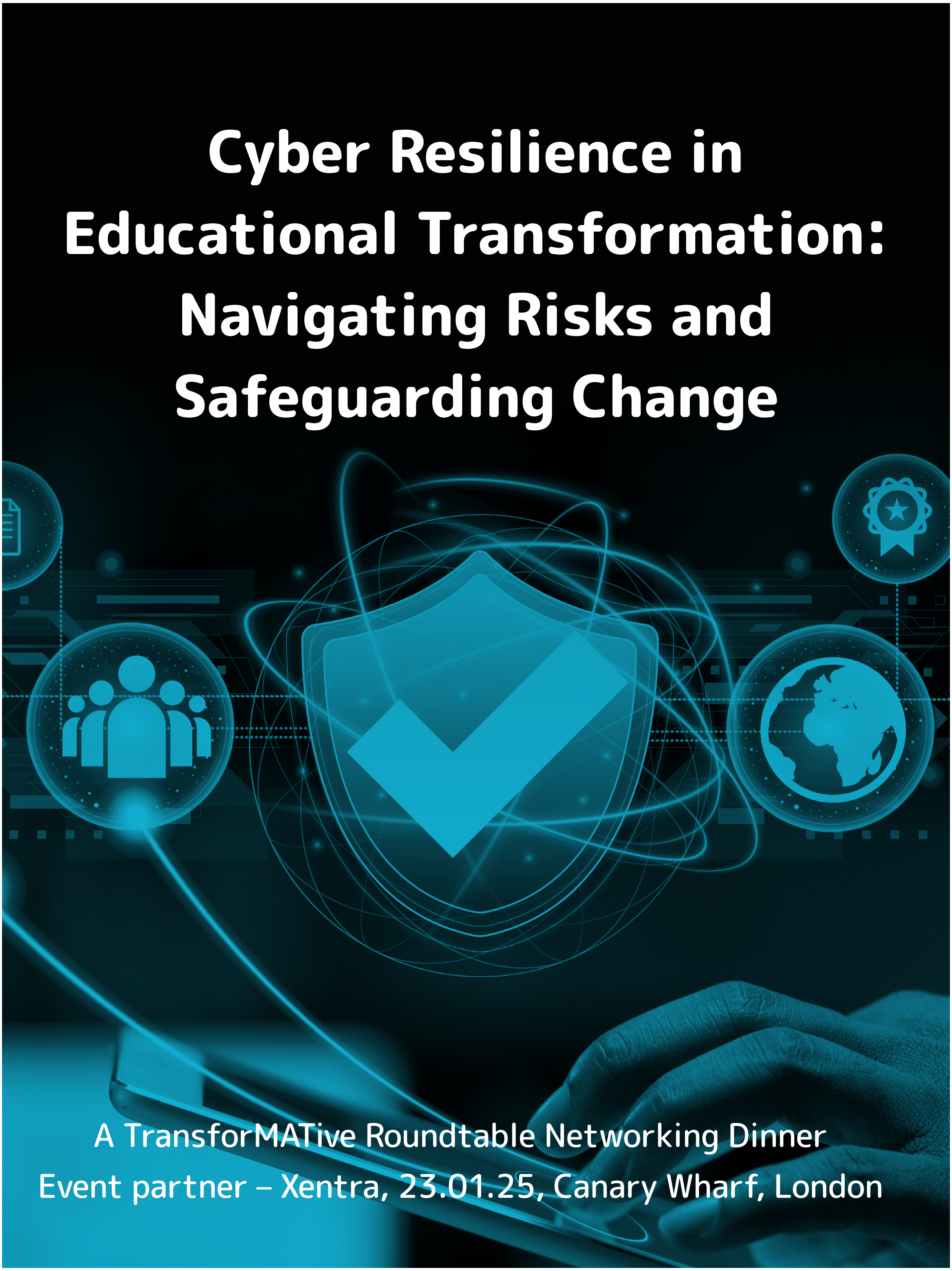
TransforMATive



# Cyber Resilience in Educational Transformation: Navigating Risks and Safeguarding Change

A TransforMATive Roundtable Networking Dinner

Event partner – Xentra, 23.01.25, Canary Wharf, London

# Executive Summary

The rapid digitisation of the education sector has amplified the need for robust cyber resilience strategies to protect critical assets, ensure operational continuity, and build trust among stakeholders. The "Cyber Resilience in Educational Transformation" roundtable, co-hosted by TransforMATive and Xentra, brought together educational leaders and cybersecurity professionals to address the challenges and opportunities of integrating cybersecurity into educational transformation.

Key insights from the event emphasised the importance of proactive risk management, fostering a culture of openness around cyber incidents, leveraging external expertise, and aligning cybersecurity strategies with educational goals. Participants highlighted that while progress has been made in many areas, the sector faces significant challenges due to resource constraints, skills gaps, and evolving threats.

# Key Learning Points

## Proactive Risk Management:

- Embedding cybersecurity into organisational risk management frameworks is critical. Trust boards must move beyond token inclusions in risk registers to detailed, actionable cybersecurity plans.
- Regular penetration testing, vulnerability assessments, and disaster recovery exercises are essential to identify gaps and refine responses.

## Cultural Shifts in Cyber Awareness:

- There is a stigma around admitting cyber breaches, which prevents knowledge sharing and collective learning. Encouraging transparency and collaboration can foster a culture of resilience.
- Cybersecurity must be viewed as an organisation-wide responsibility, with all staff understanding their roles in mitigating risks.

## Leveraging External Expertise:

- Many trusts lack in-house expertise to address complex cybersecurity challenges. Partnering with Managed Service Providers (MSPs) and implementing Security Operations Centres (SOCs) can provide 24/7 monitoring and rapid response capabilities.
- External audits of MSPs ensure accountability and uncover blind spots that might otherwise be missed.

## Importance of Cyber Insurance:

- Cyber insurance is increasingly contingent on meeting stringent requirements, such as having SOCs or multi-factor authentication (MFA) in place. Trusts must understand and adapt to these evolving standards.

## Supply Chain Security:

- Third-party vendors pose significant risks to educational institutions. Participants emphasised the need for clear cybersecurity standards and kite-marking systems for suppliers.
- Proactive measures, such as detailed vendor audits, can mitigate risks associated with the broader supply chain.

## AI and Automation in Cybersecurity:

- Artificial Intelligence (AI) plays a vital role in identifying anomalies and predicting threats. By using AI-driven tools, schools can enhance their capacity to respond to incidents promptly.
- AI-enabled threat hunting and behavioural analytics are becoming essential components of modern cybersecurity strategies.

# Future Research Questions

### Cybersecurity Maturity Models:

What frameworks or benchmarks can best support schools and trusts in assessing their cybersecurity maturity?

### Cost-Benefit Analysis of Cyber Investments:

How can educational institutions quantify the return on investment for cybersecurity measures, given constrained budgets?

### Evolving Cyber Insurance Requirements:

How can trusts adapt to increasingly stringent insurance requirements while maintaining operational flexibility?

### Supply Chain Security Standards:

What mechanisms can be developed to ensure consistent cybersecurity standards across the educational supply chain?

### Scaling Collaboration and Knowledge Sharing:

How can the sector scale successful peer-review models and knowledge-sharing frameworks to enhance collective resilience?

### Integrating Cybersecurity into Leadership Training:

What should a cybersecurity curriculum for education leaders look like to address capability gaps effectively?

## Conclusion

The roundtable highlighted that cybersecurity is no longer a peripheral concern but a core element of educational transformation. While individual trusts have made strides in enhancing their defences, the collective impact will be achieved through collaboration, knowledge sharing, and continuous improvement.

Educational leaders must strike a balance between technical safeguards, cultural change, and strategic investments to create resilient institutions. With the support of partners like Xentra, the education sector has an opportunity to lead by example, demonstrating that limited resources need not hinder robust cybersecurity practices.

By embracing the recommendations and addressing the outlined research questions, the sector can move towards a future where digital transformation and cyber resilience go hand in hand.