

# Risk Alert

A report for clients and colleagues of Marsh on risk-related topics

## **Information Risk—Protecting Your Organization in a Networked World**



# Contents

<b>Introduction</b> . . . . .	1
<b>Who's at Risk?—Common Myths</b> . . . . .	2
Value of Assets . . . . .	2
Web-Based Revenue . . . . .	3
Scope of Internet Security . . . . .	4
Hackers Are the Biggest Nightmare . . . . .	4
Managing Security Equals Managing Risk . . . . .	5
Demythologizing Your Company . . . . .	6
<b>What Are the Risks?</b> . . . . .	7
Criminal Attacks . . . . .	7
Privacy Violations . . . . .	10
Publicity Attacks . . . . .	10
Third-Party Liabilities . . . . .	11
<b>The Legal Landscape</b> . . . . .	14
The Health Insurance Portability and Accountability Act . . . . .	14
The Identity Theft and Assumption Assurance Act . . . . .	14
The Gramm-Leach-Bliley Act . . . . .	15
The Sarbanes-Oxley Act of 2002 . . . . .	16
The President's Critical Infrastructure Protection Board . . . . .	16
<b>Information Security</b> . . . . .	19
The Process and the Tradeoffs . . . . .	19
The Reporting Structure . . . . .	20
<b>The Insurance Response</b> . . . . .	21
Traditional Insurance . . . . .	21
Cyberinsurance . . . . .	24
<b>Conclusion</b> . . . . .	27

Marsh publishes *Risk Alert* to keep its clients and colleagues informed on critical issues related to risk. For additional copies, please contact [questions@marsh.com](mailto:questions@marsh.com). This report is also available for download at <http://www.marsh.com>.

## Acknowledgments

Much of the information for this report was provided by members of Marsh's Information Risk Advisors—Peter Foster, senior vice president; Christopher Keegan, vice president; Arturo Perez-Reyes, vice president; Judith Platt, knowledge manager; Seth Shapiro, senior vice president; and Henry Whiting, managing director—and by Jill Dalton, managing director with Marsh's Property Practice, and Harry Shah, senior vice president with Marsh's Technology & Information Services.



## Introduction

Imagine having to send this letter to thousands of your clients:

**Dear Sir or Madam:**

**We regret to inform you that the personal information with which you entrusted us may no longer be confidential. Someone gained unauthorized access to our database.**

**The intruder may have downloaded your Social Security number, your date of birth, and your full legal name, putting you at risk for identity theft. Therefore, we recommend...**

Loss of information can harm a company's reputation, decrease its bottom line, and expose the company to lawsuits from a wide range of sources. In this age of instant connectivity, with virtually all information available in electronic form, information is more vulnerable, more at risk than ever.

Cyber risk, information risk, virtual risk—whatever you want to call it—is not just for companies like eBay or Amazon.com; it applies to every business, every organization. Information-risk losses cost businesses and governments hundreds of billions of dollars per year. And they're on the rise. In just the past year, for example, reports of identity theft have doubled. Even if you do no business over the Internet and have only a modest Web site, information theft and cyberattacks are a real threat to everyone and every business.

But risk is risk. The basic paradigm of risk management—identify the risks, evaluate the risks, select techniques to deal with the risks, implement those techniques, and monitor how well those techniques are working—works just as well for protecting electronic information as it does for tangible property.

In this issue of *Risk Alert*, we discuss information—who's at risk, what the risks are, and what you can do to protect your company.

## Customers at Risk

An insurer was missing a hard drive. It may merely have been misplaced, but police—and the insurer—treated it as a theft. The hard drive contained personal information about 180,000 life-insurance and pension-plan clients, including bank-account and credit-card numbers. It appeared that all 180,000 individuals were at risk for identity theft, one of the most pervasive and growing risks of the information age.

The hard drive was recovered a little over two weeks after it disappeared, but not before the insurer had sent notification letters to the individuals whose information had been at risk. According to authorities, there is nothing to indicate that the information was targeted or that it was used at all.

In the meantime, a class-action lawsuit has already been filed on behalf of the individuals whose information was in jeopardy.

The disturbing—and enlightening—aspect of this event is that it doesn't matter whether the insurer had a Web site, conducted online transactions, or operated in the "old-fashioned" way—offline and in electronic isolation. The information was on a hard drive, putting the insurer and 180,000 of its clients at risk.

Thirty years ago, there were no hard drives small enough to be misplaced or stolen that could hold this amount of information. Someone could have stolen information about 180,000 individuals, but it would have taken days or weeks of photocopying or transcription. Now, it's as simple as walking out with a hard drive.

## Who's at Risk?—Common Myths

Every organization is affected by the storage of critical information in an electronic format, either directly with its customers and vendors or indirectly with its trading partners. Mountains of critical information are exchanged electronically on a daily basis. But there are many myths about what organizations do and do not have an exposure, as well as about the significance of that exposure.

### Value of Assets

**Myth:** The most valuable assets for most companies are their tangible assets.

Tangible assets no longer represent the lion's share of a business's worth. Intangible assets—knowledge, intellectual property, brand, and proprietary business methods—have taken over as the majority of market value. According to research done by the Brookings Institution, tangible assets have dwindled in importance.

- A 1982 study by the Brookings Institution found that tangible assets (property, plant, and equipment) accounted for 62 percent of companies' market value, with intangible assets accounting for only 38 percent.
- A 1992 study by the Brookings Institution found that those numbers had reversed themselves, with tangible assets at 38 percent and intangible assets at 62 percent.

That trend has continued into the 21st century. Ours is an information economy. We have moved from an industrial to a post-industrial mode. Processes are outsourced, often overseas. Information must be exchanged, and the exchange is generally electronic—often via the Internet, but also over private networks and telecommunications. And telecommunications systems are often part of a company's operational systems—for example, automatically updating inventory based on sales and transferring cash and other assets.

Even if a business were self-contained, it could not avoid the electronic connections needed to do business with the financial and insurance industries. Take, for example, workers compensa-

## Web Growth

Internet growth has been staggering by any measure. The following numbers are from the U.S. Department of Commerce.

- There were only 26,000 domain names in use in 1993; now, there are over 5 million.
- In 1993, 3 million people were connected to the Internet; now, there are over 80 million.
- E-commerce sales for the third quarter of 2000 were \$7.266 billion; for the third quarter of 2002, \$11.061 billion.
- E-commerce sales for the third quarter of 2000 were 0.9 percent of total sales; for the third quarter of 2002, 1.3 percent of total sales.
- In 1965, the high-tech share of business spending was 3.0 percent; in 1996, 45 percent.

Internet growth is expected to continue, with virtually all companies doing business, to one extent or another, in the virtual world.

tion coverage. The majority of claims are filed electronically with state regulatory authorities, as is information about the policy. So even if a company has zero computers and does everything by hand, chances are that certain information about that company has been reduced to electrical impulses and sent somewhere via the Internet.

According to Judith Platt, knowledge manager for Marsh's Information Risk Advisors, "There has been a fundamental change in the way businesses and government do business. Organizations have become more and more dependent on rapid exchange of information—which has become the currency of the global economy."

## Web-Based Revenue

**Myth:** Only organizations that collect revenues through the Internet or through their networks suffer any serious economic consequences when the Internet or their networks are down.

Companies that do all—or even a substantial portion—of their business online are more likely to be affected by Internet or network downtime than others, but the effects on others can be dramatic as well. For example, many companies have Web sites—some, quite extensive—that provide only information to visitors. The Web site is a marketing tool, a way of positioning oneself as a leader in a particular field. If the Web site is down, for whatever reason, visitors are likely to move on to the next likely Web site that may provide the same type of information and, as a consequence, potentially shift their allegiance and their business to another company.

If the Web site has not been shut down, but vandalized, the damage may be worse. For example, hackers may hijack (or "Web-jack") visitors to a pornographic Web site or to a site that disparages the company. According to Christopher ("Chris") Keegan, vice president with Marsh's Information Risk Advisors, "Businesses trade on their reputations. A defaced Web site or a site that presents negative information about a company—whether that information is true or not—can damage a company's reputation, and it may take a lot of time and money to fix the Web site and rehabilitate the company's reputation."

## Viruses and Attacks— A Timeline

According to Brian Krebs in “A Short History of Computer Viruses and Attacks,” *Washington Post* (February 14, 2003), the following are some of the highlights (or, more accurately, the lowlights) of viruses and attacks:

- In 1949, John von Neumann, a Hungarian scientist, developed the theory of self-replicating programs. This provided the theoretical basis for computers to hold information in “memory.”
- In 1960, AT&T introduced the first commercial modem, known as “Dataphone.”
- In 1964, AT&T began monitoring telephone calls to try to identify “phreakers,” individuals who used “blue boxes” to generate tones that allowed them to make free telephone calls.
- In 1969, the federal Advanced Research Projects Agency launched the ARPANET, the forerunner of the Internet.
- In 1986, “The Brain,” one of the first viruses that affected personal computers, was released.
- In 1998, two California teenagers infiltrated and took control of over 500 military, government, and private-sector computer systems.
- In 1999, the “Melissa” virus infected thousands of computers. Damages were estimated at \$80 million.
- In 2001, the “Code Red” worm infected tens of thousands of computer systems. Damages were estimated at \$2 billion.

For the complete “short history,” see <http://www.securityfocus.com/news/2445>.

## Scope of Internet Security

**Myth:** Computer-network and Internet security is strictly a technology issue.

In fact, computer-network and Internet security is *information* security—a people-and-process issue. Unfortunately, the uses and the programs for computers have proliferated faster than the security systems to protect them. Thus, despite network-security systems and firewalls, there are often gaping holes in the perimeter walls. It’s as though the front door were securely bolted, but the back door left open for easy access by the cleaning crew. Consider the following examples:

- Two national bank employees circumvented the bank’s internal controls, exceeded their authority, and obtained over 60 credit-card numbers. The information was then faxed to outside individuals, who ran up bills for goods and services of almost \$100,000.
- A computer programmer, working on the frequent-flyer pages of an airline’s Web site, left a firewall open. This left the frequent-flyer mileage—and the customers’ credit-card information—available to anyone who visited the Web site.

## Hackers Are the Biggest Nightmare

**Myth:** The notoriety of being hacked is the computer-security professional’s biggest nightmare.

While hacking is sometimes the cause of damage to or destruction of data, it’s only one of the ways that a company’s information assets can be damaged or destroyed. Computer-security professionals are most concerned with the following issues:

- **Confidentiality:** If data is not handled appropriately, it can very easily be disclosed to the wrong people. Word of mouth, of course, has been a problem since time immemorial, but computers have created new areas of concern, such as e-mail.
- **Integrity:** If data is to be trusted, it must be not only correct, but also complete. But it’s easy for the integrity of data to be compromised in a networked environment. For example, if documents are distributed by mailing hard copies, alteration of those documents is difficult and easily detected. But when

**Managed security services provide only one piece of the puzzle. Risk management takes the additional step of arranging for losses to be funded.**

they're distributed by e-mail, it's easy for them to be modified before they're forwarded, with the data significantly altered.

- **Availability:** While the integrity of data must be protected, the data is useless if it's not available when needed. Downtime of computer systems can be very costly, as information has become our primary product, and it's unavailability means work slowdowns or stoppages.
- **Authenticity and nonrepudiation:** The authenticity of incoming data is also important. There must be strong and substantial evidence that the apparent source of information is authentic and that the source has the authority and position indicated. For example, there have been instances of phony press releases being accepted as authentic, being released to the public, and damaging a company's reputation and market value.
- **Control and possession:** Information and information resources must be in the control of the rightful owners. For example, one of the most vulnerable areas is password-protected data. People tend to be all too cavalier about their passwords—sharing them, not changing them very often (or at all), or basing them on well-known personal information. This makes it easier for unauthorized parties to gain access.

## **Managing Security Equals Managing Risk**

**Myth:** Having a chief information security officer (CISO), security policies, and managed security services is risk management.

Managed security services provide only the technical response. It's only one piece of the puzzle. Unfortunately, as fast as a firewall or an intrusion detection system (IDS) is built, someone out there is figuring out how to breach it. According to a 2002 survey by the FBI and the Computer Security Institute (CSI), 40 percent of the respondents with firewalls and IDS reported at least one instance of penetration from outsiders.

Risk management takes the additional step of arranging for losses to be funded with insurance or some other risk-transfer mechanism.



## **Demythologizing Your Company**

“Many companies still operate in ‘silos’,” according to Seth Shapiro, leader of the consulting practice of Marsh’s Information Risk Advisors. “The information-technology and network infrastructure are the responsibility of the chief information officer. Security often inhabits the same silo, which creates the potential for conflicts of interest. The risk management function is generally part of the treasury function. Legal, audit, and human resources have their own independent reporting structures. As a result, a lot of communication takes place vertically—upward to senior management and downward to others in the same silo—but not often horizontally. And the ‘fault lines’ between the silos are a real Achilles’ heel with respect to protecting information assets.”

A survey by The St. Paul Insurance Companies, released early last year, indicated that twice as many information technology (IT) managers as risk managers saw the Internet as a major source of risk. Are the IT managers seeing bogeymen where none exist, or are the risk managers in denial?

Part of the process of demythologizing your company is bringing risk management and IT management together to analyze your potential for loss of information through the various electronic portals into and out of your company.

## Terrorism by Web

There will be a “major cyber-terrorism event in 2003,” according to John Gantz, chief research officer for International Data Corp. Gantz went on to say that the attack will “hurt the economy. It will bring the Internet to its knees for a day or two,” as reported in *The Calgary Herald* on January 13, 2003.

Less than two weeks later, a virus-like program, the “SQL Slammer” worm, led to a pronounced slowdown in network traffic. The attack began on Saturday, January 25, 2003. Some Internet service providers (ISPs) in Japan and Korea were forced to suspend services. Five of the 13 DNS (domain name system) root servers, along with tens of thousands of servers, succumbed. Air-traffic control and emergency services were affected. And 13,000 automated teller machines (ATMs) in the United States were down for most of the day. As if all that weren’t sufficiently frightening, the worm made its way around the globe within 15 minutes.

This worm is estimated to have cost about \$1 billion in productivity worldwide—and that’s with its being released on a Saturday. Just think what a Monday-morning worm would do.

While the SQL Slammer does not appear to have actually damaged computer systems, some experts believe a newer version that carries a “damaging payload” could yet emerge.

## What Are the Risks?

“Technological advances occur almost daily. As a result, the risks are also changing almost daily,” according to Peter Foster, senior vice president with Marsh’s Information Risk Advisors. “Twenty years ago, the biggest risk to IT systems was a power surge that might wipe out data and destroy computer equipment. The emergence of the Internet, the proliferation of viruses, and the persistence of hackers have made the power surge pale by comparison.”

It’s important to remember, however, that cyberspace is not that different from real space. As Bruce Schneier states in his book, *Secrets and Lies: Digital Security in a Networked World*, there’s not that much difference between an attack and a cyberattack. “If you strip away the technological buzzwords and graphical user interfaces, cyberspace isn’t all that different from its...real-world counterpart.”

Schneier goes on to point out that “the threats in the digital world mirror the threats in the physical world. If embezzlement is a threat, then digital embezzlement is also a threat.” Virtually every sort of crime you might expect in the real world can also happen in cyberspace—only a lot more people have the means, motive, and opportunity to break into your systems from a distance than to break into your file cabinets in person.

These crimes and their consequences are precipitated by attacks against your network, including criminal attacks, privacy violations, and publicity attacks. These attacks, in turn, can result in third-party liabilities—lawsuits that can prove even more costly than the damage to your systems and the loss of information.

## Criminal Attacks

Criminal attacks are almost always launched with the intent to gain financially, although terrorism, with the goal of interrupting the infrastructure of a company or an entire country, has increasingly become a motivation. The following are some of the more common attacks.

## Sharing Salary Information

Imagine that a disgruntled human-resources (HR) employee is fired and decides to “get even” with his company by e-mailing the salary information of hundreds of senior employees to as many people as possible.

The question is, other than creating some embarrassment for HR, is there any real cost? Unfortunately, the answer is yes.

When compensation information becomes public, unavoidable inequities become known. Underpaid staff members demand raises, employees may choose to leave, and morale can suffer.

Companies have to be extremely careful about who has access to compensation information. There should be measures in place to make it difficult to gain access to and distribute such information.

An organization with a number of divisions should assign an individual HR employee to each division. Each HR employee should have access only to the division that is his or her responsibility and not to information from other divisions. That type of compartmentalization limits the scope of damage that can be done.

**Destructive attacks:** These are the attacks for which the primary motivation is disrupting your network—or disrupting whatever network can be disrupted. One of the more common methods is to introduce a virus into your system.

Generally, destructive attacks are not launched for any gain, but simply to destroy. Sometimes, they’re targeted at a particular company or a particular computer operating system, but more commonly, they’re flung out into cyberspace to attack whatever network is vulnerable. The motivation may be terrorism, or it may be “just for the fun of it.” Regardless of the motivation, such destructive attacks can be financially devastating.

The “Melissa” virus, for example, caused over \$1 billion in damage. First confirmed on Friday, March 26, 1999, it had spread to over 100,000 computers by Monday, March 29, 1999. And in 2001, the “Nimda” virus reportedly infected 8.3 million computer networks, causing \$590 million of damage, according to an article from Agence-France Presse (October 3, 2001).

**Intellectual-property theft:** These attacks are generally specifically targeted. The perpetrators want your information. This could be trade secrets—patented processes and other proprietary information that a business does not want released to the public under any circumstances. Or it could be copyrighted information that a business is willing to share for a price—software programs, movies, music, and other information and processes. In either case, it’s money out of your pocket.

In the “good old days,” prior to digital recordings, it was not uncommon for people to make copies of one another’s videotapes, records, or audiocassettes. While each copy took money out of the pockets of those who owned the rights to such intellectual property, the problem was not as widespread as it is today. Copies were clearly copies. Both the video and audio quality diminished with each generation of copies. Now, the information is often digital, with the result that the copy—and the copy of the copy, and the copy of the copy of the copy, and so on—are virtually indistinguishable from the original. Now, wholesale theft is widespread.

A case in point: The Business Software Alliance (BSA) estimates the 2001 loss of retail revenue to software piracy totaled \$1.997

## Identity Theft Booming

The incidence of identity theft has almost doubled from 2001 to 2002. The Federal Trade Commission (FTC) received 86,000 reports of identity theft in 2001, as reported in "Identity Theft," *The New York Times* (January 23, 2003). That number jumped to 162,000 in 2002, an increase of 88 percent.

The FTC started issuing reports of consumer crime three years ago, and identity theft has remained at the top of the list all three years.

- In roughly one out of four cases of identity theft, the stolen information is used to open new credit-card accounts.
- About 23 percent of the cases involve loan and bank fraud.
- Another 10 percent involve establishing fraudulent cell-phone accounts.

The average identity theft costs the individual consumer \$1,000 in personal expenses and lost work time. And some experts predict that financial institutions will lose over \$8 billion to identity theft by the end of 2004.

billion in North America, \$10.967 billion worldwide. These numbers represent a drop from 2000, when the numbers were \$2.937 billion and \$11.750 billion, respectively—a drop the BSA attributes not so much to decreased piracy, but to decreasing software prices.

**Identity theft:** This has become one of the biggest Internet issues, in part because of its widespread impact. Any company that does business with consumers should be enormously concerned about this type of attack. Identity theft has been called "stealing your life."

The basic process is to obtain credit using someone else's identity. Criminals gain access to basic personal information—Social Security numbers, full legal name, date of birth, mother's maiden name, etc. Then, the criminals can obtain new credit cards, enter into installment-sales contracts, and run up huge bills in the name of the victim.

Much of the identity theft can be attributed to carelessness on the part of consumers. Some states use Social Security numbers as our driver's license numbers, a document that then contains enough information—full name, date of birth, address, and Social Security number—to enable anyone to steal your identity. But in some of those states, you have a choice and can request a different number, a tactic that helps protect against the possibility of identity theft if you misplace your driver's license.

Many of us are careless with our mail. Those solicitations for you to sign up for yet another credit card should not be just thrown away, but shredded with a cross-cut shredder, lest someone use the form to obtain a credit card in your name. Yet many of us merely throw them in the trashcan—perhaps ripping them in half.

According to Arturo Perez-Reyes, vice president with Marsh's Information Risk Advisors, "Identity theft can also occur when hackers or insiders gain access to personal information on a wholesale basis. Employees at a variety of industries have been charged with identity fraud—health clubs, financial institutions, insurers, and medical offices among them. Law-enforcement officials cite such wholesale fraud as being the most serious aspect of identity theft."

## Information Bottlenecks?

The structure of the Internet is shifting and consolidating. Originally, it resembled a mesh, with connection points so geographically dispersed that it could “withstand failure and provide service under adverse conditions—even a nuclear attack,” as reported in “Hubs increase Net risk,” *TRN: The Latest Technology Research News* (January 8, 2003).

The article goes on to explain that some Internet service providers (ISPs) have moved toward the hub-and-spoke topology that is typical of air travel in the United States. And as every air traveler knows, a shutdown—due to severe storms, for example—in any one of a number of key hub cities can bring air travel nationwide to a grinding halt. The same could be true of the hub-and-spoke ISPs.

According to Tony Grubestic, a former Ohio State researcher and currently an assistant professor of geography at the University of Cincinnati, many ISPs have shifted to the more vulnerable hub-and-spoke system “in search of the most economically efficient network topology.” But the tradeoff for the economy is a system more susceptible to attack.

The handful of cities that have become central to the Internet include Los Angeles, New York City, Atlanta, Dallas, and Chicago.

Companies that deal directly with consumers can ill afford to have their customers’ identities stolen from company records. Such customers are more likely than not to sue—and to do business elsewhere next time, particularly if the company offers little or no assistance to financially “wounded” customers.

## Privacy Violations

Privacy violations can be criminal, but more often, they are not. Customers do not necessarily own their own data. Credit bureaus and marketing-research firms collect data and share it. Investigation and surveillance firms can legally gather a tremendous amount of data without breaking any laws. It’s disturbing to think about how much information is available, often at no cost, in the public domain.

However, when parties collecting information step over the line—for example, hacking into corporate or personal computers to get data—it is often a precursor to illegal activities, such as identity theft.

## Publicity Attacks

A lot of hackers hack because they can. It’s the Mount-Everest syndrome—because it’s there. Once having hacked, the hacker seeks publicity as validation. While hackers may not identify themselves by name, they frequently boast of their “triumphs” by posting their exploits in chatrooms.

**Kilroy was here:** During World War II, the phrase “Kilroy Was Here” began to appear as graffiti, both in the United States and wherever the U.S. military traveled abroad. Eventually, the phrase and the cartoon character that accompanied it came to represent the U.S. presence throughout the world. Some hackers just want to put their own “Kilroy” on your Web site—to establish their presence throughout the cyberworld.

Unfortunately, this graffiti mentality can be harmful to a company. A defaced Web site announces, to the world at large, that the Web site is not secure. And if the Web site is not secure, there are those who will wonder how secure it can be to do business with that company.

## Spiraling Spam

While not actually a virus, spam has become one of the major annoyances of life online. In fact, one way of orchestrating a major slowdown of the Internet is by sending an avalanche of spam. And one way of causing a Web site to crash is to overload it with spam.

Spam is defined by *The American Heritage Dictionary of the English Language* (fourth edition, 2002) as “Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail.” It’s a noun and a verb—and a source of aggravation and more for both businesses and individuals.

(Interestingly, the etymology of “spam” is unknown, although *The American Heritage Dictionary of the English Language* indicates it was probably inspired by a comedy routine on the British television series, *Monty Python’s Flying Circus*, in which the word is repeated incessantly.)

Spam is reported to account for up to 40 percent of e-mail, and analysts are predicting that by July 2003, the number will top 50 percent.

Beyond the annoyance factor, there is a real dollar cost to spam. Ferris Research, a San Francisco-based market-research company, estimates that unwanted e-mail—spam—cost U.S. corporations \$8.9 billion in 2002.

**DDoS:** One of the most recent hacker tricks is the DDoS, the distributed denial of service. One of the methods of accomplishing this is to flood the Internet with e-mail, co-opting each computer to which e-mail is sent and having it send thousands of e-mails. Multiply this by enough computers, and the system is flooded. It either slows down substantially or just plain crashes.

## Third-Party Liabilities

Almost anything that can happen to a company’s information and IT systems can also trigger third-party liability. As costly as the damaged or lost data can be, litigation is generally more expensive. The following are just some of the areas to which companies are exposed.

**Intellectual-property infringement:** Just as many people are cavalier about their passwords and other systems intended to protect the integrity of computer systems, many also take too light a view of software copyrights. But most software comes with agreements that limit the number of computers on which a particular program can be installed. Yet many people simply “pop” the same CD into one computer after another in violation of those copyrights—often innocently so, not having read the rules. (How many read the agreement, and how many just click “I Agree” and continue with the installations?) Being sued for copyright infringement can be costly and time-consuming.

Another area of infringement deals with trade dress—the totality of a company’s brand identity. This is not just the words, but the style, the colors, the graphics—the total look and feel of the way a company visually presents itself to the world. And therein lies the problem: The Internet means a company is literally presenting itself to the entire world. And that means companies in California and in Massachusetts, in Argentina and in Belgium, in Russia and in Vietnam are side-by-side in cyberspace. Companies with astonishingly similar trade dress—that otherwise would never have encountered one another—are now “duking it out” in court for which one has the right to use a particular trade dress. And win, lose, or draw, defending oneself against any third-party suit is never cheap.

**Invasion of privacy becomes a very complex issue on the Internet. The problem is the wide range of privacy laws that companies face.**

**Content and advertising-related offenses:** Defamation—especially online commentary and discussion—is another area rife with potential claims, again largely because of the wide audience. One of the areas of concern is the potential for statements made over the Internet by employees about the competition and other third parties. While federal legislation has created “safe harbors” for ISPs, protecting them from liability for defamatory statements—much as telephone companies are not held accountable for what people say on telephone calls—the same protection does not exist for those who make the statements.

If, for example, a salesperson repeats some detrimental gossip about a competing firm to a prospective customer, that statement is only heard by the prospect. If the same salesperson makes the same allegation in an e-mail, that allegation can be forwarded, intact, to anyone with an e-mail address. What was once a questionable sales practice now becomes an actionable offense—particularly if the rumor is untrue and the competitor can substantiate that it lost business as a result of the rumor.

Other issues that can result in claims include creating hyperlinks from another company’s Web site to your own without permission, altering digitized music and images without permission, violating distribution rights of digitized music and other copyrighted material, plagiarism, using testimonials or endorsements without permission, and on and on and on—the same offenses that have been with us offline since time immemorial, only now made more egregious by the worldwide audience.

**Privacy:** Invasion of privacy becomes a very complex issue on the Internet. The issue is using confidential information that identifies a person or an entity without permission in a public forum. The problem is the wide range of privacy laws that companies face. For example, there are significant differences between the European Privacy Directives and privacy regulations in the United States. And within the United States, there are a number of state-specific privacy regulations.

An inadequate privacy policy on a Web site is another potential source of liability. This could include:

- failure to disclose what information is being collected;

## Eight Million at Risk

In February 2003, it was reported that hackers had gained access to about eight million credit-card numbers through the computer system of a merchant.

One fear is that these numbers will be used online. While the individual credit-card holders would not be held responsible for unauthorized charges, online and telephone mail-order merchants would not be protected. The merchants would not be able to inspect the cards and, thus, would be required to assume all liability for fraudulent purchases.

If the information leads to identity theft, there may be millions of consumers lining up to sue whatever companies are perceived to bear some responsibility for the security breach—a scenario that could be even more costly than the fraudulent purchases.

Source: "Card Numbers Theft," Dow Jones News Service (February 18, 2003).

- failure to disclose what use will be made of the information collected;
- failure to allow consumers a mechanism to view and modify the information that has been collected; or
- failure to allow consumers to "opt out" of the company's use of their private information.

Any of these, as well as violating the company's stated privacy policy, could result in regulatory action or litigation.

**Errors and omissions:** Companies that deal in computers—either the equipment or the software—have additional exposures. The overall exposure will depend on the role of the company and its level of involvement with the organization that uses the products, as well as the scope and nature of the contractual relationship. But our increasing collective connectivity and dependence on Internet technologies raises the bar for such companies. If systems don't work as promised, the malfunctions can cause financial harm. Some of the exposures include:

- service outages and interruptions;
- faulty technical support;
- insufficient security measures used to protect third-party data or code from computer crime;
- unauthorized release of confidential information;
- breach of consumer privacy; and
- failure of software.

## Social Security Numbers

While originally and officially, Social Security numbers were not intended to be used for identification, they have become our national ID number. As such, one would expect there to be some degree of confidentiality to the numbers, but that is not the case.

Almost anyone anywhere can find out your Social Security number—legally. There are many online services where this information can be obtained. There are also online services that will provide your full name and birth date. Armed with this information, it's easy for an identity thief to steal your life.

From time to time, a member of Congress introduces legislation that would make it illegal to provide Social Security numbers online without the individual's consent. To date, none of these bills has become law.

In 1999, the General Accounting Office (GAO) issued a report, *Social Security—Government and Commercial Use of the Social Security Number is Widespread*. In this report, the GAO states, "No single federal law regulates the overall use of SSNs [Social Security numbers]." The report further states, "Both private business and government officials said their organizations could be adversely affected if the federal government passed laws that limited their use of SSNs."

It would appear that any law protecting your Social Security number has little chance of passing.

## The Legal Landscape

Beyond the need to keep your information secure—to protect your intangible assets and to avoid costly lawsuits—various laws also require certain levels of security. The following are some of the legal and regulatory issues companies face.

### The Health Insurance Portability and Accountability Act

The increasing use of the Internet and other networks has been a boon to the health-care industry, with the ability to gain instant access to critical information. Electronic connectivity has been used to improve the quality of clinical care and, ultimately, reduce cost, but it also opens up a Pandora's box of exposures. The risks associated with doing business and delivering health-care services over the Internet include violations of patient privacy and confidentiality, offenses involving intellectual property, and medical malpractice.

The federal government has made privacy of patient information a top priority. Health-care organizations have until April 13, 2003, to comply with the privacy regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The privacy rules will apply not only to health-care providers, but also to health plans, health-care clearinghouses, and organizations that have access to patient records and finances.

In addition to HIPAA, health-care organizations must comply with existing common law, plus statutory and regulatory protections under state laws safeguarding the privacy of individuals' medical information. They will also have to comply with a wide array of security requirements, such as certification, back-up plans for data, personnel security, virus checks, and authentication procedures.

### The Identity Theft and Assumption Assurance Act

The Identity Theft and Assumption Assurance Act of 1998 made identity theft a federal crime, punishable by imprisonment up to 15 years and fines up to \$250,000. Prior to this Act, identity theft was only considered a crime against the creditor that suffered



monetary loss. Now, the individual whose identity was stolen is also considered a victim of the crime. This likely strengthens a victim's position in civil court, should he or she pursue action against a company with lax security policies that allowed the identity to be stolen.

In fact, according to "ID Theft Suits in the Cards," *Business Insurance* (April 24, 2002), "Companies that contribute to identity theft by failing to protect their customers' and employees' Social Security numbers and other personal information could be held liable." The article cites a case where an employee of one company found a box holding the personnel records of 38 former employees. The employee used the information to obtain at least 75 credit cards and \$100,000 in merchandise, opened 20 cell-phone accounts, and rented three apartments.

While victims may not often be able to determine how and where their identities were stolen, when they can trace it back to the source and when that source is a company's failure to protect the information properly, a lawsuit will surely follow.

## **The Gramm-Leach-Bliley Act**

The Gramm-Leach-Bliley Act of 1999 (GLBA), also known as the Financial Services Modernization Act (FSMA), protects consumers' privacy and information security. A company that fails to comply with GLBA provisions may be the target of enforcement actions, civil penalties, governmental fines and penalties, and cease-and-desist orders. The following are some of the issues covered in this Act.

- Financial institutions must clearly disclose their privacy policies with regard to sharing nonpublic personal information with both affiliates and third parties.
- Financial institutions must notify consumers of and provide them with an opportunity to "opt out" of the institutions' sharing nonpublic personal information with nonaffiliated third parties, subject to certain limited exceptions.
- Financial institutions must disclose their privacy policy when they first establish customer relationships with consumers and not less than annually thereafter for the duration of the relationship.

**The Information  
Technology Revolution  
has changed the  
way business is  
transacted, government  
operates, and national  
defense is conducted.**

- The Federal Trade Commission, the federal banking agencies, the National Credit Union Administration, and the Securities and Exchange Commission have the authority to enforce the regulations.

A substantial portion of the GLBA speaks to the sanctity of personal information and the necessity for financial institutions to protect that information.

### **The Sarbanes-Oxley Act**

The Sarbanes-Oxley Act of 2002 was signed into law July 30, 2002. At first glance, it would appear that this corporate accountability legislation has little to do with the Internet and information security, but it's all about the information.

The Act increases the responsibility of corporate audit committees and limits the nonaudit services—including financial information systems consulting services—that an auditor may offer to its clients. It also increases penalties for violations of securities and other laws.

The principal executive and financial officers of corporations are now required to establish and maintain internal controls that ensure the accuracy of the information in financial reports and to evaluate those controls no earlier than 90 days prior to the date of the report. Part of being certain that the information is accurate is being certain that unauthorized parties cannot gain access to and tamper with the information.

### **The President's Critical Infrastructure Protection Board**

On September 18, 2002, the White House published *The National Strategy for Securing Cyberspace*. The document was a draft for comment. It covered a variety of Internet issues, including a "Statement of National Policy" and "Guiding Policy Principles."

- Part of the "Statement of National Policy" reads as follows: "The Information Technology Revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures—cyberspace."

**Technology will continue to change rapidly. New vulnerabilities and threats will be uncovered. Elements of our present programs may be determined to be ineffective in the future.**

The statement goes on to say that “maintaining the integrity of the national economic and social fabric over the long term [in part] requires attention...to the security of information systems...”

- Part of the “Guiding Policy Principles” reads as follows: “[P]rivate sector owners and operators should be encouraged to provide maximum feasible security for the infrastructures they control....”

In the cover letter that accompanied the draft, then-chair Richard A. Clarke and vice-chair Howard A. Schmidt note:

Technology will continue to change rapidly. New vulnerabilities and threats will be uncovered. Elements of our present programs may be determined to be ineffective in the future. America’s cybersecurity strategy must be dynamic and continually refreshed to adapt to the changing environment.

Clarke is cited in *CISO: The Magazine for IT Security Leaders* (September 2002) as suggesting that corporate officers be required to certify their information security on their filings with the Securities and Exchange Commission, as was done during the Year 2000 (Y2K) crisis. Clarke notes, “Just asking for that information had an influence on Y2K remediation.”

Clarke, the president’s top information-security advisor, has been a member of the National Security Council since 1992 and has been in government service for 30 years. He is now leaving government service and is reportedly turning over the reigns to Schmidt, a past chief security officer for Microsoft Corp.

According to “A Pared-Back Security Initiative: Revised Plan Focuses on Agencies,” *Washington Post* (January 7, 2003), this governmental initiative is being scaled back, with much of the responsibility for cyberspace security being transferred to the new Department of Homeland Security.

In an article in *Computerworld* (January 3, 2003), Clarke said that vulnerabilities in the nation’s critical infrastructure stem primarily “from unknown security holes in widely deployed software and from the constant influx of new technologies that often have unintended consequences.” He also pointed out al-Qaida’s stated commitment to disrupting the U.S. economy.

***As long as we have vulnerabilities in cyberspace and as long as America has enemies, we are at risk of the two coming together to severely damage our great country.***

In his resignation message on January 27, 2003, Clarke wrote:

As long as we have vulnerabilities in cyberspace and as long as America has enemies, we are at risk of the two coming together to severely damage our great country...Therefore, it is essential to the health of the nation's economy and the security of the country that we aggressively implement the National Strategy to Secure Cyberspace.

Surprisingly, in spite of the threats, the new federal guidelines, issued on February 14, 2003, are not as strict as many of the recommendations set forth by the President's Critical Infrastructure Protection Board.

## Best Security Practices

While the specifics of the best security system for one company may differ from the best security system for another company, there are certain basics that apply across the board.

According to the CERT® Coordination Center (CERT/CC), there are over 50 practices to help systems administrators protect their networked computer systems. Those practices can be grouped into five top-level steps:

1. hardening and securing systems by establishing secure configurations;
2. preparing for intrusions by laying the proper groundwork for detection and response;
3. detecting intrusions quickly;
4. responding to intrusions in a way that will minimize damage; and
5. improving security for the future.

CERT stands for "computer emergency response team." CERT/CC was started by DARPA, the Defense Applied Research Projects Agency, part of the U.S. Department of Defense, in December 1988, in response to an Internet worm that crippled approximately 10 percent of all the computers connected to the Internet at that time.

CERT/CC is located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

## Information Security

As both the importance and the vulnerability of data have expanded, so too has the importance of securing that data. On the frontline of that effort is the chief information security officer (CISO).

### The Process and the Tradeoffs

Turning again to Bruce Schneier and his book, *Secrets and Lies: Digital Security in a Networked World*:

Security is a process, not a product. As a process, it has many components. And like any process, some of these components are sturdier, more reliable, more oiled, more secure. Moreover, the components have to fit together. The better they fit together, the better the process works. Often, it's the interfaces between components that are the least secure.

Information-security components include cryptography (encryption of data), firewalls, intrusion-detection systems, access tokens, and countless other techniques to be sure that only those authorized to access data can actually access data.

According to Harry Shah, senior vice president with Marsh's Technology & Information Services, "It is impossible to obtain perfect security—every organization is going to have some point of vulnerability. Besides tradeoffs between security and ease of use, getting the appropriate funding is a perpetual battle. It is not economical for a business to provide an ultrasecure environment. The key here is that organizations have to accept some level of risk, a delicate balance that is a moving target in today's world. I truly believe that one needs to take a holistic view of information-security programs that is integrated into the overall environment and becomes part of the corporate culture."

The security needs of each organization are unique to that organization. For example, an organization that has one location will have different network and security needs than an organization that has many offices countrywide or worldwide. There is no one-size-fits-all solution. Each organization must come up with its own solutions, uniquely tailored to that organization.

## Top 10 Web Vulnerabilities

On Monday, January 13, 2003, the Open Web Application Security Project (OWASP) unveiled its list of the 10 most critical Web application security problems:

1. **unvalidated parameters**—information from Web requests not validated before being used;
2. **broken access control**—restrictions on authenticated users not properly enforced;
3. **broken account and session management**—account credentials and session tokens not properly protected;
4. **cross-site scripting (XSS) flaws**—transport of an attack to an end user's browser;
5. **buffer overflows**—improper validation of input;
6. **command injection flaws**—passing parameters when external systems or the local operating system is accessed;
7. **error-handling problems**—improper handling of error conditions that occur during normal operation;
8. **insecure use of cryptography**—improperly coded cryptographic functions that result in weak protection;
9. **remote administration flaws**—remote access via improperly protected Web interfaces; and
10. **Web and application server misconfiguration**—insufficiently strong server configurations.

OWASP is a Washington, D.C.-based open-source community project staffed by volunteers around the world. Source: <http://www.owasp.org>.

## The Reporting Structure

Another critical issue that an organization must decide is: To whom does the CISO report? There are at least three different reporting structures: to the chief financial officer, to the chief information officer, or to the chief executive officer.

- **Reporting to the CFO:** When the CISO reports to the chief financial officer, the CISO may have more influence in getting the funding for security initiatives. On the other hand, the CFO may not fully understand IT and security issues and, thus, may be reluctant to fund some initiatives that the CISO knows to be critical.
- **Reporting to the CIO:** When the CISO reports to the chief information officer, there may be conflicts of interest. While the CISO and the CIO may speak the same language—"computerese"—some security initiatives may interfere with or at least slow down some IT projects. The CIO may opt for sidestepping some security procedures in order to complete a project on time. If the CISO reports to the person who chooses to break the rules, it may be difficult for the CISO to enforce them.
- **Reporting to the CEO:** When the CISO reports directly to the CEO, there is some assurance that the CEO will be made aware of all the information-security concerns. However, the CEO may have too many other issues on his or her plate to give information security the attention it deserves. The larger and more complex the organization, the less practical this reporting structure.

Regardless of the reporting structure, it's important for the CISO to have sufficient standing in the organization to be taken seriously. He or she should be a senior manager. As well, there should be someone who reports to the CISO—a security officer or representative—in every business unit.

## No Safety Net in Traditional Insurance

In “Riskier Business,” *Boston Globe* (February 17, 2003), the author, Beth Healey, notes, “What happens is that when claims start flowing heavily in a quirky or complex area, the insurance underwriters who analyze claims and set rates pull the plug.”

Healey goes on to note that computer viruses are a good example, citing the “SQL Slammer” that circled the globe, wreaking havoc with productivity in January 2003.

The article also quotes Robert Hartwig, chief economist for the Insurance Information Institute, who explains, “There are a lot of new and novel types of claims being filed on policies that never contemplated these type of claims.”

## The Insurance Response

The primary goal of any risk manager—and any CISO—is to reduce or eliminate risk. Insurance should be the court of last resort. But because it is impossible to eliminate all risk, organizations need also to fund the contingency of loss. There are many ways to do this, but the most common—and often the most cost-effective—is to purchase insurance.

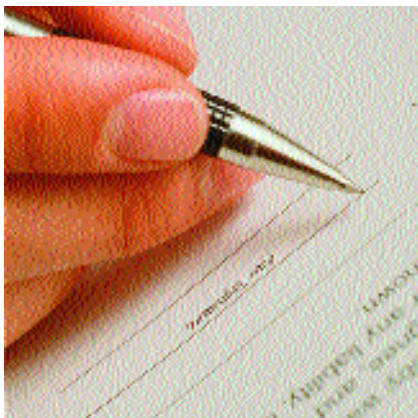
### Traditional Insurance

The traditional commercial-insurance market often uses forms developed by Insurance Services Office, Inc. (ISO). Others often use the ISO forms as a starting point, adding or deleting coverage to tailor policies to their own needs and the needs of their clients.

Two of the primary forms used to provide coverage are the Building and Personal Property Coverage Form (CP 00 10) and the Commercial General Liability Coverage Form (CG 00 01). Originally drafted in the early 1980s, these forms have undergone a number of revisions over the years, in response to various events, including court interpretations of the coverage provided and changing exposures to risk.

Two decades ago, when the original forms were drafted, the Internet was only getting started as a commercial and interpersonal means of communication. The concepts of cyberspace, cybersecurity, cybercrime, cyberinsurance—cyberanything—were in the minds of only a select few. The primary assets of businesses were their tangible assets. There was little cause for concern in the minds of those who draft insurance-policy language. As a result, neither the Building and Personal Property Coverage Form nor the Commercial General Liability Coverage Form addressed such issues as data and cyberspace.

In recent years, there have been various claims involving data and the Internet that ended up on various courts, with rulings that conflicted with one another, largely because they were addressing issues not included on the coverage form. Thus, ISO has revised these and other forms to address specifically the scope of coverage available—and not available—for claims involving the Internet, data, and other like issues.



**Building and Personal Property Coverage Form:** The April 2002 revision of this form, the latest edition, specifies that “Covered Property does not include...Electronic data, except as provided under Additional Coverages - Electronic Data.” The exclusion goes on to delineate what is meant by electronic data—“information, facts or computer programs stored as or on, created or used on, or transmitted to or from computer software (including systems and applications software), on hard or floppy disks, CD-ROMs, tapes, drives, cells, data processing devices or any other repositories of computer software which are used with electronically controlled equipment.” The form goes on to clarify, “the term computer programs, referred to in the foregoing description of electronic data, means a set of related electronic instructions which direct the operations and functions of a computer or device connected to it, which enable the computer or device to receive, process, store, retrieve or send data.”

The section on additional coverages provides a very minimal amount of coverage—“\$2,500 for all loss or damage sustained in any one policy year, regardless of the number of occurrences of loss or damage or the number of premises, locations or computer systems involved.” Obviously, this amount of coverage is insufficient for all but the smallest of businesses. Thus, this latest version of the Building and Personal Property Coverage Form makes it very clear that this is not the place to look for coverage for your information assets.

Property coverage for mid-size and large companies is often written on manuscript forms, with coverage hand-tailored to the individual company’s needs. However, many of those companies are facing similar coverage problems. For example, according to Jill Dalton, North American practice leader for Marsh’s Property Practice, “Property insurers are amending their policies across the board to exclude coverage for computer viruses.”

**Commercial General Liability Coverage Form:** The October 2001 revision of this form, the latest edition, specifies that certain parts of “Personal and advertising injury” coverage do not apply to organizations in media and Internet-type businesses—advertising, broadcasting, publishing, or telecasting;

**In the wake of  
September 11 and  
in a still-hardening  
insurance market,  
insurers are looking  
to reduce, not expand,  
the scope of coverage.**

designing or determining content of Web sites for others; and Internet search, access, content, or service providers.

While this exclusion does not apply to organizations that merely place frames, borders, or links, or that advertise for themselves or others anywhere on the Internet, it does apply to organizations that host, own, or control electronic chatrooms or bulletin boards.

The personal and advertising injury coverages excluded for such companies include such offenses as:

- publication, in any manner, of material that slanders or libels a person or organization or disparages a person's or organization's goods, products, or services;
- publication, in any manner, of material that violates a person's right of privacy;
- use of another's advertising idea in your advertisement; and
- infringing upon another's copyright, trade dress, or slogan in your advertisement.

And where there is no coverage, there is normally no defense of any claim.

**Other policies:** Other coverages—such as employee dishonesty, electronic data processing (EDP), and umbrella liability—vary widely. Some may contain some protection for information risk. For example, some EDP policies include some protection for viruses. However, these policies were, for the most part, designed before the Internet was quite so substantial a part of daily life. Coverage, in most, is incomplete at best. And some insurers are drawing back, retrenching. In the wake of September 11 and in a still-hardening insurance market, insurers are looking to reduce, not expand, the scope of coverage.

According to Henry (“Hank”) Whiting, managing director with Marsh’s Information Risk Advisors, “The bottom line is that, just as insurers had not anticipated terrorism as a major source of loss and, thus, are now charging substantial premiums to include coverage, so too, most insurers had not anticipated the frequency and severity of IT-related loss. They simply have not priced policies to include the cost to cover damage done by hackers, viruses and other malicious code, or any of the other Web-related risks.”

## Hacker Insurance

Coverage for damages caused by hackers, viruses, and other perils of the Internet has only been around for a few years. Until recently, few companies seriously entertained the thought of spending their insurance dollars on what seemed to be a “fringe” coverage—particularly in a hard insurance market where almost every policy costs more than it did last year.

But such events as the “SQL Slammer” have made CEOs, CFOs, and risk managers take more notice of this area of exposure. In “Hacker Insurance Market Boosted by Cyberattacks,” *KPMG Insiders* (January 27, 2003), the author, Gina Keating, notes, “Hacker insurance, also known as ‘network risk insurance,’ has been on the market for about three years, but is expected to explode from a \$100 million sideshow into a \$2.5 billion behemoth by 2005....”

The article notes that hacker insurance is expected to become more common because many expiring policies are being renewed with policies that contain explicit exclusions for hacker-related losses.

## Cyberinsurance

When a new exposure to loss develops, certain brokers and insurers will invariably rise to the challenge, creating new products to help their clients fund the potential for loss in the new area. In the 1980s, computer fraud was almost unknown, and coverage was only available from a few specialty insurers. Now, it’s so standard that it’s included as an option on some ISO forms.

The same progression—from unknown, to rare, to commonplace—has occurred for other exposures, such as employment practices and fiduciary liability, and is now occurring for risks related to the Internet. The following are some of the coverages that have been developed by those in the forefront.

**Liability:** Generally, the most expensive claims are for third-party liability. There are now policies available that will fill the gaps created by the Internet exclusions in standard ISO policies. Some insurers offer policies that combine the standard commercial general liability coverages with the additional coverages needed for doing business—or just being—online. The following are some of the areas covered by this new breed of policy.

- Media or content liability coverage is available for allegations of a wide range of offenses that may arise out of Internet activities, such as:
  - any form of defamation or other tort related to disparagement or harm to character, including libel, slander, product disparagement, trade libel, infliction of emotional distress, outrage, or outrageous conduct; infringement of copyright, domain name, title, slogan, trademark, trade name, trade dress, mark or service name, or any form of improper deep-linking or framing;
  - plagiarism, piracy, or misappropriation of ideas under implied contract or other misappropriation of property rights, ideas, or information; and
  - any form of invasion, infringement, or interference with rights of privacy or publicity, including false light, public disclosure of private facts, intrusion, and commercial appropriation of name, persona, or likeness.

**In the world of cyber-insurance, data is property. Coverage is available that provides for the cost of reconstructing lost proprietary data, trade secrets, and computer programs as a result of such occurrences as security breaches, viruses, and malicious damage by hackers.**

- Security liability coverage is available for actual or alleged breach of duty in the event of a computer attack—including unauthorized access, unauthorized use, disclosure of confidential or private information, or the transmission of a malicious code. This would include those increasingly frequent instances when confidential personal information is stolen and misused.

**Property and crime:** In the world of cyberinsurance, data is property. Coverage is available that provides for the cost of reconstructing lost proprietary data, trade secrets, and computer programs as a result of such occurrences as security breaches, viruses, and malicious damage by hackers.

In addition to covering that direct loss, coverage is also available to protect the earnings stream derived from Internet activities. Policies generally include loss of income that results from denial-of-service attacks, whether directed at the specific company or at the Internet as a whole.

And coverage can often be extended to include extortion and theft of information assets, money, securities, and other property.

**Identity theft:** Companies that offer consumer credit now have the option of offering or providing their customers with coverage for identity theft. While credit-card holders are not liable for the fraudulent bills racked up when their identities are stolen, the prospect of undoing the damage is daunting.

Ask anyone whose wallet or purse was ever stolen how time-consuming it was to cancel all the credit cards, get a new driver's license, and so on. Identity theft is worse because it's not just one's own credit cards, but credit cards and other debt mechanisms established by the party fraudulently using the consumer's information.

Coverage is available with limits ranging from \$250 to \$25,000 per consumer per incident for the cost to the individual consumer in personal expenses and work time lost in the process of undoing the damage. Companies can either offer the coverage to consumers or pay for it themselves as part of the loyalty or customer services they provide.

***As new sources of loss have come to light, new coverages and policies have been developed.***

Additionally, some employers are looking into the possibility of offering this coverage to their employees as a voluntary benefit, much as they do group auto insurance or group umbrella liability insurance. Premiums for coverage could be deducted from each paycheck in the same manner as other employee-paid benefits.

**Other policies:** Insurance for cyberspace is fairly new and still evolving. As new sources of loss have come to light, new coverages and policies have been developed. Just as cyberspace is virtually limitless, so are the risks—and so are the policies being designed to meet those risks.



## Conclusion

Information is the lifeblood of most companies. Losing that information can create anything from a minor inconvenience to a major headache. The consequences could run to billions of dollars in damages and loss of reputation to one's own property and to third parties.

The first answer is to protect oneself, but just as there is no building that is 100 percent burglar-proof, there is no computer or computer network that is 100 percent hacker-proof or 100 percent virus-proof. Every advance in information technology precipitates another advance in strategies to compromise the integrity of that technology—a cyberarms race that shows no sign of slowing down or ever coming to an end.

The final answer to any risk is finding a way to fund the consequences when the risk is not 100 percent avoidable. More often than not, insurance—in this case, cyberinsurance—is the answer.

## Notes

---

## **About Marsh & McLennan Companies**

### **Marsh**

Marsh meets the global needs of its clients through a wholly owned network of more than 400 offices in over 100 countries. In every country, Marsh combines a deep knowledge of local risk issues with the ability to tap global insurance and capital markets for solutions tailored to client needs. Since its founding more than 130 years ago, Marsh has steadily built its business beyond insurance broking to encompass a full range of services to identify, value, control, transfer, and finance risk.

### **Putnam Investments**

Putnam Investments plays a key role in the financial-planning decisions of millions of individuals and thousands of institutions. With more than 60 years of investment experience, Putnam provides investment-management services to over 2,700 institutional and 401(k) clients and manages more than 14 million individual-shareholder accounts.

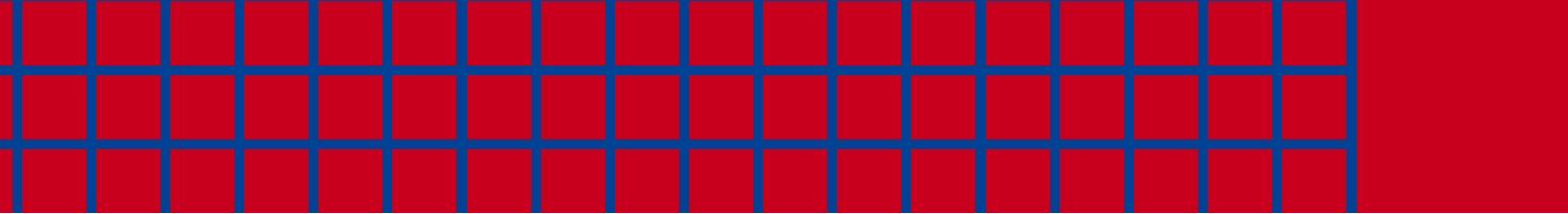
### **Mercer**

Mercer provides clients with solutions linking the three most enduring dimensions of business success—business design, organizational design, and people strategy. It does this through a unique array of consulting expertise:

- Mercer Human Resource Consulting is the global leader in human-resource, employee-benefit, and compensation consulting.
- Mercer Management Consulting helps clients achieve sustained shareholder value through innovative business design.
- Mercer Delta works with CEOs and senior teams of major companies on the design and leadership of large-scale transformation.
- National Economic Research Associates (NERA), the leading firm of consulting economists, devises solutions to problems involving competition, regulation, finance, public policy, and business strategy.
- Lippincott Mercer, the premier corporate-identity firm, helps clients create, develop, and manage their brands throughout the world.

### **Collaborative solutions**

Increasingly, the companies of MMC are working together to offer multifaceted client solutions. In so doing, they bring to bear a unique range of perspectives on the toughest issues confronting clients, industry by industry. Risk management is the focus for many of these collaborative services. Through the expertise of Marsh and Mercer, MMC is uniquely positioned to offer clients risk solutions and advice across the full range of their strategic, financial, operating, and hazard risks.



The information contained herein is based on sources we believe reliable, but we do not guarantee its accuracy. Marsh makes no representations or warranties, expressed or implied, concerning the financial condition, solvency, or application of policy wordings of insurers or reinsurers. Past performance does not guarantee future outcome. Marsh undertakes no obligation for publicly updating or revising any information contained in this report, whether as a result of new information, future events, or otherwise. This document is not an offer to sell, nor a solicitation of an offer to buy, any financial instrument or insurance or reinsurance program.

The materials, data, and/or methodologies used in this report are proprietary to Marsh Inc. The dissemination or use of this report without Marsh Inc.'s express written permission is prohibited. Marsh does not render legal advice or services, and counsel should be consulted concerning legal issues.

**Risk Alert: Information Risk**

© 2003 Marsh Inc. All Rights Reserved.

**Marsh. The world's #1 risk specialist.<sup>SM</sup>**

Item#: 100031 03/03