



## **An Enterprising Approach to Cyber Risk Management**

*By Aaron Latto*

*Market Solutions Director, Global Technology Underwriting*

*St. Paul Travelers*

Cyber risks are a growing business threat. Computer viruses, software flaws, and hackers continue to chip away at vulnerabilities in computer networks. The 2004 Computer Crime and Security survey, conducted by the Computer Security Institute and the FBI, showed that a large number of U.S. businesses and government agencies are experiencing computer security breaches that result in huge, financial losses. Although worms, viruses and hackers receive widespread media attention, the reality is that businesses simply don't talk much about how to manage cyber risk

### **The Enterprise View**

To achieve success in managing cyber risk, companies should take an "enterprise" approach to risk management.

Today, most businesses guard against cyber risk exposures by investing in technology safeguards. They purchase and configure firewalls, routers, secure servers and anti-virus software. Newer innovations such as fraud-detection software, sophisticated access-management applications, and patch-management systems prevent cyber incidents while maintaining business functionality. This much is good.

But technology safeguards are only one part of a total cyber-risk management program. Businesses must move away from an over-reliance on technology tools and embrace an enterprise risk management approach to best address cyber-risk exposures. There are three key principles to this approach:

- Integration of IT management and traditional risk management for management of cyber risks;
- Senior-level management involvement in and commitment to cyber-risk management;
- Commitment to employee training programs at all levels of the company.

These principles can be implemented in various ways according to a company's size and activities. However, commitment to the principles should not vary.

### **Bridging the Gap**

An enterprise approach to cyber-risk management breaks down traditional barriers between IT management and risk management. In many companies, these two departments operate as separate entities. IT departments focus on ensuring that the company's IT systems function

smoothly. In contrast, risk managers focus on issues such as worker safety, vehicle safety, product liability and recall matters, insurance programs and employment-practices concerns. Unfortunately, the two groups rarely cross paths.

An enterprise approach to risk management calls for committed and regular collaboration between risk managers and IT managers. These groups must work together on the following items:

- Identification of the company's specific cyber risks;
- Selection of technology-based tools and resources to manage those risks;
- Selection of tools and resources to educate all company employees;
- Implementation of the chosen risk-management strategies; and
- Forecasting new risks the company may encounter as business practices and strategies change.

### **Senior Management Commitment is Critical**

Traditionally, senior management of most companies hasn't been involved in cyber-risk management. But their participation and commitment are essential to making the process work.

Sadly, it often takes a well-publicized catastrophe or a big financial loss – caused by a widespread virus or a high-profile hack – to bring about a change in business practices and procedures. For instance, companies heard for years that they should develop and test disaster recovery plans. Yet the events of September 11 revealed that some companies had not developed such plans.

It's a challenge to win senior management support. Many corporate constituencies compete for attention and financial commitment. Cyber-risk management is but one. But as more attention and dollars are focused on ensuring corporate financial accountability through robust IT systems, a stronger focus on risk management may result. It may also provide an opportunity for IT managers to interact with finance managers, who are most often responsible for corporate risk management. And that may help advance efforts to combat cyber risk.

### **Employee Awareness and Training**

While it's essential that IT managers and risk managers forge a better working relationship and that senior managers commit to an enterprise approach to risk management, it is also critical that employees receive training to better understand and identify cyber-risks.

The training programs should cover topics such as:

- Acceptable Internet and e-mail usage;

- Strong password management and use;
- Workstation security and access control;
- Dealing with requests for company information;
- Use and storage of company information;
- Resources and/or contacts for employees with questions.

### **Enterprise Approach Guidelines**

How should businesses establish an enterprise approach to cyber-risk management? Here are some guidelines:

- Senior management should take an active and continuing role in directing the identification of and management of cyber risk.
- Senior management should set the expectation that corporate groups will work together to identify and manage cyber risk issues.
- Senior management and chief financial officers should consider sharing certain portions of IT, risk management and insurance budgets to create a broad and effective approach to risk identification, management and transfer.
- Corporate communications or public relations departments should work with IT and risk management departments to understand potential cyber risks and to develop response plans in the event of a cyber incident.
- Employee training programs should be implemented once a company's cyber risk exposures and priorities are identified.

### **The Role Of Insurance In Cyber-Risk Management**

The good news is that many businesses are taking steps to protect against cyber risks. But even the best preparations – both technological and human – cannot prevent all potential for loss. Thus, businesses increasingly look to insurance to help transfer cyber risks.

There's now a solid insurance market for "cyber" products. Cyber-insurance policies cover risks that traditional policies – such as commercial general liability (CGL), property, or professional E&O – weren't intended to cover. Policyholders can choose from basic coverages to more robust coverages. Some cyber insurance products, such as those offered by St. Paul Travelers, are designed for the unique needs of specific industries.

Businesses should consult their insurance advisors to understand what their traditional insurance program covers. Specific cyber-insurance coverage may be the best option for your business.

Each business has its own risk tolerance. But **no** business should tolerate not knowing whether it has transferred cyber risk through its insurance program.

## **Conclusion**

Insurance coverage is playing an increasingly important role in the overall management of cyber risks. But risk transfer through insurance is not enough. Companies need to implement an enterprise approach to risk management. By bringing all parties to the table — IT, risk management and senior executives — and leveraging their respective expertise, businesses will take an important step toward establishing an effective cyber risk management program.