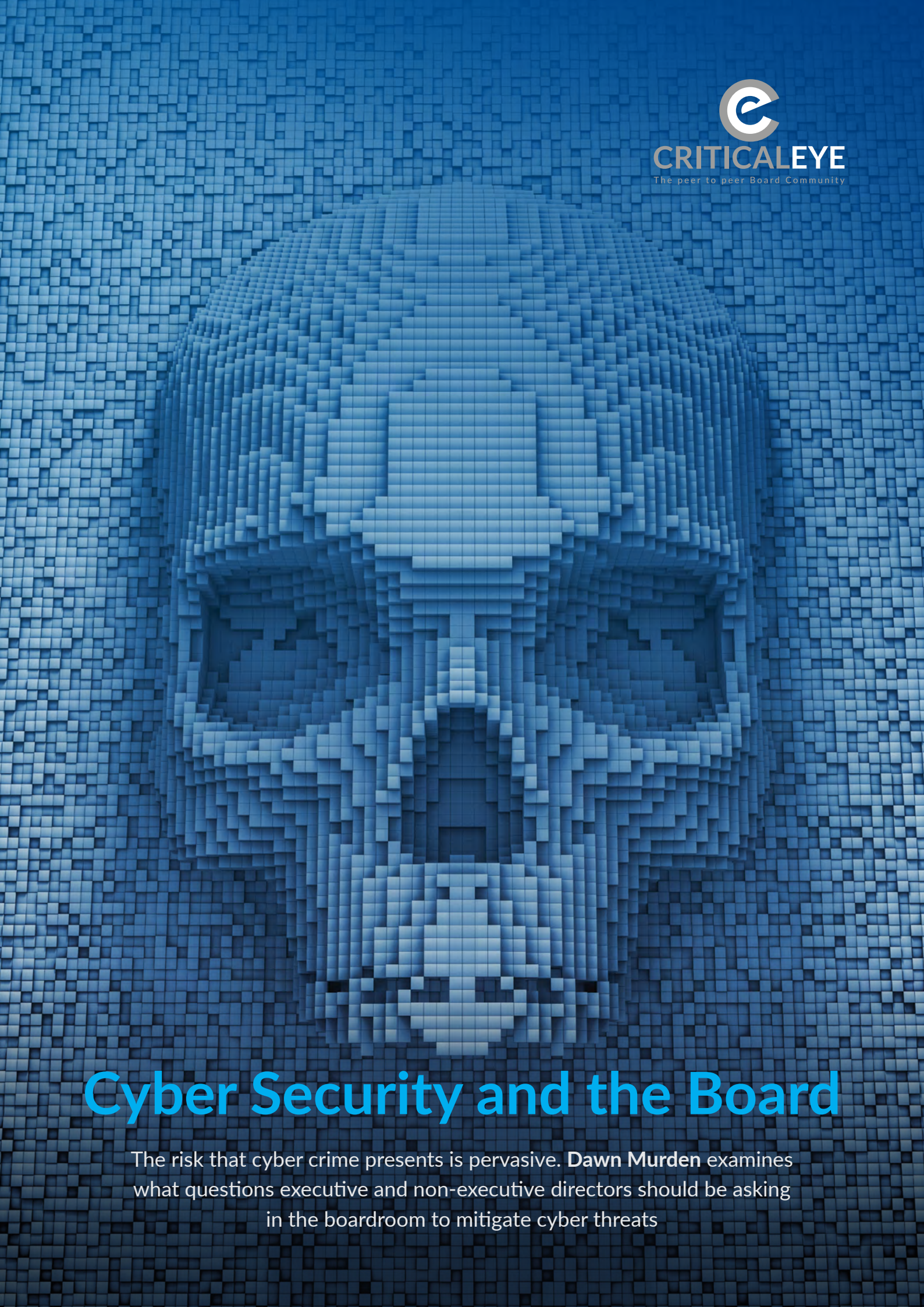

CRITICALEYE
The peer to peer Board Community

Cyber Security and the Board

The risk that cyber crime presents is pervasive. **Dawn Murden** examines what questions executive and non-executive directors should be asking in the boardroom to mitigate cyber threats

You don't have to be in the midst of a cyber attack to know that it should be at the forefront of your mind right now. The reality is that no company is immune to hacking and executive and non-executive directors need to address cyber risks thoroughly by asking the right questions.

Last year, TalkTalk was victim to a significant attack on its website, with fears that customers' bank details were hacked. Also in August 2015, the personal details of 2.4 million Carphone Warehouse customers were reportedly compromised by cyber criminals.

Both incidents created a storm in the press and the companies are yet to determine how much reputational and monetary damage was caused.

The problem is far-reaching. According to the latest data from the UK Government's Department for Business, Innovation and Skills, 81 per cent of large corporations and 60 per cent of small businesses reported a cyber breach in 2014, with the worst costing between an estimated £600,000 and £1.15 million.

"We're seeing some very sophisticated attacks on critical infrastructure. It's no longer a matter of just covering the basics," says **Justin Lowe**, Cyber Security Expert at PA Consulting Group.

The board must be asking the right questions to mitigate risks, **Justin** adds. "They need to be gaining confidence that their organisation has a good grip on what personal and sensitive information it holds. Then they need to build confidence in shareholders and stakeholders that they are adequately protected," he says.

"We're seeing some very sophisticated attacks on critical infrastructure. It's no longer a matter of just covering the basics"

Criticaleye spoke to seasoned business leaders to reveal the top five cyber security questions they're posing in the boardroom:

1. Which of our assets, if breached, would have the biggest impact on our business?

According to **Paul Brennan**, Chairman of OnApp, a board needs to define the company's most valuable assets. "Every board director should be asking how they can protect the assets of their business, clients, customers, partners and employees," he says. "Inevitably the more we enable people to interact and transact in an online world, the more we expose their data to attack."

You need to think about all the different threats the company faces, says **Crawford Gillies**, Non-executive Director at Standard Life and Barclays, and Chairman of Control Risks. "It might be intellectual property, or strategic plans, or customer information," he adds.

2. Do we think our protection mechanisms are proportionate and accurate?

By starting with the assets and their value, boards can then look at what defences should be in place. **Justin** comments: "So many times I hear security managers say: 'I've proposed this but it never got approved.' You need accountability at board level to support those important investment decisions."

Paul notes that a lot of companies now have their chief information officer on the board. "They can't just be someone who is coming to the board to present. They need to understand the strategic goals and imperatives of the business… and as a peer, be held to scrutiny about what is being done to control risks."

There should be an assessment of the vulnerabilities and a clear strategy to defend them. **Alastair Lyons**, Chairman at Admiral Group, says: "One would expect a presentation to include the standard protections, such as penetration testing, encrypting, locking down laptops and having very limited access of company devices to the internet."

3. Are we adequately prepared to respond to a security breach?

When it comes to cyber attacks, boards should think in terms of 'when', not 'if', notes **Sarah Bates,** Chair of St James's Place. "All of us, both privately and [in a business environment], rely to a greater or lesser extent on the internet, which was designed to be open and [as a result] can be vulnerable. There are many people with harmful motives who are very clever and determined, >

seeking to use the internet as a back door into our lives," she adds.

There should be clearly established protocols for reaction to a cyber attack, both in terms of internal actions and external communications.

COMMUNITY COMMENT

TalkTalk's cyber security incident reported on their website in October provided an interesting snapshot of the regulatory environment that all European businesses may face shortly. As a telecoms provider, TalkTalk is subject to breach notification rules – the obligation to proactively confess to regulatory authorities in the event of a serious data breach. EU laws are set to change soon and may require all companies to disclose details of such breaches, potentially to both regulators and to affected individuals.

That will be quite a substantial departure from the current legal position. In the UK, breach notification requirements outside of regulated sectors such as financial services and telecoms, are framed much more loosely.

This is coupled with significant increases to the maximum fines that can be imposed by data protection regulators (four per cent of worldwide turnover for breach of security notification laws) and increasing press interest in cyber breach stories, businesses need to plan now how they will meet the new standards that will be expected of them.

James Mullock
Partner
Bird & Bird

Alistair comments: "In the event of an attack there may be need to inform customers, suppliers, regulators and the media; who should do what, how and when? There should also be a realistic assessment of the cost, in particular the reputational damage.

"Similarly, if a hack disables the company's systems it should have a disaster recovery programme in place. How fast can it get itself working again? How up-to-date and reliable is that backup?"

4. Do we have a suitable risk culture?

The weakest link is often the people, not the systems, says **Jeremy Lloyd**, Chief Technical Director at ICSA Software International.

"Board-level executive sponsorship is vital. The executive in charge will need to ensure a cohesive strategy is adopted across a variety of departments, such as IT, Risk and Compliance, and HR," **Jeremy** continues. "Most importantly this person must be able to break through the traditional departmental boundaries to execute cross-organisational culture change."

Crawford notes that companies are putting more emphasis on risk culture, especially those in the financial services, which are under regulatory pressure.

"Focusing on the technological barriers is necessary but not sufficient, which takes you to the whole issue of risk culture," he explains. "How do you get people to be aware of cyber risk at all times, particularly those with access to valuable data or valuable assets?"

5. Are we constantly improving our understanding and implementation of cyber security?

Boards should discuss cyber security at least on a quarterly basis and every board report should have a risk update and commentary of assurance.

Jeremy comments: "With the significant number of cyber breaches this year it's clear that, even in these modern digital times, organisations are not properly taking account of the potentially devastating effects on their share price, reputation, and especially customers. It should be a top five item on the risk register." ■

Featuring Commentary From:

Sarah Bates
Chair
St James's Place

Paul Brennan
Chairman
OnApp

Crawford Gillies
NED
Standard Life

Jeremy Lloyd
Chief Technical Director
ICSA Software International

Justin Lowe
Cyber Security Expert
PA Consulting Group

Alastair Lyons
Chairman
Admiral Group

Contact the contributors through:
www.criticaleye.com