WHITE PAPER

symantec

The Value of Information Security

INSIDE

INSIDE

- The forms of cyber threats
- Tallying cyber attack damages
- The benefits of effective information security

Contents

Executive summary 3

Background 4

- Beyond network defense 4
- Privacy and security regulations 5
- Increasing connections, data flow, and security risk 5

The forms of cyber threats 6

- Malicious code 7
- Beyond malicious code 7

Tallying cyber attack damages 8

- Halted business operations: lost productivity, lost revenues 8
- Restoring hacked networks 8
- Liability and litigation 9
- Reduced competitiveness 10
- Available solutions 11

The benefits of effective information security 12

Symantec Enterprise Security: Technology, Service, and Response 13

- Symantec Security Technology 13
- Symantec Security Services 14
- Symantec Security Response 14

References 15

Executive summary

Today's global business environment appears to thrive on change. Enterprises are merging, acquiring other firms, being acquired, forming partnerships and alliances, diversifying, and reinventing themselves as e-businesses. But one constant is emerging from this activity: the rising value of information resources. Along with people, information is a firm's most valuable asset; yet high-level decision makers often overlook the threats to these information assets. Enterprises have long acknowledged computer viruses and other malicious code as threats to productivity, but there is a range of other malicious cyber activity that can also adversely impact a firm in various ways. This paper presents the key drivers behind increasing awareness of information security needs and summarizes the most prevalent forms of cyber threats facing enterprises, outlining the types of costs that firms could incur without comprehensive security measures, and highlighting the key elements of an effective security system.

Background

Several global business and technology-related trends are converging to transform information security from a necessary IT function to a critical-path business pursuit. Business drivers behind increasing information security awareness include current and emerging e-business and mobile commerce opportunities, for effective security is a key enabler of these opportunities. Technology drivers include the proliferation of, and reliance on, Internet-enabled and wireless technologies for communication and information exchange. This increasing electronic connectedness calls for adequate security measures to protect against cyber attacks. At the same time, the value of mission-critical business information such as intellectual property and strategic plans is rising—dangling like a carrot for information thieves. Enterprises must also comply with an increasingly wider range of customer information privacy laws and other regulations throughout the world.

As a result of these trends, the range of decision makers that are interested in information security issues is expanding. In addition to network administrators, IT directors, and chief technology officers, a growing number of chief financial officers and other CxO business executives are now involved in information security decisions.

BEYOND NETWORK DEFENSE

In the traditional model of information security, policies and practices focused almost exclusively on keeping outsiders, and outside code, from breaching an organization's internal network. All mission-critical information remained inside the internal network and a security perimeter was established to prevent access to this information to everyone but employees.

Today, the "internal network" is part of the larger global Internet (see Figure 1). Instead of blocking access to internal networks, enterprises now actively encourage their customers, suppliers, partners, contractors, and telecommuting employees to access select portions of their network to enhance productivity and engage in business transactions. For example, supply chain management involves supplier access to networks. B2C e-commerce involves customer access. New business arrangements involve partner access. The changing workforce (and workplace) necessitates remote employee access. And, acquisitions and diversification involve access by remote offices, subsidiaries, and other players to the network.

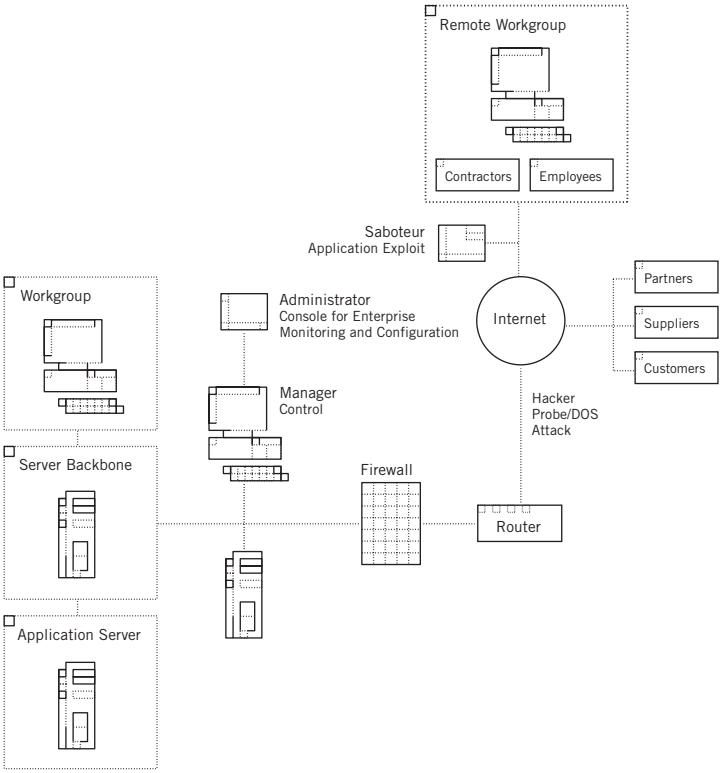

Figure 1. The increasing complexity of today's enterprise networks illustrates corresponding rises in security challenges.

Although these types of mutually profitable interactions introduce business opportunities for the participants, they would be untenable for most companies without implementing appropriate security measures. Moreover, the complexity of the needed security has increased dramatically. For example, each type of user must be granted access to only selected portions of corporate information. Customers must be able to purchase, but not access corporate planning documents; remote employees must be able to access their email, but not human resources files. Hence, the dynamics of today's networks pose a range of information security challenges.

PRIVACY AND SECURITY REGULATIONS

Against this backdrop of new business practices, legislatures, government agencies, and standards bodies, both in the U.S. and abroad, are now issuing directives compelling organizations to ensure data security and confidentiality—or face possible legal, monetary, or procedural consequences. This effort to safeguard security and privacy includes a U.S. Department of Health and Human Services rule guaranteeing patients greater access to, and control over, their medical records (mandated by the Health Insurance Portability and Accountability Act, or HIPAA). Another U.S. example is the Gramm-Leach-Bliley Act, which requires financial institutions to disclose their policies for protecting customers' personal information. The European Union (E.U.) Directive on Data Protection, issued in 1998, sets stringent standards for the use of personally identifiable information and restricts its exchange beyond the E.U. (U.S.-based organizations may participate in the Commerce Department's Safe Harbor agreement, which enables qualified enterprises to traffic in personal information with E.U. member organizations.) Enterprises are becoming increasingly aware of their need to comply with security and privacy regulations as they diversify into other industries and acquire, merge, and interact with other firms in the United States and throughout the world.

INCREASING CONNECTIONS, DATA FLOW, AND SECURITY RISK

The increasing electronic interconnectedness of business and society provides cyber attackers more opportunities to misappropriate or corrupt an organization's data resources. In the 2001 CSI/FBI Computer Crime and Security Survey, conducted by policy group Computer Security Institute in conjunction with the FBI, 70 percent of respondents cited their Internet connection as a frequent cyber attack point, up from 59 percent the prior year.[1]

At the same time, an increasing number of hacker-oriented Web sites are providing downloadable tools and step-by-step instructions for would-be cyber-attackers. This malicious content grows along with the beneficial information on the public Internet because, like all relatively new media, the Internet harbors both useful information and potentially harmful information. This dichotomy is at the crux of online business opportunities: the potential rewards are significant, but business risks are high as well.

[1] Richard Power, Computer Security Institute, "Computer Security Issues and Trends," 2001 CSI/FBI Computer Crime and Security Survey.

The forms of cyber threats

Cyber threats assume a variety of forms, ranging from a simple virus attached to a single email, to a sophisticated multi-pronged attack. In some cases, these threats target particular enterprises, while in other instances they are broadcast indiscriminately. The consequences of the attack range from nuisance emails clogging an in-box to loss of competitive advantage due to theft of confidential information. Common types of threats include, but are not limited to, the following:

- Malicious code attacks: viruses, worms, and Trojan horses. These well-known cyber attackers hide inside other applications or files to surreptitiously enter an organization and then either self-replicate and self-propagate, or rely on unwitting assistance to infect other computers and systems.
- Denial-of-Service (DoS) attacks. DoS attacks enlist Internet-connected servers, without the knowledge of the affected servers' administrators, to flood a target network with traffic. The torrent of information requests prevents dissemination of the site's legitimate information, potentially "crashing" the site's servers.
- Hacking. Using unauthorized or illegal methods and tools, many of which are commonly available on the Internet, the uninvited hacker probes for security holes through which to access, remove, duplicate, or otherwise tamper with a network or data resources. Hackers may also employ "social engineering" techniques to manipulate an insider into disclosing restricted access information.
- Blended threats. A combination assault, blended threats involve a mix of destructive elements including viruses, hacking, and other malicious approaches. Blended threats like the recent Nimda worm signal the dawn of a new era of virus and malicious code threats to enterprises and institutions alike. The multi-pronged attack of this worm—using not only email, but also Web pages as transmission routes—is redefining network security. The widespread infection that this worm inflicted "in the wild," often spread by simply visiting a Web site, means that a multi-layered, multi-function defense is needed to maintain network security.
- Disgruntled employees. Even with limited hacking experience, a motivated employee or contractor can dig wide and deep using pre-existing passwords and other access privileges. Statistics show that this group is responsible for a surprising percentage of cyber threats. Moreover, they often account for the most expensive attacks.

MALICIOUS CODE

The costs that the most damaging viruses, worms, and Trojan horses impose are significant, despite the wide availability of virus protection software for several years. For example, Computer Economics estimates the costs from the year 2000 'ILOVEYOU' virus at $8.75 billion.[2] Analysts agree that the "big three" viruses in 2001 were CodeRed, Nimda, and SirCam, and that they cost businesses billions of dollars. Those same businesses could have avoided much of these costs by installing antivirus software with automated updating features. In fact, the decrease in the annual costs of malicious code attacks from 2000 to 2001—the first such decrease since costs were first reported in 1995—is primarily attributed to the automated cleanup technology, now widely available, that the ILOVEYOU virus helped spawn.[3] Table 1 shows that prior to 2000, the cumulative worldwide economic impact of malicious code attacks roughly doubled each and every year from 1996 through 1999. But despite the recent softening of virus-related costs, the total still tallied $13.2 billion in 2001.[4]

Year	$ U.S. billions
2001	13.2
2000	17.1
1999	12.1
1998	6.1
1997	3.3
1996	1.8
1995	0.5

Table 1. Worldwide Economic Impact of Malicious Code Attacks. Source: Computer Economics[5]

The collective damage from the many more prosaic virus-related incidents that organizations regularly undergo is also substantial. More than 90 percent of organizations participating in the *Information Security* magazine 2001 survey reported virus-based infections, which are more costly than any other single attack category.[6]

BEYOND MALICIOUS CODE

As indicated in the list of threat types above, more than viruses and malicious code can breach an organization's security system and create problems. Corporate spies, insiders (including employees and contractors), terrorists, career criminals, and hackers of every kind may try to tamper with an organization's data resources. Their motivation ranges from financial and competitive gain to notoriety or revenge.

Although more cyber attacks originate from outside an organization than inside, insider attacks are probably more costly than external ones. Such insiders are potentially more dangerous than their outside hacker counterparts because of their presumed greater company knowledge, authority, and access. For example, Timothy Lloyd planted a logic bomb timed to detonate after his dismissal from former employer Omega Engineering Corp. The bomb systematically erased all the contracts and proprietary software on the company's network, causing an estimated $12 million in damages.[7]

In an area related to information security, more than 90 percent of the CSI/FBI survey respondents reported encountering employee misuse of online resources, such as surfing pornographic Web sites and emailing friends. Such activities reduce employee productivity and can also expose the enterprise to potential litigation.[8]

[2] "2001 Economic Impact of Malicious Code Attacks," www.computereconomics.com.
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Andy Briney, The 2001 Information Security Industry Survey, *Information Security* magazine, October 2001.
[7] "Economic Downturns Could Mean Upswings in Insider Threats," *Information Security* magazine, Security Wire Digest, Vol. 3, No. 12, February 12, 2001.
[8] Richard Power, Computer Security Institute, "Computer Security Issues and Trends," 2001 CSI/FBI Computer Crime and Security Survey.
[9] "Internet Security Threat Report," Riptech, http://www.riptech.com, January 2002.

Tallying cyber attack damages

Most security experts believe that the frequency of cyber attacks will continue to rise. One recent study found that the worldwide attack rate had increased 79 percent during the last half of 2001 alone.[9] Nearly one-third of these cyber attacks were reported in the United States—especially in the energy, high-tech, media, and financial services sectors.

Many factors comprise damage assessment. Some are easily quantifiable, such as the consultant's bill to clean up the damage. Others, such as a damaged brand in the marketplace, are more difficult to quantify.

HALTED BUSINESS OPERATIONS: LOST PRODUCTIVITY, LOST REVENUES

Downtime equals work that is never performed and revenues that companies never receive. According to *Information Security* magazine's 2000 survey, as much as 97 percent of virus costs can be productivity related. Of CodeRed's estimated $2.6 billion damages worldwide, *Computer Economics* attributes $1.5 billion to the negative productivity impact on system users, support staff, helpdesk staff, and other staff responsible for assisting internal users, IT staff, and customers worldwide. Similarly, of SirCam's $1.035 billion damages worldwide, $575 million was attributed to negative productivity impact.[10]

North American businesses forfeited 6,822 person-years in productivity in the 12 months preceding July of 2000 due to security breaches, downtime, and virus-attack cleanups—according to Reality Research and Consulting, which assisted *InformationWeek* Research and PricewaterhouseCoopers (IWR/PWC) in compiling the 2000 Global Security Survey.[11] (A person-year is defined as one person working 24 hours per day, 365 days per year.) Downtime related to security breaches or espionage has increased steadily since the first IWR/PWC survey in 1998. In a 2002 information security report from the United Kingdom, IT managers cited downtime as the second-most damaging aspect of a security breach (after loss of customer confidence).[12]

[10] "2001 Economic Impact of Malicious Code Attacks," www.computereconomics.com.
[11] George Hulme, "It's Time to Clamp Down," InformationWeek.com, July 10, 2000.
[12] John Leyden, "Curious employees are biggest security risk," *The Register*, March 3, 2002.

RESTORING HACKED NETWORKS

An organization that has been hacked typically disperses a team of staffers and/or consultants—often while downtime accumulates—to determine what happened, repair the damage, plug the security holes, investigate responsible parties, and enable employees and partners to return to business as soon as possible. Cleanup and testing sometimes continue long after connections have been restored.

Post-hack experts gather evidence using data recovery programs and forensic tools to reconstruct attack details. These experts can charge as much as $20,000 per computer to assemble a comprehensive picture of the attack, according to CNET News.com.[13] Of CodeRed's estimated $2.6 billion total damages worldwide, $1.1 billion was spent cleaning, patching, testing, and certifying systems for return to normal service. Likewise, of SirCam's $1.035 billion total damages worldwide, $460 million was attributed to recovery efforts.[14]

LIABILITY AND LITIGATION

Hacked organizations may also find themselves as a defendent—or even a plaintiff—in court. In cases of intellectual property theft, prosecuting suspected thieves is just the beginning of a lengthy legal process. Additional costs could be incurred to protect against possible infringements on existing patents, copyrights, and trademarks as a result of the theft. For example, many organizations hold dozens, hundreds, or even thousands of patents, and litigating a single patent claim can exceed $1 million dollars, according to a survey report by the American Society for Industrial Security and PricewaterhouseCoopers (ASIS/PWC).[15]

Companies required to comply with privacy and security regulations, such as those mandated by HIPAA, the Gramm-Leach-Bliley Act, and the European Union Directive on Data Protection, risk extensive liabilities if they are not able to prove due diligence in minimizing their exposure to cyber attacks and guarding against misuse.

[13] Robert Lemos, "Digital Sleuthing Uncovers Hacking Costs," CNET, www.news.com, March 22, 2001.
[14] "2001 Economic Impact of Malicious Code Attacks," www.computereconomics.com.
[15] "Trends in Proprietary Information Loss" survey report, American Society for Industrial Security and PricewaterhouseCoopers, July 2000.

REDUCED COMPETITIVENESS

Losing proprietary information, a partner's trust, customer confidence, or brand strength increases the likelihood of reduced competitiveness and, in extreme cases, may lead to bankruptcy. For example, a company that loses intellectual property can suffer irreparable and potentially fatal damage, since nearly 70 percent of a typical U.S. company's market value resides in its intellectual property assets. According to the ASIS/PWC "Trends in Proprietary Information Loss" survey report, Fortune 1000 companies lost more than $45 billion from proprietorial information theft in 1999, and such incidents, which result in an average yearly $15 million loss, are increasing. Surveyed companies cite the global Internet and increased connectivity as key factors in the rise.[16] The "2001 CSI/FBI Computer Crime and Security Survey" confirmed that, as in previous years, proprietorial information theft caused the greatest financial damage of all security failures.[17]

Successful cyber attacks prevent business partnerships from forming and drive a wedge into existing partnerships. Many business partners today seek and rely on real-time access to each other's sensitive, back-end information. An organization is less likely to share its databases if it believes such a linkage opens it to cyber attack.

According to "Trends in Proprietary Information Loss," shareholders and consumers alike are quick to abandon companies once an information-loss incident is publicized, thus leading to decreased stock value.[18] A majority of senior managers believe that organizations will lose market share if consumers and shareholders perceive lax information security, according to *Information Security* magazine's 2000 survey.[19] In a 2001 report by Jupiter Media Metrix entitled "Enterprise Security: Managing Services for Maximum Coverage," IT executives revealed they are more concerned with the impact of online security problems on consumer confidence and trust in e-business than about suffering financial losses.[20] And one in three IT managers polled in the United Kingdom in 2002 said the greatest harm from failed security is the negative effect on customer confidence.[21] Diminished customer confidence and a tarnished brand, especially for companies heavily invested in brand equity, mean reduced revenues.

[16] Ibid.
[17] Richard Power, Computer Security Institute, "Computer Security Issues and Trends," 2001 CSI/FBI Computer Crime and Security Survey.
[18] "Trends in Proprietary Information Loss" survey report, American Society for Industrial Security and PricewaterhouseCoopers, July 2000.
[19] Andy Briney, The 2000 Information Security Industry Survey, Information Security magazine, September 2000.
[20] Elizabeth Blakely, "Study: E-Biz Worries More About Consumer Confidence Than Security Losses," E-Commerce Times, October 11, 2001.
[21] John Leyden, "Curious employees are biggest security risk," *The Register*, March 3, 2002.

AVAILABLE SOLUTIONS

Organizations can build a security system to minimize most effects of the contemporary cyber attacks described above. The most effective of these systems weave, or layer, multiple security components—at the Internet gateway, server level, and client level—into a coherent, comprehensive entity. Each overlapping layer provides certain protection or enables particular functions, so the system's multi-tier integrity can resist even coordinated blended threat attacks. A brief overview of a few key types of solutions follows:

- Firewalls. Virtually all organizations with an online presence rely on some level of firewall protection. Securing the connections to the Internet and those between networks, firewalls protect enterprise assets and business transactions. Once the modern-day equivalent of a moat, today's firewalls are capable of providing greater granularity, allowing outsiders in and insiders out in a manner consistent with increasingly sophisticated rules. However, firewalls are only part of a comprehensive security solution; rarely does a firewall alone provide adequate protection against the myriad of threats that exist.
- Virtual Private Network (VPN). Many organizations are updating their firewalls with VPN technology. VPNs use advanced encryption to establish secure, end-to-end "tunnels" between users, protecting the information as it is transferred across the network. Because VPNs run over existing public networks (e.g., the Internet), do not require permanent or dedicated links, support high-bandwidth technologies such as DSL, and are highly scalable, they provide a cost-effective security layer for dispersed organizations.
- Antivirus (AV) software. The LoveBug attack served to re-emphasize the need for high-quality AV software, which can intercept and disinfect known viruses. Virus definitions must be periodically updated, across platforms and enterprise-wide, because many new malicious codes and variants of existing viruses are released every week. Increasingly, AV software uses heuristics to detect unknown viruses as well.
- Internet content filtering products. These applications scan incoming and outgoing email plus attachments and Web traffic, implementing filtering decisions based on an organization's rules. Such policing actions help ensure that only approved email, attachments, and Web content enter or exit the network. Organizations are therefore better protected against liability claims, spam (unsolicited email) attacks, and proprietary information loss; are able to improve user productivity; and ultimately preserve network bandwidth.

- Intrusion Detection Systems (IDS). Detection complements prevention. These products recognize and log inappropriate, incorrect, or anomalous network or host activity. And because host- and network-based IDS provide separate yet complementary functionality, many organizations deploy them in tandem.
- Vulnerability management software. Due to rapidly evolving threats, effective information security has become a moving target; thus, periodic assessments of both existing information security systems and current liabilities are recommended. Vulnerability management software uncovers security gaps and points the way to improvements. For example, vulnerability management software can ensure that the most up-to-date security patches are installed on all operating systems and applications.
- Security policies and training. Perhaps the most important part of any security system is an assessment of what to protect, to what degree, how, and by whom. Security policies must be comprehensive yet concise, tailored to the organization, understood and easily actionable by all employees, supported by senior management and enforceable enterprise-wide, as well as employ an appropriate mix of protection and productivity.

Many companies seek to simplify solutions by implementing security application and management integration. One way to accomplish this integration at the gateway is by combining firewall, VPN, antivirus, content filtering, and intrusion detection technologies into a single appliance.

Not surprisingly, many organizations choose to outsource some or all of the security detail after confronting the complexity and costs involved in creating and maintaining their own security system. Firms that offer consulting or managed security services can either assist in or assume full responsibility for developing and operating a layered information security system. This approach, favored most often by small- and medium-sized firms, relieves companies of attracting and retaining high-salaried information security professionals; maintaining up-to-date security approaches, hardware and software in the face of an ever-expanding set of perils; and providing 24/7 security coverage.

The benefits of effective information security

Organizations implement information security systems for what they can prevent: downtime, intellectual property theft, misuse or destruction of data resources, expensive legal action, public embarrassment, as well as dwindling stock prices, revenues, and market share. Preventing these occurrences bolsters the bottom line to a significant extent.

However, another way to evaluate information security involves what it can *enable*. Effective information security promotes business objectives and expands business opportunities. For example, effective information security enables the following business tasks: online banking, online trading, online shopping, supply-chain management, wireless transactions, access to remote or mobile sites, in-house database sharing with partners, and B2B and B2C e-commerce. Essentially, effective information security enables organizations to conduct business in newer and more profitable ways, particularly in the rapidly developing global marketplace.

Symantec™ Enterprise Security: Technology, Service, and Response

SYMANTEC SECURITY TECHNOLOGY SOLUTIONS

With threats to information systems coming from all sides and growing in number and complexity, enterprise customers know that hardening network perimeters is not enough. Symantec provides enterprise-class security products for all tiers of a network: at the gateways between the network and the outside world; at the servers that act as the network's vital organs; and at end-user devices including desktop PCs, laptops, and handhelds.

Enterprises and individuals both use the firewall products offered by Symantec to protect data and assets without slowing performance. Symantec also provides enterprises with intrusion detection technology that acts as a "security force" inside the perimeter to spot intruders that penetrate the outer defenses.

Most businesses are now establishing comprehensive security policies. Symantec's vulnerability management software helps customers define and enforce policies from a central location, as well as probe for network vulnerabilities and suggest remedies. Additionally, the world's leading antivirus products developed by Symantec offer critical protection from Internet-borne threats for workstations, servers, and at the gateway for businesses of all sizes.

Symantec Gateway Security is an appliance that incorporates five core security functions into a single security solution to effectively prevent security breaches at the network perimeter. This first-of-its-kind security offering combines firewall, antivirus, intrusion detection, content filtering, and VPN capabilities into a single, easy-to-manage appliance to provide small-to-medium organizations with cost-effective, secure protection in today's new world of blended Internet attacks.

Symantec's Norton line of consumer security products is the market leader in desktop protection, providing peace of mind with integrated products that work to protect computers from virus outbreaks or malicious hacker attacks.

SYMANTEC SECURITY SERVICES

Symantec™Security Services, a key component of Symantec Enterprise Security, provides information security solutions that incorporate best-of-breed technology, security expertise, and global resources to help enable e-business success. Through its three service families, Symantec offers industry best practices, proactive monitoring and management, and security education:

Consulting Services provide professional security assessments as well as architectural planning and design of security systems to help organizations better protect business-critical assets.

Managed Security Services provide outsourced solutions for the management and monitoring of security systems.

Education Services provide the knowledge to develop internal security skills and resources.

SYMANTEC SECURITY RESPONSE

Symantec Security Response offers a range of powerful security resources, including world-class product support, and the non-stop vigilance of Symantec's industry-leading global research and technical support centers. Symantec's intrusion experts, security engineers and virus experts work together to provide thorough coverage around the clock, constantly researching viruses, malicious code, evolving vulnerabilities and exploits, and the latest intrusion techniques. In addition, Symantec Security Response is continuously at work developing automated emergency response systems that detect security problems, alert customers, and securely deliver cures to Symantec Enterprise Security customers.

References

American Society for Industrial Security and PricewaterhouseCoopers, "Trends in Proprietary Information Loss" survey report, July 2000.

Cary Azzara, "Quantifying Infosecurity," *Information Security* magazine, September 2001.

Bob Blakely, "An Imprecise But Necessary Calculation," *Secure Business Quarterly*, vol. 1, issue 2.

Elizabeth Blakely, "Study: E-Biz Worries More About Consumer Confidence Than Security Losses," *E-Commerce Times*, October 11,.

Susan Breidenbach, "How Secure Are You?" InformationWeek.com, August 21, 2001.

Andy Briney, "Security Focused," The 2000 Information Security Industry Survey, *Information Security* magazine, September 2000.

Andy Briney, "The 2001 Information Security Industry Survey," *Information Security* magazine, October 2001.

Honeynet Project, "Know Your Enemy: Statistics," http://project.honeynet.org, July 22, 2001.

George Hulme, "It's Time to Clamp Down," InformationWeek.com, July 10, 2000.

Information Security magazine, Security Wire Digest, "Economic Downturns Could Mean Upswings in Insider Threats," vol. 3, no.12, February 12, 2001.

Robert Lemos, "Digital Sleuthing Uncovers Hacking Costs," CNET, www.news.com, March 22, 2001.

John Leyden, "Curious employees are biggest security risk," *The Register*, March 3, 2002.

Richard Power, Computer Security Institute, "Computer Security Issues and Trends," 2001 CSI/FBI Computer Crime and Security Survey, spring 2001.

Riptech, "Internet Security Threat Report," http://www.riptech.com, January 2002.

SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOLUTIONS TO INDIVIDUALS AND ENTERPRISES. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY MANAGEMENT, INTRUSION DETECTION, INTERNET CONTENT AND EMAIL FILTERING, REMOTE MANAGEMENT TECHNOLOGIES, AND SECURITY SERVICES TO ENTERPRISES AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS LEADS THE MARKET IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM.

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
1.408.253.9600
1.800.441.7234

www.symantec.com

For Product Information
In the U.S., call toll-free
800-745-6054.

Symantec has worldwide operations in 38 countries. For specific country offices and contact numbers please visit our Web site.