Boardroom Exchange

Virtual roundtable for non-executives and governance professionals

Halex CONSULTING

Agenda

- Introductions and roundtable hygiene factors (meeting being recorded, use of raise hand function, Chatham House rule, blog)
- Subject matter expert
  - Vish Nayi, Chief Solutions Architect, CyberQ Group
- Today's discussion topic:
  - Anatomy of a ransomware attack
- Wrap up:
  - Free board cyber risk governance assessment
  - Blog
  - Next session Thursday 11th December. Topic to be confirmed

CyberQ group

Ransomware Preparedness: A Roundtable for Today's Leaders

Prepared by Vishvas Nayi

cyberqgroup.com

Agenda

- Welcome & Introductions
- The Current Threat Landscape: A brief overview
- Roundtable Discussion 1: Before the Attack - Are We Ready?
- Roundtable Discussion 2: During the Attack - The Critical Decisions
- Roundtable Discussion 3: After the Attack - Recovery & Resilience
- Key Takeaways & Closing Remarks

UK Threat Landscape in Context

Ransomware is not just a technical issue; it is a critical business risk.

19,000 UK businesses affected by ransomware (**52** Daily)

Phishing is most common with **93%** of businesses impacted & Ransomware is third most common with **7%** impact

On average, UK businesses encounter a cyberattack every **44 seconds**

Cybercrime costs the UK economy approximately **£27 billion** annually

Supply chain attacks spiked by 35%, while 45% of global organisations expected to face such threats by 2025.

Discussion 1: Before the Attack – Are We Ready?

How does the board gain assurance that cyber-risk, particularly ransomware, is being managed effectively?

Do we have a clear understanding of our "crown jewels" – the critical systems and data essential for our survival?

Have we defined our organisation's risk appetite? What level of risk are we prepared to accept versus the cost of mitigation?

Discussion 2: During the Attack – The Critical Decisions

Who holds the authority to decide whether to pay a ransom? Has this been documented and communicated?

Have we tested our incident response plan with a realistic ransomware simulation involving the executive team? What were the lessons learned?

How do we manage communications with regulators, customers, insurers, and staff in the first 24 hours?

Discussion 3: After the Attack – Recovery & Resilience

How confident are we in our ability to restore critical operations from backups without paying a ransom? How is this confidence validated?

What are our legal obligations for reporting a breach, and are we prepared to meet them under pressure?

How do we ensure that lessons from an incident are embedded back into our strategy and culture to prevent recurrence?

Key Takeaways & Actions for the Board

Preparedness & Validation

Decision-Making Clarity

Financial Resilience

Thank you!

CyberQ Group Ltd, Alpha Tower, Alpha Works, 21st Floor, Suffolk Street,

Queensway, Birmingham B1 1TT, United Kingdom

0800 0614 725 | theteam@cyberqgroup.com | cyberqgroup.com

Wrap up

- Date for your diary:
  - 9am, Thursday 11th December
- Look out for our blog of this discussion in the coming weeks
- Encourage your board members and governance colleagues to join our Boardroom Exchange. Just drop me an email: chris.burt@halex.uk.com or message me on LinkedIn Chris Burt | LinkedIn
- Get in touch if you are thinking about an external board performance review this year or would like some help with an internal assessment of board performance.