Duo Security and Global Risk Institute Host Discussion on Cyber Risk and Security in Canada

Author
Josh Yavor, Duo Security's Director of Corporate Security
Brian O'Donnell, Executive-in-Residence, Global Risk Institute

GRI | GLOBAL RISK INSTITUTE

On April 11th, Duo Security and the Global Risk Institute (GRI) co-hosted an executive breakfast in Toronto to provide an update on current security trends and key information that leaders need to know.

While board members and company executives have a growing awareness of the risks and potential cost of data breaches, many of the educational resources available are still aimed at security professionals and are most useful for those in technical roles.

In the results of the GRI's latest annual member survey cybersecurity risks topped the list of member concerns, outranking uncertainty in the housing market, consumer debt challenges, and regulatory changes. This highlights the increasing awareness that, as client interphase applications and remote access by employees, contractors and third party suppliers have significantly broadened the periphery of corporate networks, hackers have been increasing the velocity and sophistication of their attacks; the result is a continuous flow of corporate and government institutions reeling from the impacts of successful hacking attacks.

A report published in February by the World Economic Forum entitled "Advancing Cyber Resilience: Principles and Tools for Boards" outlines a ten-step process with practical strategies and recommended questions for a holistic view of security, including:

- Building a culture of executive cybersecurity responsibility.
- Understanding the intersection of both cybersecurity and the strategic risk posed by technology (e.g. disruption), and ensuring the Board members are both sufficiently aware and knowledgeable to properly govern these risks (defined as Cyber Resilience).
- Accurately modeling which threats pose the greatest risk.
- Utilizing an "Enterprise Cyber Risk Management Framework" approach to managing cyber risk, and ensuring that all employees, contractors, third party suppliers, executives and board members understand the evolving cyber risk faced by the firm, and their role in cyber security.

Duo's presentation focused on the shift to cloud services, the vanishing perimeter, and how organizations can maintain strong security policies whether they are protecting on-site or cloud-hosted resources. The BeyondCorp model applies to companies with a traditional perimeter-based security model and can make incremental improvements while modernizing their approach to information security.

Duo's approach security is called Trusted Access - rather than relying on a private intranet behind a traditional firewall:

- At the point of access, Duo checks to make sure the user, their device, and the network they're on meet the organization's policy standards.
- The tools available in Duo Access allow organizations to easily enforce policy, conduct health checks on all devices and networks reaching critical systems, and enable self-remediation for out-of-date devices and services by users.
- Duo Beyond gives organizations the ability to enroll and set policy for corporate-managed devices for both internal and external applications, allowing for more nuanced policy settings.

The migration to cloud services and prevalence of users bringing their own devices are forcing businesses to reconsider their approach to effective security. While this poses new business challenges, executive teams willing to evaluate their approach to technology and leadership can leverage these changes for a more resilient, manageable and flexible security program.

The threat landscape continues to evolve, and a broader dialogue is required to ensure that institutions are, and continue to be, cyber resilient; the evolving threat increasingly requires that firms ensure that all players connected to their network are ready, willing and able to play their role in cybersecurity, or risk being exposed by the hackers as the next "weakest link".