

Recovery After a Breach in Network Security

The third in a series entitled *Network Security Investment—The Executive ROI Briefcase*, this white paper discusses best practices for disaster recovery that involve information security and IT professionals, as well as law enforcement.

Other white papers in the series include:

- **Economic Impact of Network Security Threats**

This white paper describes the dynamics in today's business climate that are driving network security requirements, and provides an understanding of the threats facing business leaders today.

- **Privacy Protection Depends on Network Security**

This white paper reviews some of the laws that mandate consumer privacy protection and how network security helps ensure data privacy.

- **The Return on Investment for Network Security**

This white paper quantifies the value of network security with regard to the economic consequences of a security breach.

- **Action Steps for Improving Information Security**

This white paper describes the steps you should take to ensure a secure network infrastructure.

Executive Summary

When a breach in network security occurs, an organization enters into an incident response process. The goal of the process is to confirm the security breach and accumulate accurate information about the incident. A good incident response process will minimize disruption to business operations. Three teams of people will generally be involved in the incident response process:

- In-house information systems security staff
- IT staff responsible for network systems operation and maintenance
- Law enforcement officers

When computer systems are hacked or intruded upon by an unauthorized party, the U.S. Federal Bureau of Investigation (FBI) and the National Infrastructure Protection Center (NIPC) recommend that the following actions:

- Respond quickly. Contact law enforcement. Traces are often impossible if too much time is wasted before alerting law enforcement or an internal incident response team. In most cases contacting the FBI is necessary.
- If unsure of what actions to take, DO NOT stop system processes or tamper with files. This may destroy traces of intrusion.

- Follow organizational policies and procedures as documented. (Your organization should have a computer incident response capability and plan in place.)
- Use the telephone to communicate. Attackers may be capable of monitoring e-mail traffic.
- Contact the incident response team for your organization. (Quick technical expertise is crucial in preventing further damage and protecting potential evidence.)
- Establish points of contact with general counsel, emergency response staff, and law enforcement. Pre-established contacts will help in a quick response effort.
- Make copies of files an intruder may have altered or left. Copying files may assist investigators in determining when and how the intrusion occurred.
- Identify a primary point of contact to handle potential evidence. Establish chain-of-custody of evidence and identify which individuals will be involved to assure that evidence is handled properly. Potential hardware and software evidence that is not properly controlled may lose its value.
- DO NOT contact the suspected perpetrator.

Information Systems' Security Response to Intrusions

The information systems security staff will take several steps after an intrusion has occurred. These steps are designed to determine how the incident occurred and to reduce or eliminate the possibility of the same tactics being used again to intrude into an organization's systems:

- Conduct an initial investigation of the incident to determine the scope of damage
- Collect or assemble readily available evidence
- Evaluate system logs and attempt to identify how the attacker entered and from where the attack occurred
- Prepare for law enforcement to enter and conduct structured forensic studies for examining evidence
- Determine if other systems in the organization are vulnerable to the same method of attack
- Formulate recommendations for security upgrades or changes
- Devise new security procedures if necessary
- Report to IT managers steps they should take with similar systems

The IT Response to Intrusions

The IT personnel who are responsible for keeping systems operating efficiently will take several steps after an intrusion has occurred. These most often occur after systems security personnel or law enforcement officers have completed their work. In the event that the investigations take many days to accomplish, IT personnel will install and configure a replacement machine. To restore network equipment, servers, and client hardware IT staff will take the following steps:

- Inspect systems to determine damage
- Remove hostile or destructive code
- Reload necessary operating system software
- Restore configurations
- Restore and test operations
- Patch system to reduce vulnerability
- Inspect applications to determine damage
- Reload software if necessary
- Test functionality
- Inspect files to determine damage
- Restore files from backup if necessary
- Replicate damaged files when no backup is available
- Confirm with users that data is restored

The Law Enforcement Response to Intrusions

The FBI has greatly improved its computer crime investigation skills over the last decade. If called, the FBI, or national law enforcement organizations in other countries, will conduct a thorough and structured investigation to gather evidence necessary to identify and prosecute the perpetrators. Information that law enforcement investigators will find helpful includes the following:

- Date, time, and duration of incident
- The name, title, telephone number, fax number, and e-mail address of the point of contact for law enforcement, as well as the organization name, address, city, state, zip code, and country
- The physical locations of computer systems and/or networks that have been compromised
- Whether the systems are managed in-house, or by a contractor or a managed service provider
- Whether the affected systems or networks are critical to the organization's mission
- The nature of the problem, which could include intrusion, system impairment, denial of resources, unauthorized root access, Web site defacement, compromise of system integrity, theft, or damage
- Whether the problem had been experienced before
- The suspected method of intrusion or attack that could include a virus, exploited vulnerability, denial of service, distributed denial of service, trapdoor, or Trojan horse
- The suspected perpetrators and the possible motivations of the attack that could include an insider or disgruntled employee, former employee, or competitor
- Whether the suspect is an employee or former employee; if so, determine and report the type of system access that the employee has or had
- The apparent source (IP address) of the intrusion or attack, if known, and if there is any evidence of spoofing
- What computer system (hardware, operating system, or applications software) was affected
- What security infrastructure was in place, this could include an incident response team, encryption, firewall, secure remote access or authorization tools, intrusion detection system, security auditing tools, access control lists, or packet filtering
- If the intrusion or attack resulted in a loss or compromise of sensitive, classified, or proprietary information
- If the intrusion or attack resulted in damage to systems or data
- What actions to mitigate the intrusion or attack have been taken, which could include the system being disconnected from the network, system binaries checked, backup of affected systems, or log files examined
- What agencies have been contacted, which could include state or local police, the Computer Emergency Response Team (CERT) or national equivalent in other countries
- The last time the system was modified or updated, and the name of the company or organization that did the work, including address, phone number, and other point of contact information

Information to Determine Damages or Loss

- It may also be necessary for an organization to determine a dollar value of damage, business loss, and cost to restore systems to normal operating conditions. The following information is helpful in determining dollar amounts:
- In the event that a contractor performed repairs or recovery, determine the charges incurred for services
- If in-house staff were involved in determining extent of the damage, repairing systems or data, and restoring systems to normal operating conditions, then determine the number of hours staff expended to accomplish these tasks and the hourly wages, benefits, and overhead associated with each employee involved in the recovery
- If business was disrupted in some way, then determine the number of transactions or sales that were actually disrupted and the associated dollar value. (If systems were impaired to the point that actual disrupted transactions or sales cannot be determined, then determine the dollar value of transactions or sales that occur on a comparable day for the duration of the system outage)
- If systems are used to produce goods, deliver services, or manage operations, then determine the value of that disruption. (Calculations from similar experiences—for example, if operations were disrupted because of inclement weather, fires, earthquakes, or other disruptive incidents—may help in this effort)
- If systems were physically damaged, then determine what was paid to acquire and install the systems

- If systems were stolen, then determine the cost to acquire and install the systems and the cost of actions taken to assure that information on the stolen systems cannot be used to access systems
- If intellectual property or trade secrets were stolen, then determine the value of that property
- If a competitor or other party used intellectual property or trade secrets, then determine the impact on business revenue or other financial measures

These steps, used in concert with each other, can help identify a perpetrator of a security breach and possibly recoup any dollars lost in restoring business to secure, working order.

Summary

A breach in security can have devastating effects on a company's business processes, and can have legal ramifications. Malicious attacks can also have financial costs, including loss of revenue and an incredible negative impact on productivity. With a secure foundation for information sharing, you can increase your revenue through e-business and benefit from an increase in the productivity of your employees. Learn about the value of network security with regard to the economic consequences of a security breach through the fourth white paper in this series, *The Return on Investment for Network Security*.

Other white papers in the series include:

- **Economic Impact of Network Security Threats**

This white paper describes the dynamics in today's business climate that are driving network security requirements, and provides an understanding of the threats facing business leaders today.

- **Privacy Protection Depends on Network Security**

This white paper reviews some of the laws that mandate consumer privacy protection and how network security helps ensure data privacy.

- **Action Steps for Improving Information Security**

This white paper describes the steps you should take to ensure a secure network infrastructure.

You can find these papers, design and implementation guides, and case studies that demonstrate how other companies implemented security and VPN solutions over a secure network to expand connectivity and reduce costs at <http://www.cisco.com/go/security>.

About Computer Economics' Methodology

Independent research firm Computer Economics has collected and analyzed data on the impact of malicious code attacks, hacking and intrusion incidents, and the cost of system downtime for several years. Much of this work dates back as far as the early 1990s. The analysis of malicious code attacks intensified in the late 1990s as major virus incidents such as Melissa, I Love You, Code Red, and Nimda became commonplace.

- The research has largely been client-driven. When Computer Economics' clients needed to determine the ROI for security and virus protection, an in-depth research process was initiated. Data collection is ongoing and involves the following:
 - Reviewing numerous statistical reports and studies on computer crime and malicious attacks of all sorts
 - Collecting data on the economic aspects of malicious attacks
 - Benchmarking cleanup and recovery costs from major incidents
 - Benchmarking the impact on productivity that attacks have on different types of organizations
 - Benchmarking lost revenue from downtime
- Monitoring the activity reports of security companies, including the frequency of different types of attacks and the recurrence of virus activity
- Conducting ongoing surveys of IT spending, security practices, and the cost of malicious attacks

The economic impact analysis and models that Computer Economics creates are based on numerous research efforts over a period of several years. Data has been obtained from more than 2000 organizations from virtually every industry sector and every major industrial country around the world.

The analyst teams for these projects have been led by Michael Erbschloe, vice president of research for Computer Economics of Carlsbad, California. Mr. Erbschloe is the author of *Information Warfare: How to Survive Cyber Attacks* and *The Executive's Guide to Privacy Management*. He also coauthored *Net Privacy: A Guide to Developing & Implementing an Ironclad ebusiness Privacy Plan*. In addition, he has presented at professional conferences around the world.



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: 65 317 7777
Fax: 65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and EtherChannel are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)