Article

Communication breakdown:

How higher education CISOs can close the credibility gap with their boards

Harder for Hackers.
Simpler for you.

September 2024
Trend Micro

Successive governments have been accused of ignoring the rising challenge posed by cyber threats. In March 2024, the Joint Committee on the National Security Strategy (JCNSS) penned a robust commentary decrying what it described as the previous administration's "ostrich strategy" on cyber. Unfortunately, many boards tend to do the same – dodging difficult decisions and doing the bare minimum to get by. The higher education sector (HE) is no different.

Yet such a strategy is fraught with risk. The sector is an increasingly popular target for both nation state and cybercrime actors – given that it contributes **£130bn** annually to the UK in general economic output. By the government's own reckoning, **97%** of HE institutions experienced a breach in the past year. Building cyber-resilience should therefore be a priority. But as research reveals, too often these efforts are undermined at a board level, by a lack of trust in the CISO.

An estimated **97%** of HE providers include cyber on their risk register. But that's just the first step. Much more is needed – and it must start by closing the CISO credibility gap.

£130bn
contribution to UK economy

97%
of HE institutions experienced a breach

97%
of HE providers include cyber on their risk register

Risk is surging

According to Jisc, the most "acute and pervasive threat" facing the UK's HE institutions is ransomware. It cites National Cyber Security Centre (NCSC) figures claiming the agency received 297 reports of ransomware activity between September 2022 and August 2023 alone. Of these, **50** came from academia, more than the manufacturing sector (28) and IT (22). HE institutions have both a low tolerance for outages and store large volumes of personally identifiable information (PII) on staff and students, making them particularly attractive targets, as per the catastrophic ransomware attack on the University of Manchester which impacted over one million NHS patients.

Yet there are also troves of world-leading research which attract more sophisticated state-sponsored actors. Irrespective of the aggressor, their job is made easier by the sheer size of the typical HE attack surface. According to the NCSC, many university networks contain "a collection of smaller, private networks, providing close-knit services for faculties, laboratories and other functions". Then there are the remote students and workers who may log-on to access HE resources via insecure personal devices and home networks. Social engineering via phishing remains a top threat vector, highlighting the persistent challenge of human error.

While threat actors have the advantage of agility and a thriving cybercrime economy at their disposal, HE CISOs are often battling budget constraints. A recent analysis claims **40%** of universities expect to run budget deficits in 2024, with an increasing number facing "a material risk of closure" if they don't drastically cut costs. This is where proactive cybersecurity platforms offer significant financial savings over reactive point solutions.

A pathway to resilience

Yet most education CISOs we spoke to still claim that they feel fully (**56%**) or somewhat (**42%**) confident in their organisation's cyber-resilience. This is likely to be wishful thinking. 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 organisations, CISOs simply aren't credible in the eyes of the board.

Some **72%** of those we spoke to claim to have felt pressure from their board or advisory committee to downplay the severity of cyber risks facing the organisation. Of these, over two-fifths say it's because they are seen as being "repetitive" (**43%**) or "nagging", or viewed as overly negative (**39%**). Two fifths (**41%**) claim they have been dismissed out of hand. This is not the way to build a cyber-resilient organisation.

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 allocating funds 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 funding actually perpetuates security coverage gaps, whilst failing to address the underlying cause of a breach.

72%

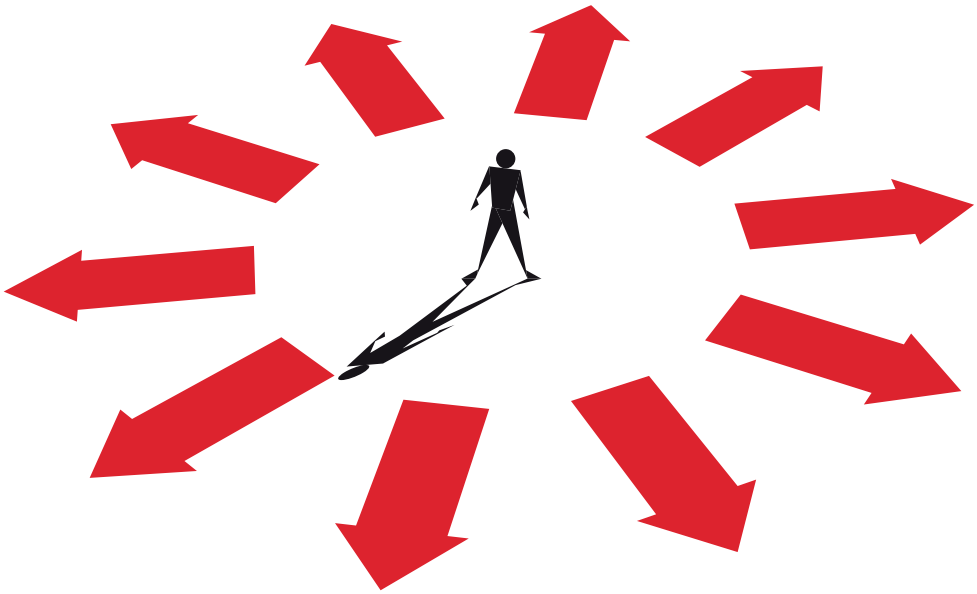
of global cybersecurity leaders have felt boardroom pressure to downplay the severity of cyber risks facing their organisation

43%

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

39%

that they are viewed as overly negative



Speaking their language

Given the importance of student fees to the bottom line, and especially those of international students, a serious breach or outage could have a significant reputational and therefore financial impact on a HE institution. That in itself should focus the minds of HE leadership on building cyber-resilience, in the form of attack surface risk management (ASRM) and rapid threat detection and response. That's the line CISOs could be taking.

So why aren't they 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.

But to truly make an impact, HE CISOs 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.

Closing the credibility gap won't be easy for HE CISOs. But the benefits are too great to ignore. They can be seen at institutions like University College Cork, which has been able to effectively manage risk across a complex IT environment, with the help of Trend Micro.

Two-fifths or more of respondents 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 board-level credibility starts here.

Discover how Trend can enhance your higher education institution's cyber-resilience by booking a 15-minute consultation today.