

Insurers have moved out in front of technology risks with cyber exposure coverage products. Clients are beginning to catch on.

Cyber Risk: Insuring the Escalating Threats From New Technology Exposures

BRAD GOW

Information technology has wrought vast and rapid changes in the global economy. In virtually every industry, a revolution in computing and communications has radically altered the way business works. The ability to send massive amounts of data around the world in milliseconds has enabled businesses to communicate and collaborate worldwide, to set up back office and customer service operations an ocean away, and to efficiently build and market products globally. Whole new industries have arisen, from Internet portals to online retailers. This transformation has created a wide range of new opportunities for those businesses adept enough to take advantage of new technology.

New Opportunities, New Risks

The Information Age, however, has engendered not only new opportunities but also new risks and liabilities. As business becomes ever more information-based, the value of that information — and the ease with which it can be transmitted — creates opportunities for criminals who can quickly turn purloined data into profits. Companies that fail to adequately protect sensitive proprietary and client information risk not only the loss of sales and customers but also claims and lawsuits for loss sustained by customers and the public at large.

The risks have escalated sharply in recent years as computer-savvy criminal gangs have mounted increasingly sophisticated attacks to steal personal and proprietary data from corporate networks. The heightened threat level has made data security a critical concern for businesses as well as for their clients and customers.

Criminals are not the only entities creating new liabilities for business. Responding to consumer fears about privacy and identity theft, state and federal legislators are mandating increasingly strict standards for collecting, managing, and protecting sensitive data. The technology revolution has been followed by a regulatory revolution.

A rapidly growing specialty market has emerged that offers new coverages specifically targeting the exposures inherent in a digital economy.

The new regulations have transformed the liability landscape for businesses, which now face the possibility of heavy fines and lawsuits should their data-protection efforts fail. Businesses also face severe damage to their reputations as state laws increasingly require them to publicize security breaches.

While businesses typically look to insurance to transfer risk, they cannot count on traditional insurance policies to protect against these new technology risks, because most insurers exclude “cyber” risks from their programs. To deal with the new risks, a rapidly growing specialty market has emerged that offers new coverages specifically targeting the exposures inherent in a digital economy.

This article discusses how technological changes have altered the global economy and the risk landscape for business, how cyber criminals are taking advantage of new vulnerabilities, how new regulations have changed the liability landscape, and how the insurance industry is dealing with emerging and evolving cyber risks.

The Technology Revolution

The ability to accurately calculate, manipulate, and publish huge amounts of data is taken for granted in today’s world of high-powered computers. But the quest to build a machine to accurately perform calculations and print out the results dates to the dawn of the Industrial Revolution. The first efforts to create a mechanical means to reckon repetitive sums, such as interest and astronomical tables, were made by leading 17th Century European intellectuals such as Blaise Pascal and Gottfried Leibniz.¹

The need to produce accurate astronomical tables for navigation and seaborne trade — a crucial market for the nascent insurance industry at Lloyd’s — helped to spur the design in 1820s Britain of a machine to calculate and print mathematical progressions. English mathematician Charles Babbage endeavored at the time to build a mechanical computer called the “Difference Engine” — a machine that was finally built and proven to work in 1991.² The calculating portion of Babbage’s machine, built for the Museum of Science in London, has 4,000 moving parts, is 11 feet long, and weighs nearly three tons.³

More than a century after Babbage designed his mechanical computer, the first modern programmable electric computer was built on an even more massive scale. The Electronic Numerical Integrator and Computer, or ENIAC, developed to calculate artillery firing ranges for the U.S. Army and dedicated in 1946, weighed 30 tons, had 18,000 vacuum tubes, and filled a large room.⁴

The development of integrated circuits in 1959 sparked the trend of ever-increasing computing power, summed up by Intel Corp. founder Gordon Moore’s famed prediction, known as Moore’s law, that the number of transistors that could be placed on a computer chip would double every two years.⁵ The rapid escalation in computing power is highlighted by the fact that a three-pound laptop today has a thousand times more computing power than ENIAC.

The Internet Revolution

The revolution in computing was accompanied by a revolution in communications. The Internet Age began in 1969, when researchers at University of California at Los Angeles connected a computer to a refrigerator-sized switch, the first step in getting

two computers to talk to each other.⁶ Twenty years later, the World Wide Web was created by Tim Berners-Lee, who also developed the first browser a year later, in 1990.⁷

The growth in Internet communications and business since that time has soared. The Internet began to take off with the popularization of Netscape's browser in the mid-1990s. By 2004, three out of four Americans had access to the Internet at home.⁸ Just over a year and a half later, two out of five Americans, or nearly 121 million people, had high-speed broadband access to the Internet.⁹

Business has moved online just as quickly. While a major corporation setting up a consumer Web site was still news in the mid-1990s, by 2003, nearly \$1.6 trillion in goods and services were sold online in the United States, accounting for roughly 10 percent of all shipments in industries tracked by the U.S. Census Bureau.¹⁰

Besides transforming traditional industries, the Internet has spawned new ones. Google grew in just 10 years from an idea for an Internet search engine developed by two Stanford University graduate students to a publicly traded company with a market value of more than \$100 billion, rivaling the worth of the world's most valuable and long-established companies.

The Risks of the Information Economy

Advances in computing and telecommunications have transformed business. Where once business ran on reams of paper, much of commerce is now conducted via streams of digital data. Information technology has become an integral part of every industry, from agriculture to professional services.

The global public Internet also allows computer users to buy goods online, pay electronically, and query corporate networks for information. Now anyone with access to a computer can connect to corporate Web sites, which, if not properly managed and secured, can be used as gateways to networks holding vast amounts of valuable personal and proprietary information. By exposing their networks to the outside world, companies have opened themselves up to new risks. The data that companies have spent decades collecting represents not just a highly valuable business asset but also a treasure trove to defend.

At the same time that businesses have built huge databases of consumer information and developed increasingly powerful e-commerce capabilities, they have paved the way for criminals to exploit overlooked vulnerabilities in their technology. Internet gateways to corporate systems offer openings to criminals as well as clients and consumers. While businesses have spent billions of dollars to harden their systems, criminals have kept pace by developing new attacks. As Internet-based operations and communications have become critically important for businesses, they have engendered a new class of criminal activity — cyber crime.

As Internet-based operations and communications have become critically important for businesses, they have engendered a new class of criminal activity — cyber crime.

The Criminal Revolution

While technology allows businesses to communicate and collaborate on an unprecedented scale, technology-savvy criminals have taken advantage of new technology-based opportunities to commit crime. Whether by exploiting security glitches to break into corporate systems or by using malicious code to create armies of remote-controlled “zombie” computers, criminals have adopted new technology as avidly as businesses have.

The paradox for business was summed up neatly by authors Stewart Brand and Matt Herron in 1984: “On the one hand, information wants to be expensive, because it's so valuable,” they said. “On the other hand, information wants to be free, because the cost of getting it out is getting lower and lower all the time.”¹¹ Criminals, of course, recognize the value and mobility of digital information and look to steal it. The Internet enables them to do so from a desktop thousands of miles away from where the data are stored.

The theft of information via the Internet is a rapidly growing problem as criminals keep pace with technology and employ increasingly sophisticated and fast-spreading attacks. As new technologies are adapted by wider numbers of people, criminals respond by trying to find new vulnerabilities. For instance, as cell phones and wireless networks become more powerful and allow callers to connect to the Internet, they present increasingly tempting targets. Criminals also have been quick to change their tactics, shifting in some cases from attacks against operating systems to attacks against applications such as media players, database software, and even antivirus programs.¹²

Attacks are difficult to defend against because the worldwide reach of the Internet means they can be launched from individual computers located all over the world.

The increasing sophistication and organization of computer criminals poses a serious threat. No longer is the lone hacker the main concern for corporate computer security. Now, more and more computer attacks are being carried out by professional criminal gangs operating freely from places such as Eastern Europe. Criminals account for about 90 percent of the malicious code being released onto the Internet, according to an estimate by the computer security company Kaspersky Labs.¹³

The motivation for the attacks against computer systems is simple: that's where the money is. There's plenty of illicit profit to be gained from stealing, or even threatening to publish, confidential information.

Malware and Botnets

The most well-known attacks have been highly publicized viruses such Code Red, Sobig, and MyDoom. The MyDoom virus, in early 2004, for instance, spread by sending around 100 million infected e-mails in the first 36 hours.¹⁴ Those viruses, however, rep-

resent just a small fraction of those that are loosed upon the Internet every day. In October 2005, for example, a record 1,685 new viruses and variants hit the Internet, although none were particularly widespread or dangerous.¹⁵

Today, most viruses are being written with illegal profits in mind. Criminals may seek to leave behind bits of code, known as Trojan horses, to track a computer user's key strokes and to steal confidential information such as passwords and credit card numbers. Increasingly, criminals are seeking to infect huge groups of personal computers with code that allows them to remotely control those systems.

These armies of compromised computers, known as botnets, can then be used to send huge amounts of spam or to organize denial-of-service attacks against corporate computer systems or Web sites. By some estimates, nearly three-quarters of all spam is now sent over botnets, with U.S. spammers hiring out time on zombie networks managed from places such as Russia.¹⁶

By using thousands of widely dispersed personal computers to carry out attacks, criminals can hide their tracks or simply switch to a different group of computers when the first is shut down. Fast-spreading viruses have allowed criminals to assemble massive groups of compromised computers. In 2005, Dutch police broke up a ring that had assembled the largest-ever botnet, made up of 1.5 million computers and servers.¹⁷ Criminals have been known to rent out botnets on the black market for as little as \$100 an hour.¹⁸

Cyber Shakedowns

For businesses, distributed-denial-of-service attacks strike at the heart of their Internet operations. By swarming Web sites with thousands of simultaneous hits, these attacks shut out legitimate customers and clients from the site. The MyDoom virus, for example, was used to infect thousands of computers and direct them to attack a software company's Web site at a specific time and date, bringing the site down on schedule.¹⁹

Unscrupulous businesses have also sought to shut down rivals' Web sites. In early 2005, a Michigan owner of a Web-based sportswear business hired a New Jersey teenager to mount denial-of-service attacks against his rivals. The teenager, who was paid

in sports clothes and designer sneakers, not only shut down the rival sites, but disrupted other businesses as far away as Europe.²⁰

Such attacks are difficult to defend against because the worldwide reach of the Internet means they can be launched from individual computers located all over the world. Criminals also have turned to using the mere threat of such attacks as a way to shake down businesses.

The Internet has enabled criminals to update the old "protection" racket with modern technology in a growing crime known as cyber extortion. Rather than threatening to physically damage a business, criminals now threaten to shut down a Web site, release confidential information, damage corporate networks, or erase valuable data. Now, criminals can credibly pose a threat from thousands of miles away and demand that target companies electronically transfer the extortion payments.

Thousands of organizations are believed to be paying off criminals to avoid having their businesses or reputations damaged.²¹ When one online retailer refused to pay, the would-be extortionists posted 25,000 of the retailer's customer's credit card numbers on the World Wide Web.²²

Particularly vulnerable are companies that rely on online business or seasonal sales and can ill afford a shutdown at the wrong time. While payoff demands typically run in the thousands or tens of thousands of dollars, some criminals have sought millions.

The threat that personal information will be misused is a major concern for both businesses and consumers. With identity theft in the headlines every day, consumers are increasingly afraid that they will be stuck holding the bill for fraudulent purchases or phony accounts set up in their name. Businesses are worried that security breaches may cost them dearly, not only in expenses to repair the actual damage but also in lost business from consumers and corporate clients.

Consumer Fears

As electronic commerce has become a part of everyday life, consumers have grown increasingly concerned about identity theft over the Internet. Millions of U.S. citizens have had their personal information stolen, with the thief then ringing up charges on an existing account or opening fraudu-

lent new accounts. The number of U.S. citizens who became victims of identity theft in 2004 was 8.9 million.²³ According to a survey done for the Federal Trade Commission, the losses for all forms of identity theft for 2003 were estimated at nearly \$48 billion for business and resulted in \$5 billion in out-of-pocket expenses for consumers.²⁴ In addition, victims of identity theft had to spend dozens of hours to clear up their accounts.

As consumer fears have intensified, state and federal legislators have reacted with laws to require businesses to take greater steps to protect privacy.

Sixty-two percent of consumers are worried that their financial information could be stolen online, more than the percentage who were concerned about having such fraud happen at a restaurant or a retail store, another survey showed.²⁵ Consumer fears about Internet theft are tied to the portability of information in an online environment. While thefts of personal information at a brick-and-mortar establishment typically take place one account at a time, breaking into a consumer database can allow criminals to harvest thousands of accounts in seconds.

A security breach at a credit card payment-processing company in 2005 exposed more than 40 million accounts to fraud. Information on about 200,000 accounts was estimated to have been copied from the company's network.²⁶ That incident followed a breach earlier in the year when a consumer-data collection company was infiltrated by an identity-theft ring, which gained access to consumer data such as credit reports and Social Security numbers. An estimated 100,000 people nationwide were affected.²⁷

The breach at the credit card payment-processor spurred two U.S. senators to introduce a federal bill that would force companies to notify consumers when the security of their personal information is jeopardized. Such a bill would, however, merely be the latest in a string of increasingly stringent laws aimed at protecting consumers' private information.

The Regulatory Revolution

As consumer fears about identity theft have intensified, state and federal legislators have reacted with laws to require businesses to take greater steps to protect privacy. The first of these laws started out as parts of larger bills regulating the health-care and financial sectors of the economy. Later bills have taken a broader approach, requiring greater data security on the part of all publicly traded companies and mandating that companies notify customers when a breach in security exposes personal information to potential misuse. While the intention was to increase the safeguards for personal information, a side effect has been to force industry to spend billions of dollars to upgrade technology and security procedures.

By making top executives responsible for data security, Sarbanes-Oxley has elevated the issue to the highest ranks of management.

The first regulation at the federal level affecting consumer privacy was the 1996 Health Insurance Portability and Accountability Act (HIPAA), which was aimed primarily at making sure that workers could keep their health insurance and obtain coverage for pre-existing conditions should they change jobs. Spearheaded by Sen. Edward Kennedy (D-Mass.) and Sen. Nancy Kassebaum (R-Kansas), the bill included provisions mandating that health-care providers and insurers keep patients' personal data and medical history private.

At the White House signing ceremony in 1996, President Clinton said the bill would "provide steps to protect the privacy of people in the system..."²⁸ As in so much of politics and regulation, the devil remained in the details, and the privacy regulations were not promulgated and put into effect until 2003.

Failure to comply with the regulations can bring fines of up to \$25,000 annually for multiple violations of each standard, while obtaining information under false pretenses carries fines of up to \$100,000 and up to

\$250,000 if the intent is to sell the information.²⁹

The next federal bill to mandate increased privacy strictures for business was the Financial Modernization Act of 1999, which repealed the Depression-era Glass-Steagall Act and allowed banks to affiliate with insurers and securities firms with fewer restrictions. Better known as the Gramm-Leach-Bliley Act (named after its Republican sponsors Sen. Phil Gramm of Texas, Rep. Jim Leach of Iowa, and Rep. Thomas Bliley of Virginia), the law also mandates that financial institutions take greater measures to protect the personal financial information of their customers.

The bill requires financial institutions to protect personal financial information from unauthorized access and to provide customers with an outline of the institution's privacy practices, including the kind of information the company collects and the conditions under which that information is shared with others.³⁰ Violations can bring civil penalties of up to \$100,000 for financial institutions as well as fines of up to \$10,000 for officers and directors. Criminal penalties can be as severe as up to five years in prison.

Just as HIPAA and Gramm-Leach-Bliley increased the regulatory burden on the health-care and financial industries, the Sarbanes-Oxley Act of 2002 made data security a priority for every publicly traded business.

Sarbanes-Oxley and Notification Laws

Among the federal laws affecting data privacy, the Sarbanes-Oxley Act, which came to fruition in reaction to big accounting scandals, has been particularly difficult for business. Sponsored by Maryland Democrat Sen. Paul Sarbanes and Ohio Republican Rep. Michael Oxley, the law mandates stricter accounting controls at publicly traded companies.

Among the law's many provisions — and 40 pages deep in the bill — are the few paragraphs of Section 404 that have left businesses scrambling. Section 404 requires business management to establish and maintain adequate internal controls for financial reporting and to provide an annual assessment of those controls.³¹ Because financial data are now hosted on computer networks, compliance with the law means that companies must pay particular attention to protecting the integrity of their networks. By making top executives responsible for data security,

Sarbanes-Oxley has elevated the issue to the highest ranks of management.

In addition to federal laws, businesses have had to keep up with privacy initiatives at the state level. Chief among those is the 2003 California law, SB 1386, which requires companies to notify consumers when their personal information has been exposed to possible misuse. Other states have since followed California's lead in requiring some notification, and two U.S. senators introduced a federal bill in 2005.

After the breach at a credit card payment-processing company in 2005 exposed millions of accounts to fraud, Republican Sen. Arlen Specter of Pennsylvania and Democratic Sen. Patrick Leahy of Vermont introduced a bill that would make notification of customers mandatory nationwide.

"Insecure databases have become low-hanging fruit for hackers looking to steal identities and commit fraud during a time when we are seeing a troubling rise in organized rings that target personal data to sell in online, virtual bazaars," Leahy said in a press release after introducing the Personal Data Privacy and Security Act.³²

While consumers may welcome the tougher standards, businesses face substantial costs to meet the new mandates. The notification laws have forced businesses, which formerly may have tried to keep networking breaches quiet, to come forward and have made it impossible to avoid reputation-damaging publicity. Businesses also face steep costs to notify tens of thousands or even hundreds of thousands of customers in the event of a breach.

All told, complying with new data security standards will cost U.S. businesses some \$80 billion over the next five years, according to a 2005 study by AMR Research.³³ The Boston-based research firm estimated that spending on compliance in 2005 alone would total more than \$15 billion. Spending for compliance with Sarbanes-Oxley was estimated at nearly 40 percent of the total, or more than \$6 billion, while spending on HIPAA was estimated at \$3.7 billion, or just under one-quarter of total spending. While technology forms a significant part of those costs, investment in internal staff was the largest cost.

A Threat to the Balance Sheet

The cost to business of survival in the digital economy cannot be measured simply by the billions

of dollars required to comply with new regulations. As the criminal threat has escalated, so too have the dangers. The failure to adequately protect confidential data can lead to a loss of business, leave a company open to lawsuits, and severely threaten its balance sheet.

In the past, businesses could seek to protect their assets with physical barriers and security guards. In the digital age, the critical battle has moved online. As businesses seek to take advantage of the Internet, they have to allow outsiders to access portions of their carefully protected computer systems, making themselves vulnerable in the process. As a company's dependence on the Internet grows, so does its potential loss exposure.

The failure to protect confidential information not only can damage a company's reputation in the public sphere but also can open it up to litigation.

Naturally, criminals target the companies that depend on the kind of personal information that is most valuable for Internet scam artists. Because they routinely deal with credit card information, online retailers, financial-data processing companies, and the medical industry are among the most attractive targets. For example, online fraud was expected to cause losses of about \$2.8 billion in electronic commerce in 2005, up \$200 million, or 8 percent, from 2004, according to a study by CyberSource Corporation.³⁴

Besides fraud, businesses face other losses from cyber crime and security breaches, such as lost productivity, system downtime, and the costs of repair and recovery.

Cyber Exposures and Liabilities

Companies that depend on the Internet for their livelihood can be devastated by attacks that shut down their Web sites. Businesses also face shutdowns when crucial infrastructure is attacked or operations at a vendor's site go down. For example, the Slam-

mer virus in 2003 temporarily brought down most of a national bank's automatic teller systems, as well as a major airline's online reservation system.³⁵ The Sobig virus the same year disrupted U.S. freight and passenger rail traffic.³⁶

Besides Web site and network shutdowns, businesses have to factor in the cost of lost trade secrets and lost proprietary information. If crucial product plans are corrupted or stolen, a business could be set back for months as it tries to restore the data or it could be forced to recreate months of work to get back to where it was, at the same time facing the possibility of losing a critical market opportunity.

Businesses should implement widely recognized standards for data-management security.

In addition to those risks, however, businesses face some worrying exposures that may not be as apparent, such as the loss of future business as customers or clients lose confidence in the company's ability to protect private information.

For instance, when a security breach at a credit card payment-processor exposed about 40 million accounts to potential fraud, major credit card brands quickly said they would stop using the company, dealing it a potentially fatal loss of business.³⁷ As a company's reputation suffers among its clients and consumers, its investors also may become wary, potentially hurting its market value and its ability to attract new investors.

The failure to protect confidential information not only can damage a company's reputation in the public sphere but also can open it up to litigation. When the security breach at the credit card processor became public, lawsuits accusing the company of negligence and seeking class action status were quickly filed.³⁸

In addition, businesses that rely on outside information technology (IT) suppliers need to recognize that while data services, such as transaction processing, billing, and collecting, may be contracted to outside vendors, companies cannot outsource the responsibility for protecting confidential data.

Critical data becomes especially vulnerable when it moves outside of a company and beyond the borders of the company's own security and risk management procedures. Businesses can still face substantial fines, lawsuits, damaged reputations, and a loss of consumer and investor confidence if a breach at an outside IT service provider exposes confidential data.

Making Data Security a Priority

For most of the four decades since businesses began moving to computerized operations, securing systems and networks was treated as one of many issues for the information technology staffs and not as a concern for top management. That approach made sense when security concerns were focused on keeping out teenaged hackers, but the threat level has since escalated sharply with the entry of organized gangs into computer crime.

Now, a failure to adequately secure a company's network and personal and proprietary data can jeopardize the future of the entire organization. Because the threats are continually evolving, security is an issue that needs to be kept on the front burner. The survival of the business may depend on management's focus on keeping personal and proprietary data confidential.

Assess and Prioritize Vulnerabilities

The first task for any organization in assessing its vulnerabilities and potential risks is to catalogue the kind of data that it collects and stores. That information should then be prioritized by its value and the potential risks its loss or theft would pose.

For example, companies that collect and process confidential consumer data, such as credit card accounts, need to take into account the legal and reputational exposures they face should that information be exposed through security lapses or theft from them or a contractor. Businesses need to be careful not only with the confidential client and consumer information but also with personnel information. All companies keep records such as Social Security numbers that can be misused if not properly guarded.

Evaluate Security for Intellectual Property

Companies should evaluate how they secure their own intellectual property. Businesses that depend on keeping intellectual property secret need to assess the

potential risk in exposing that material to third parties, including the risk of outsourcing work involving proprietary material to countries without a strong record of intellectual-property protection.

Once a company has inventoried its data and intellectual property, it should set out clear procedures and policies for handling that data and for keeping confidential information private. Businesses should implement widely recognized standards for data-management security, such as ISO standards, and make sure that third-party technology contractors comply with such standards as well. The security procedures should cover everything from the mainframe to the laptop.

Enforce In-House Security

As part of a concerted focus on security, companies need to enforce their in-house security measures. That effort should be driven by top management and its importance continually stressed to employees. Companies should educate employees as to proper procedures for handling proprietary information.

Along with establishing and communicating security standards to employees, companies should make a concerted effort to examine data security at every stage of the information lifecycle, from collection through storage and transmission. Criminals seek to attack corporate security at the weak points, so companies need to make a thorough assessment of their vulnerabilities at every point in the process.

Create Security Audit Checklists

To keep track of their data-security programs and to ensure that they are up-to-date, companies should devise audit checklists to periodically evaluate and test their data security. Along with scheduled evaluations, companies should regularly update their procedures to take into account both new risks and new technologies.

Extend Security Beyond Technology to Employees

While making sure that their networks and their security procedures are strong enough, companies should not limit their measures to technology but should also take into consideration the human element. Employees remain a major source of breaches, through both inadvertent mistakes and willful misconduct.

For that reason, it is imperative to properly vet employees who will have access to sensitive information, from part-time employees to executives. A part-time employee can compromise confidential data just as effectively as a skilled hacker. Besides their own employees, companies should make sure that any technology vendors that they use also vet their own employees, including running criminal background checks.

Relatively small market penetration may be due to lack of appreciation for the severity of emerging cyber risks and lack of knowledge about new coverages available.

Protecting Data Outside the Enterprise

Data becomes more vulnerable when it leaves a company's systems, so particular care is needed when shipping physical copies of confidential information to make sure that records are kept safe through every step of their journey. Because digital technology allows the storage of massive amounts of data in a small space, media such as disks or tapes containing information can easily be misplaced or stolen. Companies need to make sure that they keep track of all physical copies of any kind of data while in transit.

Check Shippers' Security Standards

In two separate incidents in 2005, one major bank reported that computer tapes containing account data on 3.9 million customers had been lost in transit, while another major bank said it had lost computer tapes with data on 1.2 million customers.³⁹ To avoid such incidents, companies need to make sure that their shippers adhere to adequate standards to protect back-up tapes and disks in shipment. Measures can include barcodes or radio frequency identification tags to enable the constant tracking of physical copies of data in transit.

Confirm Outside Contractors' Security Measures

As more and more companies seek to cut costs by outsourcing information-technology functions to domestic and foreign contractors, they often fail to take into account the risks that come along with sending vital business processes or confidential data outside the company. Companies need to carefully assess potential contractors to make sure that their data security standards and measures are strong enough to protect their clients.

In the cyber insurance specialty market, products are available to meet the full range of new exposures.

Vet Your Vendors

Companies should ask potential vendors to detail their formal records-management process. They also should ensure that vendors meet applicable legal and regulatory standards and should check to see if a potential contractor has a history of violations. Once a deal is signed, managers should demand regular status reports on security from their technology vendors. Companies that don't adequately vet a potential IT vendor may find that their new risks far outweigh the potential cost savings.

Insuring Cyber Risks

Even the most rigorous data-security measures cannot prevent all losses, such as those from a so-called "zero-day" attack, where hackers exploit a new vulnerability that software vendors have not yet had the opportunity to patch. While many companies have made strong moves to strengthen their data security, far fewer have taken advantage of risk transfer opportunities offered by the insurance industry. According to the 2005 CSI/FBI Computer Crime and Security Survey, only 25 percent of respondents (in a group of security-focused companies) had purchased insurance to cover their organizations against cyber risks.⁴⁰ That relatively small market penetration may be due to both a lack of appreciation for the severity of the emerging cyber risks and a lack of knowledge

about the new coverages available.

Just as it has taken time for businesses from banking to retailing to adopt and adapt to new technology, so it has taken the insurance industry time to understand the new risks and to assess the potential pitfalls and opportunities. While insurers have long experience with traditional property and casualty risks such as fires, floods, and theft, technology has magnified some traditional risks in unexpected ways and created entirely new exposures.

New Risks Require New Insurance Products

Before the Internet, thieves would have to steal one credit card number at a time or perhaps break into an office to steal files filled with personal information. Now, criminals can extract information on thousands of accounts in seconds from thousands of miles away. Besides loss from theft, the insurance industry has had to recognize the potential for class action lawsuits, damages, and losses caused by network shutdowns and by the misuse of intellectual property. As insurers have recognized the scope of the risks, they have begun to develop specific products to deal with the new exposures.

Hurt by its past experience of providing coverage for poorly understood risks such as asbestos and pollution claims, the insurance industry has been seeking to avoid repeating the mistake with regard to digital exposures. Reinsurers have become particularly wary as the potential for accumulation of losses with no geographic limits or legal boundaries has become apparent. A major worldwide virus, for instance, could cause massive losses around the world, potentially leaving a reinsurer on the hook for large payments.

Over the last few years, insurers have gone through a process of separating the new risks from the traditional ones. Initially, the new exposures were handled through traditional lines of coverage, but the industry has since excluded cyber liabilities from standard policies. Standard ISO general property and liability forms have been rewritten to affirmatively exclude cyber exposures. In addition, larger insurers have excluded cyber exposures from their standard forms. Because they cannot accurately price the risks, traditional insurers that lack the expertise to fully assess a potential insured's risk management and loss protection measures for network security and data security management have not been eager to underwrite cyber exposures.

Development of a Specialty Market

In the meantime, a specialty market has developed among companies willing to devote the resources to understanding the new risks and developing products for cyber exposures. The market for dedicated cyber coverage has grown rapidly as insurers have sought to take advantage of new opportunities while carefully managing their exposures.

The specialized coverages were first offered a half-dozen years ago, but many of the new products have been developed only over the last three or four years.

The fluid nature of the current market is highlighted by the variety of approaches by which insurers have chosen to address cyber exposures. Some insurers have targeted high-risk industries, such as financial institutions or online retailers, while others have looked to extend cyber coverage to companies with more moderate, but still substantial, risks. Insurers have developed a wide range of products, leaving buyers in the position of having to do a lot of homework to come up with the right policy. For instance, buyers can opt for coverage for specific risks or purchase protection for the spectrum of cyber exposures.

New Coverages

In the cyber insurance specialty market, products are available to meet the full range of new exposures. Those products include coverage for the loss or corruption of data caused by hackers, rogue employees, or malicious codes. Insurers also offer business interruption coverage for network attacks, such as denial-of-service attacks, and lost income if a network attack shuts down a corporate Web site. Contingent business interruption coverage is available to handle losses caused by network outages due to problems at a service provider, including Web-hosting companies or outsourced e-commerce service providers.

On the liability side, insurers have developed coverage for exposures such as the release of confidential information, retransmission of a computer virus due to inadequate network security, intellectual property disputes, and even costs to restore public confidence after a cyber attack.

Insurers also offer coverage for emerging risks. Cyber extortion coverage, for example, covers the expenses arising from criminal threats to release sensitive information or to bring down a network.

Notification coverage provides reimbursement for the cost of notifying customers, as required by law, after a security breach exposes personal information to possible fraud—an exposure that businesses would not have faced until just a few years ago.

Growth in the cyber insurance market has been rapid, although from a small base. Annual gross written premiums were estimated at \$250 million to \$300 million for 2005 by the Betterley Report, up from \$150 million to \$200 million in the prior year.⁴¹ As companies across the business spectrum come to recognize the new cyber exposures, further growth will be significant as the industry provides needed products to meet the evolving risks inherent in adopting new technology.

Conclusion

Advances in information technology have transformed virtually every industry. While businesses across the economy have readily adapted, far fewer have sought to adequately protect themselves financially from the new exposures they face. The risks are not limited to technology companies. All businesses that have made the Internet and new information technology an essential part of their operations face significant cyber exposures.

Many companies have failed to recognize that the threat to their businesses from cyber risks has escalated sharply on several fronts.

- On the criminal front, organized gangs have adopted new technology and used it to launch more powerful attacks against corporate networks to extort protection payments or to steal confidential information or crucial intellectual property.
- On the regulatory front, lawmakers have enacted stricter data-privacy standards, requiring businesses to take significant measures—and commit significant resources—to protect personal and financial data and to notify customers of security breaches.
- On the litigation front, businesses face greater liability and the increased likelihood of class action suits should their data protection measures fail.
- Finally, businesses face the very real possibility of

a fatal loss of clients and customers should a security breach result in the exposure of confidential personal or client information.

The insurance industry has responded to the emerging exposures by creating products to specifically address the new cyber exposures, while excluding those risks from traditional policies. To date, a small proportion of businesses have taken advantage of those new products to insure against cyber risks, making cyber coverage a specialty market with significant potential for growth.

The cyber insurance market has become a rapidly growing niche for insurers willing to devote the time and resources to understanding and properly underwriting the new risks. Insurers can foster the development of the market by helping clients to evaluate the new exposures they face, by encouraging them to take adequate security measures, and by educating them about the risk transfer potential of new cyber coverages.

The insurance industry, however, cannot remain static when it comes to covering cyber risks. As technology continues to evolve rapidly, transforming business and business exposures in new and unexpected ways, insurers must continuously adapt their products to meet the evolving exposures and to keep pace with rapidly changing technology and its risks.

Endnotes

- Swade, Doron, *The Difference Engine; Charles Babbage and the Quest to Build the First Computer* (New York: Viking, 2001).
- Ibid.: 30, 306.
- Science Museum of London, "Difference Engine No. 2." See <http://www.sciencemuseum.org.uk/on-line/babbage/page4.asp>.
- 50 Years of Army Computing*, ed. Thomas J. Bergin (Adelphi, MD: Army Research Laboratory-SR-93, September 2000): 17. See <http://www.arl.army.mil/main/Main/default.cfm?Action=235&Page=148>.
- Intel Corp., "Intel Executive Bio: Gordon E. Moore." See <http://www.intel.com/pressroom/kits/bios/moore.htm>.
- Fitzpatrick, Michael, "Internet just leaving its Stone Age — U.S. experts," *Reuters News* (Sept. 2, 1999). See <http://www.paksearch.com/br99/Sep/4/INTERNET.htm>.
- World Wide Web Consortium, "Tim Berners-Lee." See <http://www.w3.org/People/Berners-Lee/>.
- Nielsen Net Ratings, "Three Out of Four Americans Have Access to the Internet" (March 18, 2004). See www.netratings.com/news.jsp?section=new_pr#.
- Nielsen Net Ratings, "Two Out of Five Americans Have Broadband Access at Home" (Sept. 28, 2005). See http://www.netratings.com/news.jsp?section=new_pr#.
- U.S. Census Bureau, "E-commerce 2003 Multi-sector Reports: Highlights" (May 11, 2005). See <http://www.census.gov/eos/www/ebusiness614.htm>.
- Brand, Stewart and Matt Herron, "1984 Ad," *Whole Earth Review* (May 1985). See http://www.findarticles.com/p/articles/mi_m1510/is_1985_May/ai_3754618.
- SANS Institute, "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus" (Nov. 28, 2005). See <http://www.sans.org/top20/>.
- Ilett, Dan, "Antivirus firm says organized crime growing online," *C/NET News.com* (Dec. 9, 2004). See http://news.com.com/Antivirus+firm+says+organized+crime+growing+online/2100-7348_3-5486201.html.
- F-Secure Corporation Weblog, "One particular outbreak a year ago" (Jan. 26, 2005). See <http://www.f-secure.com/weblog/archives/archive-012005.html#00000454>.
- Guadin, Sharon, "Barrage of Viruses Hits in October," *eSecurityPlanet.com* (Nov. 1, 2005). See <http://www.esecurityplanet.com/trends/article.php/3560696>.
- Ilett, Dan, "Most Spam Generated by botnets, experts say," *ZDNet UK* (Sept. 22, 2004). See <http://news.zdnet.co.uk/internet/security/0,39020375,39167561,00.htm>.
- Sanders, Tom, "Botnet operation controlled 1.5m PCs," *vnunet.com* (Oct. 21, 2005). See <http://www.vnunet.com/vnunet/news/2144375/botnet-operation-ruled-million>.
- Warner, Bernhard, "Home PCs rented out in sabotage-for-hire racket," *Reuters News* (July 7, 2004). See http://www.usatoday.com/tech/news/computersecurity/2004-07-07-zombie-pimps_x.htm.
- Stevenson, Reed, and Bernhard Warner, "MyDoom knocks down SCO Web Site," *Reuters News* (Feb. 1, 2004). See <http://www.forbes.com/personalfinance/retirement/news-wire/2004/02/02/rtr1237981.html>.
- "Michigan Man Arrested for Using New Jersey Juvenile to Launch Destructive 'DDOS for Hire' Computer Attacks on Competitors," Federal Bureau of Investigation, press release (March 18, 2005). See http://www.usdoj.gov/usao/nj/publicaffairs/NJ_Press/files/arab0318_r.htm.
- Ilett, Dan, "Expert: Online extortion growing more common," *C/NET News.com* (Oct. 8, 2004). See <http://news.com.com>.

- [com.com/Expert%3A+Online+extortion+growing+more+common/2100-7349_3-5403162.html](http://www.com.com/Expert%3A+Online+extortion+growing+more+common/2100-7349_3-5403162.html).
22. "The Rising Epidemic of Cyber Extortion," *SANS Advisor* (July 2005): 5. See www.sans.org/newsletters/advisor/1.1.pdf.
 23. "Identity theft losses grow, Web a small factor" (January 31, 2006). See http://news.yahoo.com/s/nm/20060131/wr_nm/crime_identitytheft_survey_dc.
 24. Synovate, "Identity Theft Survey Report," (Federal Trade Commission, September 2003). See http://www.consumer.gov/idtheft/media_writing.htm.
 25. Experian Interactive, and The Gallup Organization, "Experian-Gallup Personal Credit Index Show 18 Percent of Consumers Report Being Victims of Identity Theft," *PRNewswire* (Aug. 3, 2005).
 26. Evers, Joris, "Lawsuit seeks disclosure in credit card heist," *C/NET News.com* (June 27, 2005). See http://news.com.com/Lawsuit+seeks+disclosure+in+credit+card+heist/2100-7350_3-5765383.html.
 27. Menn, Joseph, "Fraud Ring Taps Into Credit Data," *Los Angeles Times* (Feb. 16, 2005).
 28. Clinton, William J., "Weekly Compilation of Presidential Documents," 32, no. 34 (Aug. 21, 1996): 1477. See <http://frwebgate1.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=205244139720+0+0+0&WAISaction=retrieve>.
 29. American Medical Association, "HIPAA Violations and Enforcement" (Nov. 1, 2005). See <http://www.ama-assn.org/ama/pub/category/11805.html>.
 30. U.S. Federal Trade Commission, "In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act." See <http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm>.
 31. Sarbanes-Oxley Act of 2002, H.R. 3763, Section 404. See <http://thomas.loc.gov/cgi-bin/query/F?c107:1:./temp/~c1078u06Lo:e143423>.
 32. Leahy, Patrick, "Specter, Leahy Introduce Personal Data Privacy And Security Act Of 2005," press release (June 29, 2005). See <http://leahy.senate.gov/press/200506/062905a.html>.
 33. Reilly, Kevin, "AMR Research Predicts Compliance is an \$80B Issue," AMR Research press release (March 14, 2005). See <http://www.amrresearch.com/Content/View.asp?pmillid=18086&docid=12362>.
 34. CyberSource Corporation, "Fraudsters will take \$2.8 Billion out of eCommerce in 2005," press release (Nov. 9, 2005). See http://www.cybersource.com/news_and_events/view.xml?page_id=1425.
 35. Krebs, Brian, "Internet Worm Hits Airline, Banks," *Washington Post* (Jan. 26, 2003). See <http://www.washingtonpost.com/wp-dyn/articles/A46928-2003Jan26.html>.
 36. "SoBig worm not slowing down yet," *CNNMoney.com* (Aug. 21, 2003). See <http://money.cnn.com/2003/08/21/technology/sobig/?cnn=yes>.
 37. Krim, Jonathan, "Credit Data Firm Might Close," *Washington Post* (July 22, 2005): D02. See <http://www.washingtonpost.com/wp-dyn/content/article/2005/07/21/AR2005072102465.html>.
 38. Evers, Joris "Lawsuit seeks disclosure in credit card heist," *C/NET News.com* (June 27, 2005). See http://news.com.com/Lawsuit+seeks+disclosure+in+credit+card+heist/2100-7350_3-5765383.html.
 39. "Citigroup: UPS Lost Data on 3.9M Customers," *Reuters News* (June 6, 2005). See <http://www.foxnews.com/story/0,2933,158727,00.html>.
 40. Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Robert Richardson, "2005 CSI/FBI Computer Crime and Security Survey," *Computer Security Institute* (July 14, 2005): 10. See <http://www.gocsi.com>.
 41. Betterley, Richard S., "CyberRisk Market Survey 2005: More Products, More Insureds," *The Betterley Report* (June 2005): 2. See <http://www.betterley.com/products.html>.

Brad Gow is vice president of ACE Professional Risk, where he is responsible for technology product development as well as overseeing technology errors and omissions underwriting operations. Gow has more than 16 years' experience in the insurance arena, specifically in product development for professional liability and cyber risk exposures and in developing network security, incident response, and forensic computer investigation services for the insurance industry.

ACE USA is the U.S.-based operating division of the ACE Group of Companies, headed by ACE Limited (NYSE: ACE). ACE USA, through its underwriting companies, provides insurance products and services throughout the United States. Additional information on ACE USA and its products and services can be found at www.ace-ina.com. The ACE Group of Companies provides insurance and reinsurance for a diverse group of clients around the world.