Nearly Three-Quarters of Canadian Organizations Think They'll Be Breached in 2022

Remote working, third-party applications, and mobile devices top cyber risk for organizations

TORONTO, April 18, 2022 – Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today announced the findings of its latest global *Cyber Risk Index* (CRI) for the second half of 2021, standing globally at -0.04, which is an elevated risk level with North America being at -0.01. Canada received a score of 0.16, which shows that the country has a moderate cyber risk level in comparison to global and North American (NA) organizations. The research also found that Canada is more prepared than all of North America to handle cyber risk (at a score of 5.41 vs. 5.35 in NA). However, respondents revealed that nearly three-quarters (74%) of Canadian organizations think they'll be breached in the next 12 months, with 30% claiming this is "very likely" to happen.

Cyber Risk Index Ratings	
Range	**Interpretation**
5.01 to 10	Low Risk
0.1 to 5.0	Moderate Risk
0 to -5.0	Elevated Risk
-5.01 to -10	High Risk

Cyber Preparedness Index Ratings	
Range	**Interpretation**
7.51 to 10	Low Risk
5.01 to 7.50	Moderate Risk
2.51 to 5.0	Elevated Risk
0 to 2.5	High Risk

"As organizations constantly navigate the ever-evolving security landscape, understanding what makes their businesses vulnerable is critical," said Greg Young, Vice President, Cybersecurity at Trend Micro Canada. "This is where reports like the CRI can be a great resource in highlighting areas of possible concern to help organizations develop an effective cybersecurity strategy."

The biannual CRI report asks pointed questions to measure the gap between respondents' preparedness for attacks and their likelihood of being attacked*. In Canada, 83% of organizations claimed to have suffered one or more successful cyber-attacks in the past 12 months, with 32% saying they'd experienced seven or more.

Ransomware, phishing/social engineering, denial of service (DoS) and botnets top the list of key concerns, with negative consequences of a breach including stolen or damaged equipment, lost revenues and costs of outside consultants/experts.

When it comes to IT infrastructure, Canadian organizations are most worried about security risks in relation to mobile/remote employees (score of 7.55/10), third-party applications (score of 7.25/10), and mobile/ smart phone devices (6.55/10).

While digital investments were necessary to support remote working and drive business efficiencies during the pandemic, this report brings to light the increasing corporate attach surface and ongoing challenges business face securing such investments.

“Organizations are facing demanding security challenges every day, from software vulnerabilities and data breaches to ransomware attacks and more,” said Dr. Larry Ponemon, Founder and Chairman of Ponemon Institute. “The semi-annual survey has been a tremendous asset in evaluating the rapidly evolving cyber risk landscape to help organizations improve security readiness and serving as a guidance in strategic planning.”

In Canada, the highest levels of risk were around the following statements:

- My organization’s IT security function strictly enforces acts of non-compliance to security policies, standard operating procedures, and external requirements
- My organization’s IT security function supports security in the DevOps environment
- My organization makes appropriate investments in leading-edged security technologies such as machine learning, automation, orchestration, analytics and/or artificial intelligence tools.
- My organization’s IT security function complies with data protection and privacy requirements.
- My organization’s IT security leader (CISO) has sufficient authority and resources to achieve a strong security posture.

This clearly indicates that more resources must be diverted to people, processes, and technology to enhance preparedness and reduce overall risk levels.

As organizations and security teams struggle to manage the increasing complexity introduced by digital transformation, data privacy, compliance, and more, the need for a platform-based approach will be critical.

* *An index value is calculated from this information based on a numerical scale of -10 to 10, with -10 representing the highest level of risk. In this report, the Canada CRI stood at 0.16 versus -0.01 for North America and -0.04 for global, indicating a moderate level of risk.*

Read the French version here.

About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fuelled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defence techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

---

https://newsroom.trendmicro.ca/2022-04-14-Nearly-Three-Quarters-of-Canadian-Organizations-Think-Theyll-Be-Breached-in-2022