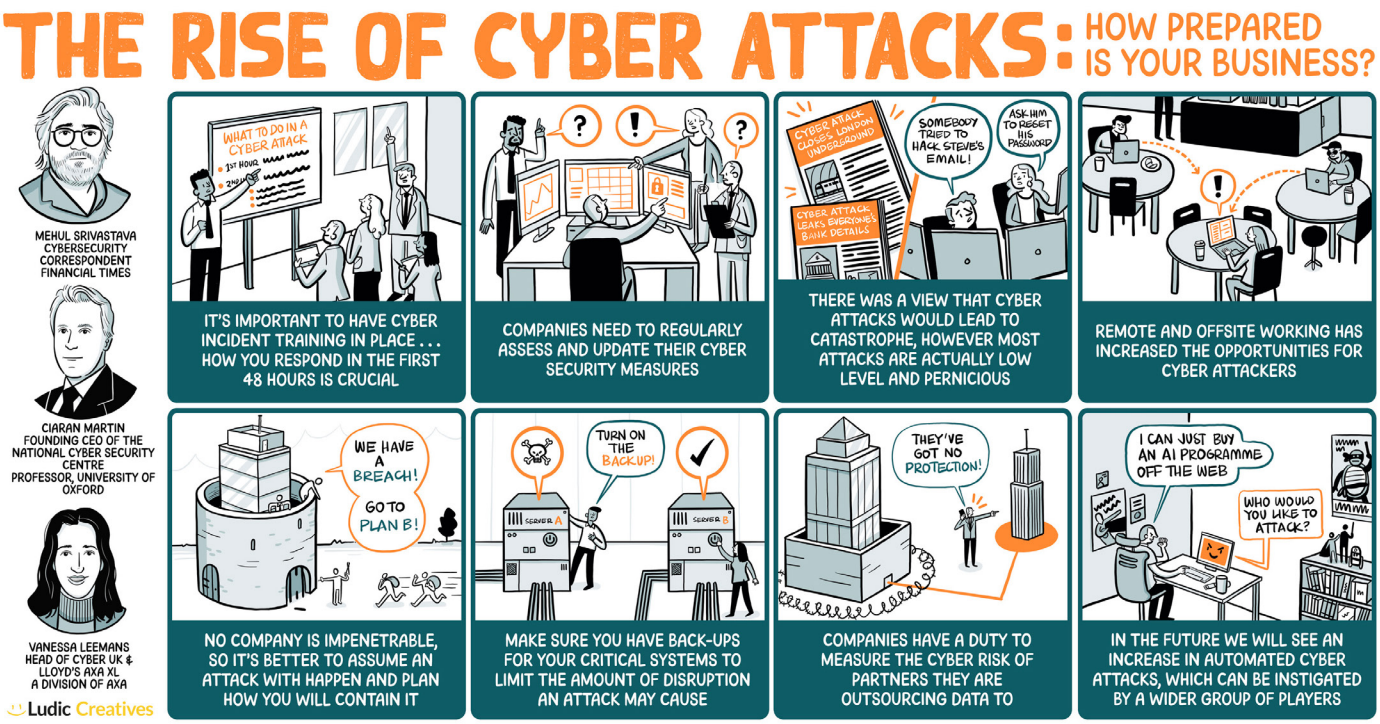
FT BOARD NETWORK

THE RISE OF CYBER ATTACKS: HOW PREPARED IS YOUR BUSINESS?

6 JUNE

SPEAKERS

Mehul Srivastava, cybersecurity correspondent, Financial Times
Vanessa Leemans, head of cyber, UK and Lloyd's, Axa XL
Ciaran Martin, professor of practice in the management of public organisations, Blavatnik school of government, Oxford university



In the latest FT Board Network event, Mehul Srivastava, the FT cybersecurity correspondent, moderated a discussion on the most effective ways to prevent cyber attacks and how to deal with the consequences should they succeed.

On the panel were Vanessa Leemans, head of Cyber UK and Lloyd's at Axa XL, and Ciaran Martin, professor of practice in the management of public organisations at Oxford university and founding CEO of the National Cyber Security Centre, part of the UK Government Communications Headquarters (GCHQ).

Here are the highlights from the event.

The best way to protect your business from a cyber attack? Be prepared

Vanessa Leemans said preparation was “the name of the game”. Every company’s precautions should include having a chief information security officer (Ciso); using multifactor identification; keeping back-ups of critical systems and testing them regularly, and holding cyber incident training, especially on what should happen in the first 48 hours of an attack.

Don’t build a fortress. focus on mitigation

Ciaran Martin said cyber security used to be about building a “perimeter fence” with an aim to “repel 100 per cent of attacks”. That is not the goal today because of the scope of computer networks and the scale of attacks. Instead cyber security is now about mitigation. It is accepted that bad things happen, so how do you contain them?

At a policy level, regulation is seen as increasingly important. In the banking sector, it has been key to minimising attacks while recognising the impossibility of stopping all cyber fraud. Martin said the telecoms industry was applying a regulatory model pioneered by banks. He said the Product Security and Telecommunications Infrastructure Act 2022 was taking effect.

The most vulnerable companies are those holding most data

Data-rich organisations are “probably most susceptible” to cyber attacks, Leemans said, and for this reason they pay higher insurance premiums. She listed healthcare, professional services, financial services, retail and manufacturing as being most vulnerable.

Watch out for spillover risks

Ten years ago, Martin said, the focus was on “the catastrophisation of cyber risk”. He pointed to one publication whose front page showed “a crumbling skyline caused by a cyber bomb”. Now, though, it is recognised that the bulk of the risks “are of the chronic and pernicious kind: data theft, business disruption and the exfiltration of intellectual property”.

Nevertheless he warned of the dangers of “spillover risks” from large-scale criminal attacks or hacks sanctioned by rogue nations. In 2017 when he was chief executive of the National Cyber Security Centre, part of GCHQ, there were two attacks in six weeks with huge spillover effects.

The first was the WannaCry ransomware attack that emerged from North Korea and affected more than 100 countries. It cost billions of dollars and disrupted healthcare services in the UK. The second was the NotPetya attack that the NCSC said was “almost certainly” the work of the Russian military. This compromised major companies and inflicted billions of dollars of damage. It led to “titanic lawsuits”.

Soon after the Russian invasion of Ukraine, governments warned of spillover affecting organisations in Europe and the US. So far nothing significant has happened. Martin suggested that Russia is “too busy trying to hack Ukraine” while Moscow is wary of a broad attack on the west as the source could be easily detected.

He said: “It’s a myth that you can secretly escalate in a way that you can’t in the real world.” If there had been a major attack on the critical infrastructure of London or Paris, “it would have been as escalatory as an accidental border incursion”.

Spillover risks remain, though, and Martin said “hackers acting recklessly is probably a bigger threat than targeted attacks”.

Why insure against cyber attacks? What do you get for your premium?

Leemans said the job of the insurer was "to protect a company's balance sheets and help it to recover quickly". To this end, insurers typically offer a financial payout after an attack as well as "incident support" that includes access to forensic IT specialists and specialist public relations advisers.

You can outsource a service but you cannot outsource the risk

The Forum met as news broke of the cyber attack by a Russian criminal gang on the software used by a payroll provider that serves nearly half of FTSE 100 companies including the BBC, BA the airline and Boots the chemist. Martin said it was "a pretty nasty and pretty big incident". Drawing lessons from it, he said using another company's software "doesn't absolve you of responsibility to build resilience", and if you exchange data with an external supplier you must still maintain in-house risk management.

Questions from the audience

What are the cyber risks that companies will face over the next five years?

Martin said "the starting assumption" was that previous threats would continue, including thefts of cash, data and intellectual property. He said companies should watch for smarter attacks that are designed to be more destructive. He warned of the proliferation of cyber capabilities and the ability of less rational actors to use them.

Martin said companies should focus on "building higher walls and strengthening resilience".

Do businesses appreciate this is an issue for the CEO and the board or is it delegated to a chief technical officer?

Leemans said CEOs and boards now understood that this is "definitely not just an IT question". They appreciate that financial losses from an attack "could be shattering". She listed the costs as the "immediate crisis expenses" associated with responding to an attack; any legal charges and damages, and "longer term expense" such as reputational loss, a falling share price and the downgrade in credit rating.

Is cyber risk in the top three or top five of the risks facing companies?

Leemans said cyber risk stood "alongside climate change as one of the biggest risks organisations face". She said "the global cost of cyber crime is predicted to reach $8tn in 2023 and more than $10tn in 2025".

Leemans spoke of the striking acceleration in "the digital shift" during the Covid pandemic and said "many businesses are only slowly catching up". As a sign of the interest in cyber security, she said Axa XL had hired 31 more underwriters as well as a head of cyber talent to keep training up to date.

Are newer businesses run by younger people (digital natives) better prepared?

Martin said age and attitude both counted. He said it was important for companies to translate cyber security into the language of ordinary business risk. He highlighted the content of discussions between the board and the Ciso.

His advice to boards is:

- If you're on a board, you carry risk. Do not let the Ciso out of the room unless you understand what they say. There is no such thing as a stupid question.
- Do not sign up to anything you don't understand.

His advice to the Ciso is:

- Make sure the board understands what you say.
- Tell fellow directors the limits of your budget. If and when things go wrong, they will have had a proper risk assessment.

Will AI increase cyber risk?

Martin said business leaders “should keep a level head” because “for the most part in cyber security, historically, innovation gets a little ahead of security and then security catches up”.

How hard is it to explain that companies need to spend more on cyber security?

Leemans said companies were on “a journey”. Budgetary constraints meant they invested first in security measures and only later took out insurance.

If the payment of a ransom was made illegal, would the threat go away?

Martin sympathised with this view but did not believe a ban would solve the problem. He said governments should come to “a reasoned policy decision” after publishing “a white paper” with detailed analysis.

The real problem, he said, was that there is “a policy-induced crisis because of policy inertia. We don’t have a policy on [paying ransoms]. We have a policy that ‘it’s too difficult’. And that’s wrong.”