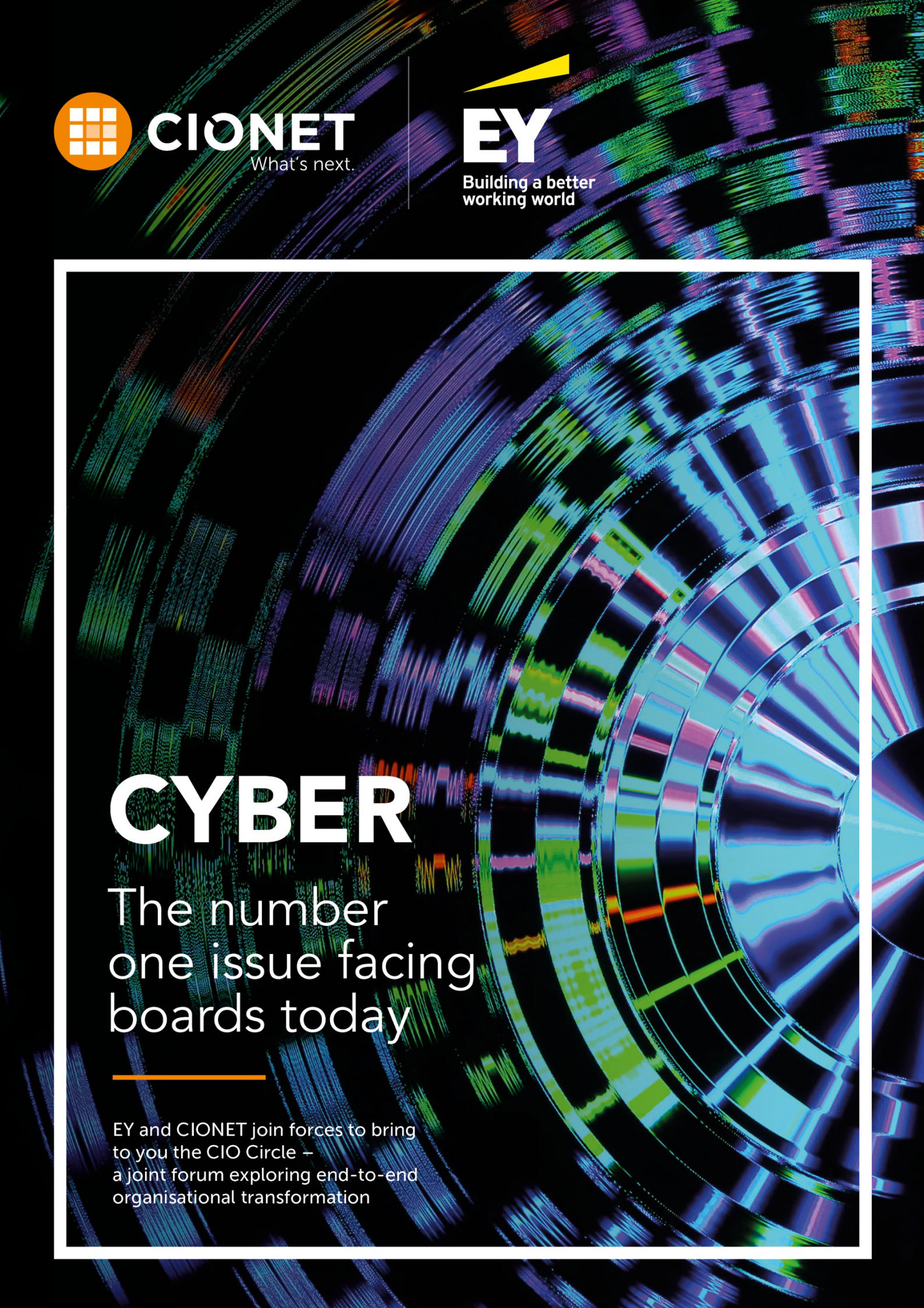
CIONET
What's next.

EY
Building a better working world



CYBER

The number one issue facing boards today

EY and CIONET join forces to bring to you the CIO Circle – a joint forum exploring end-to-end organisational transformation

Cyber: the number one issue facing Boards today

EY and CIONET have joined forces to bring you the CIO Circle – a forum exploring end-to-end organisational transformation

*This article was written by **Roger Camrass** research director of CIONET International, and is based on the conversations held during a virtual event in December 2021 entitled 'Assessing the business implications of Cyber-attacks – is the board fully engaged? This event was the first in a series of business focused discussions under the title of the CIO Circle.*

Over the last two years through the pandemic the cyber threat landscape for criminal and state sponsored actors has expanded dramatically. Countries such as China, Iran, North Korea and Russia have exploited western vulnerabilities by stealing billions of dollars of intellectual property, disrupting manufacturing and utilities and closing down administrative systems. Consequently, Cyber has risen to the top of the agenda for both government and business leaders.

What are the lessons learnt in recent months?

Our discussion evening commenced with an overview by Gavin Cartwright, Partner, EY UK&I Cyber Security Lead. His advice to CIOs, CISOs and other members of the 'C' suite included:

- Be prepared for a cyber attack by identifying who is on-point to deal with this, and by rehearsing the processes required to mitigate consequent damage
- Ensuring that your supply chain partners are part of any Cyber 'war room', and understand their respective responsibilities prior to and during an attack
- Monitor conditions with the right data, cyber skills and tooling to avoid any surprises, especially as many attacks go undetected for weeks or months
- Learn how to segregate different networks (such as IT, operations, manufacturing) in a world of blurring digital boundaries
- Incorporate cyber into business continuity planning exercises and corporate risk registers

His main observation was that Cyber has risen from a technical to a strategic discussion, involving not just the IT community but all members of the 'C' suite. It is first and foremost a business issue.

A new context for cyber attacks

All delegates recognised that we are moving rapidly into a hyper-connected economic system characterised by hybrid working, interlocking supply chains and complex ecosystems. At the same time, business models are evolving into digital structures with the blurring of functional and organisational boundaries. Cloud and software as a service have accelerated such trends and accelerated a new era of 'Zero Trust'.

The pandemic has encouraged many of our social, domestic and work activities to migrate online. Families as well as organisations have become key targets for cyber criminals. State actors have invested billions in trying to disrupt our social order in the West. In the words of a leading defence CIO, 'we are at war'. The foundation of the National Cyber Security Centre illustrates the criticality of this new era of warfare.

As we look ahead, we see growing numbers of connected products as well as connected organisations. For example, the Tesla car generates petabytes of information. Such data has

increasing commercial value both to the manufacturer and customer. All parties need to be protected from cyber-attacks and property theft.

What are our greatest points of vulnerability?

Much of the discussion centred around the supply chain. In today's digital environment this encompasses both the movement of physical goods as well as adoption of digital services such as HR, Finance and CRM delivered over the web as Software as a Service (SaaS). The Cabinet Office mentioned the long tail of small IT vendors anyone of whom could become an active source during a cyber-attack. This calls for a wide span of attention encompassing thousands of ecosystem partners.

For companies such as Diageo, CODA, BP, BT, GSK and others involved in research, manufacture, distribution and sales, the points of vulnerability have increased dramatically in recent years and have raised impact levels to include IP theft in research, supply chain disruption including the shutting down of manufacturing and operations, ransomware attacks on office systems that can close down all communications.

How best to mitigate cyber-attacks at the business level?

Given the increasing scope and impact of such attacks, the delegates described a range of activities designed to enable business continuity:

- Scenario planning to explore different types of attack and their consequences for business performance such as impact on profit, revenue and brand
- Optimising investments in cyber mitigation by allocating priorities that align with business outcomes
- Rehearsing cyber-attacks by closing all communications channels and invoking a state of emergency
- Improving cyber literacy amongst all front-line workers, recognising that this will be your first line of defence

Delegates agreed that constant communications and training were essential components of a cyber defence strategy. Tuning the corporate culture towards cyber is a board-level initiative.

Where to apply corporate governance

Some of the delegates were from health and education where organisations such as the NHS and Universities are widely decentralised as well as being high priority targets for state actors. The consensus was that a higher degree of corporate governance is required to enable such bodies to prepare for attacks. This includes more standardisation of critical processes and particular attention to legacy systems.

Today government has billions of dollars of legacy mainframes and software packages in service reaching back to the seventies and eighties. These systems are soft targets for attack and need to be carefully insulated at their perimeters to avoid disruption to national services, for example benefits, tax and health. Treasury has allocated large sums of money in 2022 to address the legacy issue.

What can we do as digital leaders?

Given the central and growing importance of cyber at board level, delegates discussed several initiatives to ensure effective communications and collaboration with the 'C' suite:

- Joint (business and IT) planning exercises to explore, simulate and rehearse cyber attacks across the organisation in 2022
- Review the corporate risk register to ensure that cyber is correctly represented and appropriate funding is allocated
- Share supply chain issues with members of the business ecosystem and identity points of responsibility within the chain