TECH LONDON ADVOCATES

What do businesses need to think about to achieve best in class cyber and network security?

Tech London Advocates, Hiscox, Aon

March 2023

HISCOX AON

What do businesses need to think about to achieve best in class cyber and network security?

INTRODUCTION

In March 2023, Tech London Advocates, Hiscox and Aon convened a group of cyber experts, insurers, and tech businesses to discuss and find solutions to the shared cyber challenges facing SMEs today.

Cyber crimes are expected to cost the world $10.5tn (£9.3tn) by 2025. On the current trajectory, small businesses will take most of the hit - they are three times more likely to be attacked by cyber-criminals compared to large businesses, with cyber attacks on small companies up by more than 150% in the year following the pandemic.

Many businesses, it seems, either don't know how to protect against cyber threats, or are simply failing to take action. Government figures estimate that almost one in three UK businesses reported a breach or attack in the last year.

Despite the rise in malicious attacks, the number of businesses implementing the most fundamental forms of defence – such as password policies, network firewalls and regular software updates - has fallen since 2021.

With supply chain issues and resourcing shortages dominating boardroom discussions, cyber risk is in danger of falling further down the collective business agenda.

This backdrop provided the impetus for the discussion. The roundtable was moderated by Russ Shaw CBE, founder of Tech London Advocates and Global Tech Advocates.

The purpose of the roundtable was:

To convene a cross-section of tech-focused businesses and insurers to better understand current cybersecurity challenges and establish what constitutes best in class network security.

This report outlines the key discussion points and conclusions from the roundtable.

What do businesses need to think about to achieve best in class cyber and network security?

ATTENDEES

Russ Shaw CBE
Founder, Tech London Advocates & Global Tech Advocates (moderator)

Wenmiao Yu
Co-founder & Director of Business Development, Quantum Dice

Munya Hoto
Chief Customer & Marketing Officer, CybSafe

Jonathan Harrison
Director, Aon

Seamus Dunne
Managing Director UK and Ireland, Digital Realty

Andrew Roughan
CEO, Plexal

Julian Davies
VP & GM EMEA, Bishop Fox

Eddie Lamb
Director of Cyber Education and Advisory, Hiscox

Matt Cheung
CEO, Founder & Board Chair, Clarasys

Ashley Grealish
Head Of Engineering, ev.energy

Janet Collyer
Portfolio Non-Executive Director

What do businesses need to think about to achieve best in class cyber and network security?

KEY FINDINGS

It's evident that what constitutes the most pressing cyber threats, and what is understood to be good governance to ensure business resilience against them, differs depending on who you ask.

This discussion was an opportunity to convene representatives from businesses of varying degrees of expertise in cyber resilience to discuss the threats concerning them. Most importantly, it sought to explore best practice and examples of tech capable of making a real difference to cyber defence.

The scale of the problem

It is clear that businesses are recognising this as a more prominent threat to their operations – globally, organisations spent around $150 billion on cybersecurity in 2021, an annual increase of 12.4%. However, increased investment doesn't always translate to an effective strategy.

Only 30% of companies properly assessed their cyber risk last year, while just one in ten reviewed risks at their immediate suppliers. Indeed, suppliers and the supply chain more broadly were identified as areas where businesses are particularly vulnerable to cyber intrusion.

It's vital that companies take time to understand their supply chain, who they are allowing into their network, for what reason and where the potential open gates are. Food manufacturers have to have a detailed knowledge of where everything in their supply chain comes from – and it was agreed that C-Suite leaders in tech should adopt a similar approach for their products if they are serious about presenting their businesses as cyber secure.

Learnings

One of the key learnings from the roundtable was that demand is growing for secure products, rather than security products. Businesses need to build in and uphold the security credentials of their products from the start of the design process – this increases trust among customers and investors and also ensures there can be rehearsed procedures in place for when things do go wrong.

We heard from insurance professionals how in their recent experience, claims related to phishing attacks are in decline. Cyber trends are fickle, however, and from a risk management perspective phishing remains front of mind in the concerns of underwriters.

One reason for this might be down to changing working habits, and that - rather than falling out of fashion - phishing attacks have simply become less visible. When staff were all in the office every day, employers had access to comprehensive datasets on cyber training completion or clicks on phishing links. In a hybrid world with employees working from various locations and Wi-Fi routers, the picture is less clear.

Ultimately though, the roundtable agreed that the weakest link in cybersecurity defences is human error and behaviour. People guard the technologies keeping systems safe, and the challenge therefore lies in quantifying the human risk element to cyber defences to help boards understand the extent of the threat faced. From ransomware to data exfiltration, the nature of the cyber threat may be constantly changing, but metrics used at boardroom level have remained the same.

Solutions

Solutions were offered in the form of the 'defence in depth' model. This starts with a concept of psychological deterrent – a business' objective should be to convince hackers that it is not worth targeting them in the first place.

The next step is about monitoring and detection. If companies are not monitoring their network and that of their supply chains, controls are likely to fail without alerting to changes in activity and triggering counter measures.

Delaying mechanisms are also important – the length of time between detection and response to disrupt an attack before it has time to take hold has a significant impact on the severity of a security breach.

If humans are part of the problem when it comes to cybersecurity, then tech is most certainly part of the solution. Technology can help detect and respond to threats, secure data, provide visibility into network activity, and automate security tasks, ultimately strengthening the security of an organisation as a whole.

What do businesses need to think about to achieve best in class cyber and network security?

KEY QUOTES

Munya Hoto, Chief Customer & Marketing Officer, CybSafe

"Start-up owners are time poor. At Cybsafe, we've invested heavily in behaviour science. As opposed to telling an employee about a risk in advance, we'll literally nudge them in real time as they're about to do the thing that will get them in trouble. For small organisations, this is the answer – relying less on memory and recollection and more on just-in-time intervention."

Seamus Dunne, Managing Director UK and Ireland, Digital Realty

"IT departments in verticals like manufacturing operate in isolation and are therefore constantly looking for network events, providers or consultants who can tell them what other industries are seeing - it seems like the requirements are changing so fast."

Julian Davies, VP & GM EMEA, Bishop Fox

"Although a core part of our proposition is a technology, this is also a human problem. Hackers are humans attacking other humans - you need to have people guarding the technology and using the technology in the right way."

Matt Cheung, CEO, Founder and Board Chair, Clarasys

"We eliminate the cyber risk to our clients by making sure we use their infrastructure - typically, they have invested in cybersecurity long before we get there. Our job is to make sure their customer journey is really effective - in general, we work with enterprise-class systems where the verification of whether they are secure by design has been done from a procurement point of view."

Janet Collyer, Portfolio Non-Executive Director

"Everyone knows about the principle of 'KYC' - know your customer. But it's becoming increasingly important to also 'KNS' - know your supplier. When putting together a big product, it's vital that you make sure you know where all the component parts came from."

Wenmiao Yu, Co-founder and Director of Business Development, Quantum Dice

"We're working towards a concept called 'device independence', which takes the protection against hardware attacks to a new level and ensures quantum randomness for encryption keys."

Jonathan Harrison, Director, Aon

"Generally, companies need to move from a defensive security strategy to an offensive position. Make sure that this a living breathing part of risk management within a business and don't just pay a lip service to it at board-level agenda."

Andrew Roughan, CEO, Plexal

"We've seen a big thirst for secure products rather than security products. The key is to bring forward the security credentials of individual products and make them more trusted."

Eddie Lamb, Director of Cyber Education and Advisory, Hiscox

"Governance is not a dirty word! If you can't measure it, you can't manage it. You need to have a handle on what your business is doing."

Ashley Grealish, Head Of Engineering, ev.energy

"When building a product, we think a lot about implementing security from the very start and planning for when things go wrong. If there is an issue with a certain type of charger or manufacturer, the important thing is that the design system does not allow it to affect the grid."