A global study

The CISO Credibility Gap:

How Boardroom Comms Challenges Are Hurting NHS Cyber-Resilience

Harder for Hackers.
Simpler for you.

September 2024
Trend Micro

Introduction

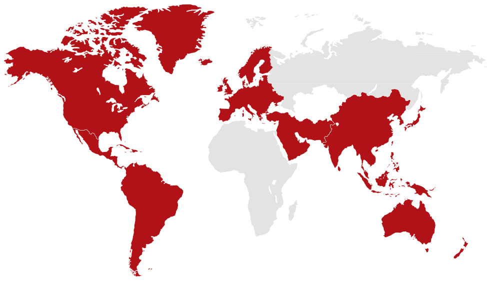
For most organisations, the biggest business impact of cyber risk tends to be financial and reputational damage. But NHS IT security leaders know that a worst-case scenario breach could have a far more deleterious effect - impacting patient health. The challenge is understanding how best to deploy finite resources amid severe cost pressures and limited IT budgets, in order to manage escalating cyber risk across an expanding attack surface. Threat actors have the advantage of surprise and, increasingly, are ably funded and resourced.

The challenge for CISOs and their peers is that many are struggling to be heard by their boards, and therefore to get the backing for the projects they know are vital to enhance cyber-resilience. This creates a fundamental credibility gap which many are finding difficult to close.

As a long-time partner of the NHS, Trend Micro wanted to find out more. We commissioned Sapio Research to interview **133 IT leaders** with responsibility for cybersecurity in their healthcare organisation—across LATAM, APAC, North America, Europe and the Middle East.

We found that, while healthcare respondents understand the intrinsic link between cyber and business risk, they're failing to land their message in the boardroom. This has serious implications for achieving their long-term strategic goals, and ultimately for the cyber-resilience of the NHS.

133 IT Leaders interviewed



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

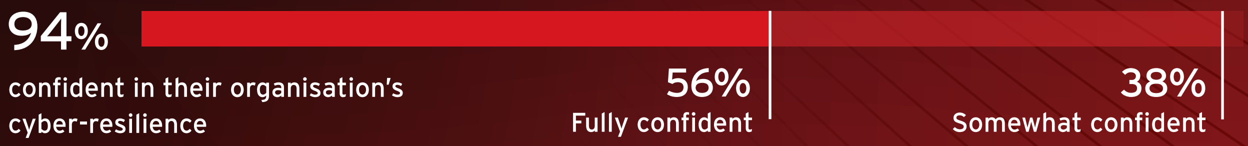
Perception and reality

NHS CISO, Phil Huggins, has warned in the past that the state of cybersecurity in the NHS supply chain is **15 to 20 years** behind other sectors. Unfortunately, the challenges facing the health service aren't just confined to suppliers. Despite technological advancements, healthcare cybersecurity often lags behind other sectors, exposing providers to the risk of data loss and operational disruption.

Legacy IT and OT exposes organisations to the risk of unpatched vulnerabilities, while large, distributed IT environments provide threat actors with plenty of security blind spots and coverage gaps to aim at. They understand only too well the low tolerance the NHS has for outages and the large volumes of sensitive data up for grabs. Compounding these challenges is the difficulty of integrating cybersecurity across diverse and interconnected healthcare systems. Providers need unified security solutions that streamline operations and effectively mitigate risks across their IT infrastructure.

Although the vast majority (**94%**) of healthcare respondents to our study claim to feel fully (**56%**) or somewhat (**38%**) 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



While **60%** of respondents recognise that cyber is their biggest business risk, a third (**32%**) admit that cybersecurity is still treated as part of IT rather than business risk. This is echoed by the view of most (**81%**) respondents that the board would only be incentivised to act decisively on business risk if a breach occurred and is reported. On average, a financial loss of **£133,000** would be enough, they claim. This points to a disinterested and unengaged board.

£133,000k 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

NHS organisations interact with a large and complex ecosystem of software, hardware, and non-digital providers, making it challenging to implement consistent security policies and manage the heightened risk of cyber-attacks. This complexity makes it easier for threat actors to expose weaknesses in the supply chain and is leading to an increase in the volume of attacks. The impact on patient outcomes and clinicians could be significant.

The credibility gap

That the NHS is under tremendous operational pressure is in no doubt. Alongside its just-in-time approach to inventory management, this means any downtime due to cybersecurity incidents could have a catastrophic impact on patient care. It is claimed that every day of downtime following a breach takes around four days to recover from. This reinforces the need for proactive cybersecurity designed to contain incidents before they cause significant disruption. It also emphasises the fact that, in healthcare, the business case for cybersecurity is closely linked to patient wellbeing.

At the same time, those financial pressures mean that any investment in IT security must be supported by an outstanding business case. That's why CISOs need to better articulate the value of platform-based solutions over existing pre-packaged, bundled solutions– in delivering stellar ROI, supporting rigorous compliance requirements, protecting patient wellbeing and managing cyber risk

Yet they are struggling to make their voice heard at a board level. Some **74%** of global cybersecurity leaders say they've 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 **43%** that they are viewed as overly negative. A quarter (**24%**) claim they have been dismissed out of hand.

74% of government cybersecurity leaders have felt boardroom pressure to downplay the severity of cyber risks facing their organisation

43% of these, 43% say it is because they are seen as being "repetitive" or "nagging"

24% and 39% that they are viewed as overly negative

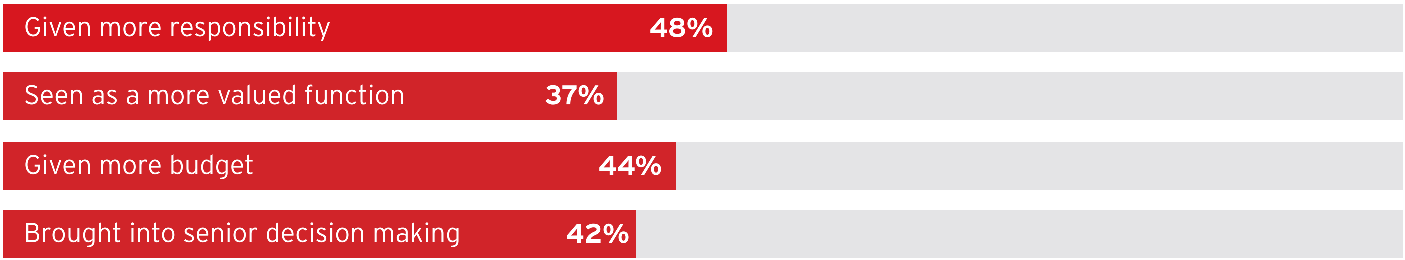
The truth is that boards have little time for death-by-PowerPoint presentations from the CISO, crammed with industry jargon and irrelevant metrics. The C-suite wants to know things like:

- **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.

Half (**42%**) of healthcare 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 NHS CISOs respond?

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 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.

Trend Micro's ASRM is part of an integrated Trend Vision One platform that offers cost-effective but comprehensive cyber risk management capabilities for diverse IT environments. Its XDR capability in particular provides deep visibility and control, for rapid threat detection and response and centralised monitoring across the attack surface, including suppliers. By minimising damaging breaches and alert overload, improving operational efficiency, and reducing spend on point products, it can deliver cost efficiency without compromising on security or patient wellbeing.

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**

Healthcare CISOs 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. For an NHS under pressure, 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 NHS organisation improve cyber-resilience, book a 15-minute consultation here.