Risk Management Advisory

CYBER INSURANCE

A new perspective on cyber risk

All too often when we think about cybersecurity and cyber risk, our thoughts turn to security technology. The reality is that cyber risk isn't solved by security technology alone. Employee knowledge, processes, culture and technology combined will help to build a strong defence against data loss and its unexpected financial impact.

The majority of cybersecurity incidents are the result of someone falling victim to an online scam, such as fraudulent email or surfing the web on an unsecure or unprotected device. And, most cybersecurity events can be prevented—if the organization takes a proactive approach.

Everyone is a target

Cyber risk is a rising and material issue not only for Canada's largest enterprises, but for every business of every size, from small businesses of less than 100 employees to medium-size enterprises of several hundred employees in manufacturing, technology, retail, financial services and more.

That's because cybercrime has become a profitable business model for organized criminal groups around the world and because the tools to commit online crimes are readily available—at a low cost and with full support.

Researchers are estimating that the global economic impact of cybercrime will rise from $500 billion in 2017 to more than $2 trillion by the end of 2021. Meanwhile, spending on traditional approaches to cybersecurity is expected to rise from $80 billion to more than $1 trillion over the same period.[1]

The experts' predictions mean that, globally, we'll be spending more than ever before on cybersecurity yet lose more to cybercriminals and other actors than ever before.

Cybersecurity spending will exceed $1 trillion in 2021.[2] Throwing money at a problem is never the lone answer. The regulatory, brand damage and unexpected financial impacts of ransomware, advanced malware and targeted attacks which start with an unsuspecting employee, speak to the need for a proactive and strategic management approach to the problem.

What can organizations do to prevent loss?

While investments in security tools, such as anti-virus and firewall technology, are important, tangible risk reduction requires an embedded culture of security within your organization.

- Educate employees about cyber risk
- Regularly inform and engage senior management and boards in discussions about cyber risk
- Make the right investments of time and money in improvements to policies, processes and technology

Building a culture of security and reducing your cyber risk will require your organization to improve its awareness, processes and policies. One of the first things you should do is ensure every employee has a basic knowledge and understanding of cyber risk, how their inadvertent actions can lead to issues and the importance to your organization.

[1,2]CSO, June 2017, online: http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

VICTOR

One approach is to use an external cybersecurity expert or firm to create and support an effective cybersecurity program, but this can be costly. Another alternative is security awareness technology, which can be used to educate employees through online courses and simulated attacks to test their knowledge. The technology can also monitor awareness and behaviour on an ongoing basis, all with a minimal burden on technology teams and resources.

The rationale for this approach is report after report on cyberattacks show a clear pattern. The overwhelming majority of successful cyberattacks are the result of social engineering (i.e., phishing and other electronic scams) which exploit unsuspecting employees, contractors or others associated with the organization. Simply put, cybercriminals know it's far easier to manipulate human emotions—fear, greed, lust, anger and curiosity—than it is to hack computer systems.

This advisory was written by David Shipley, CEO of Beauceron Security. Beauceron offers an affordable, secure cloud-based platform to automate many of the routine tasks needed to help educate people, move individuals from cyber-unaware to cyber-aware and to help entrench ideas of accountability for individuals, managers and senior leaders. For more information, visit www.beauceronsecurity.com.

Victor offers coverage for these exposures under a stand-alone Cyber insurance product.

Visit us at victorinsurance.ca to learn more.