



## Are You Covered?

by: *Nicole Ross*

**Pages: 22-25; November, 2001**

文章简介: 本文首先介绍了电子商务中存在的有别于传统商务活动中的新威胁, 以及传统保险业务难以满足电子商务对保险的需求的情况。然后提出了新兴的计算机保险业务的概念并讨论了该业务涉及到的多种风险种类。



[华安信达](#)

*With the tremendous benefits of conducting business online comes a deluge of vulnerabilities. Cyberinsurance can help shelter you from a number of risks to your e-business.*



In October 2001, a white-hat hacker discovered a large security gap in Microsoft's customer service Web site that gave anyone with a browser access to customer sales records and other personal information, including names, purchasing histories, shipping and billing addresses, phone numbers, e-mail addresses, and credit card types.

Although Microsoft repaired the unsecured hole within an hour of notification, the corporation still had to go public to ensure customers and shareholders that the problem, due to human error, was fixed and that they would continue to be vigilant in their efforts to protect customer data.

Conducting business over the Internet creates new threats for businesses, including risks to security, theft of confidential information, and loss of customer confidence. According to the 2001 Computer Security Institute (CSI)/FBI survey on computer crime and security, 70 percent of respondents (up from 59 percent in 2000) cited their Internet connections as frequent points of attack, as opposed to their internal systems (31 percent).

Not surprisingly, corporations often find themselves unprepared to contend with risks associated with e-business. The 1999 ICSA/Global Integrity Industry Survey reports that 52 percent of organizations surveyed said that their information security rests at either average or below, and 35 percent reported that security

doesn't have a high visibility across their organizations.

Yet e-commerce, which accounted for more than \$100 billion in sales in 1999 alone and is estimated to exceed \$1 trillion by 2003, possesses the tremendous capability to allow corporations to reach millions more customers worldwide, and to slash service costs while improving the overall speed of delivery. For example, if the global reinsurance industry switched much of its business transactions to e-commerce, insurance provider Lloyds of London estimates that it could save \$10 billion dollars.

But if companies want to enter the cyber-marketplace to boost profitability, they can't ignore the risks that taking business processes and operations online poses to themselves and their constituents: internal attacks, security breaches, hackers, viruses, denial-of-service attacks, privacy violations, and intellectual property infringements. At a time when traditional insurance is reluctant to cover these cyberrisks, organizations should reassess their online risks, and as part of their business continuity planning programs, investigate their need for special cyberinsurance policies.

The Internet's always-on availability, speed, and convenience have morphed businesses from brick-and-mortar establishments to extremely accessible storefronts in an interactive marketplace. The windows in these storefronts, however, are not made of glass. Hackers, disgruntled employees, and corporate insiders don't make much noise when they enter your site, but when the damage is done, the repercussions echo farther than ever before. Cyberinsurance is a necessity now to ensure critical business operations.

### **Cracks in Traditional Insurance**

Traditional insurance policies chiefly safeguard physical assets—people, facilities, equipment, or products—against incidents such as fires, hurricanes, earthquakes, product liability, or malpractice suits. Unfortunately, they don't necessarily

safeguard networks or intellectual property such as customer lists, data, trademarks, copyrights, brands, and domain names against cybercrimes like denial-of-service attacks, malicious code, security breaches, or information theft.

Electronically stored intellectual property is often ill-defined as "data" and isn't covered by traditional property policies. While insurers may define computer hardware and software as physical property, if a hacker accesses your system and steals or destroys data that resides on the system, it usually won't be covered.

Traditional personal property insurance will cover machinery, equipment, and personal property for which the business is responsible; however, insurance companies may exclude protection of computer hardware and software as well as electronic data. In addition, under property policies, business interruption/extra expense is activated if the direct loss is insured; since property direct losses were designed for physical assets and perils, information assets and e-commerce risks are not covered.

Commercial general liability (CGL) covers liability claims of property damage or bodily injury, and also can include product, contractual, or other third-party liabilities. However, under CGL policies, advertisement-injury coverage doesn't completely cover intellectual property infringement, content, and advertising offenses that occur via the Internet; also, policy coverage is not global and therefore will not cover Internet crime. In traditional CGL policies, there is some intellectual property coverage only relating to copyrights and trademarks, and it's focused in the context of advertising your product, so online banner ads or non-advertising content will not be covered, explains Chris Keegan, vice president and regional practice leader for the N.Y. metro region of Marsh Risk Consulting.

If a hacker infiltrates your network and destroys your data, or leapfrogs to a third-party site and causes damage, neither of this first- or third-party network or data loss is covered by traditional policies.

In addition, while employees' intentional acts resulting in loss of money, property, or security can be covered by standard crime or fidelity policies, data and network losses will not be covered. Even if you have errors and omissions coverage (also known as professional liability or malpractice insurance), which serves to fill in the holes of what CGL policies do not cover, such as loss of customer data or software, programming, or systems failures, intentional acts of employees against networks or data still might not be covered, says Keegan.

Buyer beware: Intentional acts exclusions are common in both traditional and cyberinsurance policies, according to Steve Haase, CEO of InsureTrust.com (Alpharetta, Ga.). Haase says that 70 percent of security breaches are malicious acts committed by employees, so corporations should be sure that their policies don't exclude intentional acts.

### **Welcome to the Cyberinsurance Jungle**

"Cyberinsurance is a new and evolving coverage that's still not readily being purchased," says Jon Farber, assistant vice president of Global Technology Underwriting for St. Paul Insurance (St. Paul, Minn.). "The good news, however, is that more corporations are asking about cyberpolicies, and more carriers are offering them."

For example, comprehensive policies from InsureTrust.com, Marsh Risk Consulting (NetSecure products), or AIG (netAdvantage Suite) offer coverage for first- and third-party cyberrisks. Generally, cyberinsurance policies will provide coverage that includes Internet liability; Web media and content liability; Internet professional errors and omissions liability; first- and third-party losses and damages to data and networks; as well as expenses stemming from e-business interruptions due to network attacks, including public relations, downtime expenditures, and security measures.

Though all policies are different, the following areas of vulnerability are

covered by the typical cyberinsurance offering.

### *Internal Attacks*

Disgruntled employees or corporate insiders are a leading cause of cybercrimes, says the FBI. Unfortunately, these attackers don't necessarily need to be well versed in the art of network hacking—their insider status allows them unrestricted system access and the ability to steal confidential data or damage the network.

For example, hundreds of thousands of doctors and medical professionals worldwide depend on the National Library of Medicine (NLM) computer network for updated information on diseases, drugs and dosage units, and treatments. In January and February 1999, the system was serially attacked. System administrator passwords were stolen and hundreds of files, including sensitive medical "alert" files and programming files that kept the system up and running, were accessed.

The attacks posed a threat to public safety and resulted in monetary losses exceeding \$25,000. The perpetrator was identified by the FBI as a former NLM computer programmer, whose access to the computer system had been previously revoked; he entered NLM's system through a door he had inserted into the programming code.

In addition to a proliferation of internal attacks, the 2001 CSI/FBI report states that 91 percent of 538 respondents detected employee abuse of Internet access privileges, such as downloading pornography or stolen software, or improper use of e-mail.

This means that not only should companies be mindful of the dangers of deliberate insider attacks that could distribute a virus within the corporate network or to third parties, or destroy or alter data, but they have to be aware that their employees' daily activities may also cause them to be liable. Employees who receive or distribute pornographic images or material offensive to other parties may bring a lawsuit upon you. A carefully drafted cyberinsurance policy can mitigate these

potential losses.

### *Hackers, Viruses, and DoS Attacks*

Hacker attacks—inserting viruses (Love Bug, NIMBDA, Code Red) or Trojan horses into a corporate network, spamming, launching denial-of-service (DoS) attacks (Yahoo!, Amazon.com, CNN.com), snatching Web sites, or inundating a Web site with false data—can cause a host of unwanted network jams, downtime, and monetary losses. Understandably, many organizations are reluctant to publicly report hacker attacks or DoS attacks for fear of diminished customer and shareholder confidence; however, if uninsured, the results and liabilities can be far-reaching.

If an internal attacker or a hacker enters your corporate network or Web site, your company, employee, or customer data and intellectual property can be stolen, altered, deleted, or dispersed. Customers, business partners, or shareholders who depend on being able to reach you electronically or need to conduct online transactions may be unable to do so if a virus (either deliberate or random) or denial-of-service attack cripples your systems. Also, if any third-party information on your networks or Web site is stolen or infringed upon, you will be liable.

The third-party liabilities become much stickier and more numerous. For example, if a hacker gains access to your system and sends a virus via your system to a third-party system, that third party will want to know why you didn't protect against it. Many hackers will gain access by "island hopping" through another site, perhaps yours, before they launch a virus attack. Today, the standard of care is that everyone should have updated virus software, firewalls, and regular security for breaches such as "back doors" and unauthorized access. If you don't meet that standard, you could end up with a lawsuit, explains Haase.

Currently there are 65,000 known computer viruses, with 300 to 600 appearing each month, and 10 to 20 appearing each day. Viruses quickly

self-replicate and can infect such vehicles as disks, program files, Excel spreadsheets, Word documents, and Java applications. *Internet Week* reported that in 1999, 6822 person-years were spent responding to virus and denial-of-service attacks, among others, in North America. Virus attacks alone cost North American companies \$1.6 trillion. The ICSA/Global Integrity 1999 Industry Survey reports that 77 percent of respondents had suffered losses from virus attacks, and 38 percent claim that threats from hackers and malicious code are their greatest sources of concern. They should be a source of concern to all organizations that rely on e-commerce. The dangers of these forms of outside attacks can be addressed through insurance specifically targeted to such activity.

#### *Cyberextortion and Terrorism*

Another type of hacker, perhaps an even more malicious one, will not only hack into corporate systems, but will steal confidential company or customer data, such as credit card information, and then threaten to publicly disseminate it unless payment from the company is received. An uninsured organization faces one of two painful choices: paying out high sums of money to a cybercriminal, or risking the release of their corporate or customer information.

For example, according to AIG, a hacker stole 300,000 customer credit card numbers from an online retailer. The hacker then attempted to use the stolen information to extort \$100,000 from the company. Upon the firm's refusal to cooperate, the hacker posted 23,000 card numbers online. As a result of credit card cancellations and re-issuance, the online retailer suffered approximately \$2,000,000 in lost income and third-party damages. The ramifications of this type of attack are enormous and should be considered a major risk.

In addition, the September 11 attacks indicate that terrorists can, and will, target corporate America. As businesses continue to rely heavily on the Internet and networks to store data and conduct business transactions, they need to have sound security measures in place. The procedures for keeping systems and the Internet

secure are still evolving, and the next area terrorists might target is the U.S. technology infrastructure, says Keegan.

### *Privacy Violations*

The 1999 ICSA/Global Integrity survey states that companies engaging in e-commerce are 57 percent more likely to experience a leak of confidential information than are those that don't. Privacy concerns on the part of regulators, organizations, employees, customers, suppliers, and business partners increase daily as organizations store their personal, confidential information on networks that may be vulnerable.

Perhaps most vulnerable are financial institutions, as well as healthcare providers that are subject to Health Insurance Portability and Accountability Act (HIPAA) regulations, which require that the technology used to hold and provide information is properly safeguarded. These organizations especially need to have measures and insurance in place to protect them from lawsuits that may arise out of the mishandling of private information, says Keegan.

Even though cyberinsurance policies can protect companies against lawsuits arising from privacy violations, upper management should also put into practice good security measures and communicate those defenses to customers and other parties.

### *Media Liability*

With so much easily downloadable material, the Internet generates a slew of exposures to theft of advertising and content. Though not unlike traditional copyright or trademark infringements, this type of theft is easier to commit and easier to detect.

Under cyberinsurance policies, it's important to know that all material posted on a Web site can be copyrighted as intellectual property, which includes content, data, advertising, media, and patented information. Even business processes

implemented over the Web, such as Amazon.com's one-click shopping, can also be copyrighted, says Keegan.

According to AIG, covering all your bases on your Web site is also important if you have third-party information posted. A third party can sue you if someone copies the material they own but resides on your site. Also, it's important to be aware of the traditional dangers associated with third-party exposure to alleged libel, slander or defamation, and invasion of privacy. Even users who access your Web site or bulletin boards you facilitate may be offended by some content, and there may be liabilities involved there.

According to Lloyds, there are two chief intellectual property risk (IPR) products available: "defense," which safeguards the insured against alleged infringement of another's intellectual property rights, and "enforcement." Smaller businesses and organizations tend toward "enforcement" or "pursuit" policies, which cover legal costs and expenses resulting from instances where the intellectual property rights of the insured have been infringed upon.

In addition, for smaller businesses, underwriters can provide a policy option that safeguards intellectual property rights, in which they furnish monies to cover legal assistance during licensing disputes. Also, if small businesses are unable to come up with the funds to create a product from their ideas, they usually will contract with a larger company to exploit it in return for a royalty. Such policies enforce the licensing agreement if the manufacturer or producer violates the patent rights of the insured.

### **A Good Start**

Since cyberinsurance policies are not one-size-fits-all, corporations should start by assessing their cyberrisks, either in-house or by consulting with an insurance carrier, says Emily Freeman, national practice leader for Marsh Risk Consulting. Financial and healthcare institutions will probably be first in line for cyberinsurance because

of the risks associated with privacy violations, but all companies have some degree of risk that they should investigate.

There are a multitude of reasons why cyberinsurance will ensure the survival of your business and maintain the confidence of your customers, employees, business partners, and shareholders. Shouldn't you be covered?

## **Selecting and Applying For Cyberinsurance**

*by Emily Freeman*

Some of the most significant e-business risks are either not covered or not covered adequately by traditional insurance. Disputes could arise with insurers over the interpretation of insuring agreements, definitions, and exclusions. Upon renewal, traditional insurers are reducing or eliminating previously granted coverage, such as direct and indirect losses arising out of computer viruses. Court decisions may reinterpret policy language to further affect future coverage.

In response, cyberinsurance products have been developed by a number of major insurers, which provide varying forms of protection and scope, and there is no standard industry product. Specialty underwriters with an understanding of the technology and legal issues underwrite these policies. Available coverages typically include security liability, multimedia liability, cybercrime, cyberextortion, crisis management, damage to data, and Web outages (business income and extra expense) arising from a security failure.

It is prudent to consider these policies in the context of any coverage provided by existing traditional policies, the results of an e-business risk assessment, and overall risk-financing philosophy. For large enterprises, manuscript catastrophic coverage may be an attractive alternative.

In terms of evaluating the different cyberpolicies, the following factors should be evaluated:

- The financial strength and experience of the insurer/underwriter
- Scope of the policy coverage and the policy exclusions, definitions, valuation clause, and conditions
- Desired limits of insurance and retention
- Flexibility of the insurer to amend policy language to meet the specific needs for coverage

- How the cyberpolicy would pay a loss in relationship to other insurance
- Relationship with the insurer on other lines of business
- Claims handling procedures and selection of legal counsel

Underwriters require an application to provide them with an overview of the business and the particular applications/activities involving computer networks and the Internet. They want to understand the revenues or traffic associated with these activities and the level of risk associated with security, privacy, and access failures. Some of the questions on the application pertain to vetting and control of content published on the company's Web site, the controls surrounding chat rooms and bulletin boards, and the use of third-party vendors (particularly for hosting). All of this could affect the likely size of a loss or the size of liability to third parties.

In addition to the application, the underwriters require additional information on systems security policies and procedures. They rely on two types of security assessments. One is a self-assessment tool available on the Web, which is typically a series of questions the applicant fills out. The other is a third-party security assessment. The standard practice is for underwriters to require a copy of a third-party security assessment only for higher-risk applicants, requests for limits above \$5 million, or larger companies. Security controls must meet baseline underwriting standards for the insurer to provide coverage.

*Emily Freeman is a senior vice president of Marsh Inc. and their e-business risk management and consulting director. She can be reached at [emily.freeman@marsh.com](mailto:emily.freeman@marsh.com)*