CRITICALEYE
The peer to peer Board Community

THE BOARD'S ROLE IN CYBER SECURITY

There is still a huge knowledge gap on Boards when it comes to the inevitability of a cyber-attack and the enormous damage it can cause. Criticaleye's **Bridgette Hall** talks to **Bill Payne** and **Reece Donovan** about what needs to be done

A cyber-attack can swiftly put an organisation on its knees, causing huge amounts of damage both reputationally and financially.

Cyber constitutes an increasingly serious business risk. Eighty-two percent of Boards or senior management within UK businesses rate cyber security as a 'very high' or 'fairly high' priority, according to the UK Government's 2022 Cyber Security Breaches Survey. However, only half of businesses say that they update the Board on cyber security matters at least quarterly.

A gap in knowledge in the Boardroom will leave an organisation at risk, especially as more people work from home as hybrid working becomes normalised in many sectors. "A lack of Board level expertise presented a significant barrier to securing the appropriate level of funding and driving the right action in terms of an organisation's overall cyber security approach," said the UK Government's 2022 Cyber Security Breaches report.

"I've come across numerous companies where the Board, not just the execs, but in particular the non-execs, are clueless about the real risk and intelligence of the cyber criminals. You wouldn't go on holiday and leave your front door unlocked, but in many cases that's what businesses are doing," says **Bill Payne**, a Board Mentor at Criticaleye and Non-executive Chair of Atento. "It's quite bizarre that people don't see this area as mission critical."

Bill's words proved truer than ever in 2022 with a string of high-profile cyber security breaches that included companies in healthcare and financial services, not to mention politicians.

> *" It's quite bizarre that people don't see this area as mission critical "*
>
> Bill Payne

"Cyber security is a business-critical consideration," says **Reece Donovan**, CEO of Iomart Group. "A strong cyber security strategy can set an organisation apart from the competition, but an approach that is not fit for purpose can bring an organisation down."

The scale of the threat continues to grow. Companies faced an average of 270 attacks in 2021, which represents a 31 percent increase over 2020, finds research by Accenture. The costs of these attacks are also rising, with the global price-tag expected to reach as much as $10.5 trillion annually by 2025.

Without a clear cyber strategy in place, most organisations are simply sitting ducks. Bill explains: "At the moment criminals are finding it really easy because they've developed software that scans multiple corporate systems, multiple connected systems, third-party systems and can detect where the vulnerabilities are. And they're able to because of the lack of education in a lot of companies and lack of real-time attack vulnerability. Phishing emails through customer services, which can impregnate corporate systems with ransomware code, are a real issue."

Bill, who is also a NED of RoomRocket, a US VC-backed hotel platform, admits to being a bit of tech junky and says: "The lack of knowledge and active questioning at Board level is a bit frightening."

From a Board perspective, a robust strategy needs to be both in place and reviewed regularly. **Reece** adds: "When the risk could impact every level of a business, it's important that those dealing with it are at the very top and have the authority and a sufficiently broad understanding of the business to act."

Both **Reece** and **Bill** agree that the CEO needs to be on top of cyber security. "If someone gets into your infrastructure and shuts you down with sophisticated ransomware, you don't have a business," says Bill. "The costs can be frightening. IT repair, lost customers, lost revenue, lost credibility, lost reputation, corporate fines, higher insurance, ransomware – yes some choose to pay it –, and for some it will mean the end of the road."

The danger is for Boards to defer the finer details of a cyber security approach to their IT teams – in the case of larger organisations – or third parties and external providers in the case of smaller organisations. It's crucial to have non-executives who, while not necessarily experts in IT, still have the knowledge and experience to know what questions to ask. >

"Most companies have an Audit and Risk Committee," says **Bill**. "Audit and risk aren't just about audit and financial risks, it's about business, reputation, and IT risk." He states that this Committee needs to ensure the Board is fully educated around any weaknesses when it comes to cyber security.

"So that the Board is fully aware of the risks and working with the CEO to increase cyber security budgets because in most companies it's an underspend, and an underspend is always going to leave you vulnerable. And the issue is that the virtual crooks get smarter every day and their entire lives are devoted to breaking into your corporate house and extracting data and ransom."

Moreover, he says, "Understand what your vulnerabilities are, when you're going to fix them and how you're going to fix them. Then, put a structured response and communication plan in place when you do get attacked, because you will be."

Reece agrees with this and notes the importance of a joined-up, holistic approach. "Identifying and mitigating business risks requires input from teams across an organisation. And, of course, there are all the employees who are using systems and accessing networks on a daily basis," he adds.

"Security, and the associated risks to the business, need to be understood across the entire organisation, and making it a Board issue sets the tone from the top and prevents it from becoming a siloed responsibility of one team or function."

> *"Cyber security is a business-critical consideration"*
>
> Reece Donovan

Just like reading a balance sheet, Boards should be reading IT risk sheets. This entails looking at a risk map of the vulnerabilities of the technology systems and asking questions such as:

- When was the last penetration test?
- What did it reveal?
- What are the vulnerabilities in all our systems?
- What insurance cover do we have in place?

"Your response and communication plan is critical to manage your recovery and reputation. The Board should be satisfied that there isn't just a detection and prevention plan in place but a prediction plan as well," adds **Bill**. "The other thing is – what is your risk response and reputation plan? What have you done to set up a crisis centre to deal with an attack?"

This often includes having external consultants and negotiators lined-up, as criminals may demand large payments to stop an attack.

"Increasingly, breaches are a case of when and not if," confirms **Reece**. "So, once an organisation has decided what its crown jewels are, it needs to develop a recovery plan for when a breach does occur. Often recovering quickly is more important than investing huge amounts in building a wall, which will never be impenetrable – so finding the balance is key."

Whenever cyber security is discussed, one of the most fundamental points holds true: staff education – knowing not to click on links, spotting phoney email addresses and flagging any suspicious messages.

"We have to put more time, effort and resource into educating all our staff as to what fraudulent, and criminal behaviour looks like, what cyber-crime and cyber-attacks look like, what they need to do to prevent them and the reporting to make sure the systems are secure," says **Bill**. ■

Featuring Commentary From:

Bill Payne

Bill is the former Non-executive Chair of Atento (NYSE), one of the world's top five largest providers of customer relationship management and business process outsourcing services, the leader in Latin America, as well as a leading provider in the United States. He is also NED of RoomRocket, a US VC-backed hotel platform. Prior to his portfolio career, Bill was a senior executive at IBM.

Reece Donovan

Reece is CEO of Iomart Group plc, a Glasgow-based information technology and cloud computing company. He has a demonstrable track record of achievement in roles both in the UK and internationally. Before joining Iomart Group, Reece was Group CEO at Nomad Digital, a global provider of passenger and fleet-connectivity solutions to the railway industry.

Contact the contributors through: www.criticaleye.com