EY AND CIONET FEMALE LEADERS FORUM

MANAGING BOARD RESPONSIBILITY

FOR CYBERSECURITY AND RISK

Roger Camrass
CIONET UK

Discussion Documents May 24

MANAGING BOARD RESPONSIBILITY FOR CYBERSECURITY AND RISK

Summary

This is a summary of the second Female Leaders Forum event held at Balthazar in London and sponsored by EY and CIONET. Lopa Ghosh, EY UK Cybersecurity Leader and Partner, introduced the event. She explained how the event creates a safe space for women to network and talk about technology. Lopa introduced Maureen Wedderburn, Non-Executive Chair on the Medicines Manufacturing Innovation Centre Supervisory Board and former CIO at GSK. Maureen invited other attendees to give a brief introduction. Attendees said potential topics of interest included dealing with cyber challenges, creating and structuring an IT security team, defining cyber in the right language, maintaining data integrity, and building networks. Lopa discussed forthcoming cyber legislation, and Maureen drew on her wide-ranging experiences to provide context. Attendees then discussed a range of topics, including:

- Recognising the role of legislation and educating the board
- Managing cyber threats and investing in protection
- Understanding the variability of risk and using cyber insurance
- Dealing with accountability and inclusion in a digital era

Key points from the discussion

Recognising the role of legislation and educating the board

The Cyber Code of Conduct is out for consultation in the UK. This code changes how organisations think about cybersecurity and places new pressures on CISOs and the board. The Code means the board is now culpable for cyber threats and damages. This new level of accountability means boards must think carefully about cyber. They'll look to CISOs and other IT leaders for education and leadership in the security space.

Evidence suggests boards are already willing to invest in security across five key areas: risk management, cyber strategy, upskilling the workforce, incident response and planning, assurance and oversight. But digital leaders should also be aware that boards aren't necessarily aware of the fine details of the Code and its legal and financial ramifications. Find something critical to the business that emphasises the risk of not focusing on the Code.

Use language the board understands. Don't talk about bits and bytes. Talk about risks, costs, efficiencies and revenues. Deliver a message that shows your credibility. Show the board how an attack, such as at a production facility or a service centre, could mean downtime and a big revenue hit. Show how a data leak could lead to legal penalties and financial ramifications. Submit information and data points to the board that build awareness.

Also, use the code as a lever for investment. The cyber risk is only going to increase. There is an inevitability to a cyberattack that the board must understand. Attackers get smarter and their techniques evolve. Think of the impact of new risks powered by artificial intelligence (AI), whether using new hacking techniques or deep fakes to con professionals into transferring cash to errant actors.

Managing cyber threats and investing in protection

An investment in technologies and practices, such as proactively patching systems, building firewalls and monitoring incidents, can help to keep errant individuals at bay. However, CISOs and their IT peers should also remember that an effective cyber response is all about building accountability and supporting a culture shift across the organisation.

Remember the vast majority of attacks result from human rather than system errors. Business continuity plans are limited in their scope and applicability. Educate the organisation and show people how to respond to circumstances. Develop a capability to respond through exercises. Show people how they should react in an emergency. Use training sessions and show employees, for example, how a phishing incident might take place.

Also, remember that the cyber-education journey varies by department and country. Modern businesses are collaborative. People work across functions and boundaries. Some places and professionals will have a low level of awareness. You're only as strong as your weakest link. Take a global approach to security and then tailor your approach to local conditions.

Understanding the variability of risk and using insurance

There is a split between the value of customer and commercial data. The threat from a public sector organisation losing personal data is greater than a private enterprise losing supply chain information. However, all organisations suffer a hit to reputation from a cyber incident. UK-registered companies must comply with the Code. Remember that companies are not allowed to pay a ransom to hackers.

Perception is everything. It was suggested at the event that companies perceived to have responded effectively to a cyber incident could see a boost to the bottom line by as much as 7%. Companies that don't respond effectively could lose 15% of their share price. It's those kinds of numbers that will help CISOs prove the value of proactive cybersecurity to boards.

Cyber insurance can be used, but insurers will only pay out if the attacks meet certain criteria. Be transparent, look for weak spots and show what you can't do. Ensure the right people are accountable for filling in forms for insurers that demonstrate potential cyber risks.

Regulatory audits are time-consuming and demanding. However, don't always think of audits as a negative. Use audits to show the board how the threat landscape changes and how investment can help. Digital leaders can use audits to prove the business is ready and to show insurers that they tested their continuity plans regularly.

Dealing with accountability and inclusion in a digital era

The procurement and control of systems and data are becoming decentralised in the cloud era. The complex range of cloud-based services means CISOs and CIOs are losing control of the defensible perimeter. It's difficult to keep control of a disparate range of vendors and third-party relationships.

The board must be aware of the risks of these arrangements and the potential liabilities. Just as the board is accountable for profits or sustainability, they must be for technology and security. This accountability means digital leadership is crucial and must be elevated to the board level. Yet few CISOs and CIOs sit on the board, even in the digital age.

Digital leaders must earn their place on the board. However, you won't relate to the board unless you can articulate the importance of cyber risks. Men often dominate enterprise-level boards. In all circumstances, tell a compelling story that helps the board understand the cybersecurity threat and the requirement to develop a cultural shift across the organisation.

You can't overcome the cyber challenge with a one-size-fits-all strategy. All business functions must recognise the importance of inclusion in security. Take a progressive approach that ensures your organisation has a diverse cyber team that understands the broad spectrum of capabilities and experiences in a modern organisation.

Key takeaways from the event

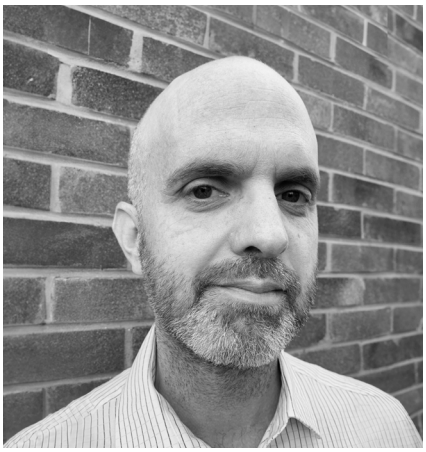
1. **Get ready for change** – The Cyber Code of Conduct is out for consultation. This Code means the board is culpable for cyber threats and damages. CISOs and IT leaders must educate boards on the challenges of modern cybersecurity.
2. **Give specialist guidance** – Find something critical to the business that emphasises the risk of not focusing on the Code. Use language the board understands, such as risks, costs, efficiencies and revenues.
3. **Focus on the human angle** – Technology can help provide protection but an effective cyber response is about supporting a culture shift. Educate the organisation and show people how to respond to circumstances in different localities.
4. **Recognise the risk to reputation** – Successful cyberattacks have a devastating impact on customer perceptions and bottom lines. Make the most of insurance and audits.
5. **Provide strong leadership** – Tell a compelling story so the board understand the threat. Take a progressive approach that helps your business develop a diverse cyber team.

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