. With the ability to expertly investigate compromised systems and preserve data across the worldwide network, exposing digital traces of seemingly invisible crimes has become a reality. In addition, computer forensics makes up one of the most important components of Information Assurance: Information Integrity. Using proven tools and processes, experienced security professionals can provide forensically sound evidence that significantly supports the investigation of internal breaches, and the unauthorized access or use of confidential data. Whether information is fragmented, altered or deleted, computer forensics provide a process to recover data to recreate incidents, retrieve critical documentation and preserve suspicious activity for further examination.

Within a large-scale framework, government entities can simultaneously investigate possible policy violations while monitoring mission critical business units such as Finance and Accounting. Enterprise forensics and incident response systems allow for a comprehensive look into the activity of any system attached to the network. In-depth analysis and response to incidents of hacking, insider information misuse and policy violations are supported by industry proven forensic methodologies and investigative strategies.

Many in the information security field are either unaware or reluctant to acknowledge that employing proper and established incident response processes and tools are critical components of the information security equation. Notably, however, key regulatory agencies do not share this lack of awareness. Specific industry regulations in the United States mandate that incident response processes consistent with best practices be implemented as part of an overall information security plan.

In the United States, existing regulatory regimes, including the Health Information Portability and Accountability Act (HIPPA), Gramm-Leach-Bliley Act (GLBA), and the Federal Trade Commission Safeguards Rules, require that companies subject to those rules and regulations institute a comprehensive information security plan.

These regulations are not merely guidelines, but mandates subject to aggressive enforcement, particularly by the FTC and OCC. The FTC recently initiated enforcement actions against Microsoft, Eli Lilly, the ACLU, Guess, Inc., and others concerning the failure to protect computer-stored customer information with proper information security safeguards, including incident response protocols.

More than just being able to defend its interests, companies are increasingly seeking to prosecute individuals, particularly in cases of industrial espionage, financial fraud, theft of intellectual property and trade secrets. However, a company may not be able to prosecute or obtain a civil injunction against an employee who leaves the company with source code or the customer list. Digital evidence must be properly collected and handled in a manner consistent with best practices in order to uphold a company’s right to seek legal action. (Congressional
Federal Register, 2003). Additionally, claims under cyber-insurance policies, which are growing increasingly popular, often require proper incident handling and preservation of evidence (usually under the provisions of ISO 17799).

Since its adoption, ISO 17799 has quickly emerged as the international standard for information security best practices. Implementation of ISO 17799 is likely to become even more widespread as insurance companies mandate its adoption for companies seeking cyber-liability (“hacker”) insurance, and companies that have already implemented ISO 17799 demand that their vendors/partners likewise adopt the standard. An enterprise’s overall security framework must, under this standard, include an effective incident response approach. An ISO 17799-compliant enterprise should employ the best methods and tools available to respond to breaches or suspected breaches of its information security, and must collect and preserve the resulting evidence in a forensically sound manner.

ISO 1799 and Incident Response

While ISO 17799 addresses many aspects of information security and internal controls, the need for formal incident response procedures and tools is a significant and integral piece of the ISO 17799 equation. According to the standard, ‘information security is achieved by implementing a suitable set of controls’ (ISO 17799). Among the necessary measures identified by the standard that establish “suitable controls” is an incident response process that enables an enterprise to ‘minimize the damage from security incidents and malfunctions, and monitor and learn from such incidents’ (ISO 17799, 2003).

As an initial matter, ISO 17799 (2003) recommends that an enterprise should establish procedures ‘to ensure a quick, effective and orderly response to security incidents. These procedures should cover:

- Analysis and identification of the cause of the incident;
- Planning and implementation or remedies to prevent recurrence, if necessary;
- Collection of audit trails and similar evidence;
- Communication with those affected by or involved with recovery from the incident;
- Reporting the action to the appropriate authority.

The enterprise that has suffered a security incident must properly collect evidence for three purposes (ISO 17799, 2003):

- Internal problem analysis;
- Use as evidence in relation to a potential breach of contract, breach or regulatory requirement or in the event of civil or criminal proceedings, e.g., under computer misuse or data protection laws;
- Negotiating for compensation from software and service suppliers.

Clearly, the second item (and potentially the third) requires that the evidence be collected in a forensically sound manner. ISO 1799 (2003) recognizes this explicitly, as it notes that an enterprise ‘should ensure that their information systems comply’ with the requirements applicable to the production of admissible evidence.

If an enterprise does not have the tools necessary to collect evidence in a manner that preserves its admissibility, it risks compromising its legal (and most likely its financial) position.

When an incident is first detected, it may not be obvious that it will result in possible court action. Therefore, the danger exists that necessary evidence is destroyed accidentally before the seriousness of the incident is realized (TEP, 2000).

An enterprise can minimize this danger by employing the best forensic tools available in its response to a security incident. ISO 17799 calls on enterprises to use computer forensics to preserve the admissibility of evidence:

- For information on computer media: copies of any removable media, information on hard disks or in memory should be taken to ensure availability. The log of all actions during the copying process should be kept...(ISO 17799, 2003).

Finally, compliance with applicable government laws and regulations concerning information security standards is another important component of ISO 17799 certification.
A Critical Defence Against Data Destruction and Evidence Spoilage

The destruction of computer evidence is another monumental cyber-liability problem; citing as an example several companies in the United States who are being battered with substantial criminal penalties and civil damages in recent cases. The business pages are rampant with stories of rogue insiders deleting or altering computer data to thwart auditors and regulators, often resulting in liability to the company for failing to effectively investigate and respond to the incident, which is an integral component of the internal corporate control process. Companies involved in civil litigation have lost tens of millions of dollars due to the destruction of relevant computer evidence, not only arising out of intentional deletion, but negligent mishandling as well.

Rapid response to incidents of intentional or negligent destruction of computer evidence is a crucial capability for an incident response team. However, a Computer Incident Response Team (CIRT) with a “patch and proceed” mind-set will lack the tools, training and urgency to perform such a mission, thereby subjecting an enterprise and its executives to potential criminal and civil liabilities.

Recent legislation and court decisions strongly establish a compelling obligation for businesses to preserve electronic data that may be relevant to an audit or legal matter. On the legislative front, the Sarbanes-Oxley Act of 2002 (USA), passed in response to the American Enron/Arthur Anderson debacle, imposes severe penalties for the destruction of records, including electronic data. The new law imposes fines up to $5 million and/or imprisonment of up to 20 years against “whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document or tangible object with the intent to impede, obstruct, or influence any government investigation or official proceeding.” The Act expressly prohibits the destruction of records in ‘contemplation’ of such an investigation or proceeding (Sarbanes-Oxley, 2002).

In an interesting case involving a company insider and illicit materials stored on the corporate networks, the Australian Industrial Relations Commission upheld the termination of a factory worker for storing a large amount of pornography on workplace computers despite the worker’s claim that he had never been notified of any company policy to the contrary.

The employee brought a worker arbitration proceeding before the commission after he was fired. He claimed that he never received written notification of a company policy against storing offensive material on company computers, and clicked through pop-up boxes that restated the policy without reading them. An arbitrator concluded that the worker’s failure to read the policy pop-up windows did not excuse him from knowledge of their contents (Darwich v. Kaal Australia Pty Ltd., 2003).

These cases typify the ongoing trend in pursuing legal action and utilizing computer forensics to bolster corporate claims of theft, fraud and impropriety worldwide.

In light of legislative and court developments, it is clear that the deletion of electronic records relevant to an audit or legal matter, whether intentional or otherwise, is a critical “computer incident” that necessitates a proper and immediate response in the same manner that network intrusions require instantaneous action. In the Arthur Anderson case, the firm failed, with devastating consequences, to convince federal officials and ultimately a jury that the destruction of electronic records was the unauthorized actions of a few rogue employees and managers and not at least tacitly endorsed by upper management. Other organizations should learn from Arthur Anderson’s demise by implementing an immediate computer forensic investigation and response mechanism to preserve computer evidence and recover critical deleted information.

From even a remote location, today’s computer forensics can quickly identify and efficiently recover deleted information that remains on the computer, while preserving the integrity of the data. This enables investigators to accurately reconstruct an incident while preserving the evidence. They can also assist in mitigating the permanent loss of data, and establishing whether any destruction was the result of unauthorized misconduct on the part of an individual.

Seamless Referrals to Law Enforcement and Consultants

Enterprises with a comprehensive computer forensics response plan have had much better fortunes in both dealing with law enforcement and successfully admitting evidence in civil or criminal trials. When a computer security incident occurs, the ability to create drive images of the subjects’ computer will preserve the investigation scene and allows a seamless transition of any investigation to law enforcement when necessary. A large percentage of law enforcement involved in computer investigations either currently utilize or are looking to purchase advanced forensic tools to improve the efficiency and solidity of data collection. Many companies employing computer forensics technology have simply provided their files to law enforcement, who seamlessly and successfully continued the investigation. This compatible computer forensic investigation process often fosters an advantageous atmosphere of cooperation, which allows the company to better work with law enforcement in managing the disclosure of sensitive information, greatly minimizing any disruption to
operations, and retaining at least some control over the investigation. Importantly, with the company’s investigation team being the first responder with proper computer forensic tools and training, the data can be preserved from any location, procuring disk images without disrupting network operations.

The same advantages hold true for civil litigation and internal investigation matters. When an organization receives notice of a lawsuit, IT security personnel can immediately obtain bit-stream images (as opposed to mere file copies) from company servers and employee workstations that may contain relevant information. The resulting files can then be provided to internal investigators or outside consultants for further analysis.

**CONCLUSION**

Information security best practices are standards that evolve with the new technologies. As it would not be advisable to use 8-year-old firewall appliances or out-of-date antivirus software, it is also not advisable to leave computer forensics to third-party sources or unqualified employees. Training, proper tools, and an understanding of your country’s legal mandates and incident response and audit requirements, provides a security framework that strengthens worldwide business operations.

Network-enabled computer forensics and incident response infrastructure provide a long-awaited means for enterprises to rapidly respond (without disrupting operations) to and investigate computer security breaches; an essential component of any security framework.

It remains the responsibility of individual corporations to implement proper technology in line with best practices and industry standards.

**REFERENCES**


**LEGAL AUTHORITIES**


IRLWed (P&F) 2217

[Aus Indus Rel Comm’n, 2003]

Australia
LEGISLATION


COPYRIGHT

John Patzakis, Scott Mann, and Melisa LaBancz ©2003. The authors assign to ACIS and educational and non-profit institutions a non-exclusive license to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to ACIS to publish this document in full in the Conference Papers and Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission from the authors.