



# **New Incident Response Best Practices**

---

Patch and Proceed is No Longer Acceptable Incident Response Procedure

**SEPTEMBER 2003**

By John Patzakis

# New Incident Response Best Practices

By John Patzakis<sup>1</sup>

Information security technology traditionally focuses on protecting the perimeter to keep the bad guys and the bad code out of the enterprise. But as every CIO knows, information security breaches in large enterprises are inevitable. Hackers will penetrate the network, or — in what many believe are more frequent occurrences — insiders will compromise customer and company data. With such compromises a certainty, enterprises are left scrambling to manage these proliferating incidents.

Recently, intrusion detection systems (IDS) have emerged to help detect perimeter breaches and intrusions. However, organizations that install these systems quickly find that in order to be effective, they need a process to immediately respond to those alarms and confirm the incident to enable sound incident management, containment and mitigation. According to Gartner research, “intrusion detection sounds like a good idea but alerts you only that something is going on. It is not always so effective to just see the alarms going off” and not have the tools to address the problem.<sup>2</sup> Too often, however, the IDS bells ring, but with no effective means to respond and sort out all the false positives, the IDS becomes white noise, and, ultimately, shelfware.

So how are enterprises responding to and addressing all these, alarms, intrusions and compromises? After all, any effective security process — whether it be home security, industrial security, or national security — needs an effective response mechanism that enables effective incident handling and containment. By analogy, home security systems that do not provide an armed response do little more than annoy the neighbors.

Proper incident response is a critical component of the information security framework, as dictated by necessity, and mandated by industry best practices and regulations. For too many organizations, however, the incident response process is either non-existent or merely consists of attempting to patch systems and restore them to their believed previous state, often days or weeks after the incident has occurred and the damage proliferated. The typical incident response is often *ad hoc* and haphazard, involving tedious analysis of log files, invasive analysis of compromised systems using disjointed tools, and the disruption of mission critical systems. When and if the incident is finally confirmed, the problem is kept under wraps with organizations content to move on without preserving evidence and properly documenting the incident for reporting, prosecution or internal “lessons learned” analysis. However, failing to adopt a formal incident response, or simply employing a so-called “patch and proceed” approach is no longer viable under the current state of industry best practices for several reasons, which are set forth below.

## **Effective Containment and Mitigation Requires Immediate Response**

Computer security incidents are like cancer—early intervention and containment are critical in order to prevent the spread of the problem. In many cases, however, the incident response process involves weeks-long delays while the organization’s computer incident response team (CIRT) or outside consultants travel to the site of the compromised systems, followed by painstakingly inefficient analysis of log files and other data with stand-alone utilities. Meanwhile, either the damage proliferates while the CIRT tries to confirm whether the incident did in fact take place, or mission-critical systems are taken off-line, causing disruption of operations and substantial monetary loss. In incident response investigations, the analysis must be as rapid as possible to mitigate the loss and increase the likelihood of identifying the culprit. As the European Convention on Cybercrime has noted, “effective collection of evidence in electronic form requires very rapid response.”<sup>3</sup>

Emerging best practices — which evolve with new technology — call for the use of network-based computer forensics tools, such as EnCase® Enterprise Edition, specifically designed for on-demand incident response and forensic analysis. These network-based applications enable the incident response team to immediately, and without taking systems offline, respond to, confirm and contain the incident anywhere on a wide area network, thereby ultimately mitigating the damage while greatly improving the incident management and decision making process. This is particularly important because computer security breaches are highly transient events that require the rapid and thorough response capabilities of network-enabled computer forensics systems.

For instance, hackers and malevolent insiders often cover their tracks by deleting event log and system files, hiding their installed malware by renaming it with innocuous file extensions, cloaking created backdoors, and other similar techniques. Deleted file recovery is a particularly crucial incident response function, as in addition

to erasing log files to mask the incident, perpetrators will also maliciously delete system files and other critical company data. This deleted information must be quickly restored before it is overwritten and lost. Network-enabled computer forensics tools can quickly undelete files, locate hidden malware (even if renamed) through file signature and hash analysis, find backdoors and other evidence, and make complete bit-stream image backups of drives housing compromised data. Additionally, network-enabled computer forensics operate in a live environment, which allows a very rapid response without taking any systems off-line and thus disrupting operations. Additionally, as the target systems are not taken off-line, the key live data of the compromised system (open ports, live registry, RAM dumps) can be easily captured and preserved. Rapid deleted file recovery, disk imaging, file signature and hash analysis, and live data capture are only some of the key functions that network-enabled computer forensic software provide for effective incident response.

Ironically, incident response teams that simply seek to “patch and proceed” without understanding the cause of the intrusion and the extent of the compromise either fail to fully contain the damage, or at a minimum leave systems vulnerable to further compromise. Far from being a hindrance to quickly and safely proceeding with business, rapid enterprise incident response with network-based computer forensics tools enable prompt and detailed incident identification, management and recovery, all while preserving data for subsequent post-mortem analysis. Among many other benefits, this allows the CIRT to fully understand the scope and nature of the incident for proper and thorough recovery and remediation.

### **Effective Incident Detection Requires an Integrated Response Process**

In June 2003, Gartner created a major stir in the information security industry when it issued a research report calling into question the effectiveness of intrusion detection systems. The report listed several problems associated with the IDS process, including a high rate of false positives and negatives, the burden associated with the need full-time monitoring by information systems staff, and “a taxing incident response process.” The report ultimately questions the value of future IDS investments and recommends that organizations spend their resources on perimeter protection such as firewalls.<sup>4</sup>

However, network-enabled computer forensics analysis represents a natural extension of an IDS alert by providing a very rapid and thorough incident response process, anywhere on the network. An enterprise-wide computer forensics system can be utilized to quickly and concisely confirm whether or not the system is truly compromised. Instead of manually pouring through log files to attempt to confirm an incident, network-enabled computer forensics tools provide a means to thoroughly analyze, from one central location, any potentially compromised system anywhere on the network. This capability greatly enhances the effectiveness of IDS by providing an accurate confirmation and response mechanism to intrusion alerts.

Further, this rapid response and confirmation ability greatly reduces the administrative burden in monitoring and responding to IDS alerts. The latest generation of network-enabled computer forensics systems represent a quantum leap in the power, efficiency and accuracy of the incident response process. Integrating IDS monitoring with a networked computer forensics system is a crucial step that enables organizations to greatly improve the effectiveness of their IDS, while providing a broad and highly effective enterprise-wide investigation capability.

### **The Insider Threat Requires Response and Investigation**

Many computer security professionals tend to think of computer security incidents as problems that originate from outside the perimeter, such as denial of service attacks, worm infections, and website defacements. As a result, many incident response teams fail to recognize and prepare for security compromises perpetrated by insiders. This is a serious mistake that results in substantial losses and costs.<sup>5</sup> As reflected by recent surveys, many incidents, particularly those resulting in significant financial harm, are the work of rogue employees and other trusted individuals.<sup>6</sup>

The insider threat takes many forms, whether it is unauthorized access to customer privacy information, theft of intellectual property and trade secrets, financial fraud, improper deletion of computer files (as in the case of Arthur Andersen) or various employee policy violations such as email harassment and Internet pornography. Notably, industry regulations and best practices do not differentiate between computer incidents with internal or external origins. As such, the incident response process needs to be just as effective in addressing the internal theft of intellectual property as with denial of service attacks.

A recent case involving an insider fraud investigation illustrates the essential importance of network-enabled computer forensics tools. In May 2003, an examiner at a major financial institution recently employed EnCase Enterprise in New York to successfully preview two drives in Asia connected to the wide-area-network for purposes of investigating a very sensitive case of insider trading. The drives were previewed less than an hour after management determined that the investigation was necessary and that time was of the essence. The preview process revealed that one of the drives contained highly relevant information, and that drive was promptly acquired for further forensic analysis in New York without the knowledge of anyone in Asia and without disrupting operations. The investigation also revealed that the other drive did not contain relevant evidence. Notably, with the SARS outbreak at its apex at the time of the incident, EnCase Enterprise essentially enabled an investigation that otherwise would likely not have taken place.

Even without a SARS epidemic, an investigation involving international travel, flyaway kits, and stand-alone computer forensics utilities would have delayed the process by several days, if not weeks, thus resulting in destroyed or otherwise changed evidence due to the critical delays. Further, an on-site response process would have likely compromised the investigation in this case or, at a minimum, impacted business and morale due to the very non-clandestine physical presence of investigators.

While, as noted above, “patch and proceed” is at best a problematic approach to responding to breaches of perimeter security, it is completely antithetical to properly investigating incidents involving rogue insiders. Organizations must address the inside threat with proper internal computer incident response processes to limit liability and establish proper internal controls. Network-enabled computer forensics tools are ideal for investigating and containing compromises caused by insiders.

### **Industry Regulations Mandate Incident Response Processes**

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.

The Federal Trade Commission’s Safeguards rule, for instance, requires that covered entities maintain information security programs that include responding to attacks, intrusions or other systems failures.<sup>7</sup> The FTC rules went into effect May 2003. The Office of the Comptroller of the Currency (OCC), which regulates banking institutions, issued similar regulations that specifically require banks to implement response programs specifying actions to be taken for internal and external security breaches, “including appropriate reports to regulatory law enforcement agencies.”<sup>8</sup> The Department of Health and Human Services issued nearly identical regulations stemming from HIPAA that cover health care providers.<sup>9</sup>

These regulations are not mere 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.

In terms of defined industry best practices, ISO 17799 provides very detailed requirements for incident response, internal investigations, and preservation and analysis of computer evidence consistent with best practices and computer forensics protocols. An enterprise’s overall security framework must, under ISO 17799, include an effective incident response approach “to ensure a quick, effective and orderly response to security incidents.”<sup>10</sup> 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 for investigation and reporting purposes.<sup>11</sup>

The leading international financial standards-setting institution, the Basel Committee on Banking Supervision (the “Basel Committee”) has promulgated important new standards for electronic banking.<sup>12</sup> In a report entitled “Risk Management for Electronic Banking,” the Basel Committee addresses several components of information security, including a strong focus on the necessity of incident response processes. In the report, the Basel Committee establishes that “[e]ffective incident response mechanisms are . . . critical to minimize operational, legal and reputational risks arising from internal and external attacks.”<sup>13</sup> As a result, banks should “develop

appropriate incident response plans . . . that ensure business continuity, control reputation risk and limit liability associated with disruptions in their e-banking services.”<sup>14</sup>

In order to implement this Risk Management Principle, the Basel Committee highlighted eight specific actions that should be undertaken by banks, including the following four functions or capabilities that banks should develop:

- Incident response plans to address recovery of e-banking systems and services under various scenarios, business and geographic locations . . .
- Mechanisms to identify [a] crisis as soon as it occurs, assess its materiality, and control the reputation risk associated with any disruption in service.
- Incident response teams with the authority to act in an emergency and sufficiently trained in analyzing incident detection/response systems and interpreting the significance of related output.
- A process for collecting and preserving forensic evidence to facilitate appropriate post-mortem reviews of any e-banking incidents as well as to assist in the prosecution of attackers.

Thus, a key factor for banks is to be able to quickly and thoroughly respond to security incidents. In order to manage risks adequately, banks must have contingency plans in place to address incidents as they occur, and those plans “should set out a process for restoring or replacing e-banking processing capabilities, reconstructing supporting transaction information, and include measures to be taken to resume availability of critical e-banking systems and applications in the event of a business disruption.”<sup>15</sup>

Under these compelling regulations and defined best practices, organizations must 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. For incident response, “best practices” is embodied by network-enabled incident response and computer forensics systems for computer security incidents that occur throughout an organization’s network.

Conversely, the “patch and proceed” methodology is not compliant with these regulations and standards for two reasons. First, with the growing standardization of network-enabled computer forensics tools, “patch and proceed” is simply no longer consistent with best practice. Secondly, without the proper response, collection and preservation of evidence, the internal and regulatory incident reporting requirements under these regulations and standards cannot be met.

## **The Defense and Prosecution of Claims Require Preservation of Evidence**

In addition to information security regulatory requirements, enterprises face an increasing risk of various cyberliability claims stemming from such security breaches as theft of customer privacy data, denial of service attacks that are launched from a company’s compromised systems, misappropriation of intellectual property, insider financial fraud, and the destruction of computer data. These legal claims take many forms, including government enforcement actions, class action suits from customers, shareholder suits (for lack of internal controls to investigate and stem insider fraud), and other claims.

Under a new California law, effective July 1, 2003, companies that conduct business in California (a broad standard) must disclose computer security breaches to any California resident if their unencrypted computer stored privacy data is compromised by a hacker or rogue insider in the course of that breach. A similar federal law is under consideration. Organizations that fail to properly respond to a myriad of potential liability-causing incidents will find themselves unable to defend their interests in court, subjecting the enterprise to significant legal exposure.

More than just being able to defend its interests, companies are increasingly seeking to prosecute perpetrators, particularly in cases of industrial espionage, financial fraud, and 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 if the digital evidence trail is not properly collected and preserved. Courts mandate that computer evidence be collected and handled in a manner consistent with best practices.<sup>16</sup> 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).

The destruction of computer evidence is another monumental cyberliability problem, with several companies being battered with substantial criminal penalties and civil damages in recent cases. The business pages are replete 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. "One of the surest ways to lose a civil case," according to Manny Abascal, a Latham & Watkins partner and former US Department of Justice prosecutor, "is to delete relevant computer evidence. If such deletion does occur, the sooner it can be recovered, the better."

Rapid response to incidents of intentional or negligent destruction of computer evidence is a crucial capability for an incident response team. However, a 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 liability.

## **Conclusion**

Information security best practices are standards that evolve with the new technology that supports the field. It is not acceptable to use 10-year-old firewall appliances or out-of-date antivirus software. As network-enabled computer forensics software, such as EnCase Enterprise Edition, provides a long-overdue means for enterprises to very effectively, rapidly and without disrupting operations, respond to and investigate computer security breaches—an essential component of any security framework—it is incumbent upon enterprises to implement this technology as a matter of best practices and regulatory compliance.

## NOTES:

---

<sup>1</sup> John Patzakis, Esq. is President and CEO of Guidance Software

<sup>2</sup> InfoWorld, "Gartner names top security issues for 2003" March 25, 2003, quoting Gartner vice president Victor Wheatman.

<sup>3</sup> Council of Europe's Convention on Cybercrime, Explanatory Report, 298

<sup>4</sup> June 11, 2003 Gartner Information Security Report, see [www.gartner.com/5\\_about/press\\_releases/pr11june2003c.jsp](http://www.gartner.com/5_about/press_releases/pr11june2003c.jsp)

<sup>5</sup> According to the CSI/FBI 2003 Computer Crime and Security Survey, IP theft by insiders represented the greatest cost to organizations.

<sup>6</sup> The CSI/FBI 2003 Computer Crime and Security Survey ties the majority of computer security incidents to disgruntled employees and other malevolent insiders.

<sup>7</sup> 16 CFR Part 314.4(b)(3)

<sup>8</sup> 12 CFR Part 30, Appendix B, III(C)(g)

<sup>9</sup> 45 CFR Part 164.308(a)(6)

<sup>10</sup> ISO 17799, § 8.1.3. Note also that that the standard provides that security incidents should be reported to management as soon as possible, which requires a prompt assessment of the incident. *Id.*, § 6.3.1.

<sup>11</sup> *Id.*, § 12.1.7.3.

<sup>12</sup> The Basel Committee on Banking Supervision provides a forum for regular cooperation on banking supervisory matters. Established in 1974 by the governors of the G10 central banks (Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom and the United States), it serves as standard-setting body on all aspects of banking supervision. Members also include non-central bank supervisory authorities, and are mainly (but not exclusively) from G10 countries. It has its secretariat at the Bank for International Settlements ("BIS"), an organization that fosters international monetary and financial cooperation and serves as a bank for central banks. Established in 1930, it is the world's oldest international financial organization.

<sup>13</sup> Risk Management for Electronic Banking," Executive Summary, available at: [www.bis.org/publ/bcbs98.pdf](http://www.bis.org/publ/bcbs98.pdf), at note 3.

<sup>14</sup> *Id.*

<sup>15</sup> *Id.* at Appendix VI

<sup>16</sup> *Gates Rubber Co. v. Bando Chemical Indus., Ltd.*, 167 F.R.D. 90 (D.C. Col., 1996)