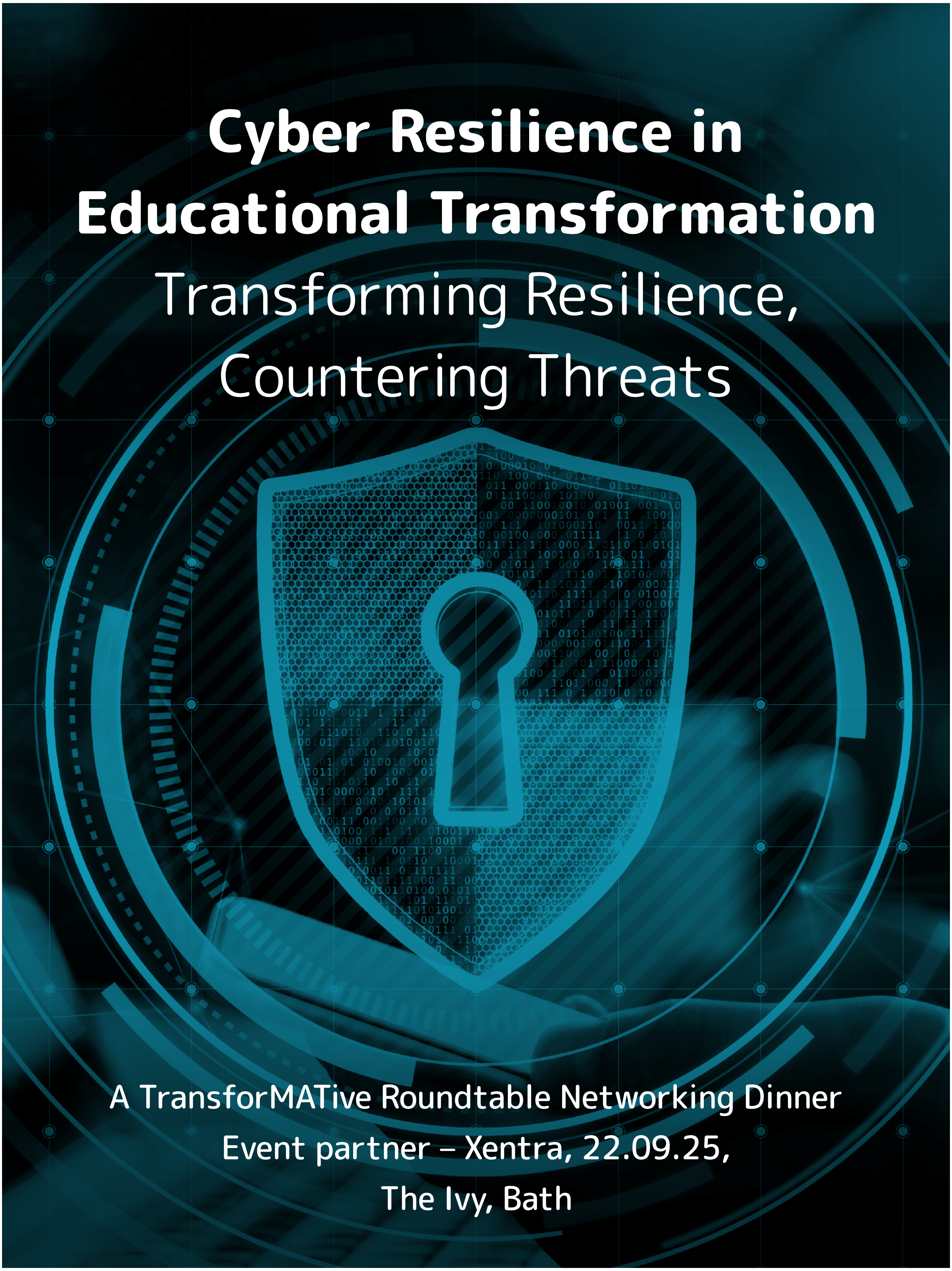
TransforMATive



Cyber Resilience in Educational Transformation

Transforming Resilience, Countering Threats

A TransforMATive Roundtable Networking Dinner

Event partner – Xentra, 22.09.25,

The Ivy, Bath

Executive Summary

The roundtable discussion brought together multi-academy trust (MAT) leaders, IT directors, safeguarding specialists, and industry partners to explore the critical theme of cyber resilience in education. Several recurring themes emerged: the inevitability of cyber incidents, the tension between safeguarding learners and protecting institutional systems, the need for cultural change in how cyber is prioritised, and the systemic underfunding that schools must navigate while still meeting rising expectations.

Participants recognised that cyber resilience is no longer an isolated technical challenge but a core component of educational leadership, safeguarding, and trust governance. With increasing digitisation of learning and administration, schools face growing risks including data breaches, ransomware, supply chain vulnerabilities, and reputational damage. Yet the discussion highlighted that schools can leverage both collaboration and pragmatic prioritisation, such as focusing investment on 24/7 monitoring and testing of continuity plans, to strengthen resilience without diverting disproportionate funds from classrooms.

The overarching conclusion is that cyber resilience in education demands a whole-organisation approach, shared responsibility, and proactive partnerships. It cannot be left solely to IT teams, nor postponed until after mergers or incidents occur.

Key Learning Points

1. Inevitability of Cyber Incidents

- Participants agreed that cyber-attacks are not a matter of **if** but when.
- Incidents often originate in human error such as clicking phishing emails, poor account management, or gaps in due diligence during mergers.
- Recognising this inevitability shifts focus from purely defensive measures to resilience and recovery.

2. The Expanding Risk Surface

- Digitisation has embedded technology in every aspect of school life: safeguarding systems, cloud-based MIS, one-to-one devices for pupils, and marketing platforms.
- This broader digital ecosystem multiplies vulnerabilities, especially where safeguarding, IT, and leadership teams operate in silos.

3. Supply Chain and Mergers as Critical Vulnerabilities

- MAT mergers frequently overlook cyber due diligence. Pressure to complete deals can result in joining with unknown vulnerabilities, later inherited by the trust.
- Supplier compromise, such as breaches within third-party software vendors, was cited as a recurring source of incidents. This highlights the need for systematic supplier risk management.

4. Funding Constraints and Strategic Prioritisation

- Schools face chronic underfunding, forcing leaders to make difficult trade-offs between classroom resources and cyber defences.
- Several contributors argued that if only one investment can be made, it should be in continuous monitoring and incident response capacity, rather than fragmented in-house tools.

5. Human Behaviour and a Culture of Responsibility

- Cyber resilience depends on raising awareness across the organisation, from CEOs to cleaners, so that all staff recognise their role in safeguarding digital assets.
- Training must be continuous, realistic, and linked to everyday scenarios, for example payroll fraud attempts or safeguarding risks linked to AI scraping.

Key Learning Points

6. Governance and Accountability Gaps

- Cybersecurity is often absent from board-level reporting or national accountability frameworks.
- Standards such as the DfE Technology Standards and the ESFA handbook are beginning to raise visibility, but many schools see them as compliance checklists rather than drivers of resilience.

7. Testing, Simulation, and Shared Learning

- Business continuity and disaster recovery (BCDR) plans are often untested or unrealistic.
- Simulation exercises, such as the NCSC’s Exercise in a Box, and cross-department tabletop drills build awareness that cyber incidents are whole-trust events, not IT-only problems.
- Participants emphasised the importance of creating safe spaces to share mistakes without stigma, similar to education learning culture.

Future Research Questions

1. Measuring Maturity

- How can trusts benchmark their cyber resilience maturity in a way that accounts for cultural, financial, and technical dimensions?

2. Cyber-Safeguarding Integration

- What models best integrate safeguarding and cyber resilience, ensuring children’s digital identities are protected alongside physical wellbeing?

3. Cost-Benefit of Monitoring Models

- What is the long-term comparative impact of investing in 24/7 Security Operations Centres (SOCs) versus piecemeal in-house tools in the education sector?

4. Supply Chain Assurance

- What frameworks can be developed for proportionate but effective cyber due diligence on educational suppliers, especially during mergers?

5. Accountability and Regulation

- Should cyber resilience become embedded within Ofsted or DfE accountability frameworks, similar to safeguarding? What are the risks and benefits of such a move?

6. AI and Emerging Threats

- How will generative AI, deepfakes, and automated attacks reshape the risk profile for schools, and what proactive safeguards should be tested now?

7. Resilience Beyond Technology

- How can schools design operational models that allow continuity of learning during outages, such as fallback to paper registers or manual payroll?