A global study

The CISO Credibility Gap:

Why Higher Eduation Boards and IT Leaders Need to Align on Cyber-Resilience

Harder for Hackers.
Simpler for you.

September 2024
Trend Micro

Introduction

Higher education (HE) is an under-valued but vital contributor to the UK economy. The sector accounts for **768,000** full-time jobs, **£71bn** in terms of gross value added (GVA) and **£116bn** in terms of general economic output. Yet those kinds of figures inevitably attract the attention of cybercriminals. A government report from April 2024 claims that **97%** of HE institutions identified a breach or cyber-attack in the previous year, versus **50%** of businesses. Around six in ten claimed that they had been negatively impacted by a breach.

768k

full-time jobs

£71bn

gross value added (GVA)

£116bn

general economic output

6 in 10

claimed that they had been negatively impacted by a breach

Although **97%** of HE providers include cyber on their risk register, and **87%** regularly report on cyber risk to their executive board, that doesn't make the challenges simply go away. CISOs need to articulate the value of investing in cybersecurity in business terms in order to turn the heads of their boards and advisory committees. Yet many struggle to be heard due to a credibility gap which is often difficult to close.

As a long-time partner of the education sector, Trend Micro wanted to find out more. So we commissioned Sapio Research to interview **144** IT leaders in the sector with responsibility for cybersecurity in their organisation–across LATAM, APAC, North America, Europe and the Middle East.

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 with boards and advisory committees. That has serious implications for achieving their long-term strategic goals, and ultimately for the cyber-resilience of the organisation.

of HE providers include cyber on their risk register

regularly report on cyber risk to their executive board

144 IT Leaders interviewed

Perception and reality

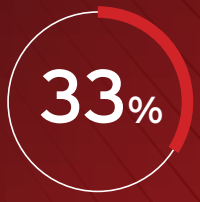
Although the vast majority (**95%**) of respondents claim to feel fully (**45%**) or somewhat (**50%**) confident in their organisation's cyber-resilience, this perception may be misleading. The education sector ranks in the top four globally in terms of malware campaigns identified by Trend Micro and in the top seven when ranked by volume of risk events last year. Ransomware is assessed to be the number one threat, and phishing emails account for **90%** of initial compromises globally. True resilience requires close alignment between cyber and business strategy, which is not happening in many responding organisations.

Cyber-Resilience

While **58%** of respondents recognise that cyber is their biggest business risk, over a third (**33%**) admit that cybersecurity is still treated as part of IT rather than business risk. This is echoed by the view of most (**76%**) respondents that the board would only be incentivised to act decisively on business risk if a breach occurred. On average, a financial loss of **£122,393** would be enough, they claim. This points to a disinterested and unengaged board.

£122,393k 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 one-off events like this 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 credibility gap

Universities face "long-term, systemic, pressures on their financial sustainability and viability", according to lawmakers. Macroeconomic headwinds and a continued cap on tuition fees have further tightened the screw. This inevitably has knock-on effects when CISOs look at how much they have to spend on cyber-resilience. But settling for "good enough" bundled security can create more problems than it solves.

The truth is that HE institutions manage huge volumes of sensitive data – including world-leading research that's of interest to state-sponsored threat actors, and staff and student personal information (PII), which cybercriminals are keen to exploit. Given the importance of student fees to the bottom line, any serious breach or outage could have a significant reputational and therefore financial impact.

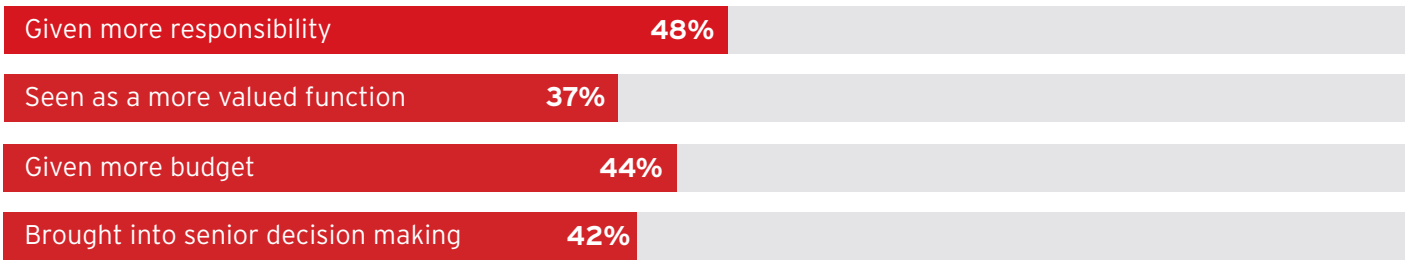
Unfortunately, these challenges are being compounded by a breakdown in communication between technology and HE business leadership. Some **72%** of HE cybersecurity leaders say have felt boardroom pressure to downplay the severity of cyber risks facing their organisation. Of these, **43%** say it is because they are seen as being "repetitive" or "nagging", and **39%** that they are viewed as overly negative. Two-fifths (**41%**) claim they have been dismissed out of hand – way more than the average across sectors (**33%**).

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. 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.

Two-fifths (**38%**) of education sector 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 HE IT security leaders respond?

First, they need to ensure that the information generated by their security tools is consistent and easily digestible. That is a challenge when many HE institutions 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.

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
- Expand communication to educate staff and students about best practice security

HE 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. Given the financial pressure universities are under and the potential RoI of effective cybersecurity, the rewards are too big to ignore. It's time to close the CISO credibility gap.

To find out how Trend can help your higher education institution build cyber-resilience, book a 15-minute consultation today