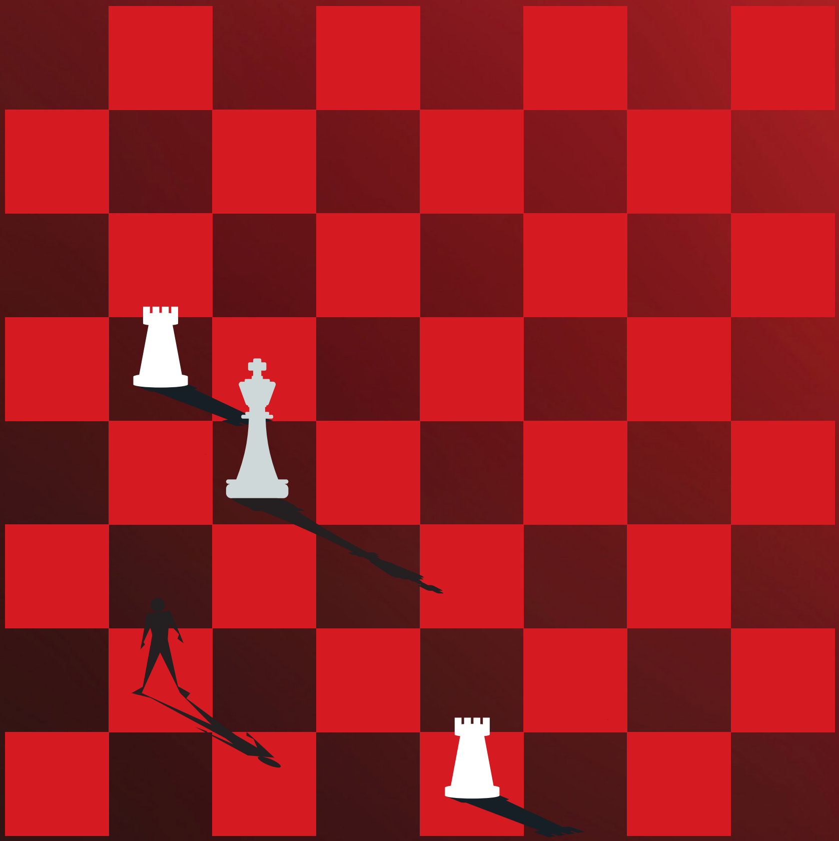
Article

Government in the crosshairs:

How CISOs can close the boardroom credibility gap to support transformation

Harder for Hackers.
Simpler for you.



September 2024
Trend Micro

There's no such thing as a typical government department. But there's one thing that they all have in common: a growing threat from state-backed spies and financially motivated cybercriminals. With a low tolerance for outages, millions of citizens relying on their services and huge volumes of sensitive information in their digital vaults, these organisations collectively represent perhaps the biggest target for cyber-attack there is. The target continues to grow with each new digital initiative, while compliance obligations turn up the pressure on CISOs.

That's why central government security leads are trying to build the case for improving cyber-resilience, in a cost-effective and future-proof manner. But their job isn't easy. First, they have to convince a sceptical – and sometimes downright hostile – board.

Why resilience matters

The government first published its Cloud First policy in 2013. It continues to gather pace today, although progress is far from uniform, creating hybrid environments of advanced public cloud and legacy on-premises technology. They present different security risks which must be managed in different ways to the monolithic IT systems of old. Adoption of IoT and operational technology (OT) further expands the attack surface—providing opportunities to gain a foothold in networks, steal sensitive information and disrupt critical services.

Against this backdrop, cyber-resilience is becoming increasingly important to ensure government organisations can continue to operate effectively, even if hit by a sustained and sophisticated cyber-attack. It means improving cyber-hygiene through best practices like multifactor authentication (MFA), regular security awareness training, backups, encryption, anti-malware, prompt patching and more. And enhancing this "prevention" approach with detection and response to catch any threats that may sneak through – and recover quickly before there's been any significant impact on the organisation.

Unfortunately, this is getting harder. In 2023 alone, 195 million data subjects had their rights and freedoms put at risk by central government financial data breaches, according to the Information Commissioner's Office (ICO). Ransomware isn't the only threat facing these organisations. But it has become one of the biggest, according to the National Cyber Security Centre (NCSC), which also warns that the threat is expected to increase as malicious actors get hold of AI tools.

195m

financial data breaches

Ransomware

isn't the only threat

AI Tools

used by malicious actors

Undermined and undervalued

Investing in cyber-resilience should therefore be an open-and-shut case for CISOs to make. It's not just about mitigating the immediate financial, operational and reputational risks that stem from serious security breaches. Resilience also provides the strong foundations of cybersecurity on which ambitious government IT transformation programmes must be built.

Unfortunately, this is not quite so straightforward. For cyber strategy to function as intended, the IT or security lead needs to be heard and understood. The board must buy into their vision, implicitly understanding the business criticality of effective cyber-risk management. This is not happening. Research reveals that boards are more likely to be disengaged and unenthused by cyber, viewing it as an IT risk and little more. In fact, most (**88%**) CISOs claim that their board would only be incentivised to act on cyber risk if there was an actual breach.

Reactive investments such as these often lead to point solutions which fail to address fundamental challenges, papering over the cracks when something more holistic is needed. They represent an attractive option in the context of swingeing Whitehall budget cuts, but are ultimately a false economy that fail to deal with underlying causes of cyber risk.

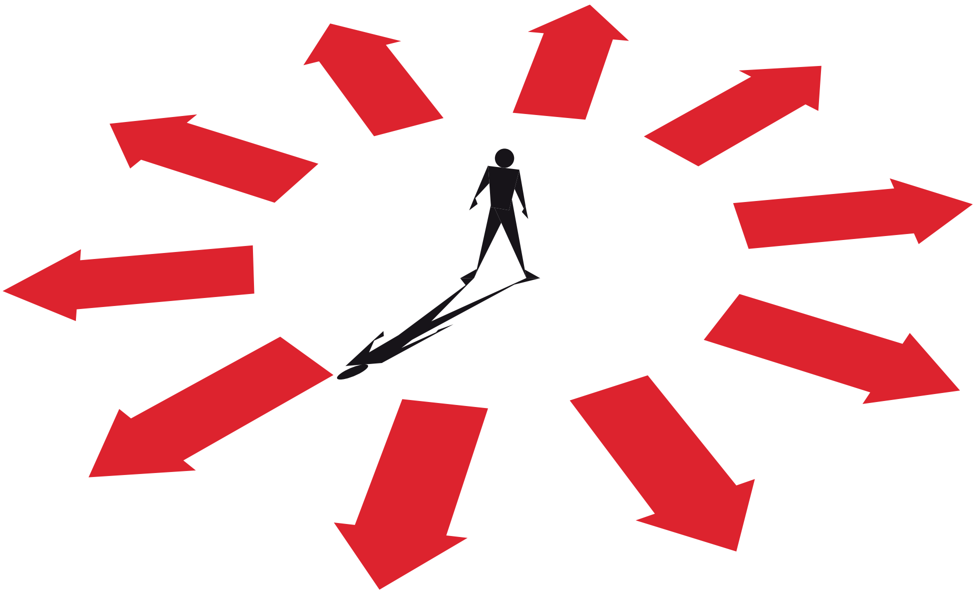
That same research finds that two-thirds (**67%**) of government cybersecurity leaders have felt boardroom pressure to downplay the severity of cyber risks facing their organisation. Many claim this is because they are seen as being "nagging" and are viewed as overly negative. A third say they have been dismissed out of hand. This kind of head-in-the-sand approach has been called out before. In early 2024, an influential parliamentary committee criticised the previous government's "ostrich strategy" – claiming it was doing too little to prepare for the high risk of a "catastrophic" ransomware attack.

88%

CISOs claim that their boards only incentivised to act on an actual breach

67%

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



Bridging the gap

This is partly the fault of the board. Government leadership must realise that security gaps created by legacy technology, investments in next-gen kit, budgetary pressures and crippling skills shortages are only getting more pronounced. And at the same time that their security, resilience and data sovereignty responsibilities under regimes as diverse as the GDPR and the Public Services Network (PSN) are also growing.

Yet CISOs can sometimes also be part of the problem, by packing their presentations with irrelevant metrics and industry jargon. That's not the way to win over a non-tech audience which wants answers to far more fundamental questions: How secure are we? What will it take us to get there?

To bridge the widening boardroom credibility gap, security leaders need to keep their communications simple, to the point and free from tech-speak. They need to align cyber with business risk, and cybersecurity outcomes to business objectives. And they need to work harder to build personal relationships with board members.

The journey starts here

How do they get there? Using the right metrics is a good start. By consolidating point solutions onto a single platform for managing cyber risk, they can generate a single source of truth for more consistent reporting—while also reducing costs. The best outcome would be a solution capable of calculating risk based on attack landscape, user exposure and security configuration, as well as overall impact to the business. This could be used to continually map risk across the corporate attack surface and take automated remedial actions to close any gaps that appear, like vulnerabilities and misconfigurations.

The results could be displayed in an easy-to-consume executive dashboard, which helps senior leaders grasp the real-world implications of nebulous concepts like cloud misconfiguration and account compromise. A high degree of automation reduces the workload for stretched security teams, and proactive threat detection ensures any breaches are caught and contained early, further minimising security-related reputation and financial damage.

This approach lights a clear pathway to closer alignment between security and government objectives, which could ultimately help to enhance cyber-resilience. It may be a long journey ahead for some departments, but the alternative is far worse.

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