

## **2. Business Drivers for Creating an Incident Response Process and Conducting Digital Forensics Investigations**

### **ROI and Peace of Mind in Having an Incident Response Process in Place**

Today, global organizations rely on the Internet, VPNs, WANs and LANs to conduct their day-to-day business. Many global organizations rely on e-commerce to produce revenue.

Skeptics ask: why the need for the elaborate processes, and why spend money on building a program that does not contribute to the bottom line? The answer to this question is provided by a sample of activities that take place in the cyberenvironment, reinforcing the need to create a cyberresponse program to investigate cyberattacks and cyberfraud and conduct digital forensics evidence recovery and analysis.

In 2005, one in five enterprises is expected to experience a serious Internet security incident targeting information and intellectual property, Gartner analysts predict. Of all future attacks, nearly one in three will be financially or politically motivated, according to Richard Hunter, a Gartner vice president and research director. Cybercriminals are taking advantage of users, enterprises and unsecured systems to usher in high-profit, low-overhead crimes.

Incident response is a vital part of any successful IT program. It is frequently overlooked until a major security breach occurs, resulting in untold amounts of unnecessary time and money spent, not to mention the stress associated with responding to a crisis. Potential risks that could occur as a result of any cybercrime incident include:

- Threat to human life
- Financial loss
- Exposure to legal liability
- Loss of customer confidence
- Damage to organizational reputation
- Loss and unauthorized modification of data
- Threat to national security

A solid incident response program can save an organization a substantial amount of money and a significant degree of embarrassment. The following are generally cited as business drivers of implementing security programs to combat cybercrime,

thus enabling executive management to improve the ROI of implementing incident response programs and use digital forensics:

- **Reduced cost**—By management acknowledging the need to put in place preventive and detective measures to combat cybercrime, management can be assured that in the event of attacks, recovery measures are in place to contain the damage and minimize loss to an organization. Without security programs, time and money could be wasted in the recovery efforts.
- **Increased security**—By establishing an incident response team and implementing an incident response program, management can have the peace of mind that the enterprise's information assets are secure through incident response tools and techniques (described in more detail in the later chapters of this document).

When a professional incident response team is deployed for a problem, it can significantly reduce the monetary loss and embarrassment the organization could suffer. The team determines, usually in a short time, the answers to the following questions:

- Who are the potential intruders?
- What is the sensitivity of the compromised information?
- What is the level of unauthorized access obtained by the attacker?
- How long will the affected systems remain down?
- How critical are the affected systems to the organization?
- How widespread is the incident to the outside world?
- How quickly can the organization recover?

Edelman, a public relations firm, questioned more than 1,000 adults and found that 43 percent said they felt vulnerable on their home computers, while 17 percent felt they were vulnerable from viruses and hackers at work.

A recent survey by Rainbow Technologies Inc., a US security vendor, indicates that the use of insecure passwords can be costly—and potentially risky—for corporate data. According to the survey, based on responses from 3,000 IT administrators, executive managers and security professionals, the problem stems from the sheer number of inherently insecure usernames and passwords in use, along with the fact that many users write down their passwords.

The US loses approximately US \$5,000 per bank robbery every year. “But according to the recent reports, losses in cyberspace are approximately 100 times more,” said Joint Commissioner of Police (Crime) Satya Pal Singh about Cybersafety Week, quoted in the *Mumbai Newsline* on 6 August 2003 (<http://cities.expressindia.com/fullstory.php?newsid=59734>).

The following real-life examples are reasons why executives and management in an organization should implement a robust incident response program as well as a digital forensics investigative process. They illustrate the risks of:

- Additional funding required to fight attacks
- Denial of service
- Extra staff hours required to address attacks
- Improper evidence to prosecute attackers
- Liability for violation of privacy regulations
- Loss of customers
- Loss of data
- Loss of intellectual property
- Loss of reputation
- Loss of revenue
- Violation of classified information regulations

### ***Security Incidents Cost Companies Business***

On 5 May 2004, a study of more than 100 large UK companies and government agencies reported that enterprises that had experienced a security breach saw a 47 percent attrition rate in their business-to-business sector. The companies that did not take their business elsewhere spent slightly less with the company than they had previous to knowledge of the breach.

### ***Impact of the Sasser Worm***

The Sasser worm attacks sent IT staffs around the world scuttling to patch vulnerable Windows systems, dealing with network slowdowns and switching to old-fashioned paper to handle business.<sup>1</sup> Reports from around the world indicate that Sasser struck viciously at some locations, mildly at others. Although by the end of a week the Sasser worms had dramatically tailed off, the attacks took their toll worldwide, for example, in:

- The US, where the following were reported:
  - Major airline computer difficulties forced cancellation and delay of flights.
  - A credit card giant acknowledged infection of internal desktops.
  - A university cancer center had 6,000 Windows machines infected. Compared to the previous summer's network worm outbreak of MSBlast, it reported being much better organized this time around. However, employing 12 teams and 50 people to clean up infected systems and patch others was a significant diversion of IT resources. The suspected source of the infection was a laptop brought into the hospital and connected to its network. Unlike most worms, Sasser did not require human intervention—such as opening an e-mail attachment—but scanned for vulnerable systems and surreptitiously planted its payload.

---

<sup>1</sup> Keizer, Gregg; "Sasser Worm Impacted Businesses Around the World," *TechWeb News*, 7 May 2004

- A press association acknowledged network infection and sluggish Internet access as it cleaned infected systems and scanned for new infections on incoming PCs.
- Australia and New Zealand, where the following was reported:
  - Some major bank branches had to abandon their PCs and revert to pen and paper to complete transactions.
- Asia, where the following were reported:
  - The postal service had 1,600 computers infected, forcing about one-third of the branches to move to paper.
  - Government networks were infected.
  - A hospital experienced delays dealing with patients because the computer system had to be ditched for paper.
  - China largely escaped the Sasser worm because of a seven-day national holiday; however, Sasser made an impact on Chinese businesses and government agencies because patches were not deployed during the time off. The National Computer Network Emergency Response Coordination Center—China’s version of the US-based CERT—detected 1.3 million instances of the Sasser worm within China.
- Europe, where the following were reported:
  - A bank closed all 130 branches, with most closed for several hours.
  - The European Commission, the European Union’s executive arm, was affected.
  - A stock exchange was hit.
  - Maritime and coast guard agency networks were disrupted.

This is not the end of Sasser, according to security analysts. Even if another variant does not appear—unlikely, what with hackers habitually releasing worms—Sasser will remain part of the malicious code back chatter.

“Sasser will be with us for a long time to come,” said Alfred Huger, senior director of engineering with Symantec’s response team.

### ***Failure to Deploy Proper Audit Trails<sup>2</sup>***

According to Roy Hills, technical director at NTA Monitors, “Most companies would not be able to supply the evidence needed to secure convictions, meaning criminals will get off scot-free despite any change in law.”

Few companies have the proper audit trails in place to get convictions against hackers. NTA monitors claims that its research shows inadequate log file maintenance, such as:

- Not switching logs on—The reasons are generally because traffic gets monitored elsewhere and it uses up too much disk space.

---

<sup>2</sup> Jaques, Robert; “Poor Evidence Taking Lets Off Hackers: Firms Failing to Deploy Proper Audit Trails, Warns Security Study,” *vnumet.com*, 4 May 2004

- Not keeping the records long enough—If log files are overwritten every 30 minutes there is no record of what had happened in case of an attack. Improper logging stores the information on public folders that hackers can access and alter easily to cover their tracks.
- Forgetting time synchronization—A serious incident is likely to involve several different systems, but companies cannot piece together what has happened if they are unable to track one log to another.

### ***Theft of Personal Information***<sup>3</sup>

US federal authorities recently charged an online advertiser with tapping into the computer system of a large database marketer and stealing “vast amounts of personal information” in what they described as one of the largest network intrusions in recent memory. Federal prosecutors charged the owner of an e-mail company with exploiting network links his company used to secretly download millions of names, e-mail and home addresses and other details from one of the world’s largest data aggregators.

The data aggregator has information about virtually every adult in America and manages and enhances data for major banks, insurers, direct marketers, credit bureaus and others. It developed some of the world’s most sophisticated data analysis software, some of which it uses for homeland security screening for government contracts. Among other details, the company keeps records on an individual’s home, work, cars, estimated income and children at home.

“We are committed to safeguarding our systems and the data that we store and manage on behalf of our clients,” the company said in a statement.

The indictment said that the advertiser gained access to the data aggregator’s computers by misusing a legitimate password and username while working for a company doing business with the aggregator. US Justice Department officials said they wanted to draw attention to the seriousness of computer security.

“The protection of personal information stored on our nation’s computer systems is critical to public trust in those networks and to the health of our economy,” said Christopher Wray, assistant attorney general of the Justice Department’s criminal division. “We will aggressively pursue those who steal private information from computer networks and make it clear there are serious consequences for such crimes.”

---

<sup>3</sup> O’Harrow, Jr., Robert; “Advertiser Charged in Massive Database Theft,” *Washington Post*, 22 July 2004

### ***Hiring E-mail Readers***

According to research from Forrester Consulting, 44 percent of large corporations in the US now pay someone to monitor and snoop on the company's outgoing e-mail, with 48 percent regularly auditing e-mail content.<sup>4</sup> Companies are employing staff to read electronic communications because of:

- Fear that employees are leaking confidential memos and other sensitive information, such as intellectual property or trade secrets
- Concern about inappropriate content and attachments to e-mails
- The possibility that e-mail is not up to compliance standards set by Sarbanes-Oxley and other legislation
- Basel II and similar financial services compliance targets. A survey of UK financial institutions found that approximately half would be unable to find an e-mail more than three years old; storing e-mail is a key demand of the new legislation.

### ***E-mail Security Problems***

The Los Alamos National Laboratory develops and applies technology to ensure the safety and reliability of US nuclear deterrent systems and reduce the threat of weapons of mass destruction and terrorism. The lab also performs research aimed at solving national problems in defense, energy and the environment. Incidents reported to the US Department of Energy and other agencies, as required by law include:<sup>5</sup>

- Workers at the facility sent out classified e-mails over an unsecure e-mail system. Scientists in the lab incorrectly judged information as being unclassified and sent it without asking for assistance about the contents of their e-mails.
- Two removable computer disks containing classified nuclear weapons data were reported missing. That incident represents at least the third time since 2000 that storage media containing classified information have been lost in the facility.

The lab suspended all activities during the investigation into the missing computer disks and the suspension continued until officials there believed the security problems were corrected. All classified activities were suspended after the disks were reported missing. Some reviews were completed quickly, while those for high-risk activities took several days or even weeks.

---

<sup>4</sup> Best, Jo; "Corporates Hiring People to Read Staff E-mail," silicon.com, 22 July 2004

<sup>5</sup> Weiss, Todd R.; "E-mail Security Problems Reported at Los Alamos National Lab: It is the Second Major Security Issue to Arise There in Recent Days," *Computerworld*, 20 July 2004

## ***Viruses in E-mail Inboxes***

A new strain of one of the most virulent e-mail viruses spread quickly worldwide, causing fresh annoyance to users worn out by the outbreak of the Blaster worm.<sup>6</sup> The virus, named Sobig.F by computer security companies, attacked Windows users via e-mail and file-sharing networks. It also deposited a Trojan horse, or hacker back door, that could be used to turn victims' PCs into senders of spam e-mail. A company that filters e-mail for corporations captured more than 100,000 copies of Sobig.F, making it by far the most active virus of the day.

A virus-like infection that plagued computers in the US was evident in Europe and Asia as thousands of users in several countries reported disruptions. Experts said the number was likely to increase. Security officials said the infection, dubbed LovSan, forced thousands of computers to restart and was part of a coordinated electronic attack against Microsoft Corp.

In Sweden, Internet provider TeliaSonera said approximately 20,000 of its customers were unable to log on to the Internet overnight after the infection clogged 40 servers that handled Internet traffic. Filters were installed to restore service. Internet security company F-secure said about 900 computers in Sweden were infected by the LovSan virus.

The infection worked by exploiting a flaw in Windows software. A malicious worm exploited the RPC DCOM vulnerability, targeting unpatched Windows 2000 and Windows XP machines. The worm attacked vulnerable machines over TCP port 135, then spawned a shell and initiated a TFTP file transfer to retrieve the worm's code.

It was first discovered in the US. Infected computers were programmed to automatically launch an attack on a web site operated by Microsoft. The site, *windowsupdate.com*, is used to deliver repairing software patches to Microsoft customers to prevent against these types of infections. Microsoft posted a free patch on the web site to protect Windows users. Government and industry experts had anticipated such an outbreak when Microsoft acknowledged that the flaw affected nearly all versions of its flagship Windows operating system software. Warnings apparently did not work, despite the high-profile alerts issued by Redmond, Washington, USA-based Microsoft.

## ***Worm Strains on the Internet***

The US Department of Homeland Security (DHS) released an advisory warning users that a variant of the Blaster worm, dubbed Nachi, Welchia or Msblast.D, could cause denial-of-service conditions within organizations. This computer virus, designed to inoculate against another infection, brought down some computer

---

<sup>6</sup> High Tech Crimes Investigation Association (HTCIA) web site posting, [www.htcia.org](http://www.htcia.org)

networks, forcing an airline in Canada to check in passengers manually. Long lines formed at counters as the virus slowed the airline's computer system. The virus of the self-spreading kind, known as a worm, affected the airline's call center and check-in systems. The worm broke into Windows-based computers to try to delete any trace of the Blaster worm infection, and then downloaded the patch Microsoft developed to fix the vulnerability that Blaster exploited. A new variant of the Sobig worm, dubbed W32/Sobig.F, also spread rapidly via e-mail and network shares.

US Internet users were warned by Microsoft of a new virus attack. The new worm, MSBlast, infected at least 7,000 computers in a matter of hours, according to Symantec. Still, security experts said the spread was slowed because the virus program had several flaws.

The Slammer worm penetrated a private computer network at a US nuclear power plant and disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall. The breach did not post a safety hazard. The troubled plant had been offline since February 2002, when workers discovered a 6-by-5-inch hole in the plant's reactor head. Moreover, the monitoring system, called a Safety Parameter Display System, had a redundant analog backup that was unaffected by the worm.

Numerous computer worms penetrated computer networks in New Zealand and forced companies to enact emergency backup procedures. A TV station, including its online service, was attacked and noncritical staff were sent home to prevent further infection. The global attack raised alarms at a computer security company, which said it had already received infection notices from Japan, Taiwan and Singapore.

Knowing previous worms were capable of shutting down any infected computer, Microsoft warned that new worms could be much worse. "People could take the existing worm and they could modify it so that it could do things that are much more violent to your machine...they could delete data or take that data and information and spread it to someone else," said Terry Allen of Microsoft New Zealand.

Another computer worm is spreading through a security hole in Microsoft Windows but, unlike the original Blaster worm, the new worm is patching the security hole. However, it is also bogging down network systems. Meanwhile, Microsoft said it received thousands of calls for help a day from those infected with the Blaster worm, which causes the infected computers to shut down. In one week Blaster infected half a million computers worldwide. Microsoft said all computers are at risk unless they have a firewall, the latest software update and the latest virus checking software.