Cyber Protection Reimagined: Are You Playing Cyber Offense or Defense?

By Stephen Paulin

Recently, while discussing with a client the need for Data Breach / Cyber Liability insurance, he made an insightful and impactful statement about protecting his two most important business assets – employees and data. His 328 employees enjoy a robust benefits plan, including health, dental, vision, life insurance, long and short-term disability, access to voluntary coverages and workers' compensation insurance. This is quite an investment, but not unusual for a business to comprehensively protect the workforce in the event of either a workplace or non-employment related injury or illness.

With employees having network access through multiple entry points, i.e. smart phone, tablet, home computer, and office computer, at a minimum this company has 1,140 access points in addition to third-party access that are vulnerable for exploitation. This data was only protected by the usual pro-active, risk prevention methods (passwords, firewalls, etc.) and guarded by his head of IT. He is responsible to secure sensitive information and verify employee access to the network as well as third-parties, keep the software and operating system up to date, ward off / turn back malware attacks, encrypt or properly dispose of sensitive data while coordinating with operations to train employees about appropriate security measures.

Each is a markedly different approach in the company's risk tolerance and risk management philosophy. Our discussion was beneficial as it opened the opportunity for my client to assess his situation from a different perspective. As it was, the lack of needed attention given to protecting his network proved to be an unintentional oversight. An injured / sick employee or compromised network has their own set of unique exposures, each representing the potential for financial loss. Given the current situation, data is the most vulnerable and likely to cause the most serious loss of earnings. Financial loss from a cyber event can take many forms, with the inability to access one's network having serious consequences. The loss of funds that are surreptitiously taken via electronic transfer as

a result of social engineering are easy to quantify. But, how does any firm accurately or responsibly forecast on loss of revenue associated with “reputation, credibility and trust” post incident?

Just as a health and wellness plan, safety program and focus on compliance are essential to employee health and success of any businesses, there is also insurance as a backstop in the event of a loss. Before disaster strikes the network, there needs to also be in place a holistic, end-to-end approach employing risk assessment and identification of vulnerabilities, monitoring, employee training with Cyber Insurance as the ultimate safety net.

Cyber security is not just an IT problem, but a business problem, with mission critical systems at stake. The core competencies necessary for an IT professional to operate a network are a completely different set of skills needed to ensure site security. Also, IT lacks the organizational authority to run a cybersecurity program. IT professionals have operational and technical responsibilities, but to run a competent cybersecurity program requires outside support to attain first-amongst-peer position.
Most businesses are under-prepared and/or under-insured for their growing cyber peril. The realization that under the current circumstance, the cost of a breach to the network could vastly exceed the financial loss associated with that of the employees, only highlighted the need for the additional level of assurance beyond what a Cyber Liability Policy can deliver.

When it comes to cyber threats, and how they continue to evolve, businesses are faced with the known and massive unknown. As such, buyers of Cyber Insurance need broader and better solutions, not just more insurance products. As the Cyber peril looms, the focus must shift from a reactive position of obtaining cover from products to a proactive, offensive approach engaging risk management, incident prevention and incident response. To truly maximize the benefits of Cyber Insurance, success is about integrating technology and forging relationships with third-party providers.

Because it’s imperative for businesses to quantify and quantifiable their own security posture, employers an end-to-end solution to identify the organization’s network vulnerability, close those gaps, provide 24/7 monitoring and obtain Cyber Insurance at a discounted cost. To help frame your exposure calculations are available to estimate these costs. Offense is the best defense.

This all comes from the understanding it’s not about “if” a cyber event will happen but “when” one will happen. A twist on the old adage is pertinent here – “Prior Proper Planning Promotes Peak Performance.” How engaged is management on this issue? How well will the company manage

business interruption? Is there a continuity plan in place, with back up vendors and all those things that are going to make sure your business is resilient and prepared, not just secure?

An attacker doesn’t have to be good every time, they just need to be successful once! Offense wins and defense loses.
