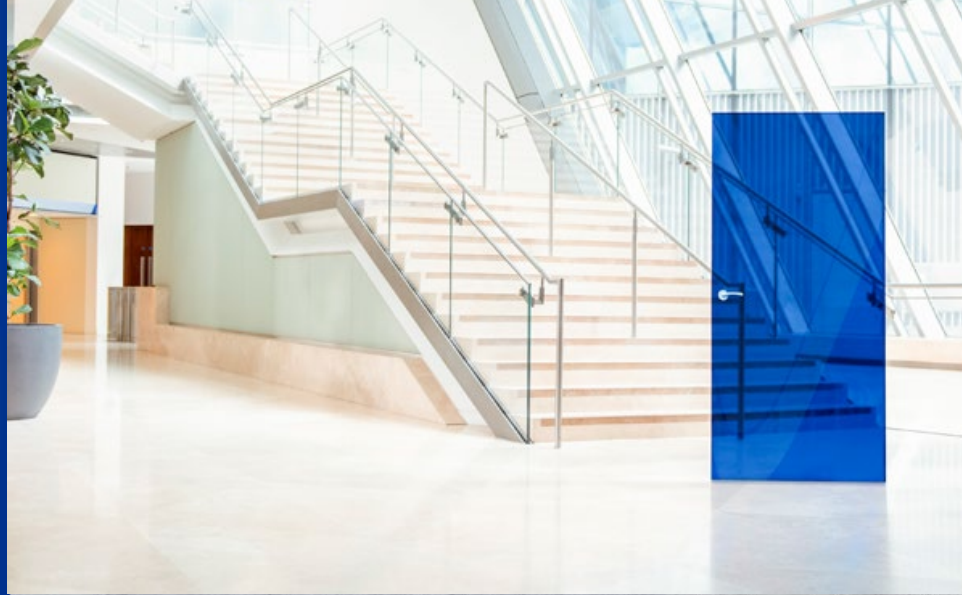
A conversation about cyber security

KPMG Board Leadership Centre



Cyber risk is now a condition of being in business. Cyber criminals, whether individual or part of organised gangs, are relentless in their activities and are constantly looking for new ways to extort financial gain. Nation states are also active, whether that be theft of IP to spreading misinformation or disrupting rival economies and businesses. It's an issue that needs to be constantly in the sights of Boards and Risk Committees. Paul Taylor – former Head of Cyber at KPMG and now chair of cyber consultancy Beyond Blue, a technology-focused NED at a global investment bank and a NED on the Technology and Innovation board at the Ministry of Defence – joined our Board Leadership Centre FTSE350 meeting to share his experience in helping boards combat the cyber threat.

To defend an organisation robustly, you first have to understand the nature of the threats facing the business. And Paul was very clear that these threats have shifted in emphasis over the last 12 months, driven by the effects of COVID-19.

The pandemic has moved organisations online at a scale not seen before. Almost everything is conducted remotely, with the online domain becoming the natural environment we work in. This has created new risks, such as fraudsters gaining access to meetings on Zoom or Teams and attempting to steal individuals' credentials. With everyone working separately from each other, the risk of falling foul of a phishing email with a fake link has also been raised – because we are no longer able to turn to a colleague next to us and get their opinion or quickly ask if they have received the same email.

There has also been an increased "dash to the cloud" – with Paul expressing some concern that with just three major cloud providers there is a dependency risk brewing. Meanwhile, the pandemic showed that supply chains can be fragile – the just in time philosophy does not work so well when everyone is trying to buy the same things at the same time. Operational risk and resilience have been placed firmly under the spotlight.

"We're in a different reality now," Paul said. "The working model has changed, probably forever. When lockdown began, we saw ten years' worth of digital change in just a matter of weeks. During the pandemic, permissions were given that didn't exist before – such as allowing certain documents to be printed off at home, or allowing individuals to approve certain transactions or trades.

The pace of change means that we have a large security debt to deal with. Regulators – especially in sectors like Financial Services – are already asking detailed questions about how businesses are mitigating the risks."

Another growing risk emerges from the Internet of Things. We will see more and more devices at both work and home connected to the internet, with varying degrees of security and regularity of updates. "Both the worry and the beauty is that everything is connected to everything else," Paul observed.

Artificial Intelligence (AI) and machine learning are all around us too, from assisted driving in cars to controlling aspects of production in factories, refineries and other industrial operations. These are all risks that need to be managed, monitored and controlled.

Ransomware boom

All of these factors have made the cyber threat even more pronounced than before. While most of the actual methods of attempted cyber fraud have not changed, some of them have become much more prominent.

Chief among these is ransomware – malware that encrypts an organisation's files, with a ransom demanded to unlock them. "Most serious cyber crime that we see now revolves around ransomware," Paul said. "Organised criminals even run 'ransomware as a service', available to buy on the dark web complete with a team of people to carry it out for you. Criminals run recruitment drives, with one gang in the Philippines even offering dental and health plans for their team members as an employee benefit!"

Other widespread threats include denial of service attacks that cripple organisations' websites and systems, and 'CEO fraud' – fake emails purporting to be from the CEO or another senior executive, often to staff in Finance or HR to make a payment or release certain sensitive information.

This fooling of unwitting employees (the insider threat) is one of the biggest gateways into an organisation for cyber criminals. In fact, Paul said, 80% of successful cyber events have an insider involved.

Most cases are unwitting, such as an employee clicking on or sharing a malicious link, but some involve conscious and deliberate insider fraud. There have been cases where an insider has waited 18 months gaining colleagues' trust before beginning to circumvent controls or pass information outside the business. This is where close control of privileged access and individual permissions is key, together with network segmentation to limit the data that can pass from one system or function to another.

What should Boards be focusing on?

Given such a potent mix of factors, clearly it's essential that Boards have cyber security firmly on the agenda. As Paul said, "Boards must be able to challenge and provide oversight. They need to be asking the right questions of the business." These include:

- Who's leading on cyber and are we confident in them?
- What are we trying to protect? What are our 'crown jewels' and how are we defending them?
- Is cyber security a key part of our business model rather than just an 'add-on' left to the IT function?
- Do we know how good we are? Have we run a benchmark exercise?
- If something goes wrong, do we have clear processes in place to deal with the consequences? Do we run regular crisis simulations?

Paul also advised that getting an independent opinion – in addition to taking assurance from the CIO or CISO – can be invaluable. "Definitely get external advice. This may well mirror what your internal leads tell you but getting an objective opinion has a different level of authority."

Some businesses, particularly in Financial Services, are also pursuing what Paul described as an "active defence" approach – taking proactive measures, often collaboratively, to stop attackers and "take the fight to the enemy".

Meanwhile, if attacked by a nation state or large-scale organised actor, the UK's National Cyber Security Centre (NCSC) is on hand to provide support to organisations.

Regulatory agenda

Boards also need to be very aware that regulatory requirements around cyber security and resilience are only likely to grow. In Financial Services, there is already a pronounced focus from regulators on cyber defences, operational resilience and supply chain security.

"Regulation normally trickles sideways and down, and I expect such requirements to spread to other sectors quite quickly," Paul said.

In response, increasing numbers of Boards have been considering their composition, actively bringing in individuals with a technology background and experience.

There is much for Boards to think about in connection with the persistent cyber threat – and no sign of that changing any time soon.

The KPMG Board Leadership Centre

The KPMG Board Leadership Centre offers support and guidance to non-executive directors, whether managing a portfolio non-executive career or embarking on a first appointment. Membership offers you a place within a community of board-level peers with access to topical and relevant seminars, invaluable resources and thought leadership, as well as lively and engaging networking opportunities. We equip you with the tools you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business.

Learn more at www.kpmg.com/uk/blc.

Contact us

Timothy Copnell
Board Leadership Centre
T: +44 (0)20 7694 8082
E: tim.copnell@kpmg.co.uk