A global study

The CISO Credibility Gap:

How a Communication Breakdown in the Boardroom is Hurting Cyber-Resilience

April 2024
Trend Micro

Introduction

In business, as in personal relationships, trust is the key to long-lasting success. And any guide to building that trust will put effective communication right at the top of the list. That's because when done correctly, it fosters a spirit of transparency, clarity, consistency and reliability. Communication is the bridge we build to create mutual understanding, nurture positive relationships, and ultimately build our credibility with colleagues. This is as true of communications with external customers as it is of engagement with different internal stakeholders.

But this is where it becomes challenging for CISOs and their peers, because many struggle to be heard by their boards. That creates a fundamental credibility gap which many are finding difficult to close.

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

While respondents certainly demonstrated awareness of the close link between cyber and business risk, it also appears that they're failing to land their message in the boardroom. That has serious implications for achieving their long-term strategic goals, and ultimately for the cyber-resilience of the organisation.

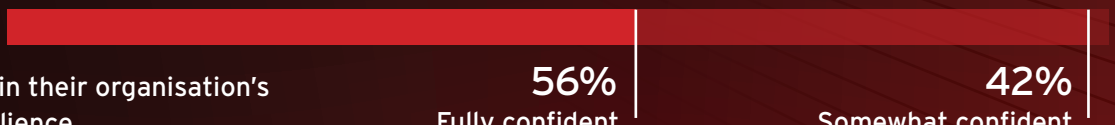
Perception and reality

Although the vast majority (98%) of respondents claim to feel fully (56%) or somewhat (42%) confident in their organisation's cyber-resilience, this perception may be misleading. True resilience means having cybersecurity embedded deep into business continuity—so that services can continue even when the organisation is under sustained attack. That in turn requires close alignment between cyber and business strategy, which is not happening in many responding organisations.

Cyber-Resilience

98%

confident in their organisation's cyber-resilience



56%
Fully confident

42%
Somewhat confident

While 59% of respondents recognise that cyber is their biggest business risk, rising to 68% in North America, over a third (34%) admit that cybersecurity is still treated as part of IT rather than business risk.

59%

of respondents recognise that cyber is their biggest business risk

34%

over a third admit that cybersecurity is still treated as part of IT rather than business risk

This is echoed by the view of most (80%) respondents that the board would only be incentivised to act decisively on business risk if a breach occurred. On average, a financial loss of £150,000 would be enough, they claim. This points to a disinterested and unengaged board.

£150k loss

enough to incentivise the C-suite to get into action

Unfortunately, C-suite action and investment that is driven by one-off events like this ends up being disjointed and lacking strategic cohesion. It can lead to the purchasing of point products which rarely fix the underlying cause of a breach/incident—and often cause additional cost and complexity headaches down the line.

The credibility gap

This disconnect between IT/cyber and business leadership is manifested in one other very obvious and damaging way. Some 79% of global cybersecurity leaders have felt boardroom pressure to downplay the severity of cyber risks facing their organisation. Of these, 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.

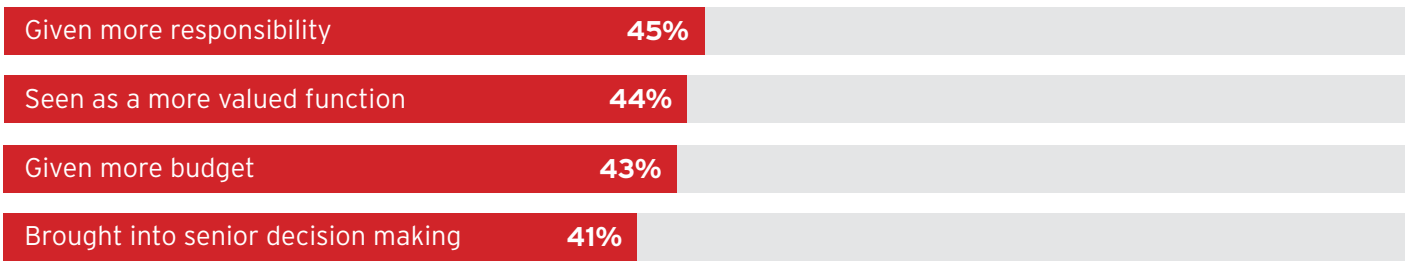
The truth is that boards have little time for death-by-PowerPoint presentations from the CISO, crammed with industry jargon and irrelevant metrics. The C-suite wants to know things like:

- **How is cyber supporting our business objectives?**
- **What is the ROI of our investments in cyber?**
- **What are the cyber-risk implications of our latest digital transformation initiative?**

These may not be easy questions to answer. But they get to the heart of the matter for boards. They aren't interested in the minutiae of managing a cybersecurity programme. They want to know answers to big-picture strategic questions like "how secure are we?" and "how does our security programme compare with our peers?"

CISOs unable to answer these questions suffer a major credibility gap, which is why boards are belittling and shutting them down. On the other hand, when they are able to align cyber with business strategy, the benefits are clear.

Half (46%) of respondents say that when they have been able to measure the business value of their cybersecurity strategy, they've been viewed with more credibility. Cyber as business value and associated benefits include that they have been:



A single source of truth

So how can IT security leaders respond? Over half (58%) believe that they'll need an increase in IT comms skills in order to rectify the situation. But this risks being another expensive sticking plaster solution that fails to address the underlying problem.

First, CISOs need to ensure that the information generated by their security tools is consistent and easily digestible. That is a challenge when many organisations are labouring with dozens of point solutions installed across the distributed IT environment—each of which may have a different way of processing and presenting data.

believe they'll need an increase in IT comms skills to rectify the situation

This is where an Attack Surface Risk Management (ASRM) platform can add real value—providing a single source of truth for security teams to unite around, across protection, detection and response capabilities. When displayed through an executive dashboard, this information can empower the CISO to elevate their narrative to board level.

Of course, this is only half the battle. CISOs must also adapt their language and improve their communication skills to help close that credibility gap with the board. That means:

- **Using plain language, free from acronyms and jargon**
- **Alignment of cybersecurity programme to business objectives**
- **Focusing on clear risks**
- **Using relevant data/metrics**
- **Reporting little and often to the board – as the risk landscape changes**
- **Putting time in to build personal relationships with board members**

Respondents to our survey are unequivocal about the potential "cyber dividends" that could result. Everything from greater business efficiency and happier partners to innovation and profitability, better data insight and enhanced talent/client acquisition. The rewards are too big to ignore. It's time to close the CISO credibility gap.