A global study

Underfunded and unaccountable:

How a lack of corporate leadership is hurting cybersecurity

July 2024

Trend Micro

Introduction

Global regulators are increasingly concerned that cyber risk is spiraling out of control. Trend Micro blocked 161 billion threats in 2023 alone, a 10% annual increase. As organisations continue to invest in digital transformation to enhance back-office efficiencies and the customer experience, the digital attack surface continues to expand. And a determined cohort of agile threat actors can obtain with ease all the tools and know-how they need to take advantage.

2023
161 billion threats blocked

That's why lawmakers and regulators are increasingly looking to hold business leadership more accountable for managing cyber risk. In the US, SEC rules mandate not only disclosure of material cybersecurity incidents, but also that organisations share their processes for assessing and managing such risks, including the role of management and the board of directors. And in the EU, the travel of direction is broadly the same. The new NIS2 directive has specific provisions requiring that management approves cyber risk management measures, oversees their implementation and undergoes specialised security training. They can even be held personally liable for serious infringements.

Are regulators right to be concerned? To find out more, we commissioned Sapio Research to interview 2600 IT leaders with responsibility for cybersecurity in their organisation–across LATAM, APAC, North America, Europe and the Middle East. Respondents hailed from organisations of all sizes and across multiple verticals.

2600 IT Leaders

LATAM, APAC, North America, Europe and the Middle East

We found that, at least on some level, regulators are justified in taking a harder line on boardroom accountability. Many organisations seem to lack the resources or strategic leadership to implement important cybersecurity controls and best practices.

Concerns mount as the attack surface expands

The threat landscape is in constant flux. But the overall picture has remained unchanged over recent years. A highly efficient and expansive cybercrime underground worth trillions of dollars provides everything a budding cybercriminal needs to launch successful attacks – whether they want to defraud consumers or extort multinationals out of millions. And fast-emerging AI tools threaten to give them yet another advantage.

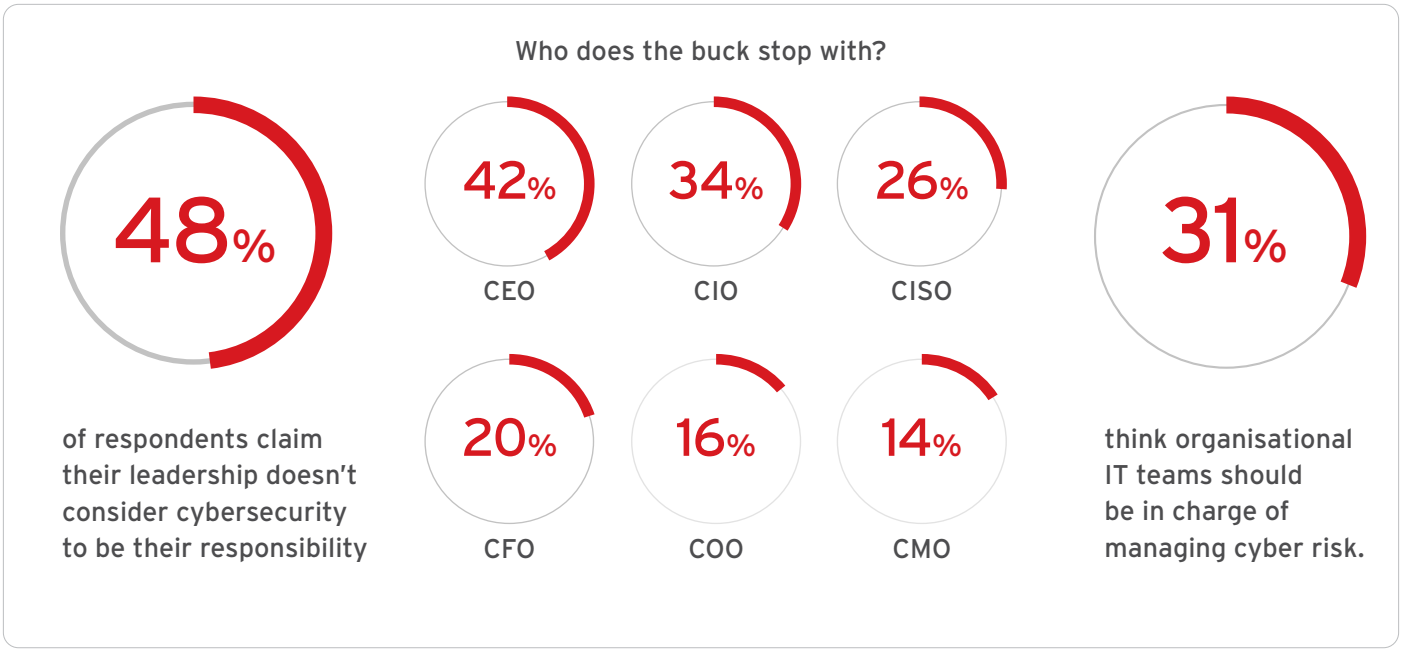
On the other side, security teams are often overstretched and under-staffed. A workforce shortfall of nearly four million globally means competition for talent is fierce. Digital investments not only expand the corporate cyber-attack surface, but also create new skills challenges, as vendor innovation outpaces the ability of IT teams to effectively configure and protect systems.

Our research finds that 96% of IT leaders are concerned about their attack surface. Nearly two-fifths (36%) are worried about not having a way of discovering, assessing and mitigating high-risk areas, and a fifth (19%) aren't able to work from a single source of truth. The latter suggests that many companies are struggling with tool bloat, with siloed point solutions creating coverage and visibility gaps.

Who's in charge?

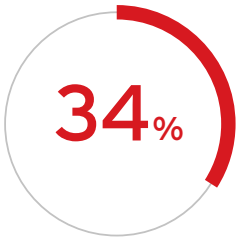
We can hypothesize that many of these problems stem from a lack of clear leadership on cyber. Half (48%) of respondents claim their leadership doesn't consider cybersecurity to be their responsibility. Just 17% disagree strongly with that statement. However, when asked who does or should hold responsibility for mitigating business risk, respondents aren't aligned on their answers. Although the most popular answer is CEO (42%), a large share believe the buck should stop with the CIO (34%), CISO (26%), CFO (20%), COO (16%) and even the CMO (14%). An additional third (31%) think organisational IT teams should be in charge of managing cyber risk.

A lack of clarity in reporting lines and accountability can translate to erratic policymaking and an absence of strategic long-term vision. In fact, over half (54%) of responding IT leaders complain that their organisation's attitude to cyber risk is inconsistent and varies from month to month.

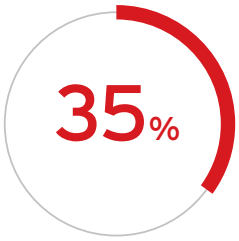


Why accountability matters

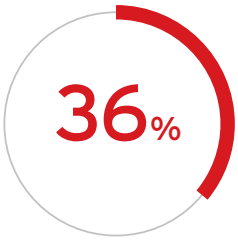
There are potentially much worse outcomes. A sizeable share of respondents also identify major gaps in cyber-resilience, including not having:



A plan to follow regulatory and other frameworks like the NIST Cybersecurity Framework



Attack surface management techniques to measure the risk of the attack surface



Sufficient staffing for 24x7x365 cybersecurity coverage – which just 36% have

It goes without saying that gaps of this sort can have a serious and negative impact on organisations' risk scores – increasing the chances of a financially and reputationally damaging breach. Publicly reported data compromises in the US hit an all-time high last year, impacting over 353 million victims. The most important thing organisations do is to fix these problems now, rather than wait until a serious security breach. The latter tends to end in reactive security spending, which may increase the number of half-used point solutions and not actually fix the root cause of an issue.

Yet unfortunately, too often boards are prepared to let cybersecurity be someone else's business. Respondents tell us that only a mean loss of £133,500 or more would incentivise the C-suite to act more decisively to manage risk. With more regulations on the way and potential criminal liability at stake, it's time to act now.