Risk Management Advisory

CYBER INSURANCE

The evolution and mass market of cybercrime

While cybercriminal markets have been flooded with billions of personal records, criminals have improved their business model by using technology and extortion. Now, rather than steal and try to sell an organization's data, criminals will simply deny access to an organization's data via so-called ransomware scams.

Canadian law firms, accounting firms, construction companies, universities and colleges, hospitals, municipalities, government agencies and more have all been victims of this type of online extortion, and incidents have been on the rise globally.

In some cases, when criminals don't receive payment or the amount they feel they deserve, they'll often threaten to leak stolen data to media organizations or the general public to cause reputational harm to their victims. Regardless of the scenario, cybercriminals are able to monetize your investments in devices, data, applications and process automation.

How cybercriminals get in

If you consider the number of employees, customers, suppliers and third parties that digitally interact with your organization via email, purchases, supply arrangements, contracts, services, payments, and so on, each instance and point of contact represents multiple points of entry into your organization for a cybercriminal. Cybercriminals know you are unable to secure every device, network or online interaction that touches your organization. They find the weak links and exploit them.

Research has shown that, nine times out of 10, the weak link is via an unsuspecting human. This is why security technology alone can't solve the problem.

The total number of phishing attacks in 2016 was 1,220,523, a 65% increase over 2015.[1] Can your security team deal with 65% growth in just a single cybercriminal tactic? How are you mitigating the risk?

Focus on the cause not the effect

The breadth of your organization's human attack surface is well beyond the scope of any technology-centric security program. Instead, a prudent and strategic step is for you to quantify the source and nature of unknown human risk then take steps to measure, manage and monitor the risk.

[1]APWG, "Phishing Activity Trends Report for Q4 2016," February 23, 2017, online: https://apwg.org/trendsreports/

Once known, management of human-centric risk becomes a key input into business priorities, processes and security technology investments. Further, following the adage, "what gets measured is what gets done," tangible measures enable leaders to take actions based on risk insights which drive improvements in effectiveness and efficiencies of security processes.

Mitigate your risk – The three 'M's (and an I)

According to a research report commissioned by FICO[2], "cyber risk insurance has a vitally important role to play" in addressing the cybercrime problem. The same research report also found "organizations need a holistic cybersecurity strategy that involves all areas of the business," and, "to improve their cybersecurity status, organizations must take care to objectively measure it." The three 'M's—measuring, managing and monitoring risk—are a key part of the strategy to ensure all areas of the business are accountable for cyber risk and to provide the means to effectively reduce it.

[2]FICO, "What the C-Suite Needs to Know About Cyber Readiness", May 3, 2017, online: http://www.fico.com/en/blogs/fraud-security/what-do-the-c-suite-think-about-cybersecurity/

Figure 1 - proactive identification of human cyber risk hotspots

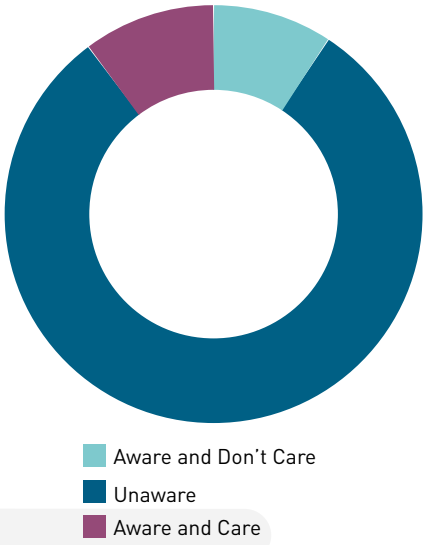
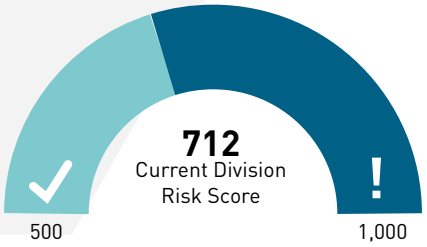


Figure 2 - clear metrics to manage cyber risk



This bulletin 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.