More C-Suite Engagement Needed in 2022 to Mitigate Cyber Risk

Trend Micro Research reveals widespread concern about threat from ransomware

TORONTO, 2nd February 2022 – Trend Micro Incorporated (TYO: 4704; TSE: 4704), the global leader in cloud security, has published new research* revealing that persistently low IT/C-suite engagement may imperil investments and expose organizations to increased cyber risk. In Canada 93% of the IT and business decision makers surveyed expressed particular concern about ransomware attacks.

To read a full copy of the*global re****port, please visit: https://www.trendmicro.com/explore/en_gb_trendmicro-global-risk-study***

Despite widespread concern over spiralling threats, the study found that only 2-in-5 (42%) of responding IT teams discuss cyber risks with the C-suite at least weekly.

“Businesses of all sizes need to prioritize open, clear, and consistent communication with their IT teams, especially as organizations continue to adapt to a mobile workforce” said **Antoine Saikaley, Technical Director of Trend Micro Canada** “While executives understand the need for transparency and to be informed, they often feel overwhelmed by the rapidly evolving cybersecurity landscape. As a result, it’s more important now than ever for IT teams to communicate effectively, highlighting the organization’s risk and how it can be best managed.”

Fortunately, current investment in cyber initiatives is not critically low. Just under half (46%) of respondents claimed their organization is spending most on “cyber-attacks” to mitigate business risk. This was the most popular answer, above more typical projects like digital transformation (40%) and workforce transformation (32%). In addition, nearly half (44%) said they have recently increased investments to mitigate the risks of ransomware attacks and security breaches.

However, low C-suite engagement combined with increased investment suggests a tendency to ‘throw money’ at the problem rather than develop an understanding of the cybersecurity challenges and invest appropriately. This approach may undermine more effective strategies and risk greater financial loss. 1-out-of-2 respondents (50%) said that cyber threats were an IT problem, while just 34% found it to be an overall business risk. Less than half (40%) of respondents claimed concepts like “cyber risk” and “cyber risk management” were known extensively in their organization. Even more troubling, 8% of respondents said that their company does not assess cyber risk at all.

Three quarters of Canadian respondents (75%) want to hold more people in the organization responsible for managing and mitigating these risks, which would help to drive an enterprise-wide culture of “security by design.” The largest group of respondents (32%) favoured holding CEOs responsible. Other non-IT roles cited by respondents included CFOs (26%) and CMOs (14%).

The study follows previous Trend Micro Research revealing a worrying cybersecurity disconnect between business and IT leaders – perpetuated by self-censorship from cyber experts and disagreements over who is ultimately responsible.

*Trend Micro commissioned Sapio Research to interview 5321 IT and business decision makers from enterprises larger than 250 employees across 26 countries.

French Release Found Here

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled 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 defense 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.