

The Unlikely HEROES of Cyber Security

Viruses, privacy breaches, and other malicious cyber activity regularly threaten organizations' vital information. Cyber insurance providers hope to control the damage risk.

SHANNA GROVES

A customer's confidential account information is broadcast over the Internet without his or the bank's knowledge. An unknown computer hacker, whose future plans may shut down the bank's e-business network for days or even weeks, causes the breach.

This scenario, while fictitious, sounds all too familiar given today's headlines. Malicious cyber activities, including hacking, viruses, and denial-of-service attacks leave destructive, and often costly, scars on vital e-business operations.

According to the Computer Security Institute's 2002 Computer Crime and Security Survey, 90 percent of respondents – 503 computer security practitioners primarily in large U.S. corporations and government agencies – had detected computer security breaches within the previous year, and 80 percent reported financial losses because of them. Nearly half the respondents reported combined financial losses of more than \$455 million.

Some risk management analysts predicted that the insurance industry would neglect cyber insurance, also known as e-risk insurance, after dealing with enormous post-

At the Core

This article

- examines cyber insurance, its costs, and its benefits
- explains how organizations can use ISO 17799 to meet cyber insurance coverage requirements
- explains why organizations must protect their information assets from cyber hazards

September 11 (9/11) insurance claims. However, as companies take a closer look at protecting their information assets from probable cyber attacks, demand for this form of insurance is growing.

“The insurance industry does play an important role in securing cyberspace,” says John Sacia, CEO of Sacia Risk Solutions LLC, a Seattle-based e-business risk coverage provider. “Fortunately, there are a few companies . . . that are committing risk capital to this class of business, which, given the state of the insurance industry and the substantial losses arising from 9/11, asbestosis, and corporate wrongdoing, is commendable.”

Companies offering cyber risk coverage report that it is gaining new attention in retail, financial, medical, and communications companies because these industries want to protect their bottom line: the computer-networked information assets that make up their infrastructures.

“The insurance industry has done a good job of educating clients about the value of e-business insurance policies,” says David O’Neill, vice president of e-business solutions for Zurich North America Financial Enterprises in Baltimore, Maryland. “People are also making a more educated decision about it. They’re asking, ‘What is the benefit? What’s in it for me? What’s it for? Maybe I ought to look into it.’”

Targeting common threats that affect organizations helps cyber insurance providers define where coverage is needed. According to Mark Greisiger, founder of NetDiligence, existing and emerging cyber hazards include virus/worm damage, hackers, cyber extortion, Internet liability, Web vandals, denial of service, Web site disability access discrimination (universal access), computer/server malfunctions, intellectual property infringement, rogue administrators, application service provider (ASP) service outages, Internet service provider (ISP) outages, malicious code transmission, Unix and Windows operating system flaws, privacy breaches, and human mistakes.



“In the five years since [cyber] insurance has emerged, there has been a more traditional [insurance-based] risk management appreciation and approach to protecting information and helping customers eliminate risks,” Greisiger says. “Companies will be required to demonstrate vigilance, a ‘security mentality,’ and solid daily practices involving the use of some industry-recognized safeguard processes and technologies, all of which is verified with an e-risk assessment . . . in order to qualify for this insurance.”

A common misconception among businesses is that traditional insurance covers cyber liabilities. The insurance industry is starting to make it clear that basic brick-and-mortar insurance coverage plans are different than the plans covering information loss and business interruption resulting from cyber attacks.

“Frankly, this has taken some time, and the insurance industry needs to do a better job of articulating those uninsured exposures,” Sacia says. “Ultimately, companies will determine that they cannot rely on traditional insurance policies to protect their business, and when this occurs, companies are inclined to consider their options, including better risk management and security and the purchase of cyber insurance.”

Cyber Security Guidelines

Cyber insurance has gained considerable public attention with the publication of the U.S. Department of Homeland

Security’s (DHS) National Strategy to Secure Cyberspace. The 76-page document, released in February, enforces a national cyberspace security response system for improving the U.S. government’s response to cyber incidents and outlines programs to prevent future cyber attacks and related damage within the public and private sectors.

“Because the National Strategy document explicitly mentions cyber insurance, I believe this will have a positive impact on the insurance market,” says Rick Davis, principal advisor with

DigitalRisk Advisors, a Boulder, Colorado-based risk management consultancy. “As the contents of the strategy circulate, business executives and other organizational leaders around the world will take notice.”

ISO 17799, which was created in 2000 and superseded British Standard (BS) 7799, is highly regarded as the most-recognized standard for managing information security. ISO 17799 defines

Organizations often fail to realize that exposure to cyber liabilities affects the bottom line

information security as the process of protecting “information from a wide range of threats in order to ensure business continuity, minimize business damage, and maximize return on investments and business opportunities.” Information security, it concludes, comes from protective technology, management, and procedures supported by all employees of an organization. Participation from suppliers, customers, shareholders, and specialists from outside organizations also may be needed.

ISO 17799 identifies as crucial to organizations several information security management practices, including

- creating an information security policy document
- allocating information security responsibilities
- providing information security education and training
- reporting security incidents
- establishing a business continuity management plan

Some insurance providers regard ISO 17799 as the most important tool organizations have for meeting cyber insurance coverage requirements.

Michael Lamprecht, a national practice leader in e-insurance for Chicago’s Gallagher CyberRisk Services, notes that from his consulting experience with *Fortune* 500 companies, organizations need to be better coached on the standard’s requirements; however, many of them are trying to be as compliant as they can.

“Insurance companies require a minimum level of compliance with ISO 17799. The average company is 65 to 75 percent compliant, and the best companies are over 80 percent compliant,” Lamprecht says. “Information security consultants could be brought in to help companies understand the ISO standard. It typically takes about six months for companies to understand it and to comply.”

Changing Attitudes

While cyber insurance providers require ISO 17799 compliance – a process Greisiger likens to getting “pre-approved for a home loan” – the reality is that few organizations are willing to fully adopt the standard’s stringent requirements. Instead,

organizations often select elements of the standard that they consider most important for information security.

Some companies, for instance, regard having the best firewalls and security technology more important than enforcing company-wide privacy guidelines. The ideal scenario, cyber insurance experts say, is that companies achieve a balance between the technological and procedural aspects of their information security management.

In the early days of cyber insurance, Davis saw the underwriting risk assessment process as an uphill struggle, particularly when evaluating high-security firms that regularly passed government inspections.

“It was very difficult to get insurance applicants to understand why paying attention to security management and operations was just as important as getting the technical aspects right,” he says. “Whenever we talked about the non-technical risk management issues like policy, procedure, personnel, and physical security, nearly all of the security managers would glaze over until we returned to the bits, bytes, and firewall conversation.”

With the possibility of corporate information assets being lost to privacy breaches or unintentional employee errors, however, companies and cyber insurance providers are starting to give the human element more focus when implementing protective information security initiatives. As Davis notes, “The world of digital risk management is first and foremost about managing people.”

Protecting the Bottom Line

Vital information assets, including content, knowledge, and business intelligence, are closely tied to an organization’s financial health, and cyber insurance providers are emphasizing this fact in their consultations with customers.

They say organizations often fail to realize that exposure to cyber liabilities affects the bottom line, as well as relationships with customers, vendors, and partners. An example Greisiger gives is a hacking incident that results in customer information being stolen; what would likely turn the company’s attention toward improving its cyber security posture is a class-action lawsuit brought by the customers against the company that failed to protect their privacy. Without security measures in place for their cyber systems, organizations – and the customers and vendors they do business with – are at risk.

In the article “Countering Cyber War,” Pittsburgh-based Computer Emergency Response Team (CERT) Analysis Center experts Timothy Shimeall, Phil Williams, and Casey Dunlevy paint an even harsher reality of cyber vulnerabilities. “Advanced, post-industrial societies and economies are critically dependent on linked computer information and communication systems,” they write. “Sophistication has itself become a form of vulnerability for enemies to exploit.”

In addition to financial consequences, organizations that do not adequately protect their information assets from cyber hazards face risks to their reputations. In the event that an organization's reputation is harmed by a cyber attack, the insured's cyber insurance policy would reimburse public relations expenses.

"As they say in business, reputation is hard to win but easy to lose," Sacia says. "Our economic growth or stagnation is dependent on confidence that transactions will not be repudiated, and productivity gains are clearly based on efficiencies arising from the Internet and technology to a great part."

Information Security: A Collaborative Effort

ISO 17799 suggests developing a "cross-functional forum of management representatives from relevant parts of the organization" as a precursor to effectively implementing a company-wide information security management program.

While not specifically stated in the standard, those with vested interests in information security, including information technology, risk management, and information management professionals, could participate. The forum would map out specific responsibilities, methodologies, and processes for company-wide information security, support a security awareness program within the organization, and review information security occurrences.

An effective information security program, Sacia says, would combine "physical security, employee training and procedures, and technology in the form of firewalls, intrusion detection, virus protection, and legal review to eliminate Internet provider (IP) infringement and content litigation, plus contingency planning coupled with a comprehensive cyber insurance product."

An Opportunity for Information Managers

Because information management professionals work with their companies' information retention programs, they have an opportunity to collaborate with IT and risk managers in assessing what information needs protection.

Greisiger describes a typical collaboration scenario within a company, based on his work in security consulting. "My firm would meet individually with one to six people in the client company, including the CIO, IT manager, information manager, privacy officer, and legal counsel. It would be like a 'network blood test,' a sampling approach of the key areas that are not only important to the company but also to the underwriter.

"By taking a panoramic sampling approach," Greisiger continues, "we would focus on a '90-10 rule': make sure you can mitigate the risk by 90 percent and that the company implements, at least, a baseline standard of care."

Companies that involve information managers in this process are better able to inform security consultants or underwriters about information practices. Information managers also can assist in developing the corporation's written policies necessary to protect information assets. These include a records retention policy, e-mail usage policy, and general security/privacy policies, according to Greisiger.

ISO 17799 explicitly outlines what measures a company should take with its information assets in a security program and recognizes that such measures require an information management background. "It is important that an appropriate set of procedures are defined for information labeling and handling in accordance with the classification scheme adopted by the organization," ISO 17799 reads. "These procedures need to cover information assets in physical and electronic formats."

Among the procedures to define, the standard notes, are

- information copying practices
- storage
- transmission by post, fax, and electronic mail
- transmission by spoken word, including mobile phone, voice-mail, and answering machines
- information destruction

Finally, ISO 17799 recommends that an organization be able to identify the value and importance of its information assets through an inventory. Lamprecht sees opportunities for information managers to help conduct "a comprehensive inventory of physical assets before the company seeks insurance," he says. "First of all, find out what are we going to insure here? What are we trying to protect? If the network is down, how much will the company suffer per hour? Per day?"

Collaborating with Other Organizations

When creating a security plan, ISO 17799 strongly suggests that companies seek the guidance of appropriate outside agencies and organizations. These contacts include law enforcement

agencies, regulatory bodies, information service providers, and telecommunications operators to "ensure that appropriate action can be quickly taken, and advice obtained, in the event of a security incident."

Hiring a Security Consultant

Consulting firms that specialize in security and risk management often are brought in to assess a company's practices before cyber insurance is provided.

Security consultants may be hired by the client company and, in an increasing number of cases, by the insurer, Greisiger says. "Having security consulting streamlines the [insurer's] loss-control assessment process and can actually test or confirm whether, for instance, the [client] company really has the fire-wall and hardened servers it says it has."

Insurers that use security consultants gain greater insight into the client's compliance with cyber insurance requirements. An added benefit is that consultants can do their assessments at a cost that is "borne by the underwriters," Sacia says.

Pricing Cyber Insurance

Budgeting for information security initiatives requires researching the costs of cyber insurance plans.

According to Greisiger, based on the coverage type and policy limits sought by the client company, annual premiums range from \$10,000-\$50,000 on a \$1 million policy coverage limit, (depending on a variety of factors associated with e-risk exposures facing a particular business model and their networks), to \$200,000-\$500,000 annually on coverage limits of \$10 million.

"Often, the insured has a dollar deductible or a self-insured retention that must be eroded before coverage is triggered," Greisiger notes. "Example deductible ranges would be \$20,000-\$200,000 and up into the millions. For business interruption coverage, the 'deductible' might be an hourly waiting period, such as the first 12 hours of a network outage."

Cyber Insurance at Work

Although reviewing cyber insurance options and deciding on a coverage plan can be a lengthy process, these efforts are minor compared to the work that takes place once an organization submits a cyber loss claim. Only then can the organization clearly see the benefits of this type of insurance.

In his article "Investigating Cyber Claims" for *Claims* magazine, Greisiger wrote that the cyber insurer will ask the organization many questions to investigate the facts of the cyber liability incident, including:

- Was there really an occurrence (as defined in the insurance policy)?
- Did the hacker event really cause damage?
- When did this event occur (date, time, place, machine, file)?
- What was the hourly duration of the server outage?
- Who is the culprit and where did the attack originate?

Tying in Records Management

Soon, records management practices will also be part of the risk assessment conducted by insurers writing cyber insurance. ARMA International is working with Net Diligence to incorporate elements of ISO 15489, the international standard on records management, into the risk assessment tool used by Net Diligence.

This is a major step toward acknowledging the importance of a quality records management program in protecting companies' information assets.

- What loss prevention or compliance process failed?
- Which network security feature was defeated?

Then the investigation gets more involved. The company's computer hardware, software, and e-mails are analyzed. To prove or disprove an allegation, the insurer uses legal procedures to obtain this vital evidence, Greisiger wrote. "Part of the investigation is an audit function possibly involving forensic analysis, backward tracing, attack route hypothesis, and possibly attack re-creation."

Future Opportunities and Challenges

While cyber insurance providers are betting this type of coverage will gain greater acceptance and exposure in the next five years, they are realistic about the current challenges facing the insurance industry and the economy in general.

"Overall, the insurance industry is in a difficult financial situation due to the largest-ever September 11 WTC claims, hard hits in the stock market, and the dramatic decrease in investment income," Davis says. "This relative financial hardship has led to a hardening of the insurance market where each risk/reward decision comes under severe scrutiny like nothing our generation has ever seen. Under the dark clouds of war and continued global uncertainty, times are tough for the insurance industry and conservation of precious capital is the key to survival."

Others view cyber insurance as an evolving industry that can significantly benefit companies in their continued quest to conduct global business transactions. Says O'Neill, "I think the industry is going to experience some good growth [just as] the issue of electronic commerce is going to continue to grow."

"We're seeing a trend now ... that a risk manager will be placed in a technology department," Lamprecht says.

Greisiger goes even further by suggesting that company utilization of cyber insurance could be "standard fare in a couple of years." He predicts that brokers will take more of an active role in a company's pre-assessment for cyber insurance and will strive to become more educated about general cyber security protection.

In the same respect, organizations will likely work more at collaborating internally on cyber security initiatives. "We're seeing a trend now, particularly in *Fortune* 100 companies, that a risk manager will be placed in a technology department," Lamprecht says. "We found that, to begin with, risk management departments didn't really communicate with technology departments. Now they are starting to come together . . . and, from my personal experience, *Fortune* 500 companies are far more likely to have an active dialogue."

As for future cyber insurance policies, Sacia predicts a greater demand for business interruption coverage and a need for expense coverage with huge limits. Convincing more organizations to justify the cost of cyber insurance because it is a valuable asset, however, is the current challenge.

"We need to encourage companies to fund this cost, pre-arrange for those professional services, and mitigate further damage, plus pay for the cost of investigation, so that the root cause or source of the security breach or malicious code can be found," Sacia says. "By providing the funds to pay for this contingency, having those resources arranged for before they are needed is simply good business, and good for cyberspace." ■

Shanna Groves is a former associate editor of The Information Management Journal and a freelance writer based in Kansas. She may be contacted at sgrovesuss@msn.com.

References

- British Standards Institution. *BS ISO/IEC17799: 2000 Information Technology. Code of Practice for Information Security Management*. London: British Standards Publishing LTD, 2000. Available at www.bsi-global.com/index.xalter# (accessed 6 March 2003).
- Computer Security Institute. "Cyber Crime Bleeds U.S. Corporations, Survey Shows." Available at www.gocsi.com/press/20020407.html (accessed 6 March 2003).
- Davis, Rick. "Risk Management in the Digital Age." *The CEO Refresher*. Etobicoke, Ontario, Canada: Refresher Publications, 2001. Available at www.refresher.com/digitalage.html (accessed 6 March 2003).
- Friedman, Ted. "How Secure Is Your Business Intelligence Environment?" Gartner Research. 28 August 2002. Available at www4.gartner.com/DisplayDocument?id=367264&ref=g_search (accessed 6 March 2003).
- Greisiger, Mark. "Investigating Cyber Crimes." *Claims*. September 2002. Available at www.claimsmag.com/Issues/Sept02/investigating.asp (accessed 6 March 2003).
- _____. "Cyber Risk & Internet Liability." NetDiligence, 2002. Available at www.netdiligence.com (accessed 6 March 2003).
- Power, Richard. "What's the Role of Insurance in Cyber Security?" *Computer Security ALERT*. December 2001. Available at www.gocsi.com/pdfs/alert1201a.pdf (accessed 6 March 2003).
- Shimeall, Timothy, Phil Williams, and Casey Dunlevy. "Countering Cyber War." *NATO Review*. Winter 2001/2002. Available at http://www.cert.org/archive/pdf/counter_cyberwar.pdf (accessed 6 March 2003).
- U.S. Department of Homeland Security. "The National Strategy to Secure Cyberspace." February 2003. Available at www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (accessed 6 March 2003).