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

Trend Micro Research reveals widespread concern about threat from ransomware

DALLAS, Feb. 2, 2022 /PRNewswire/ -- 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. Over 90% of the IT and business decision makers surveyed expressed particular concern about ransomware attacks.

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

Despite widespread concern over spiralling threats, the study found that only around half (57%) of responding IT teams discuss cyber risks with the C-suite at least weekly.

"Vulnerabilities used to go months or even years before being exploited after their discovery," said Eva Chen, CEO of Trend Micro. "Now it can be hours, or even sooner. More executives than ever understand that they have a responsibility to be informed, but they often feel overwhelmed by how rapidly the cybersecurity landscape evolves. IT leaders need to communicate with their board in such a way that they can understand where the organization's risk is and how they can best manage it."

Fortunately, current investment in cyber initiatives is not critically low. Just under half (42%) 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 (36%) and workforce transformation (27%). Around half (49%) 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. Less than half (46%) of respondents claimed concepts like "cyber risk" and "cyber risk management" were known extensively in their organization.

Most (77%) 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 (38%) favored holding CEOs responsible. Other non-IT roles cited by respondents included CFOs (28%) and CMOs (22%).

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.*

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.

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---