HotTopics

What the Boardroom Really Thinks About Cybersecurity - and Your CISO

in partnership with

BT Means Business

Cybersecurity, once relegated to backroom IT discussions, has slowly but surely earned a place in the boardroom. Yet true C-suite awareness, alignment and action remain mired in a web of complexities

World-weary technology executives have long argued that the technology 'is the easy part' - getting people to conform to new habits and ways of working is a far tougher nut to crack.

For some, that has meant trying to convince system administrators the advantages of moving to cloud computing, for others rallying academics and researchers on the advantages of remote learning tools, doctors and nurses on a future of electronic records, or the general public on how their data is being used.

Security is still seen as the 'department of no'

As the great novellist Leo Tolstoy once remarked, 'everyone thinks of changing the world, but no one thinks of changing himself' – and it is this resistance to personal and organisational change that often plagues the CIOs, CSOs and CISOs entrusted with the information security of their organisations.

Despite the increasing recognition, from the boardroom down, of security's importance to everything from share prices and business valuations to customer loyalty, information security continues to fight against widespread inertia, restrictive reporting lines and a hard-to-shake perception that security remains a cost centre rather than an enabler.

Yet a glimpse back in time shows the depth of the problem; perhaps unfairly chastised for becoming the 'department of no', the pace of change in information security (still often reporting to IT) has lagged that of technological innovation.

Take the introduction of the World Wide Web in the 1990s, which saw the first viruses and worms followed by early security functionality like SSL certificates, web authentication and public key encryption. The first versions of Microsoft Windows operating systems suffered a similar feat, prior to the introduction of antivirus and service packs, and so too did early email servers, web browsers and the earliest Wi-Fi routers and connected devices.

This two-speed approach must change. As organisations become more digital, service-led and customer-centric - while facing greater pressure from global regulators, cybersecurity must be reframed as a key enabler of innovation and resilience, requiring true C-suite commitment, action and investment.

In this Food for Thought lunch, hosted by leading C-suite community HotTopics in partnership with BT Business at the famous Churchill War Rooms, C-level business, technology and security executives explored the boardroom nuances of cybersecurity, the wrestle for control and accountability, varying risk appetites and more.

Our attendees:

Yasemin Mustafa
Director of Cyber Security Portfolio
BT Group

Martin Sivorn
CISO
Department for Education

Minu Ali
CISO
Francis Crick Institute

Natasha Towner
Deputy CISO
Francis Crick Institute

CK (Chuang) Kee Ong
Director, Data Product
GSK

Daniel Hobden
Fractional CFO

Steve Westgarth
Global Head of Engineering and Architecture
Haleon

Westley Adams
Global Head of Information Risk - Markets & Securities
HSBC Services

Mark Cameron
Head of Architecture & Cyber Security
WPP

Chris Clark
Non Exec Director
Aviva

Jeptha Allen
Senior Director - Head of Digital Infrastructure Advisory
CBRE

Maria Papastathi
Chief Data Officer - Technology
Shell

Doug Drinkwater
Editorial and Strategy Director
HotTopics

Peter Stojanovic
Editor
HotTopics

The CISO's impact varies by communication and expertise

Most organisations today employ a Chief Information Security Officer (CISO), often reporting into the CIO, CFO or - ideally, in the eyes of a CISO at least, the CEO.

These are hard jobs. The average tenure of a modern-day CISO is typically between 18 and 26 months – paling in comparison with the CIO's 4.5 years – and often fraught with tales of inadequate investment, overstretched security operations teams and a deluge of incidents. All roads, as some security leaders attest, lead to physical and mental burnout.

If that wasn't enough, the issue of accountability has become more prominent in recent months, with high-profile cases seeing CISOs bearing the full brunt of the risk.

With cases like Solarwinds and Uber, CISOs have found themselves before a judge - which has led some to express that CISOs should not be accountable for the overall business risk - or at the very least be afforded the same D&O protection as other boardroom directors.

Much of it comes back to the personal relationships from the top-table down, the reporting lines, the type of CISO the organisation has or needs - and the skillset of the leader occupying said seat.

> *"We're talking about CISOs as if there's one type of CISO, and maybe because as a CISO I discern the differences more than others in the same way,"* said one CISO, citing regional, technical and communication differences.

> *"You can be a smart techie, or you can also be smart in something else,"* he added. Another speaker told their story about 'working with some of the smartest CISOs', who still had an inability to articulate "correctly or clearly, what the risk was".

> *"We tried to get down to two slides to break it down…and everyone was sitting there like 'whoosh'* [intimates information flying over their heads]*. That was really difficult."*

> *"I worked with other people who clearly lacked the technical competence this lady had, but they broke it down into a way this other lady was unable to really articulate. And everyone [across the boardroom] was like, 'right, cool, okay'."*

“She almost had ultimate accountability, and was totally trusted, because she could communicate effectively.”

An attending CIO told his story of how to communicate effectively, even through the occasional disconnect between cost-driven boardrooms and protection-obsessed security leaders. There’s a need to focus on the business case for security, how it safeguards customer trust, compliance and protects market share - which therein repositions security as an enabler mitigating risk and impacting bottom line.

“I use the CISO, I use my team of information risk experts globally. We build analogies, translations and [educate through] sessions,” he said.

“We use organisations who are former government ‘crazies’ who explain the threat landscape at a non-business level, and then we help build sessions to translate that into business activity. So we have this layered approach of how to get the information to the leadership.”

Security culture begins with alignment, training and risk ownership

For these leaders, sat in the original command and control centre of the Churchill War Rooms where Winston Churchill organised Cabinet meetings and plotted Nazi Germany's demise during World War II, this communication works both ways; there is a need to 'cut through the technical stuff' and 'get to the essence of revenue and other business matters'. At the same time, CISOs require a degree of some technical nous to effectively implement and deploy a myriad of technologies across the security stack.

Boardrooms are not immune from this. One speaker said that while CIOs and CISOs must confidently relay the whole picture, the risk, the bad actors and their intentions, the boardroom must at least grasp the basics.

> *"I think the board should be challenged...to go away and do a bit of bloody homework. IFRS 17 is the new accounting standard [for insurance contracts]...I have to [do homework], I can't say, 'No, can we have five accountants in the room?"*

> *"You have to be able to say to your great paymasters, regardless of where they sit, 'you've got to go and figure out some of this for yourself'. You've got to be able to read through this subject."*

The same rule can also apply to line-of-business departments, from finance and HR to marketing, often not fully understanding the risk but all too quick to release products and services without security's purview. One speaker gave the example of a healthcare organisation which recently shipped an AI product; the first the information security heard of it was having seen the product in a TV commercial.

If the CISO's impact varies by their background, expertise and a clear two-communication, there's an argument that security maturity can also evolve through process and systems. As discussed here, some organisations have 'shifted left' towards SecDevOps and embedding security principles much earlier in product development lifecycles.

> *"We have to make security the responsibility of everybody in our business, and we're doing a lot of work to drive cross functional teams, value stream aligned teams, particularly in engineering,"* said one speaker. *"One of our approaches is we are creating an architectural landscape that's made up of experiences, capabilities, platforms and data."*

For others, driving security maturity has been about splitting security accountability across the business; in one such case, an organisation hired a head of resilience (who reports to board, thereby giving them ownership and accountability), a CISO, and - in IT - a head of security operations.

> *"That group will make sure the business knows the risk, the board knows the risk and then the IT team has to deliver on what budget they're given to remediate the risk,"* he said.

A far greater challenge remains security's achilles heel, or Churchill's questionable temper; getting C-suite alignment and action may be one thing, getting people to care is quite another.

As the speakers discussed here, security incidents have become somewhat normalised and desensitised, even through notable issues like the NHS Wannacry attack and the Crowdstrike incident.

Some have experimented with concepts of security advocates or champions in business units disseminating security awareness programmes and materials; others have taken the more draconian act of punishing those who fall foul of internal exercises, even deducting bonuses or requiring additional training. Take Microsoft which, following a Russia-based cyberattack last year, restructured its CISO leadership team, hired 34,000 full-time engineers to its new security reset and is now tying security work to employee performance reviews. Whatever the most effective approach, success comes back to repetition and making the training personalised and relevant to employees roles.

Geopolitical situation changes the risk register

For these business and technology leaders, the focus turns to threats ahead. Speakers around the table here noted that their risk register notes everything from ransomware-as-a-service and third-party supply chain risks to advancing multiple jurisdictional regulations and the double-edged sword that is Generative AI - already in cybercriminal armories, particularly for phishing attacks.

Remediation and post-crisis communication becomes increasingly paramount, not least given the varying successes of the British Library and - on the flip side - CrowdStrike, and a willingness for ‘pragmatism’ when it comes to debating platforms or best-of-breed solutions.

Perhaps taking inspiration from the maps room within Churchill War Rooms, from where Churchill anxiously tracked US ships crossing the Atlantic amid scurrying U-Boats, eyes also turn to the issue of localisation, the challenge of entering new markets and threats emerging from the East.

> *“We're looking at China – we're looking at what's happening, because it's not just data, it's all people as well. We look at security in totality so we’re looking at our strategy if there’s an issue, and what the response is.”*

Ultimately, for these business, technology and security leaders, engaging the C-suite comes back to appointing the right leaders, clear communication and expectations on both sides, positioning security as a bottom-line business enabler and a focus on embedding security across teams earlier - and into culture from the bottom-up. There should also be a realisation that change happens through people, and smart people, processes and systems will always beat throwing money at the money.

> *“Unless you can outspend the resources of a nation state who may be interested in targeting your organization, then you can't spend your way out of this problem, and therefore, it's not a problem solved by money,”* summarised one leader.

This Food for Thought was hosted by HotTopics in partnership with BT Business, as part of the Secure Tomorrow community.

BT Means Business