

# Action Steps for Improving Information Security

The last in a series entitled *Network Security Investment—The Executive ROI Briefcase*, this white paper describes the steps you should take to ensure a secure network infrastructure.

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.

- **Recovery After a Breach in Network Security**

This white paper discusses best practices for disaster recover that involve information security and IT professionals, as well as law enforcement.

- **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.

## Introduction

Your organization can take several steps toward building more secure networks and information systems. It is important to start with a firm foundation which senior-level managers, IT staff, and employees throughout the organization understand and support. This may require the appointment of a chief security officer (CSO) or a chief privacy officer (CPO). Next, you must approach technology in an organized, systematic way to assure that the technology you install is secured. It is advisable to conduct vulnerability audits. Lastly, you can participate with other organizations in your community to help prevent or thwart computer crime. Other white papers in this series have outlined the many risks and threats that exist and threaten network security. Independent research firm, Computer Economics recommends the following steps for developing a plan for improving network security.

## Developing a Solid Foundation

Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. Managers analyze risks for many aspects of their business; they consider alternatives and implement plans to maximize returns on their investments. A risk management process for information systems enables managers and their organizations to develop in-depth knowledge about their systems.

A comprehensive risk analysis also can become a guide for achieving organizational network security goals. It is advisable to look at alternatives for services and products. Depending on your organization, it may be more cost-effective and convenient to contract for managed security services, or it may be critical to keep certain aspects of security planning and management in-house. In dealing with any IT functions or applications it is key that appropriate skill levels are attained. This may necessitate contracting for managed security services to achieve all security requirements.

For many years, the United States General Accounting Office (GAO) found weaknesses in the information systems of federal agencies. Many agencies had not instituted information security programs to establish controls for their systems and to monitor those controls for their effectiveness. To gain a broader understanding of successful security programs, the GAO studied the management practices of eight nonfederal organizations. The focus was on the management framework that the organizations had established rather than on specific controls that had been adopted.

The nonfederal organizations studied by the GAO manage the same types of risks as federal organizations. Both federal and nonfederal organizations are concerned with protecting the confidentiality, integrity, and availability of information. Secure information systems are essential to providing high-quality services to customers, avoiding fraud and disclosure of sensitive information, promoting efficient business operations, and complying with laws and regulations. All of the organizations studied had reoriented their network security programs to make them visible, integral components of their business operations.

The GAO identified five principles of risk management, which had been adopted by the organizations studied:

1. Assess risk and determine needs
2. Establish a central management focus
3. Implement appropriate policies and related controls
4. Promote awareness
5. Monitor and evaluate policy and control effectiveness

The GAO noted that successful organizations applied these principles by linking them into a cycle of activity that enabled the organizations to address risks on an ongoing basis. The success of security programs depended upon the recognition and understanding by the senior executives that their information systems were subject to risks and that these risks affected their business operations. After assessing risks of their business operations, the organizations established policies and selected controls. They emphasized increased awareness of users to the policies and controls. They monitored the effectiveness of the policies and controls and used the results to determine if modifications of policies and controls were needed. Central security management offices coordinated this cycle of activities.

All organizations studied said that risk considerations and related cost-benefit tradeoffs were a primary focus of their security programs. Security was not an end in itself, but a set of policies and controls designed to support business operations.

The GAO found that there were general practices associated with each risk management principle and that these practices were common to the organizations studied. Below are the risk management principles and the practices associated with each.

Principle: Assess risks and determine needs

**Practice 1.** Recognize information resources as essential organizational assets that must be protected. In the GAO study, the efforts of high-level executives to understand and manage risks helped to ensure that network security was taken seriously at lower levels in the organization and that security programs had adequate resources. Security specialists kept managers at all levels informed of emerging security issues. For some organizations, the high-level interest was driven by an incident that demonstrated system vulnerabilities. Some organizations were exploring new ways to improve operational efficiency and services to customers through information technology and were concerned about the security of these new systems.

**Practice 2.** Develop practical risk assessment procedures that link network security to business needs. While the organizations explored a variety of risk management methodologies, they were generally satisfied with relatively simple risk assessment practices that could be adopted by different organizational units and that involved both technical people and those with knowledge of business operations. In one organization, simple automated checklists were used. Another organization established standard procedures for requesting and granting new network connections, requiring documentation of the business need for the connection and the risks associated with it. None of the organizations tried to quantify the risks precisely because of the difficulty of identifying such data.

Computer Economics contends that in just the few short years since these principles were established, circumstances have indeed changed. CTOs are under considerably more pressure to establish what the potential ROI is for almost any expenditure. Other papers in this series help the upper-level managers understand how to determine that ROI.

**Practice 3.** Make program and business managers accountable. The organizations studied felt that business managers should be held accountable for managing the information security risks associated with their operations, just as they are held accountable for other business risks. Security specialists in these organizations had an advisory role, including keeping the management informed about risks. Similarly, program managers in federal agencies are also considered to be in the best position to determine which of their information resources are the most sensitive and to assess the impact of security problems.

**Practice 4.** Manage risk on a continuing basis. The organizations studied understood that network security is a constant process, and emphasized continuous attention to security. The continuity of attention helped to ensure that controls are appropriate and effective, and that individuals who used and maintained information systems complied with the organizational policies.

Principle: Establish a central management focus

**Practice 5.** Designate a central group to carry out key activities. Central network security groups served as catalysts for ensuring that information security risks were considered in planned and ongoing operations. These groups provided advice and expertise to all organizational levels and kept managers informed about security issues. They developed organization-wide policies and guidance; educated users about information security risks; researched potential threats, vulnerabilities, and control techniques; tested controls; assessed risks; and identified needed policies.

**Practice 6.** Provide the central group with ready and independent access to senior executives. The organizations studied knew that security concerns could be at odds with the desires of business managers and system developers to develop new computer applications quickly and to avoid controls that might impede efficiency and convenience. Elevating security concerns to higher management levels helped to ensure that the risks were understood and taken into account when decisions were made.

**Practice 7.** Designate dedicated funding and staff. Unlike many federal agencies, the organizations studied defined budgets that enabled them to plan and set goals for information security programs. The budgets covered central staff salaries, training, and security software and hardware. In these organizations, information security responsibilities had been clearly defined for the groups carrying out the security programs, and dedicated staff resources had been provided to carry out these responsibilities.

**Practice 8.** Enhance staff professionalism and technical skills. The organizations studied had taken steps to provide personnel involved in information security programs with the skills and knowledge that they needed. Staff expertise was updated frequently to keep skills and knowledge current. Staff members attended technical conferences and specialized courses, connected with other professionals in the field, and reviewed technical literature and bulletins. Special training courses were provided for system administrators who were the first line of defense against security intrusions and often in the best position to notice unusual activities. Because of the strong demand for security professionals, these organizations made special efforts to attract and keep expert staff members.

Principle: Implement appropriate policies and related controls

**Practice 9.** Link policies to business risks. The organizations studied stressed the importance of current policies that made sense to users and others who were expected to understand them. A current and comprehensive set of policies is a key element in an effective security program. These policies must be adjusted on a continuing basis to respond to newly identified risks. The policies of the organizations studied paid particular attention to user behavior. In today's interconnected network environment, users can accidentally disclose sensitive information to many people through e-mail or introduce damaging viruses that are then transmitted to other computers in the organization's networks.

**Practice 10.** Distinguish between policies and guidelines. Policies generally outlined fundamental requirements that managers considered mandatory, while guidelines contained more detailed rules for implementing the policies. By distinguishing between the two, the organizations studied were able to emphasize the most important elements of information security while providing flexibility to unit managers in implementing policies.

**Practice 11.** Support policies through the central security group. The organizations studied had central security management groups responsible for writing policies in partnership with other organizational officials. The central groups provided explanations, guidance, and support to the various units in the organization. This practice encouraged business managers to support centrally developed policies that addressed organizational needs and were practical to implement.

Principle: Promote awareness

**Practice 12.** Continually educate users and others on risks and related policies. The central security management groups worked to improve everyone's understanding of the risks associated with information systems and of the policies and controls in place. They encouraged compliance with policies and awareness on the part of users of the risks involved in disclosing sensitive information or passwords.

**Practice 13.** Use attention-getting and user-friendly techniques. The techniques used included intranet Web sites that explained policies, standards, procedures, alerts and special notices; awareness videos with messages from top managers about the security program; interactive presentations by security staff with various user groups; security awareness days; and products with security related slogans.

Principle: Monitor and evaluate policy and control effectiveness

**Practice 14.** Monitor factors that affect risk and indicate security effectiveness. The organizations studied directly tested the effectiveness of their controls. Most of the organizations relied primarily on auditors to carry out this function, enabling the security organizations to maintain their roles as advisors. The central security management groups kept track of audit findings and the organization's progress in implementing corrective actions. In some cases, the central security management groups conducted their own tests, and some organizations allowed designated individuals to try to penetrate systems. The testing of controls enabled the organizations to identify unknown vulnerabilities and to eliminate or reduce them. All of the organizations monitored compliance with policies, mostly through informal feedback to the central security group from system administrators. All of the organizations kept summary records of actual security incidents to measure the types of violations and the damage suffered from the incidents. The records were valuable input for risk assessments and budget decisions. Many of the organizations expressed an interest in developing better techniques to measure the benefits and costs of security policies and controls.

**Practice 15.** Use results to direct future efforts and hold managers accountable. Organization officials said that monitoring encourages compliance with information security policies, but the full benefits of monitoring are not achieved unless results are used to improve the security program. Results can be used to hold managers accountable for their information security responsibilities.

**Practice 16.** Be alert to new monitoring tools and techniques. Security managers of the organizations studied said that they continually looked for new tools to test the security of their systems. They found current professional literature and involvement with professional organizations useful in learning about the latest monitoring tools and research efforts.

The SAFE Blueprint for Secure e-Business: Cisco's Security Architecture

Fighting back against security violators requires that you develop policies and procedures. The first step in any security plan is to instill an awareness of the vulnerability in all users of computer systems. If your organization does not employ security experts, bring in an outside consultant. Be prepared to respond to the consultant's recommendations, but keep in mind that even with the best of consultants, a security breach is inevitable. Your organization should be prepared to respond to a security attack.

The principle goal of the SAFE Blueprint for Secure e-Business is to provide best practice information to interested parties on designing and implementing secure networks. SAFE serves as a guide to network designers considering the security requirements of their network, taking a defense-in-depth approach to network security design. This type of design focuses on the expected threats and methods of mitigation, rather than on "Put the firewall here, put the intrusion detection system there." The SAFE strategy results in a layered approach to security where the failure of one security system is not likely to lead to the compromise of network resources. While the SAFE Blueprint comes to you from Cisco Systems, it can be based on Cisco products and those of its partners, or on products from other vendors.

The SAFE architecture is not a revolutionary way of designing networks, but merely a blueprint for making networks secure. As the security architecture for AVVID, the SAFE Blueprint emulates as closely as possible the functional requirements of enterprise networks.

Implementation decisions vary, depending on the network functionality required. However, the following design objectives, listed in order of priority, guided the SAFE development process:

- Security and attack mitigation based on policy
- Security implementation throughout the infrastructure (not just on specialized security devices)
- Secure management and reporting
- Authentication and authorization of users and administrators to critical network resources
- Intrusion detection for critical resources and subnets
- Support for emerging networked applications

SAFE is a network security architecture. It must prevent most attacks from successfully affecting valuable network resources. The attacks that succeed in penetrating the first line of defense, or originate from inside the network, must be accurately detected and quickly contained to minimize their effect on the rest of the network. However, in being secure, the network must continue to provide critical services that users expect. Proper network security and good network functionality can be provided at the same time.

SAFE is also resilient and scalable. Resilience in networks includes physical redundancy to protect against a device failure whether through improper configuration, physical failure, or network attack. Although simpler designs are possible, particularly if a network's performance needs are not great, SAFE uses a complex design as an example because designing security in a complex environment is more involved than in simpler environments.

At many points in the network design process, you need to choose between using integrated functionality in a network device and using a specialized functional appliance. The integrated functionality is often attractive because you can implement it on existing equipment, or because the features can interoperate with the rest of the device to provide a better functional solution. Appliances are often used when the depth of functionality required is very advanced or when performance needs require using specialized hardware. Make your decisions based on the capacity and functionality of the appliance versus the integration advantage of the device.

For example, sometimes you can choose an integrated higher-capacity Cisco IOS<sup>®</sup> router with Cisco IOS Firewall software as opposed to a smaller Cisco IOS router with a separate firewall. Throughout this architecture, both types of systems are used. Most critical security functions migrate to dedicated appliances because of the performance requirements of large enterprise networks.

Although most enterprise networks evolve with the growing IT requirements of the enterprise, the SAFE architecture uses a green-field modular approach. A modular approach has two main advantages. First, it allows the architecture to address the security relationship between the various functional blocks of the network. Second, it permits designers to evaluate and implement security on a module-by-module basis, instead of attempting the complete architecture in a single phase.

## The VPN as a Secure Environment

One of the most popular approaches to establishing a secure computing and network environment is the virtual private network (VPN). VPNs enable organizations to use Internet transport to connect remote offices and remote users to the main corporate site, thus eliminating expensive dedicated WAN links and modem banks. Furthermore, with the advent of cost-effective, high-bandwidth technologies like DSL, organizations can use VPNs to reduce their connectivity costs while simultaneously increasing remote connection bandwidth. The Cisco VPN 3000 Series Concentrator is primarily designed for deploying remote-access solutions.

Site-to-site VPNs are an alternative WAN infrastructure that are used to connect branch offices, home offices, or business partners' sites to all or portions of a company's network. VPNs do not inherently change private WAN requirements, such as support for multiple protocols, high reliability, and extensive scalability—but instead meet these requirements more cost-effectively and with greater flexibility. VPNs constructed using Cisco VPN routers and Cisco IOS Software provide a comprehensive feature set to meet diverse networking requirements, including support for routing, multiprotocol, and multicast across the VPN, as well as enhanced features like firewall and quality of service (QoS).

Cisco Easy VPN, a software enhancement for existing Cisco routers and security appliances, simplifies deployment for remote offices and teleworkers. The Cisco Easy VPN Remote feature allows Cisco IOS Software routers, Cisco PIX<sup>®</sup> Firewalls, and Cisco VPN 3002 hardware clients or software clients to act as remote VPN clients. As such, these devices can receive security policies from a Cisco Easy VPN Server, thus minimizing VPN configuration requirements at the remote location.

This feature makes VPN configuration as easy as entering a password, increasing productivity and lowering costs as the need for local IT support is minimized. In addition, a Cisco Easy VPN Server-enabled device can terminate VPN tunnels initiated by mobile remote workers running Cisco VPN client software on PCs. This flexibility makes it possible for mobile and remote workers, such as salespeople on the road or teleworkers, to access their headquarters intranet where critical data and applications exist.

Designed for organizations with many remote office environments, the Cisco VPN 3002 hardware client combines the ease of use and high scalability features of a software client while providing the reliability and stability of a hardware platform. The Cisco VPN 3002 client supports Easy VPN Remote, allowing it to connect to any Easy VPN server site concentrator. The VPN 3002 hardware client works with any operating system, including Solaris, Macintosh, and Linux. It supports 56-bit Data Encryption Standard (DES), 168-bit Triple DES (3DES), 128/256-bit Advanced Encryption Standard (AES), or IP Security (IPSec).

## Managed Security Services

The managed security services initiative is a comprehensive set of programs that enhance service providers' abilities to meet growing enterprise customer demands. As corporations embrace e-business strategy, concern about Internet security implications and the deployment and management of security and VPN solutions require a highly skilled technical staff and sufficient time to implement a focused and disciplined approach. In today's fast paced world of information technology, these can be scarce or non-existent resources. Consequently, many organizations are exploring outsourced solutions for all or part of their security infrastructures.

Fortunately, an increasing number of service providers are offering managed security services to enterprise customers based on Cisco solutions that include managed firewall, VPN (network-based and premises-based), and managed intrusion detection systems (IDSs). Cisco security solutions and technologies offer a competitive differential advantage by allowing the end customer to migrate to a new deployment model, while preserving their confidence with a trusted solution set. This is especially important as many enterprises increase their dependency on managed services, and move from pilot phase to broad deployment.

## Security Policy Management

As networks grow in size and complexity, the requirement for centralized security policy management tools that can administer security elements is paramount. Sophisticated tools that can specify, manage, and audit the state of security policy through browser-based user interfaces enhance the usability and effectiveness of network security solutions. Cisco provides a centralized, policy-based, security management approach for the enterprise.

CiscoWorks VPN/Security Management Solution (VMS), an integral part of the SAFE Blueprint, combines Web-based tools for configuring, monitoring and troubleshooting enterprise Virtual Private Networks (VPNs), firewalls, and network and host-based intrusion detection systems (IDS).

CiscoWorks VMS includes the following modules:

- Management and Monitoring Centers
  - Management Center for PIX Firewalls
  - Management Center for IDS Sensors
  - Management Center for VPN Routers
  - Monitoring Center for Security
  - Auto Update Server
  - Common Services
- *Cisco Secure Policy Manager*
- *Cisco IDS Host Sensor*

- *VPN Monitor*
- *Resource Manager Essentials (RME)*
- *CiscoView (CD One)*

VMS delivers the industry's first robust, scalable architecture and feature set that addresses the needs of small and large-scale VPN and security deployments.

## Antivirus Packages

Virus protection software is packaged with most computers and can counter most virus threats if the software is regularly updated and correctly maintained. The antivirus industry relies on a vast network of users to provide early warnings of new viruses, so that antidotes can be developed and distributed quickly. With thousands of new viruses being generated every month, it is essential that the virus database be kept up to date. The virus database is the record held by the antivirus package that helps it to identify known viruses when they attempt to strike. Reputable antivirus software vendors will publish the latest antidotes on their Web sites, and the software can prompt users to periodically collect new data. Network security policy should stipulate that all computers on the network are kept up to date and, ideally, are all protected by the same antivirus package—if only to keep maintenance and update costs to a minimum. It is also essential to update the software itself on a regular basis. Virus authors often make getting past the antivirus packages their first priority.

## Intrusion Detection

Organizations continue to deploy firewalls as the central gatekeepers to prevent unauthorized users from entering their networks. However, network security is in many ways similar to physical security in that no one technology serves all needs—rather, a layered defense provides the best results. Organizations are increasingly looking to additional security technologies to counter the risk and vulnerability that firewalls alone cannot address. A network-based IDS (NIDS) provides around-the-clock network surveillance while a host-based IDS (HIDS) protects servers.

Given the complexity of an enterprise site, the variety of attack techniques, and the typical hacking scenario, there is a clear need for a comprehensive solution. The solution should protect against the different attack techniques and prevent the malicious actions performed during a typical hacking cycle. The Cisco IDS solution addresses this need by offering a combined solution that includes NIDS and HIDS components. The NIDS primarily addresses the network attacks, whereas the HIDS protects the servers against OS and application attacks.

The NIDS sensors are installed in multiple locations. One important location is in front of the firewall that monitors communication coming into the organization. In addition, every important network segment is covered with a sensor. The HIDS is first deployed on Internet-facing servers such as Web, mail, and DNS servers. Because the Internet-facing servers are connected to back-end servers, HIDS is also deployed on all the other critical servers within the corporate firewall. In addition to IDS appliances and HIDS Software, Cisco also provides IDS capabilities in both its IOS routers and its Catalyst switches.

An IDS sensor analyzes packet data streams within a network, searching for unauthorized activity, such as attacks by hackers, and enabling users to respond to security breaches before systems are compromised. When unauthorized activity is detected, the IDS can send alarms to a management console with details of the activity and can often order other systems, such as routers, to cut off the unauthorized sessions. In the physical analogy, an IDS is equivalent to a video camera and motion sensor detecting unauthorized or suspicious activity and working with automated response systems such as watch guards to stop the activity.

## Firewalls

A firewall is a hardware or software solution implemented within the network infrastructure to enforce an organization's security policies by restricting access to specific network resources. In the physical security analogy, a firewall is the equivalent to a door lock on a perimeter door or on a door to a room inside of the building—it permits only authorized users, such as those with a key or access card, to enter. Firewall technology is even available in versions suitable for home use. The firewall creates a protective layer between the network and the outside world. In effect, the firewall replicates the network at the point of entry so that it can receive and transmit authorized data without significant delay. However, it has built-in filters that can disallow unauthorized or potentially dangerous material from entering the real system. It also logs an attempted intrusion and reports it to the network administrators.

The Cisco IOS Firewall provides integrated firewall and intrusion detection functionality for every perimeter of the network. Available for a wide range of Cisco IOS Software-based routers, the Cisco IOS Firewall offers sophisticated security and policy enforcement for connections within an organization (intranet) and between partner networks (extranets), as well as for securing Internet connectivity for remote and branch offices.

A security-specific, value-added option for Cisco IOS Software, the Cisco IOS Firewall enhances existing Cisco IOS Software security capabilities, such as authentication, encryption, and failover, with state-of-the-art security features, such as stateful failover application-based filtering (context-based access control), defense against network attacks, per-user authentication and authorization, and real-time alerts.

The Cisco IOS Firewall is configurable via Cisco ConfigMaker software, an easy-to-use software tool based on Microsoft Windows 95, Windows 98, or Windows NT 4.0. The Cisco IOS Firewall provides great value in addition to these benefits:

- *Flexibility*—The all-in-one solution provides multiprotocol routing, perimeter security, intrusion detection, VPN functionality, and dynamic, per-user authentication and authorization
- *Scalable deployment*—Scales to meet any network's bandwidth and performance requirements
- *Investment protection*—Takes advantage of existing multiprotocol router investment
- *VPN support*—Provides a complete VPN solution based on IPSec and other technologies based on Cisco IOS Software, including Layer 2 Tunneling Protocol (L2TP) and QoS

Built upon a hardened, purpose-built operating system for security services, Cisco PIX OS, Cisco PIX Firewalls provide the highest levels of security and have earned many industry accolades, including ICSA Firewall and IPSec certification as well as Common Criteria EAL4 evaluation status. Cisco PIX firewalls provide a wide range of security and networking services including NAT; Port Address Translation (PAT); content filtering (Java/ActiveX); URL filtering; authentication, authorization, and accounting (AAA); Remote Authentication Dial-In User Service/Terminal Access Controller Access Control System (RADIUS/TACACS+) integration; support for leading X.509 PKI solutions; Dynamic Host Configuration Protocol (DHCP) client/server; Point-to-Point Protocol over Ethernet (PPPoE) support; and much more. Cisco PIX Firewalls also provide advanced security services for multimedia applications and protocols, including voice over IP (VoIP), H.323, Session Initiation Protocol (SIP), Skinny and Microsoft NetMeeting, giving you peace of mind when deploying next-generation converged network services.

Administrators can choose from a wide variety of solutions for remotely configuring, monitoring, and troubleshooting Cisco PIX Firewalls. These solutions range from an integrated, Web-based management interface (Cisco PIX Device Manager) to centralized, policy-based management tools to support for remote monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog. Administrators can also manage Cisco PIX Firewalls using a convenient command-line interface (CLI) through a variety of methods including Telnet, Secure Shell (SSH), and an out-of-band console port.

The Cisco PIX Firewalls are purpose-built security appliances that deliver unprecedented levels of security, performance, and reliability. These platforms provide robust, enterprise-class security services, including stateful inspection firewalling, standards-based IPSec VPN, intrusion protection, and much more in cost-effective, easy-to-deploy solutions. The Cisco PIX Firewall ranges from compact, plug-n-play desktop firewalls for small and home offices to carrier-class gigabit firewalls for the most demanding enterprise and service provider environments.

## Identity

Identity is the accurate and positive identification of network users, hosts, applications, services, and resources. Identity mechanisms are important—ensuring that authorized users gain access to the enterprise computing resources they need, while unauthorized users are denied access. Cisco networks use the authentication, authorization, and accounting (AAA) capabilities of the Cisco Secure Access Control Server to provide a foundation that authenticates users, determines access levels, and archives all necessary audit and accounting data.

## Encryption

Encryption technology ensures that messages cannot be intercepted or read by anyone other than the authorized recipient. Encryption is usually deployed to protect data that is transported over a public network and uses advanced mathematical algorithms to scramble messages and their attachments. Several types of encryption algorithms exist, with some more secure than others. Encryption provides the security necessary to sustain the increasingly popular VPN technology.

## Check Your Insurance Coverage

From dot-com companies to brick-and-mortar businesses using the Internet to dispense information or sell products, few organizations have implemented the type of comprehensive risk management program that can limit electronic exposures and reduce liability. As a result, many companies can expect to spend hundreds of thousands of dollars, if not more, recovering from electronic disasters. Some of the most common and costly network security risks facing the business community include the following:

- Business interruptions caused by hackers, cyber thieves, viruses, and internal saboteurs
- Multi-million-dollar litigation and settlement costs stemming from employees' inappropriate e-mail and Internet use
- Claims that products or services advertised on the Web fail to deliver
- Web-related copyright and trademark lawsuits
- Patent infringement claims with defense costs averaging \$1 million and judgments running into the hundreds of millions of dollars

The E-Risk Survey, conducted for Assurex by the Human Resource Institute (HRI) of Eckerd College, involved Fortune 500 companies and national associations.

The Assurex E-Risk Survey found that many companies are doing a good job with basic prevention: installing, monitoring, and filtering antivirus software; adding firewalls and encryption programs; and educating employees about hackers. Few U.S. businesses, however, have purchased electronic insurance products to mitigate network security risks and reduce liability costs after electronic disaster strikes. Many companies are underinsured in the information age:

- Business interruption insurance policies are held by fewer than 24 percent of businesses
- Only 18 percent have crime loss insurance
- Under 13 percent have unauthorized access, unauthorized use insurance
- Fewer than six percent have crisis communications insurance to cover public relations costs following e-disasters
- Not even two percent have extortion and reward insurance to cover costs associated with cyber attacks

IT-related insurance requirements should be examined at least every two years. However, focus group research conducted by Computer Economics over the last decade clearly shows that insurance policies are seldom reviewed. In addition, many organizations have very little understanding of how their IT investments are insured.

## Summary

Improving information security is critical to the operations, reputation, and economic stability of any organization. New laws require greater privacy protection and new threats to computer and network security are emerging daily. The principle goal of the SAFE Blueprint for Secure e-Business, from Cisco, is to provide best practice information to interested parties on designing and implementing secure networks. SAFE serves as a guide to network designers considering the security requirements of their network, taking a defense-in-depth approach to network security design. This type of design focuses on the expected threats and methods of mitigation. Key steps that managers should take in improving security include the following:

- An individual or work group should be designated to take the lead role in the information systems (IS) security process
- IS security policies should be established and documented
- An assessment of needs and weaknesses should be initiated
- Awareness should be increased through employee training
- Effectiveness of security measures should be monitored and evaluated continuously

It is critical that upper-level managers provide support for security improvement initiatives. The principles, processes, and procedures documented in this series of white papers will guide a new security team through the difficulties of getting organized and gaining momentum. Existing security teams can benefit from the return on investment (ROI) analysis procedures and the concepts inherent in the SAFE Blueprint.

This series of white papers provides data that CEOs, CFOs, and others can use to evaluate and justify security expenditures along with a step-by-step guide to determine return on investment for security in your organization. It delivers executive level managers an understanding of what happens when network security is breached, the process for recovering from a breach in security, and provides comprehensive information on how to evaluate the potential return on investment for network security protection. Finally, action steps that management should take to improve network security are also provided.

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.

- **Recovery After a Breach in Network Security**

This white paper discusses best practices for disaster recovery that involve information security and IT professionals, as well as law enforcement.

- **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.

You can find this series of white 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](http://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](http://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](http://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](http://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](http://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 PIX 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)