PUBLIC ENEMY #1

DOES THIS MEAN YOU?

You face cyber risk if:

• You rely on technology – and the greater the reliance, the greater the risk.
• You contract with internet-based vendors or purchase cloud-based services.
• You take credit card payments, do business through a website, or share crucial information via the web.
• Your revenues are dependent on your internal network.
• You're in an industry that hacktavists don’t like.
• You have potentially disgruntled employees with access to crucial company systems.
• You can download files from the internet, opening the gate to viruses, spyware or malware.
• You rely on another organization’s data, systems or software.
• Another organization relies on your data, systems or software.
• You store any type of confidential or proprietary information.

If any of the above hold true for you, you potentially face two types of cyber loss: liability and direct loss.

Liability arises when a cyber incident prevents you from performing a contractual obligation or ends up causing harm to a third-party who sues. The cyber liability that most frequently makes the news these days involves a breach of confidential information, which includes personally identifiable information (PII), such as credit card information and social security numbers that could be used in credit card fraud or identity theft, as well as confidential business information. When confidential information is compromised, organizations responsible for that data may be liable – even if no known damage occurs. Fines can result, and significant costs can be incurred for notifying the parties whose data has been exposed.

Direct loss – loss to your company – also falls into two categories. First is the loss of assets, usually data, which can be costly to replace and is sometimes irreplaceable. Second is the revenue interruption that results if a cyber event prevents you from transacting business.

ARE YOU READY?

Outgoing cyber security chief for the FBI, Shawn Henry, warned last year that cyber criminals are winning the cyber wars, and that in fact many companies have lost data to hackers and are not even aware of it. Despite the best efforts of IT – your IT department and the IT departments of partners you rely on – the risk is too broad and fast moving to be easily managed.

One of the challenges in managing cyber risk is the way many companies are organized. In the military a strict command and control structure allows for a disciplined approach than most businesses are able to enforce. Government falls somewhere between, with a broad hierarchical structure presumably answering to a central authority. As officials in South Carolina can tell you, however, governments are not impervious to cyber intruders.
Business has to balance the need for a hardened technology perimeter with the need for flexibility and openness, which can help day-to-day business operations. Regardless of how tight a ship you may be running, you’re probably not as ready as you should be.

WHAT YOU CAN DO

The first step in facing the insecurity of our cyber world is to acknowledge the problem and accept that effective cyber risk management will likely require a combination of prevention, risk transfer and disaster planning – and steady monitoring of all three.

More specifically, we offer 10 tips recently presented in Resilience, the premier issue of Willis’ new magazine devoted to solutions for a risky world:

1) Review contracts with IT vendors, assuring they are compliant with regulatory requirements and implement appropriate controls.

2) Pre-arrange relationships with a breach service provider, outside counsel and reputational risk adviser.

3) Provide ‘certification’ via e-learning to employees on safeguarding data.

4) Create an information security policy that is communicated to staff.

5) Prepare, implement and test an incident response plan that allocates executive responsibilities following a cyber attack.

6) Keep your general counsel’s office current with disclosure laws, privacy regulations, international requirements and updates.

7) Identify key information assets and thoroughly assess their vulnerability to attack.

8) Develop an incident response plan with staff, counsel, reputational risk advisers and a breach service provider.

9) Work with your specialist cyber insurance broker to analyze how to transfer quantifiable risk and defend your organization from catastrophic exposures.

10) Conduct annual risk assessments and exercises to test crisis management plans and hold an internal privacy workshop to identify vulnerabilities.

The Cyber insurance marketplace is steadily maturing, offering options that can cover defense costs, awards, business interruption and data recovery costs when a cyber loss occurs. Careful coordination of P&C coverages with cyber insurance is the best way to get the most out of the many risk transfer options now available in the marketplace.

You should also beware of protections afforded by legislation such as the SAFETY Act of 2002, which was designed to promote anti-terrorism products and confer liability protection on the makers and users of those products. Many of those protections apply to technology products which contain security elements, offering potential relief for those seeking protection from the cyber impact of a terrorist act.

Information and idea sharing through groups such as ISACA (Information Systems Audit and Control Association) offer opportunities for education, discussion, immediate notice of real-time attacks and an exchange of ideas about protection from cyber perils. ISACA groups have been set up for a number of industries.

You can’t hide from what may be our current public enemy number one, but there is much you can do to protect yourself.

FOR MORE INFORMATION
Please contact your local Willis representative or visit www.willis.com.

Willis is a leading global insurance broker providing insurance, risk management and human resource solutions.