CYBERSECURITY FOR SMALL MEDIUM-SIZED ENTERPRISES

INTERVIEW WITH

PETER WHITTAKER

DIRECTOR
BUSINESS DEVELOPMENT,
SPHYRNA SECURITY

Q: The COVID-19 pandemic has created an urgent need for collective leadership across all sectors to address the latest cyber threats. What changes do you foresee in Canada's overall approach to cyber resilience over the next 5-10 years?

A: In three words, future cyber resilience depends on velocity, agility, and judgement.

COVID–19 forced organizations to change their cybersecurity velocity: They have had to change the direction of operations, from office-based to home-based, and they have had to do it rapidly. This has required tight focus, rapid evaluation of alternatives, and a willingness to change approaches just as quickly, e.g., when many organizations switched video conferencing systems because of perceived security flaws in a dominant player.

These changes in velocity require organizational and individual agility, both for the ability to brainstorm and adapt rapidly, and for changing not only how an organization works but, in many cases, what it does: The businesses and departments that are succeeding today are able to see a spectrum of possibilities and focus tightly on the achievable, meaningful, and valuable.

That focus requires business judgement and risk judgement: What are we really here for and how can we best balance effective risk mitigation with valuable business outcomes, in a very short time, without risking long-term exposure or loss of assets?

Organizations need to institutionalize and operationalize that velocity, that agility, and that judgement, and to maintain them for the long term. Businesses and departments that "revert to form" risk ossification as they attempt to codify everything done today, while forgetting they need to keep doing it tomorrow.

CYBERSECURITY FOR SMALL MEDIUM-SIZED ENTERPRISES

Q: What cybersecurity considerations need to be addressed by organizations during the pandemic and post-recovery?

A: Short term, organizations need to make rapid risk management decisions without panicking or overreaching: They need to rapidly ingest information on vulnerabilities, both in technologies and in processes, and decide quickly whether it is best to do nothing or to make changes, and whether changes are deft and surgical, or more holistic and all-encompassing. This requires an accurate sense of the time value of information, both to the organization and to its adversaries, so that mitigations can be chosen based on how information assets bring value to the organization today and may bring value to an adversary later.

Longer term, organizations need to regularly reassess past decisions regarding information value and rapidly deployed mitigations: Do we continue to protect that information, or does the cost of its protection outweigh its value? If so, do we delete it? This can be a tough decision, as businesses love predictable, recurring revenue, especially when it requires little maintenance. Historically, the tendency has been to maximize profit flowing from existing assets by reducing maintenance costs, especially around security, leading ultimately to breaches. Businesses may need to decide to stop a revenue stream today to prevent a breach tomorrow.

More fundamentally, though, cybersecurity depends ultimately on people. Protecting lines of business and information assets means ensuring that employees can make sound decisions.

Future cybersecurity will depend in no small part on healthy corporate cultures that value their employees as human beings and ensure they have what they need to do their jobs, including health and support.

Q: As a cybersecurity expert and active contributor to the Council's technical committee on cybersecurity, could you share your observations in designing a national standard for improving the cybersecurity posture of small and medium-sized organizations? How do you envision this standard helping organizations in managing today's cybersecurity risks?

A: Large organizations have the comparative luxury of being able to create multidisciplinary teams to solve tactical, operational, and strategic problems: Experts can digest complex standards, integrate them with corporate direction and policy, distribute work to subject matter experts (SMEs), manage questions and interpret intentions, etc.

The smaller the SMB, the more tightly focused they are on their business itself, the less time, energy, and focus they have for other concerns - and unless they work in the field, the less likely they are to have cyber SMEs available to them.

This means our standards have to be focused and clear. We need to ensure that we, as contributors, understand exactly what it is we are trying to say and that we say it as plainly as possible. Like experts in all fields, we tend to use jargon and TLAs (three letter acronyms). We need to stay away from those as much as possible, and we need to recognize that the same word can mean very different things in different contexts - and it is likely that SMB owners and employees come at things from very different contexts indeed. Those differences can mean radically different interpretations of what we, the cyber SMEs, thought was clear and plain.