



With **cyber invasions** now a common place occurrence, insurance coverage isn't found in your liability policy. So many different types of computer invasions exist, but there is **cyber risk insurance** to cover it.

Gotcha Covered

*How to protect your company
with cyber risk insurance*

Mark Greisiger and Anne DeVries

Cyber risk, a.k.a. network security liability, insurance has been around for almost a decade. Yet it is still a relatively unknown and under-utilized form of risk management.

Many businesses think they are covered for cyber risk exposures with their current traditional property, commercial general liability, errors and omissions, fidelity/crime, and employment practices

liability coverage, but this is typically not the case. Most traditional insurance policies require direct physical loss or damage to tangible assets to trigger coverage. Courts, though, have held that electronic data is not considered tangible, and hacker damage or destruction of data is not construed to be physical in nature.

Today, with network-centric operations the norm in most industries—retail, medical, financial, legal, higher education—some of a company's most critical assets are intangible: electronically stored information. In fact, a significant portion of any company's value is tied up in its electronic information assets—as much as 70 percent in some cases according to Gartner, Inc., a preeminent technology research and advisory firm.

Cyber risk insurance was developed to protect a company's intangible assets. It addresses the unique risk exposures associated with the electronic processes, interactions and digital assets arising from computer-dependent business activities. Almost every business, regardless of the product or service it provides, has some degree of cyber risk exposure, such as unauthorized access to data (from internal or external sources), computer viruses, denial-of-service attacks and poor network management.

Let's complicate the situation. Because identity theft is one of the fastest growing crimes, various privacy regulations (HIPAA, GLBA, FACTA, State Notice Laws) require that companies protect sensitive customer and employee data no matter where it resides: on the network, on standalone systems, such as billing, medical, and marketing databases; on remote devices, such as laptops; and on paper. At this point in time, 39 states have enacted legislation requiring companies to notify customers if they suspect there has been unauthorized access to their sensitive information. So in addition to the risk of lost business, companies now face a larger reputational risk and the potential for class-action lawsuits.

Now things get really sticky. Recently passed regulations and industry standards, such as PCI DSS (Payment Card Industry Data Security Standards), add to a company's overall risk in the form of fines and penalties for non-compliance. The total cost in fines and penalties can be substantial, mounting into the millions of dollars.

What's the worst that can happen?

Even the most compliance- and security-focused company can be victimized by a data breach. Bigger often means more complex, with more moving parts and more inter-dependencies. The media underscores this point on a weekly basis, with large, well-managed and well-operated companies reporting breach events.

Failure to take the necessary measures to secure information, and to mitigate potential loss if measures taken should fail, may result in significant financial costs for a

business. When a cyber risk event occurs, the consequences can be financially crippling to a company with the emergence of class action lawsuits, huge forensic and mitigation costs, possible identity theft damage litigation and the potential loss of reputation and customers.

The most damaging financial impact of these risks is most likely to come in the form of litigation. Several companies that have reported a major security breach are now facing privacy-related class action lawsuits that may require years of litigation and cost millions of dollars.

But even when there is no lawsuit, there are extraordinary expenses involved. At least 39 states now require companies, by law, to notify every person whose personal identity information was compromised—which can take weeks and a huge expenditure of manpower. Systems need to be shut down, business is interrupted, a public relations and damage control campaign needs to be launched, specialty investigation and forensic experts hired, and if it involved credit card information, cardholders, issuing banks and credit bureaus need to be notified. Information assets and records need to be restored. Consumer banks might seek reimbursement for credit card-related losses. Additionally, corporate officers can be held personally liable if they fail to provide adequate network security or act diligently to prevent breaches from occurring.

What's the worst that can happen? Following are a few more examples of real losses experienced by real businesses:

- A large retailer was hacked by an outsider and over the course of a year the hacker stole more than 45 million credit card numbers and the personal identity information of more than 400,000 people. The company faced multiple class action suits on behalf of banks who suffered losses and on behalf of the individuals whose information was stolen. Potential liability is in the tens of millions of dollars.
- One of the nation's largest drug makers inadvertently divulged the e-mail addresses of 600 patients with various conditions in an e-mail to people who had signed up for Internet service reminders. The company was sued for invasion of privacy. Data leakage can impact any company.
- A hacker stole 350,000 credit card numbers from an online music retailer and posted thousands of them on a Web site when the retailer refused to pay ransom. Resulting costs included defense of privacy lawsuits, data restoration, public relations expenses and immeasurable costs in loss of customer confidence. The company never recovered and is now out of business.
- A disgruntled, terminated employee planted a "logic bomb" in the employer's system, destroying critical information, including backups. Total cost to the company exceeded \$10M. 85 employees were laid off.

According to Kevin Kalinich, managing partner of Professional Risk Solutions for the Aon Financial Services Group, “The financial magnitude of such privacy and security breaches escalates the issue from risk managers to the CFO, GC and Board levels.”

Assessing your organization's risk

To assess your organization's cyber risk and privacy exposure, ask yourself the following questions:

- What is the value of proprietary business information assets, and what would it cost to replace, restore or rebuild data records that are lost?
- What would be the impact on your revenue stream if either your online e-commerce transactions or billing systems were unavailable for hours, days or even weeks?
- What costs would you incur if you were required to notify hundreds of thousands of individuals whose personal information was inadvertently compromised from your system?
- What financial liability or reputation injury could you face if an employee inadvertently passed a virus or other malicious code on to business partners or customers?
- How well could you recover if a disgruntled employee sabotaged your system or sold proprietary business or customer information for personal gain?

Kalinich recommends that companies use independent outside resources to assess their cyber and privacy risk. It's his belief that, “A good third-party network risk assessment not only enables improved risk management and corporate governance compliance, it can also facilitate enhanced insurance coverage options at competitive pricing.”

Ceding a portion of your cyber risk

Cyber risk exposure is divided into two degrees of risk: direct risks and indirect risks. Direct risks include the actual theft of customer information, trade secrets or money, damage to critical electronic data, and productivity losses that are real but may be difficult to quantify. Indirect risks are potentially more costly than direct risks and include loss of customers, damage to brand and loss of reputation.

A comprehensive cyber risk insurance policy covers breaches caused by both internal and external factors, including employee errors in handling sensitive data. Cyber risk insurance is usually offered in modular form, so you can select the type and amount of coverage needed for your type of business. Available coverage includes:

- Business income loss including extra expense
- Data restoration expenses
- Public relations and consumer notification expenses
- Cyber extortion expenses

- Litigation and regulatory defense expenses

While network security and privacy is still a relatively new area of coverage, the number of insurers offering this coverage has increased considerably in the past few years. There is now adequate capacity available for even the largest companies to obtain good protection against the financial and reputational crisis that could occur in the wake of a network security event.

To obtain cyber risk insurance, your organization must meet baseline network security standards and demonstrate that it maintains a sound security posture. Insurers are looking for more than virus protection and intruder detection systems. Your organization must be able to show that its security posture focuses on three key areas: people, processes and technology.

Insurance underwriters will want to know such things as:

- Do you have dedicated security personnel? Are their lines of report clearly delineated, all the way to the executive level of your organization? Is their incident escalation path defined?
- Are your security policies and procedures documented, maintained, and readily accessible to employees?
- Are all your employees trained in security procedures?
- Does your incident response plan include public relations? Are your notices already written and do you have a public relations or crisis communications firm under retainer?

Obtaining an independent, enterprise-wide network security assessment that evaluates the people, processes and technology underlying your compliance and security posture is a good first step in both managing your risk and qualifying for cyber risk and privacy liability insurance. An objective, third-party assessment allows you to identify vulnerabilities, so you can harden security and reduce overall exposure. That's a win-win for your company and your insurer.

As President of NetDiligence®, Mark Greisiger is an authority on cyber security and network risk for computer-dependent businesses, government agencies and financial institutions. He is a graduate of Penn State University; Villanova University and Drexel University.

Anne DeVries is the senior vice president for Digital Risk Managers, a division of Wells Fargo Insurance Services. With almost 20 years of experience in insurance underwriting for technology accounts, Anne teaches industry-related continuing education classes in Oregon and Washington. She holds a Bachelor of Science degree (Math/Computer Science) from Fairfield University in CT and a Master of Science degree (Computer Science) from Hofstra University in NY.

Copyright © 2008 by the Association for Financial Professionals (AFP).

All Rights Reserved.

This electronic document is designed to provide authoritative information in regard to the subject matter covered. It is not intended to offer accounting, legal or other professional advice. If accounting, legal, or other professional advice is required, or if expert assistance is needed, the services of a competent professional person should be sought.

Reprinted from AFP Exchange, 2008.

All inquiries should be addressed to:

Communications Department
Association for Financial Professionals
4520 East-West Highway, Suite 750
Bethesda, MD 20814
301.907.2862 Fax: 301.907.2864 E-mail: AFP@AFPonline.org
Web: www.AFPonline.org

© 2008 by Association for Financial Professionals (AFP). All rights reserved.