Article

Boardroom breakdown:

How NHS CISOs can leap the credibility gap

Harder for Hackers.
Simpler for you.

September 2024
Trend Micro

In December 2023, a parliamentary committee warned that the UK is at high risk of suffering a potentially "catastrophic" ransomware attack. Unfortunately, several months later these worst fears were realised, after a breach at an NHS supplier led to thousands of postponed operations and urgent referral appointments. The long-term impact on patient outcomes is still unclear. But it lays bare what many NHS CISOs have known for a long time. For the NHS, the stakes for getting cybersecurity right are as high as they get.

At a time when the new Labour government has pledged to digitally transform the NHS to drive efficiency, the challenge for IT security leaders in the sector is prioritising where to deploy limited resources across an expansive attack surface. After all, more digital means a greater need for security-by-design.

It's a challenge compounded by a communication breakdown in the boardroom. Both sides could improve. And as threat actors continue to target the health service and its suppliers, they need to. Our research shows that healthcare recorded the second highest number of malware campaigns and risk events of any vertical last year.

Risk is surging

The NHS faces a perfect storm of budget and skills shortages, complex, porous supply chains and legacy IT. Protecting a large, distributed attack surface across a decentralised health service is extremely challenging. It's a challenge acknowledged in a strategy document for cyber-resilience published in March 2023. NHS England provides national services. Then there are local NHS Trusts, GP surgeries and integrated care systems/ boards (ICBs) – of which there are 42, split into seven regions. Friction between these providers can be a roadblock on progress. The cyber-strategy document acknowledges the difficulty of setting universal standards given the size and diversity of the sector – even though patient data is shared across organisations.

Yet even if the centralised NHS England Cyber Security Operations Centre (CSOC) notifies an individual organisation about a serious threat or breach, responsibility for containing it is borne by that organisation. This should focus CISOs' minds on cyber-resilience and rapid incident response and containment.

That's easier said than done when critical IT services need to be online 24/7/365. Outdated IT may be a clear and present cyber risk. But finding the right moment to take MRI scanners and other operational technology (OT) offline for testing and patching can be difficult. Given long OT product lifespans and compatibility issues, many NHS organisations have no choice but to run legacy software. The same operational pressures might make clinicians and administrators more likely to accidentally click on phishing links or transfer funds to criminals masquerading as suppliers.

Unfortunately, threat actors need no second invitation. In the healthcare sector, official data breach reports to the regulator rose by **21%** between 2022 and 2023, with trusts paying an estimated **£1.5m** in breach claims since 2021. As the Synnovis breach highlighted, the supply chain is particularly exposed. NHS organisations interact with a large and complex ecosystem of software, hardware and non-digital providers. This complexity makes it easier for threat actors to expose weaknesses in the supply chain.

According to NHS CISO, Phil Huggins, cyber-resilience here is **15-20 years** behind other sectors. One breached supplier, Advanced, is facing a **£6m** fine from the data protection regulator for serious failings leading to a major 2022 ransomware incident. And Synnovis was responsible for perhaps the most serious disruption to NHS services since WannaCry, when ransomware struck in June 2024.

21%
rise in data breach reports in healthcare sector

£1.5m
paid in breach claims by trusts

15-20 years
behind other sectors

A pathway to resilience

This makes a mockery of healthcare CISOs' claims that they feel fully (**56%**) or somewhat (**38%**) confident in their organisation's cyber-resilience. Given continued cost pressures, IT security leaders in the NHS must make an outstanding business case for new investments – articulating the value of platform-based solutions over pre-packaged tools. That requires the trust and confidence of the board. Unfortunately, in many cases this is lacking.

Some **74%** of healthcare CISOs we spoke to claim to have felt boardroom pressure to downplay the severity of cyber risks facing their organisation. Of these, over two-fifths say it's because they are seen as being "repetitive" or "nagging", or viewed as overly negative. A quarter 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. A third (**32%**) of healthcare 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 **81%** 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 unengaged boards ignoring their CISOs and only spending after a serious incident. Reactive approaches like this are erratic – they lead to 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 failing to address the underlying cause of breaches.

74%

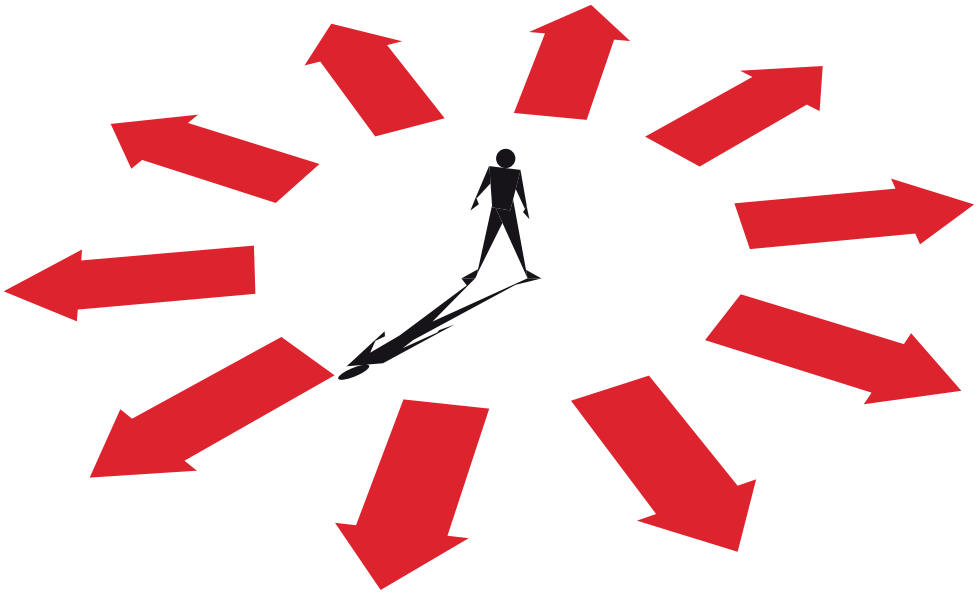
of global cybersecurity leaders have felt boardroom pressure to downplay the severity of cyber risks facing their organisation

32%

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

81%

claim that the board would only act decisively on business risk if the organisation suffered a major breach and/or financial loss



Speaking their language

Yet when presented with the facts about a potentially catastrophic ransomware attack, the government at the time stuck its head in the sand. The Joint Committee on the National Security Strategy (JCNSS) subsequently decried its "ostrich strategy" on cyber. Boards tend to do the same, as evidenced above, unless they trust their CISOs.

NHS IT security leaders 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.

There's no time to waste. A single day of downtime due to a cyber breach could take four days of recovery. Given current patient backlogs, that's not an option. So how can CISOs make the right impact on their boards? It starts with the right data. That means consistency of reporting – and 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.

Closing the credibility gap won't be easy for NHS CISOs. But the benefits speak for themselves. Over two-fifths of those able to measure the business value of their cyber strategy claim that not only are they seen as more credible and valued, but they've also been given more responsibility and budget. The journey to boardroom credibility starts here.

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