INSPIRIEN

Fundamentals of Cyber Risk Management

Cyber risk is increasing. Criminals armed with a computer, a network connection, and malicious intent are increasingly targeting small and medium-sized businesses, from retail to healthcare and array of other professions. More than 85% of cyber attacks are thought to be brought against small businesses, but fewer than one such firm in five believes that their ability to mitigate attacks is highly effective.

Cyber exposure should be on the minds of all board members and risk managers, since nearly all companies are effectively high-tech companies in today's age, by the way in which they trade and transact their services. Reliance on technology, databases, and remote connections is heavy. Every business is connected, and every connection creates vulnerabilities. Few modern-age firms are able to demonstrate complete redundancy and are consequently unable to assume that business-as-usual would carry on when their networks and servers are down, or a breach has been incurred. Everyone is reliant on technology to the degree that may prevent them from adequately operating when a cyber-incident has either put their networks out of action or compromised their data.

Key to preventing business damage arising from cyber-attacks is to introduce effective risk management before the loss. Many steps are easily implemented. Phishing, for example, is a hackers' gambit used to gather information, or to implant malware onto company systems. It is a branch of the technique known as 'social engineering,' which is little more than running a short con to manipulate employees into granting access to systems, revealing passwords, or otherwise compromising a firm's cyber security. Simple staff training programs can ensure that every individual in a company is aware of these risks, is able to identify suspect messages, calls, or visits, and knows well the procedures to follow when one occurs.

Most businesses will have adopted security protocols which are intended to protect systems from infection or attack. However, a very large number of these systems are inadequate. Hackers' techniques evolve constantly, and it is therefore important to continually review network risks management. Cyber criminals regularly look for weaknesses in commercially available security software and exploit them before the loopholes are closed. More complex systems present a greater number of vulnerabilities. Simply following security guidelines to meet, for example, an international standard, may not take into account the unique risk profile of an individual business's systems. Very careful enterprise risk analysis, often assisted by external experts, is essential.

Sadly, cyber risk management cannot be an implement-and-forget procedure. Everything is in flux, from the vulnerability of systems to the skills and motivations of those who seek to exploit security weaknesses within them. Businesses must constantly review and reassess not only the security measures which they have put in place but also the evolution of the targets and vulnerabilities that the business itself creates. When new processes or systems are introduced, it is critical to begin the assessment from the top down, since a new but protected system may create gaping new security holes when it is integrated with existing cyber protection protocols. Similarly, staff training in cyber security should be repeated regularly.

Cyber insurers provide valuable indemnity which covers claims related to cyber losses, indemnifying first-party business risks such as increased costs of working and business interruption, as well as third-party liability. Many insurers also provide current insights and services to support enterprise-wide cyber risk management. However, in the exploding cyber-insurance market, all coverage is not identical. Insurance buyers and their brokers should look carefully at the scope and nature of the coverage on offer, and compare several of the various options. Some policies exclude losses arising from social engineering, for example, or offer very low limits for related losses. Other policies provide very broad coverage which may insure risks that the ultimate buyer simply does not face.

Alongside risk mitigation and management, many cyber-risk insurers provide support after a loss. The assistance of qualified experts is covered by the better policies, some of which include post-loss services by highly regarded consultancies as part of any claim. Such support can help companies to recover quickly and minimize possible reputational damage after an attack.

Whether the need is pre- or post-event, one constant is true of every business: each is different. Every company requires appropriate risk management, including regular staff education, but exactly what those provisions constitute is not the same for each firm. Similarly, insurance coverage must be put together with the specific risks and vulnerabilities of each client in mind. Terms of coverage should be revisited and amended at least annually, to ensure that the persistent evolution of the hackers' threat is adequately covered.

Cyber risk is a real and present threat to all businesses, but it need not be a worry. With thoughtful risk management and effective insurance measures in place, companies can be confidently protected from this new and constantly evolving risk.

By Gareth Tungatt, Chief Underwriting Officer, Ascent Underwriting
Inspirien has partnered with Ascent Underwriting to provide Cyber Protection. Learn how easily you can protect your facility at www.inspirien.net

About Inspirien

Inspirien is the spirit of encouragement that drives us to do what is best for our clients. It is what motivates us to guide them, protect them and advocate for the future of their business – to join them in meeting the challenges of an evolving marketplace.

At Inspirien, we offer more than just workers' compensation, professional, general and umbrella liability coverages. We help our customers manage their risk. We understand that it is the people around the policy that make the difference which is why our customer relationships have always set us apart. It is our mission and vision to be a remarkable partner for whatever risk lies ahead by inspiring unique ideas and actions to manage our partners' risk. Find out more at www.inspirien.net.