IT Security Leaders Are Failing to Close a Boardroom Credibility Gap

Trend Micro reveals most security bosses are pressured to soften their language

DALLAS, May 21, 2024 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today revealed that four-fifths (79%) of global cybersecurity leaders have felt boardroom pressure to downplay the severity of cyber risks facing their organisation.

To read more on Trend's latest research, please visit:
https://www.trendmicro.com/explore/thecisocredibilitygap/2608-tl-en-rpt

"Over half of security leaders say cyber is their biggest business risk. But they're failing to communicate that risk in a language the board understands. As a result they're ignored, belittled and accused of nagging," said Trend Micro's Technical Director Bharat Mistry. "Unless they can engage better with senior leadership, corporate cyber-resilience will suffer. The first step is to attain a single source of truth across the attack surface."

Siloed products across the attack surface can make it difficult to tell a clear story about cyber risk to the board.

Of those security leaders who came under pressure from their board, 43% say it is because they are seen as being repetitive or nagging and 42% that they are viewed as overly negative. A third (33%) claim they have been dismissed out of hand.

This points to a serious credibility gap, closely linked to their inability to align cyber with business risk. In fact, 46% say that when they have been able to measure the business value of their cybersecurity strategy, they've been viewed with more credibility.

Other benefits of this approach include IT security leaders being:

- Given more responsibility (45%)
- Seen as a more valued function (44%)
- Given more budget (43%)
- Brought into senior decision making (41%)

Yet at present, a persistent communication gap exists between IT and business leadership.

Only half (54%) of respondents are confident their C-suite completely understands the cyber-risks facing the organisation—a figure that has barely moved since 2021 (50%). Over a third (34%) of respondents say cybersecurity is still treated as part of IT rather than business risk.

Additionally, 80% believe that only a serious breach would incentivise the board to act more firmly on cyber risk.

The heterogeneous cybersecurity environment may be compounding these challenges. Siloed point products across the attack surface generate inconsistent data points, which can make it difficult to tell a clear story about cyber risk to the board.

Over half (58%) of respondents believe they'll need an increase in IT comms skills in order to rectify the situation. But a unified Attack Surface Risk Management (ASRM) platform could eliminate the need for such hefty investments, by delivering consistent and compelling risk insight—potentially in the form of an executive dashboard.

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, media_relations@trendmicro.com

https://newsroom.trendmicro.com/2024-05-21-IT-Security-Leaders-Are-Failing-to-Close-a-Boardroom-Credibility-Gap