CIONET UK COMMUNITY PROGRAMME 2024

WHAT MUST BOARDS DO

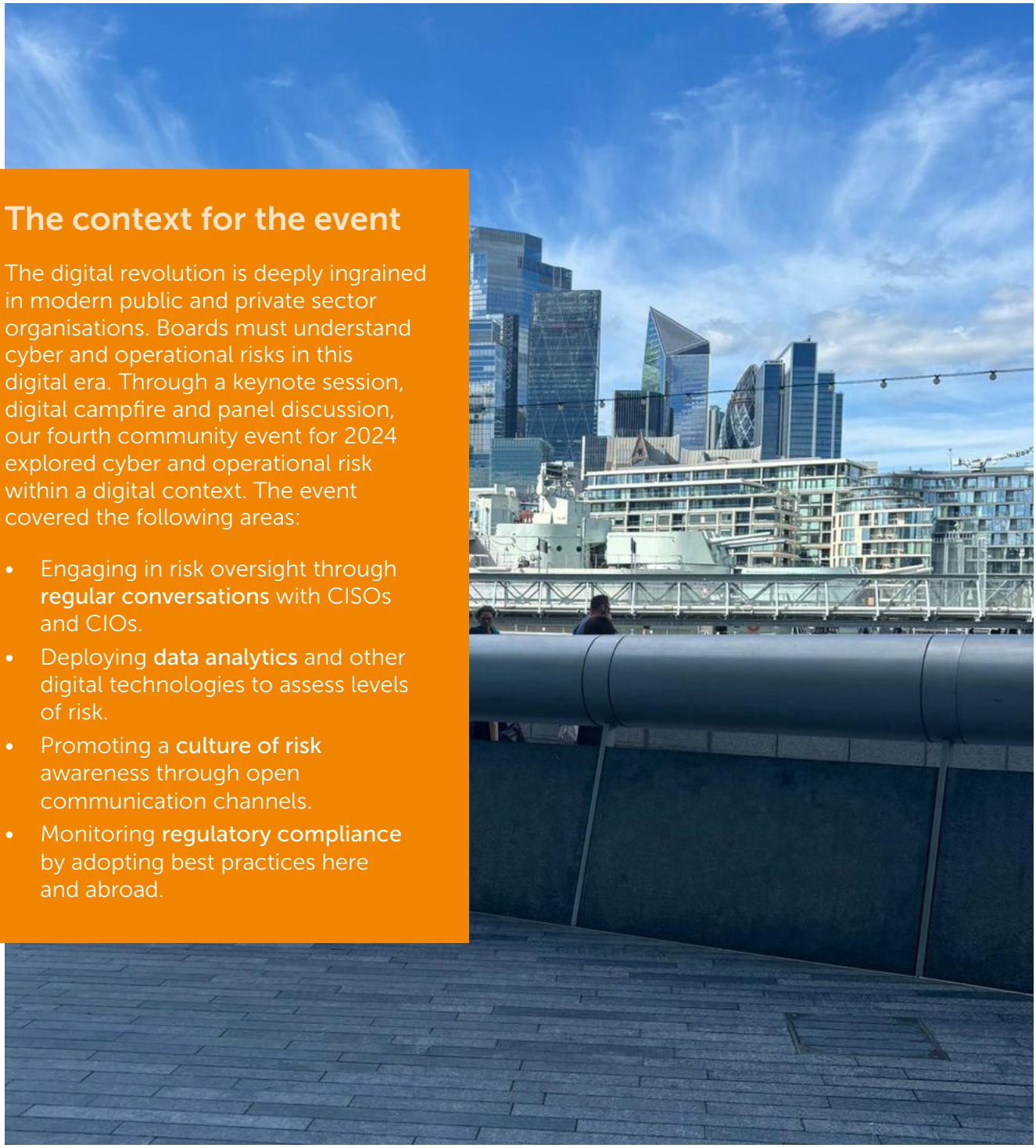
TO MANAGE CYBER AND OPERATIONAL RISK?

Roger Camrass
CIONET UK

Discussion Documents June 24

WHAT MUST BOARDS DO TO MANAGE CYBER AND OPERATIONAL RISK?

This article was written by Mark Samuels, Chief Editor at CIONET UK, and Roger Camrass, Director of Research at CIONET International. Designed by Sebastian Hartland, Art Director. The content is based on CIONET UK's Fourth Community Event of 2024. The event was held on 19 June at EY, 1 More London Place, London.



The context for the event

The digital revolution is deeply ingrained in modern public and private sector organisations. Boards must understand cyber and operational risks in this digital era. Through a keynote session, digital campfire and panel discussion, our fourth community event for 2024 explored cyber and operational risk within a digital context. The event covered the following areas:

- Engaging in risk oversight through **regular conversations** with CISOs and CIOs.
- Deploying **data analytics** and other digital technologies to assess levels of risk.
- Promoting a **culture of risk** awareness through open communication channels.
- Monitoring **regulatory compliance** by adopting best practices here and abroad.

Session One: Sanjeev Kaul, Managing Director Randstad Digital UK and Head of Service Line & DTC Engagements Europe at Randstad Digital

Roger's chat with Sanjeev centred on five questions:

1. What business areas are most susceptible to cyber and operational risk?

Sanjeev said modern businesses have multiple interfaces to defend. Randstad Digital works with thousands of people across remote sites. Applications, data centres and cloud provisions must be secure. Randstad practices a secure-by-design approach, which can restrict how employees work. However, boards must recognise it's better to be safe than sorry.

Sanjeev explained how ransomware attacks have a lasting impact on customer perceptions. The operational challenges from an attack can be huge if your systems go down. The financial impact can be significant because your organisation has to clear the rubble and start again. However, he believes the biggest impact of a cyber incident is trust in your brand.

2. What risk factors must boards consider and at what frequency?

Sanjeev acknowledged a range of political, economic, social and technical factors. Boards deal with a host of rules and regulations. The rise of AI-enabled cyberattacks is another factor. Wider macroeconomic conditions make it tough for companies to decide where to prioritise their spending. Should they invest in growth, cyber protection, or something else?

Executives must understand their technology stack. Randstad staff receive clear leadership direction every quarter. Potential cyber threats are broadcast regularly. Protecting your infrastructures, applications and devices requires strong investment. Businesses face an ever-evolving fight and we must help the good guys win.

3. What direction do you receive from the global supervisory board?

Sanjeev said Randstad's CEO has a strong understanding of cyber. Unlike many other companies, Unlike some companies, Randstad doesn't sell products but focusses on services. The company's priority is bringing talent to its customers and the firm ensures they work within the cybersecurity norms set up so as not to be exposed to risk from various attack vectors.

The board understands and prioritises cyber risk. Randstad uses its secure-by-design approach to keep clients informed of risks. The company deals with big-ticket items, such as cloud services and applications. Users who don't update their operating systems quickly can't use their devices. This approach instils discipline.

4. How much support do boards need from IT staff, including CIOs and CISOs?

It's important to prioritise investment in security over business-as-usual activities. The good news is cyber is a big area of investment for technology firms, particularly start-ups. However, cyber is also a fast-evolving area. CISOs and CIOs must invest in cyber, stay vigilant, keep people updated, and ensure staff act on these advisories. Cybersecurity is a habit.

5. How can you place a positive spin on operational risk factors?

Be honest. If you've done something wrong, let others know. Be upfront and break the news. People won't enjoy hearing that something has gone wrong but you won't lose trust. Also, be transparent. Provide reports to the board that show how you're keeping people safe. Push this information out proactively.

Digital Campfire session: Gavin Cartwright, Partner at EY, and Jonathan Lloyd White, Group CISO at Natura & Co

Roger convened an interactive session with four questions:

1. What are Natura's main areas of business and risk?

Natura is a cosmetics giant that employs six million sales representatives globally. The company collects raw products sustainably and undertakes research and development. The processes are part of a sustainability cycle where the company aims to protect the rainforests. Natura owns Avon, a company with a 100-year-plus history that helps women establish micro-businesses through a direct sales and distribution system.

Jonathan takes an all-encompassing approach to cybersecurity that spreads from the internal corporation to the extended ecosystem, including Internet of Things technologies. Natura has a highly connected ecosystem that includes disparate vendors and a huge amount of data and protocols. The key to success is driving change across cultures and languages.

2. How and when should CISOs communicate security challenges to the board?

Gavin suggested the nature of risk has changed and businesses now take a more mature approach to operational technology (OT). This focus is because companies recognise the risk of outages. Five years ago, managing risk was all about data. Today, there is a broad understanding that an interruption to OT means the business stops. However, managing OT risks is difficult in organisations where accountability is murky.

Jonathan said CISOs should see the opportunity to communicate security challenges to the board as a privilege. During his career, he's approached the conversation on a long-term basis. He looks to build the cyber agenda across four or five sessions. He advises other CISOs to give their board a sense of direction. Create a two-way contract. Make the board more confident about security and encourage them to challenge you.

3. How can frameworks be used as part of the communications process?

Jonathan said frameworks are important. Pick a framework and set your expertise within the context of recent risks. Don't rely on three-letter acronyms and complex language. Make security easy. Don't be afraid of teaching and educating.

Gavin agreed that frameworks are useful. However, build the board's understanding of the challenges. You have to answer the 'So what?' question. CISOs have a lot of data and must explain insights in business terms. Articulate the security risk effectively.

Roger asked Sanjeev for his opinions. He recognised the importance of the 'So what?' question. He said CISOs must quantify the risk of exposure. Explain what will happen if the business can't operate. Take the board on a journey. Make them understand the impact of business interruption.

4. Who should CISOs report to?

Jonathan said the executive reporting relationship must be right. Regardless of who you report to as CISO, your relationships must be characterised by autonomy and openness. CISOs need the independence of mind to report good and bad news.

However, Gavin said annual security budgets are tighter for the first time. The board is questioning the need for further spending. It's also hard to quantify the return on investment from security spending. A security-by-design approach means creating visibility. Take the board through simulations. One of Gavin's clients showed how risks could lead to millions of pounds of damage. Demonstrate how an investment in security produces visible results.

Panel discussion

Roger interviewed each of our expert panellists in turn:

- **Maureen Wedderburn**, Chair of Medicines, Manufacturing Innovation Centre – CPI)
- **Felipe Peñacoba Martinez**, CIO & Management Board Member – Revolut Bank UAB
- **Sumit Mehra**, Chief Operating Officer - Global Captives & Insurance Management Solutions and GRE – Willis Towers Watson
- **Ilona Simpson**, Executive Advisor & CIO – SoSafe

Maureen Wedderburn, Chair MMIC Supervisory Board at CPI

1. What are the operational and cyber risks associated with the pharma sector?

Maureen said the supply chain challenges in pharma are not that different to other sectors and regulatory issues persist. There are many checks and balances because of the potential consequences of supply chain problems. She referred to the importance of 'never' events. For the pharma industry, those events are about running out of medicine.

Executives in the sector must work with supply chain colleagues to build stock and avoid 'never' events. Success is all about contingency planning and practising scenarios. Take the board through scenarios to show the potential dangers of something going wrong.

2. What reactive strategies can help companies to rectify risks?

Work out the biggest thing that will help your business ensure its supply chain stays operational. You should also use technology to protect and recover data. You must have expert teams ready for a worst-case scenario. When Maureen ran operational teams, she placed experts around business functions to ensure recovery plans could be enacted.

3. What advice would you offer to CIOs to help their boards manage risk?

First, you're not in this fight alone. Your board are as accountable for any risk as you. If they don't understand the risks, educate them. Second, make the business implications of an impact clear. Third, success is not just about proactivity and you must react quickly. Practice and learn constantly. Use modern context so your preparations aren't out of date.

Felipe Peñacoba Martinez, CIO & Management Board Member at Revolut Bank UAB

1. What is uppermost in the minds of board members about operational and cyber risk?

Felipe said his firm focuses on the risks of cyber disruption as it is a digital business. Don't focus on technical details. Instead, focus on business metrics. Your board should be aware of the risk to reputation. No one wants to end up on the front page of the FT. Use that threat as a lever for investment. The cost of an attack is another lever. Get the board to understand how much the company will lose if it can't process transactions.

2. How much time should CIOs spend with the board on cyber issues?

He said the digital nature of Revolut means key risks are considered continually. Regulations, particularly in a highly governed area like finance, can help raise the spectre of risk. Your business should constantly analyse and test its digital foundations. Ensure your board is aware of risks to these foundations, too.

3. How can you build expertise within your team to mitigate risks?

All business leaders recognise that security talent is in high demand. There's no magic recipe for attracting talent. However, it's important to build a reputation. Ensure your company is attractive to talented professionals. For up-and-coming talent, an understanding of AI and data will make you an appealing candidate.

Sumit Mehra, Chief Operating Officer - Global Captives & Insurance Management Solutions and GRE at WTW

1. Do boards recognise the full extent of cyber risks?

The cyber-insurance market is growing rapidly but still represents less than 1% of the global insurance market. The good news is there is more awareness of cyber and operational risks today. He said executives are concerned with fiduciary responsibilities, potential impacts on clients and advice for identifying and dealing with risks. He said boards are more interested in control if they think there's a financial impact.

2. Do CIOs fully understand the financial metrics of risk?

There's more maturity today than in the past. CIOs and CISOs know there's a risk something bad will happen. They want to ensure the business has the right strategies in place. Sumit's business helps CIOs run simulations. They have a suite of analytical tools to quantify operational and cyber risks. CIOs share their views and work with forensic accountants to run business calculations. They can use these estimates with their stakeholders.

Ilona Simpson - Executive Advisor & CIO at SoSafe

1. How can CIOs and CISOs help the board engage in more conversations about risk?	Ilona encouraged attendees to pat themselves on the back to recognise the hard work they've already achieved. The complexity continues to grow. CIOs and CISOs must speak the language of the board. That communication process starts with operations.
2. What capabilities and tools should be in place to deal with risk?	She said a plethora of tools are available. CIOs must be better storytellers. Move away from focusing on technological tools and towards a language the business can understand. She encouraged CIOs and CISOs to start with a common-sense approach. The world is complex, so help the board to identify its top three assets and threats.
3. What form of corporate governance will ensure risk ownership is in the right place?	Ilona said regulation continues to be unveiled, including the Digital Operational Resilience Act and The EU's AI Act. The onus is on CIOs and CISOs: tell the board about the risks so they listen. They can't 'unhear' what you tell them. Educate them about risks.

Conclusion: Five key takeaways

Attendees asked a series of questions to the panel about the following issues: best-practice approaches to AI, the challenges of relying on cyber-insurance policies, the risks associated with paying (or not paying) ransoms to hackers, making the board appreciate the risk of dealing with third-party partners, and managing human-based risks. Roger then concluded the evening. There were five key takeaway points:

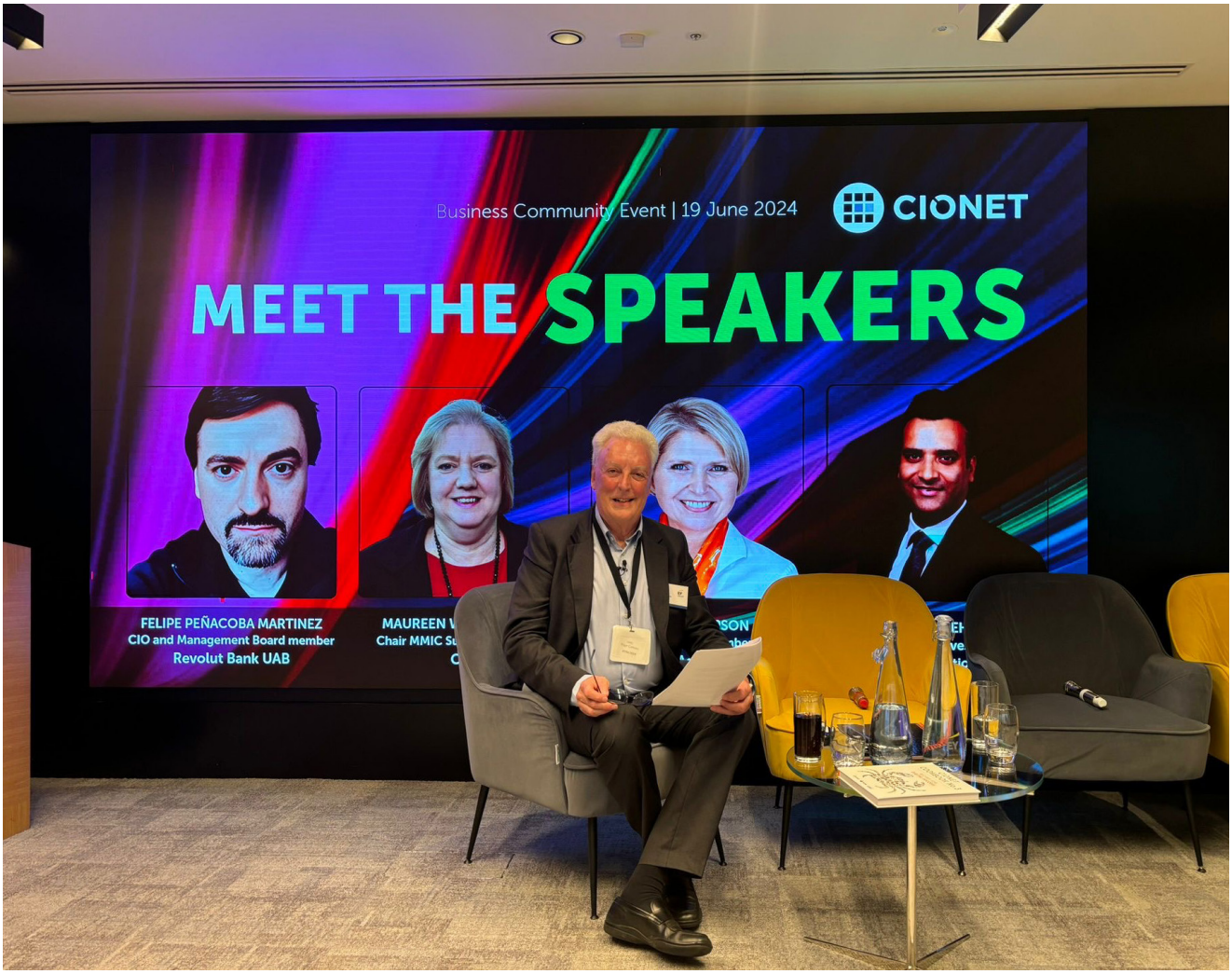
1. **Understand business parameters** – CIOs must know about cash flow, balance sheet, and EBITDA. Understanding business issues boosts your board-level communications and ability to secure cash for cybersecurity projects.

2. **Know your supply chains** – Take a broad view of your physical and digital resources. Building a digital twin of operational activities is fast becoming the norm. Assessing risk with third-party partners is tough but critical.

3. **Education is a two-way street** – Boards must become familiar with technologies. CIOs must become more familiar with operational and financial concerns.

4. **Prepare for the worst** – Scenario-planning activities are a powerful way of preparing proactively and reactively for when things go wrong. These activities can also help educate senior managers on the dangers of an attack or disruptive events.

5. **Trust is the key to success** – Significant disruptions can destroy trust and ultimately undermine business confidence. This lack of confidence can impact your customers and other third parties, such as investors.

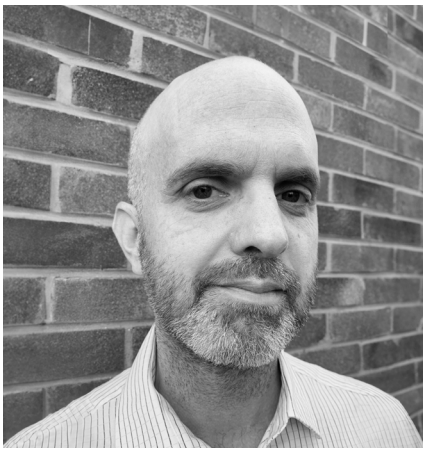

Business Community Event | 19 June 2024
CIONET
MEET THE SPEAKERS
FELIPE PEÑACOBA MARTINEZ
CIO and Management Board member
Revolut Bank UAB

Authors

Roger Camrass
Researcher Director

A pioneer of today's Internet as an ARPA research fellow at MIT in the seventies, Roger has spent over fifty years helping corporations harness the power of new technologies such as AI, cloud, mobile communications, e-commerce, voice recognition and satellite. He was a partner at EY responsible for e-commerce during the dot.com boom. He is a Cambridge University and MIT graduate and a visiting professor at the Hebrew University in Jerusalem.

See **rogercamrass.com**



Mark Samuels
Chief Editor

Mark is a business writer and editor, with extensive experience of the way technology is used and adopted by CIOs. His experience has been gained through senior editorships, investigative journalism and postgraduate research. Editorial clients include the Guardian, The Times, the Sunday Times and the Economist Intelligence Unit. Mark has written content for a range of IT companies and marketing agencies. He has a PhD from the University of Sheffield, and master's and undergraduate degrees in geography from the University of Birmingham.

Email **mark@samuelsmedia.co.uk**

Our partners