A global study

The CISO Credibility Gap:

How Local Government IT Leaders Can Build Trust and Cyber-Resilience

Harder for Hackers.
Simpler for you.

September 2024
Trend Micro

Introduction

Local government plays a critical role in the lives of virtually everyone in the UK. From roads and rubbish collection to schools and care for the elderly – the services it provides have an outsized impact on the economic, social and environmental wellbeing of local areas. But as guardians of large volumes of citizen data, these same local authorities are also an attractive target for threat actors

A Freedom of Information (FoI) request in July 2024 found that just **17** councils had suffered as many as **5,000** data breach incidents over the previous year. Given their low tolerance for service outages, those same local authorities are also in the crosshairs of ransomware attackers.

17
councils

5,000
data breach incidents

In this context, it's vital that CISOs are trusted and listened to by their boards and local council leadership. Yet unfortunately, in many cases the opposite appears to be true. That will make it harder for them to comply with a new Cybersecurity Assessment Framework (CAF) initiative introduced by Whitehall in 2024.

To find out more, we commissioned Sapio Research to interview **86** government 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.

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 local government.

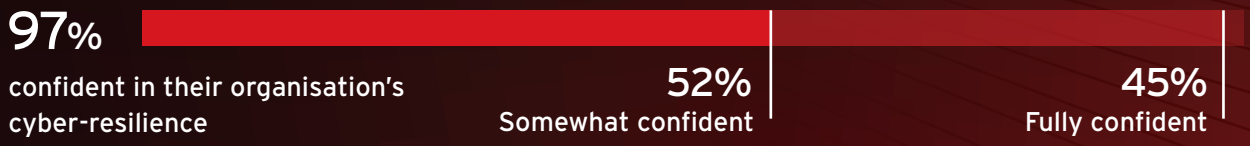
86 Government Leaders interviewed

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

Perception and reality

Although the vast majority (**97%**) of respondents claim to feel fully (**45%**) or somewhat (**52%**) confident in their organisation's cyber-resilience, this perception may be misleading. A 2022 report reveals that around a third (**37%**) of UK councils reported **2.3 million** cyber-attacks in the first eight months of that year. Incidents in 2024 impacting several Greater Manchester councils, and a serious ransomware attack on Leicester City Council show the threat is still elevated.

Cyber-Resilience



True resilience to such threats 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 government organisations.

While **63%** of respondents recognise that cyber is their biggest business risk, over a third (**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 just £111,153 would be enough, they claim. This points to a disinterested and unengaged board that may not even be aware of the CAF and how it could boost their organisation by helping it to better assess and improve cyber-resilience.

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

of respondents recognise that cyber is their biggest business risk

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

Unfortunately, C-suite action and investment that is driven by reactive one-off events like breaches 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 frustration is that the message local government CISOs are trying to get across to their boards should have a receptive audience. Cyber-attacks such as ransomware can hit local services and budgets hard at a time when councils are already struggling to deliver for their citizens. They could even undermine the public's trust in local democracy, which could have a corrosive effect on society.

The credibility gap

Local government bodies aren't just facing budgetary pressures. Many also lack enough cybersecurity professionals. A UK workforce gap of over **73,000** is much harder to fill when councils can't match private sector salaries for in-demand talent. That leaves more work for already over-stretched IT teams, who also have to manage a patchwork of overlapping regulations, standards and codes of practice.

Against this backdrop, there needs to be clear leadership on cybersecurity. But local government CISOs are not being heard by their boards. 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.

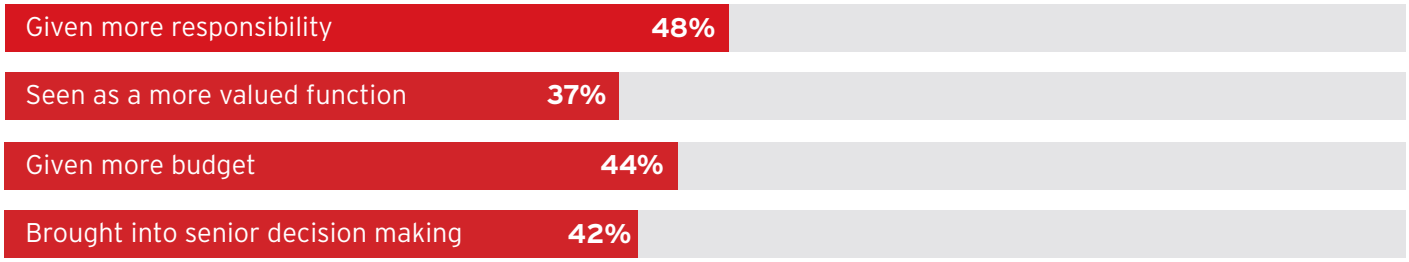
The truth is that boards have little time for death-by-PowerPoint presentations from the CISO, crammed with industry jargon and irrelevant metrics. The C-suite wants to know things like:

- **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.

Over 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 local government IT security leaders respond? Over half (52%) 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 unified cybersecurity 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. Such a platform could also help by:

- **Reducing the license costs and management overheads associated with point solutions**
- **Minimising costly breaches through better detection, response and resilience**
- **Offering GenAI tools and automated workflows to close skills gaps and increase IT staff productivity**

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 for local government to close the CISO credibility gap.

To find out how Trend could help your local government organisation build cyber-resilience, book a 15-minute consultation today.