SPOTLIGHT ON CYBERSECURITY: STOP THINKING IF. START THINKING WHEN

BENEWS

Sponsored by:

Control Risks

Pinsent Masons

technologywithin®

Hosted by:

KONTOR

Landsec

INDUSTRY GUESTS:

Andy Broad, Head of Cyber Security, Landsec

Stuart Davey, Partner, Pinsent Masons

Caitlin Egen, Global Director, Control Risks

Amanda Finch, CEO, Chartered Institute of Information Security (keynote speaker)

Louise Methven, Compliance & Cyber Security Director, Ark Data Centres

Sanjaya Ranasinghe, VP, WiredScore

James Townsend, Co-Founder and CEO, Kontor

Martin Whitaker, Development Director, technologywithin

Mark Whyte, Senior Partner, Control Risks

Liz Hamson, Editor-in-Chief, *BE News* (chair)

The Cyber Security and Resilience Bill (CSRB), which is currently passing its way through parliament, highlights what a national priority cybersecurity has become.

As businesses – and buildings – become increasingly reliant on digital ecosystems, they are also becoming more vulnerable to cyber-attacks, as demonstrated by recent high-profile attacks on leading retailers such as Marks & Spencer and the Co-operative Group and on automobile manufacturer Jaguar Land Rover.

So, how is the threat landscape evolving? Where is the industry particularly vulnerable to attack? What practical steps should companies, large and small, take to protect themselves?

These were just some of the questions debated during the fascinating – but sobering - BE News Spotlight on Cybersecurity event, sponsored by Control Risks, Pinsent Masons and technologywithin, and co-hosted by Kontor, Landsec and MYO at the latter's new King's Cross site.

The theme of the Spotlight was 'Stop thinking if. Start thinking when' and after a welcome speech by Kontor CEO James Townsend, Control Risks senior partner Mark Whyte set the scene for the following keynote speech and one-hour Question Time-style panel debate by highlighting the benefits and pitfalls of man-made technology.

Smart buildings, smart cities and connected infrastructure, bring sustainability and convenience creating liveable urban spaces, said the global head for built environment and infrastructure. But, as he succinctly put it, every silver lining has a cloud.

"With all these huge benefits, there are also new vulnerabilities," said Whyte, warning that issues can quickly cascade and "rip out entire ecosystems".

To mitigate the threat of cyber-attacks, Whyte called on the industry to "start thinking like our adversaries", to expect intelligent, coordinated attacks and to be resilient.

"We need to design adaptive systems that are anticipating the sorts of failures that may occur and not just preventing those things we can see in front of us or relying overly on our recovery plans," he said.

Keynote speaker Amanda Finch, CEO of the Chartered Institute of Information Security, picked up on the evolving nature of the threat, remarking wryly: "Had I known I'd be involved in global issues, warfare and organised crime, I would have run for the hills."

Amanda Finch

Underlining the scale of the threat, Finch noted that organised crime was the world's third biggest economy behind China and America. "The amount of resource [criminals have] to be able to [hit] our systems is extraordinary," she said, adding that the M&S cyber-attack in April 2025 was a wake-up call for the industry.

"It was a lesson for people to see what it really means when something attacks," she said. "The internet goes down. You won't be able to contact your customers. It brought it home to people about how this could affect them."

Ultimately, said Finch: "It's important you've got people you can trust that are providing good advice and support. It's equally important you engage with the business as well, so people know what their part is with that."

Finch's words were echoed by the six experts participating in the panel discussion that followed. Asked to what extent the industry currently understood the scale of the threat and how well it was prepared, Landsec head of cyber security Andy Broad said incidents like M&S had made company boards "sit up and take note of their defences".

However, he added: "Landsec own and operate property, but it's still seen as a non-digital product. It's bricks and mortar, steel and glass. The importance of cybersecurity

> ***"It's important you've got people you can trust that are providing good advice and support."***
>
> *Amanda Finch*

Caitlin Egen

and buildings is not always obvious to the customers and some stakeholders."

He added that the gap between the physical and increasing digitalisation was "one of the biggest bridges we must close".

It is crucial to have top level buy in from the board and leadership, said WiredScore vice president Sanjaya Ranasinghe. "If you [have that], you then push responsibility down into buildings and suddenly it goes from the landlord to the property manager, who then absorbs it."

Businesses should not just be concerned about their own cybersecurity, added Ark Data Centres compliance & cyber security director, Louise Methven. "It's not only just you as an organisation but also the wider issue of what is happening across your supply chain," she said.

Geopolitcial situation

How the geopolitical situation was playing out across supply chains, was "very interesting," agreed Control Risks global director Caitlin Egen, who noted that the threat landscape was evolving as physical and cyber threats converged.

The built environment was "such a broad sector", she said. "You can have a co-location data centre with legacy systems and then have smart city projects where everything's cutting-edge computing and AI technology, meaning the threat is very contextual and the blind spots can be distinct."

Touching on the threat of state sponsored cyber-attacks, technologywithin development director Martin Whitaker said that the risk did not really exist pre-2004, but that in 2026, the average person was more aware than ever of the issue.

Egen added: "We're seeing state sponsored attacks massively increase. Scam farms are playing a massively disruptive role in the West. So, it's interesting how state tactics have changed, and how the intersection with organised crime has become much more pronounced."

The Cyber Security and Resilience Bill (CSRB) builds on the existing framework of 2018 regulations, which targeted certain critical infrastructure sectors such as energy, water, the NHS and airports.

"The focal point of the bill is the technological ecosystem that underpins key parts of society," said Pinsent Masons partner Stuart Davey, adding that the bill's supply chain focus was "really important".

However, correctly reporting incidents of any cyber-attacks or near misses would be difficult, he said, warning that the bill should not overburden small and medium-sized businesses with regulations.

"I would like to see consistency among the risk management approaches," he said. "There are already good, solid frameworks to be able to manage cybersecurity, like the National Institute of Standards and Technology (NIST). If the CSRB increases ⩥

the requirement to have strong, stringent controls, that's a good thing, but it mustn't contradict anything else we've grown up with in the cybersecurity world known as best practice."

It is also important to remember that the cyber threat is constantly changing. Egen pointed to how AI was moving at a pace and now offered cybercrime organisations benefits ranging from enhanced social engineering through to vulnerability scanning capabilities.

Human error

Whitaker said that too often, the risks come from simple human error. "Shared wi-fi passwords, poor access management, and failing to remove access for guests or former employees," he said. "Most breaches don't start with hackers, they start with bad habits."

He also warned about outdated authentication methods such as MAC address authentication, which grants network access based on a device's unique hardware identifier. While it's often seen as a simple way to assign users to private networks, MAC addresses are easy to discover and spoof.

"With basic tools, someone can impersonate another device and drop straight into a private company network. It's a low-effort, high-impact attack exploiting basic weaknesses. Compromising one trusted provider can open the door to dozens of buildings at once," Whitaker warned.

> ***"There has been a race to the bottom to cut prices and get products to market fast."***
>
> *Martin Whitaker*

Stuart Davey

Martin Whitaker

Loiuse Methven

> ***There are some positive signals, but there are also immense challenges."***
>
> *Caitlin Egen*

Sanjaya Ranasinghe

Andy Broad

And wi-fi is one of the most underestimated attack surfaces. "Shared passwords or device-based authentication feel simple, but they're one of the easiest ways to hand attackers the keys to your digital front door," Whitaker added.

Unfortunately, as several panellists acknowledged, implementing good cybersecurity measures can be expensive. Broad admitted it was difficult for small companies to get access to resources they could trust. "NCC Group toolkits will help, but getting advice that isn't highly pressurised is a first step."

Encouraging a cybersecurity "muscle memory" response through effective training was vital, said Davey, adding that people needed to know how to respond swiftly, who the best people to help were and whether cyber insurance was in place.

Picking up on the last point, Ranasinghe said that getting insurance for cyber-attacks was tricky. While building insurance exists, there was a gap when it comes to insuring against computer hacking.

"The built environment isn't covered because the insurance industry is waiting for the event to happen to work out how they price it and how they build it into their products," he elaborated.

Asked how confident they were that the industry would be able to deal effectively with the cybersecurity threat, the panellists agreed that much of the industry still needed to wake up to the fact that it was a case of when not if they would be subject to a cyber-attack.

"The industry is likely to [need] some catalyst event specific to it before standing up and understanding where we are," said Broad.

Egen added that all industries were battling with the issue in different ways, but that cybersecurity was finally starting to rise up the agenda.

"I work with a lot of PE clients on due diligence for a data centre acquisition and cyber has moved up as a priority just in the last couple of years," she said. "So, there are some positive signals, but there are also immense challenges." □