Article

Closing the CISO Credibility Gap:

Why It's Time for local government to Embrace Cyber-Resilience

Harder for Hackers.
Simpler for you.

September 2024
Trend Micro

Local government plays a vastly under-appreciated role in the economic and social wellbeing of the nation. And similarly, cybersecurity is often marginalised within local authorities. At first glance, this seems nonsensical, given the various cyber-frameworks, regulations, standards, codes of practice and other initiatives which many councils are signed up to. But too often they do the bare minimum to comply, and sometimes less than that.

Why is the message on cyber-resilience not getting through? After all, local authorities regularly suffer crippling data and security breaches—providing an ample number of cautionary tales for CISOs to dangle in front of their boards. The sheer volume of citizen data they hold and number of critical public services they run should be enough to focus minds on the job. It's certainly attracting the attention of the cybercrime underground.

New research reveals that part of the problem may be that the messengers themselves are not trusted, as local authority leaders turn a blind eye to their CISOs. With a new Cyber Assessment Framework (CAF) initiative incoming, it's time local government got the memo about cyber-resilience.

Risk is surging

Cyber-criminals are laser-focused on doing one thing: making money. To do so, they look for the easiest bang for buck: organisations that are poorly defended, but which store or process monetisable data and/or are likely to pay if hit with a serious operational outage. Unfortunately, local authorities tick many of the right boxes for such threat actors.

According to one report, cyber-attacks on local government organisations surged **24%** between 2022 and 2023, with personal data breaches reported to the Information Commissioner's Office (ICO) growing **58%** over the period. They include major breaches over recent years, such as a ransomware attack on the London Borough of Hackney which cost it at least £12m. The breach led to a reprimand from the ICO, which revealed that hackers managed to access **440,000** files affecting **280,000** residents and staff. At least **9,600** of the records posed "a meaningful risk of harm" to hundreds of residents.

Local government efforts to digitalise also present threat actors with an open goal when security is not built into projects by design and default. An expansive attack surface—from the endpoint to the cloud—offers more opportunity to send email-borne malware, trick users into divulging credentials through phishing pages, exploit bugs in web-based apps, and much more.

The efforts of local government CISOs and their teams are made that much harder by the limited budget and in-house skills they have at their disposal. And the risk of third-party compromise from insecure suppliers. In May 2024, several UK councils warned that citizens' personal data may have been breached following a ransomware attack on a medical equipment supplier.

58%
personal data breaches

440,000
files affecting

280,000
residents and staff affected

A pathway to resilience

Without sufficient funding or internal talent, IT teams struggle to manage a hotchpotch of legacy and cloud-based technologies. Morale may suffer as existing staff are stretched to breaking point. Outdated equipment requires extra time and effort to manage, especially if it is no longer receiving vendor updates and security patches. Trying to meet compliance requirements against this backdrop was already challenging. With CAF incoming, the workload may get even heavier.

In this context, true cyber-resilience can only be achieved with the board and IT security function working hand-in-hand and systematically over the long term, to identify and plug key areas of risk. Yet in many local government organisations, CISOs simply aren't credible in the eyes of senior leadership.

Some **67%** of those we spoke to claim to have felt boardroom pressure to downplay the severity of cyber risks facing their organisation. Of these, over a third say it's because they are seen as being "repetitive" or "nagging", or viewed as overly negative. Over a quarter (**29%**) claim they have been dismissed out of hand. This is not the way to build a cyber-resilient organisation.

This credibility gap is also manifest in other ways. Over two-fifths (**43%**) of CISOs note that cybersecurity is still treated as part of IT rather than business risk – an admission that their message is not getting through. Some 88% claim that the board would only be incentivised to act decisively on business risk if the organisation suffered a major breach and/or financial loss.

When board members are engaged by their CISOs, they ask tougher questions, dig deeper into issues, and join the dots more readily between cyber and business risk. This, in turn, is likely to spur greater long-term investment in strategic cybersecurity projects. Unfortunately, what we're currently seeing is disinterested and unengaged boards ignoring their CISOs and only putting their hands in their pockets when there's a serious incident.

Reactive spend like this is erratic – it means piecemeal investment in point solutions that add cost and complexity for the IT team. In a worst-case scenario, this spend actually perpetuates security coverage gaps whilst singularly failing to address the underlying cause of a breach.

67%

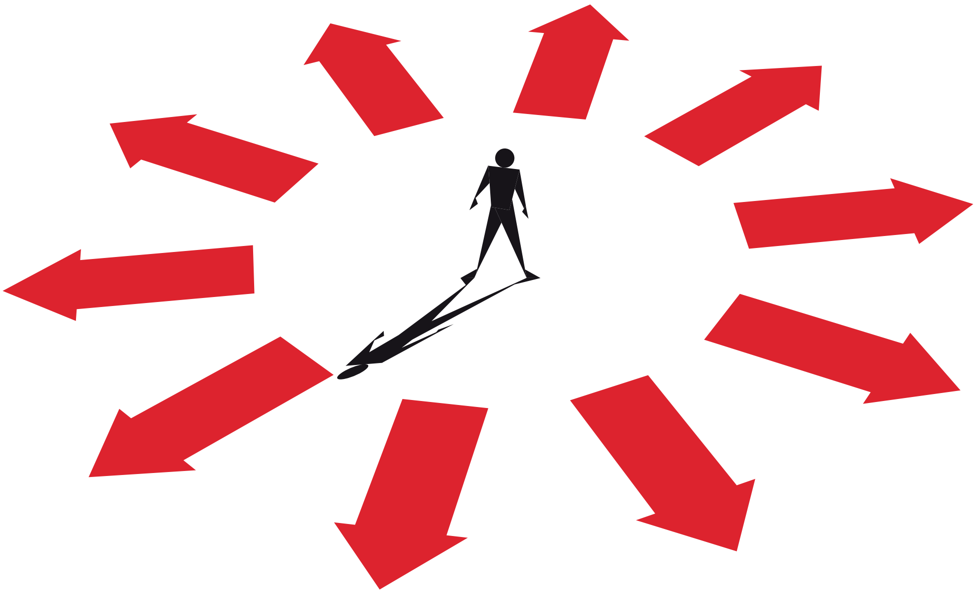
of global cybersecurity leaders have felt boardroom pressure to downplay the severity of cyber risks facing their organisation

29%

claim they have been dismissed out of hand

43%

of CISOs note that cybersecurity is still treated as part of IT rather than a business risk



Speaking their language

So why aren't CISOs more credible in the eyes of the board? A great deal comes down to language. Too often, CISO presentations are packed with jargon and obscure metrics. They don't answer the simple, high-level questions the board typically poses, like "how secure are we?" or "how can cyber support our business objectives?"

CISOs must try harder to make themselves understood. That means jargon-free language, focused on business risk. It means going that extra mile to build personal relationships with board members. And it means keeping briefings short, relevant and frequent. Business and cyber risk evolve at breakneck speed. Regular updates are essential to keep the board engaged and aware.

To truly make an impact, CISOs also need the right data. That means consistency of reporting, whether it's from protective, preventative tooling or reactive detection and response systems. The best way to achieve this is via a single platform designed to manage risk across the entire attack surface. So much the better if it offers up this information via easy-to-consume executive dashboards. A single platform like this would be far more effective than the kind of pre-bundled cybersecurity solutions that local councils often purchase due to cost pressures.

Closing the credibility gap won't be easy for IT security leaders. But the benefits speak for themselves. Around half of those able to measure the business value of their cyber strategy claim that not only are they seen as more trustworthy, but they've also been given more responsibility and budget. The journey to boardroom credibility starts here.

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