Avoid Catastrophe by Addressing Cyber Risk You could fall victim to a cyber attack or breach at any time. Keep disaster at bay with these guidelines.

By Tom Marchetti

Cybercrime is on the rise and represents devastating dangers. Understanding and guarding against these threats are now critical elements of governance.

Cyber risks include malicious assaults on people's credit cards or bank accounts. Risks also include the unintentional release of confidential employee, client, and donor information.

Besides revenue loss, cyber events can lead to costly litigation and damage to your reputation. Specific cyber risks that can affect your organization include:

- **Web site shut-down** or damage
- **Theft or damage** to intellectual property
- **Compromise of e-mails** with clients, vendors, collaborators, and service providers
- **Physical damage** to software and hardware
- **Transmission of computer viruses,** leading to destruction of systems.

To guard against these and other potential losses, follow these three steps:

Step 1: Assess Your Risks

To gauge your organization's vulnerability, start with the following questions:

Have you identified which information is sensitive and which is non-sensitive? Is sensitive information handled differently? Is it well protected?

Who has access to your computer systems? If you outsource IT, do you know and understand how information is backed up and stored?

How effective and up to date are your anti-virus and other protective programs?

Does your employee handbook include policies and procedures for data security?

Is access to private information (such as social security numbers, credit card numbers, expense reports, and copies of paychecks) limited to a few specific employees? Is this information password protected?

Does the organization have defined steps, including security measures, for transferring funds to a vendor or financial institution?

What are the procedures when employees upgrade mobile phones, laptops, tablets, and smartphones? Do you take steps to erase information from the old equipment?

Who are your outside providers? In what ways do you interface with them via technology? Do you require them to comply with your security standards?

Has your organization made any recent changes to the way it uses technology, such as uploading critical information to the cloud or installing new systems for communications and collaboration?

In addition, because many cybercrimes are carried out by employees, examine your hiring procedures. Be sure to conduct extensive background checks on candidates who will have access to financial, banking, and related resources.

> "Understanding and guarding against cyber threats are critical elements of governance."

Step 2: Manage Your Risks

Managing cyber exposure is the responsibility of everyone with computer access. Your IT professionals can help you establish security protocols, including protected password access, Web site restrictions, and e-mail encryption policies. But you and everyone else in the organization must understand the limitations of these fundamental measures and remain vigilant. Here are a few important precautions to take:

- **Have employees lock or shut down their computers** whenever they leave their work spaces.
- **Make certain that people close their Web browsers** when not in use.
- **Control access** to computers logged on to your network.
- **Be sure employees — especially those who work remotely — understand and follow** all security protocols.

Step 3: Evaluate Your Insurance Coverage

You may be covered for cyber loss through insurance policies you already have. Several types of policies — either in their general forms or through cyber-specific enhancements — cover losses related to technology breaches. These policies include:

- **business owner's** policy (BOP)
- **property** insurance
- **crime**
- **errors** and omissions
- **directors and officers** (D & O) liability insurance.

Some coverages that may be available under your existing policies include the following:

Targeted Hacker Attack/Electronic Vandalism covers costs related to the willful corruption, distortion, deletion, damage, or destruction of electronic data caused by a targeted hacker attack. Some policies extend coverage to loss from a computer virus caused by cyber vandalism. Typically, coverage only applies when these acts involve someone other than employees.

Interruption of Computer Operations provides extended "Business Income Interruption" insurance for loss of income if you're unable to operate due to damage to electronic data processing equipment.

Employee Dishonesty/Computer Fraud covers loss or damage resulting from theft by an employee, including fraudulent funds transfer.

Unfortunately, each of these coverage enhancements is typically limited at $10,000 to $100,000, which isn't much, given the potential magnitude of the exposures. Thus, you may want to consider stand-alone cyber-risk policies. A growing number of insurance companies now offer such policies. With increasing market competition, pricing has come down, making these policies more affordable. The policies often have multiple insuring agreements, or "modules," including:

Privacy Injury Liability protects your organization from the cost of judgments, settlements, and associated defense costs resulting from any unauthorized access to confidential information.

Network Security Liability covers security breaches in your computer network that give rise to:

- disruption or degradation of the network
- unauthorized use or disclosure of information
- any unplanned inability of an authorized party to gain access to the network.

Privacy Regulation Proceeding Coverage will reimburse costs associated with a civil, administrative, or regulatory proceeding by a governmental authority alleging any violation of a Security Breach Notice Law.

Privacy Event Expense Reimbursement covers expenses incurred to comply with Security Breach Notice Laws or related regulations and to retain crisis management resources (such as a defense counsel or public relations firm).

Extortion Demand Reimbursement covers expenses incurred when there is imminent danger of a loss or damage to the network, loss of confidential information, or defacement of the Web site.

First Party Network Interruption & Extra Expense Coverage covers lost income related to a network shutdown caused by unauthorized access, electronic virus, or denial of service attack.

> "Do you erase information when employees upgrade laptops and smartphones?"

Several of these coverage modules may not be available from all insurers; others may be limited or require additional premiums. Liability coverages may overlap with coverage under an errors & omissions policy. Alternatively, it may be appropriate to add broader cyber/network security coverage to your errors & omissions policy. This approach can help avoid coverage gaps and is cost-effective.

Both stand-alone policies and add-on coverages are subject to exclusions and conditions, which may create unexpected gaps. Some forms exclude claims for bodily injury or property damage. "Proprietary rights injury" exclusions encompass injury arising out of plagiarism, piracy, infringement, or misappropriation of copyright or trademark. Limits of $1 million to $10 million are common, but limits up to $50 million or more are available.

Stay Vigilant Concerning Cyber Risk

Remember that the cyber threat environment is dynamic: While security experts are improving protection and insurance companies are expanding their offerings, cybercriminals are becoming increasingly sophisticated. So cyber risk management must be an ongoing process. An experienced and knowledgeable insurance broker can help you understand the evolving risks, your current coverage, and options to address your exposure.

Tom Marchetti (tmarchetti@amesgough.com), a vice president and partner of Ames & Gough, leads the firm's Association and Nonprofit practice. Established in 1992, Ames & Gough (amesgough.com) is a specialty insurance brokerage and risk consulting firm.

Keep Your Risks in Check

For more on managing cyber (and other) risks, see articles such as these at www.NonprofitWorld.org/members:

Will You Be Ready When Disaster Strikes? (Vol. 18, No. 3)

Choosing the Right D & O Insurance for Your Board (Vol. 12, No. 1)

What Is the Board's Role in Managing Risk? (Vol. 15, No. 5)

Get the Best Protection for Your Insurance Dollar (Vol. 24, No. 4)

Do You Need a Record-Saving Policy? (Vol. 19, No. 6)

How to Prevent an Information Disaster (Vol. 23, No. 1)

Can Your Organization Afford to Lose $100,000? Safeguards Every Nonprofit Needs to Implement (Vol. 30, No. 3)

WHAT'S UP ONLINE?

To broaden online discussions on nonprofit topics, we're expanding our Discussion Forum with a ListServe, provided by Yahoo Groups. To join, you can either click on the "Yahoo" button at:

http://www.NonprofitWorld.org/social/
(free Yahoo login required)
or send a blank e-mail to:
NonprofitWorld-subscribe@yahoogroups.com

If you have any questions, contact Jason Chmura at jchmura@NonprofitWorld.org.