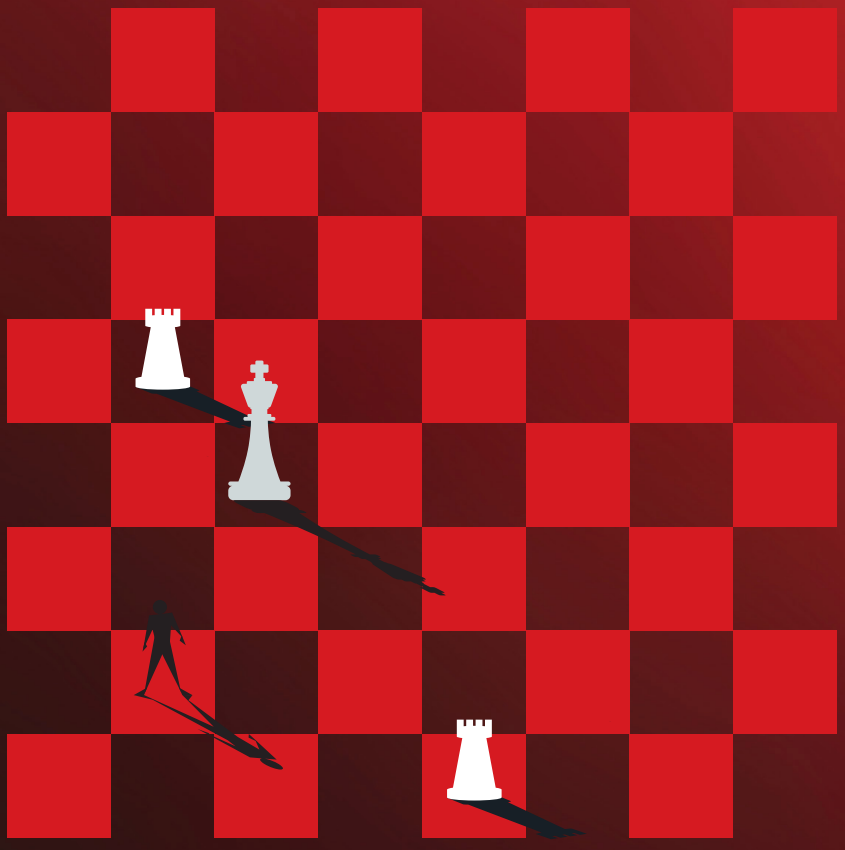
A global study

The CISO Credibility Gap:

How a Communication Breakdown is Hurting Government Cyber-Resilience

Harder for Hackers.
Simpler for you.



September 2024
Trend Micro

Introduction

In early 2024, it emerged that state-sponsored adversaries had compromised **270,000** Ministry of Defence (MoD) payroll records, belonging to nearly all members of Britain's armed forces. It's the latest in a string of embarrassing security incidents at the heart of government. In fact, by its own admission, central government is "routinely and relentlessly targeted".

An extensive attack surface that grows with each new cloud investment only increases the chance of compromise. With limited budgets, government bosses must manage these risks in line with the many regulations, standards and codes that govern how they operate. That means security which enables rather than slows digital transformation. But their ability to do so effectively is being hampered by limited respect for and collaboration with their CISOs. Many security leaders are finding this "credibility gap" increasingly difficult to close.

To find out more, we commissioned Sapio Research to interview government IT leaders with responsibility for cybersecurity in their organisation–across 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 government cyber-resilience.

270k

data breach incidents

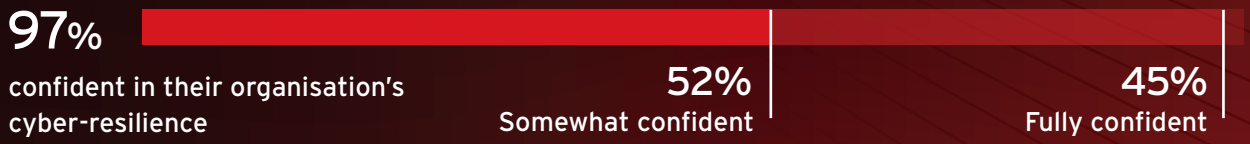
LATAM, APAC, North America, Europe and the Middle East

Perception and reality

Central government has some aggressive targets for migrating legacy systems to the cloud. However, the challenge is ensuring cyber risk is effectively managed equally across both cloud and on-premises environments, without adding cost or creating security gaps. Against this backdrop, it's surprising that the vast majority (**97%**) of government respondents to our study claim to feel fully (**45%**) or somewhat (**52%**) confident in their organisation's cyber-resilience.

True resilience means having cybersecurity embedded deep into business continuity—so that services can continue even when the organisation is under sustained attack. This in turn requires close alignment between cyber and business strategy, which is not happening in many responding organisations.

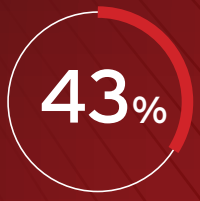
Cyber-Resilience



While **63%** of respondents recognise that cyber is their biggest business risk, two-fifths (**43%**) admit that cybersecurity is still treated as part of IT rather than business risk. This is echoed by the view of most (**88%**) respondents that the board would only be incentivised to act decisively on business risk if a breach occurred. On average, a financial loss of **£111,153** would be enough, they claim. This points to a disinterested and unengaged board.

£111,153k loss
enough to incentivise the C-suite to get into action

of respondents recognise that cyber is their biggest business risk



two-fifths admit that cybersecurity is still treated as part of IT rather than business risk

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 causes of a breach/incident—and often cause additional cost and complexity headaches down the line.

The credibility gap

Official figures from the Information Commissioner's Office (ICO) reveal that there was an **8000%** increase in the number of people affected by financial data breaches in central government between 2019 and 2023. It's further evidence of a failure of cybersecurity strategy, which must enhance cyber resilience even as budgets decline and skills shortages grow. In 2023, the MoD was called out for accruing a **£17bn** budget blackhole, while the UK as a whole is estimated to have a **73,000-person** shortfall in IT security skills.

In this context, it's vital for government CISOs to demonstrate the value of investments in cyber resilience. But their credibility gap continues to get in the way. Some **67%** of government cybersecurity leaders have felt boardroom pressure to downplay the severity of cyber risks facing their organisation. Of these, **36%** say it is because they are seen as being "repetitive" or "nagging", and 34% that they are viewed as overly negative. Over a quarter (**29%**) claim they have been dismissed out of hand.

8000%
increase in data breaches

£17bn
budget blackhole

67%
of global cybersecurity leaders have felt boardroom pressure to downplay the severity of cyber risks facing their organisation

36%
say it is because they are seen as being "repetitive" or "nagging"

34%
that they are viewed as overly negative

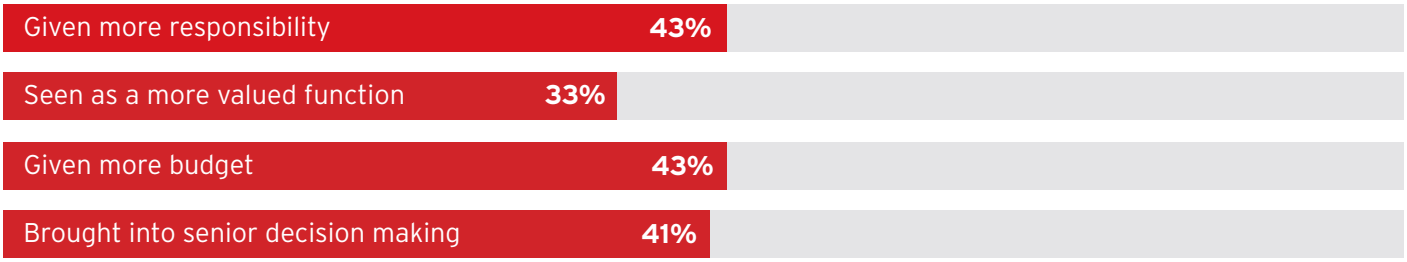
The truth is that boards have little time for death-by-PowerPoint presentations from the CISO, crammed with industry jargon and irrelevant metrics. The C-suite wants to know things like:

- **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.

Two-fifths (**41%**) 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. Other benefits include that they have been:



A single source of truth

So how can central government 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.

This is where a combined Attack Surface Risk Management (ASRM) and XDR platform can add real value—providing a single source of truth for security teams to unite around, for protection, detection and response. This is the kind of centralised visibility and control across disparate systems that can help reduce operational complexity, support regulatory audits, and prevent costly breaches. When displayed through an executive dashboard, critical information can also 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**
- **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.

To find out how Trend Micro can help your Central Government organisation improve cyber-resilience, book a 15-minute consultation here.