Centre for the New Midlands

Cyber Resilience in the Age of AI Roundtable

21st October 2026



Sponsored by:

Talent Today
IT TALENT ON DEMAND

Reimagining the Region





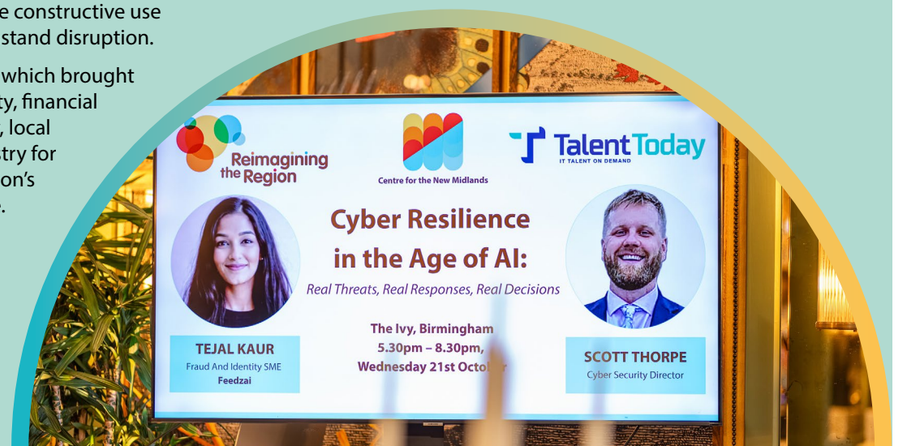
AI, cyber security and resilience: what does the Midlands need to be ready for?

On 21st October, the Centre for the New Midlands hosted a roundtable at The Ivy Temple Row to explore the opportunities and risks of artificial intelligence, and how businesses, public services and communities can strengthen their resilience.

Artificial intelligence is accelerating the pace of cyber threats, transforming how organisations operate and raising urgent questions about responsibility, preparedness and public trust. But the challenge facing the Midlands is not simply how to defend against increasingly sophisticated attacks. It is how to help businesses and communities make constructive use of AI while ensuring they can withstand disruption.

These themes shaped the session which brought together voices from cyber security, financial services, law, policing, technology, local government, education and industry for an open discussion about the region's readiness for an AI-enabled future.

Held under the Chatham House Rule, the discussion encouraged delegates to speak candidly about their experiences and concerns. The event considered both the changing threat landscape and the practical steps needed to build resilience across organisations of very different sizes and capabilities.





AI is changing the pace and scale of cyber risk

The opening contributions explored how AI is changing the economics and accessibility of cyber attacks. Threat actors do not necessarily need exceptional technical expertise: stolen credentials, convincing impersonation, social engineering and weaknesses in routine processes can still provide routes into organisations.

AI can make these familiar techniques faster, more credible and easier to deploy at scale. Phishing messages can be more persuasive, public information can be assembled into convincing targeted approaches, and synthetic voices or images can make impersonation harder to recognise.

Our delegates also highlighted the speed at which vulnerabilities can emerge, be identified and exploited. Organisations accustomed to working through security issues during conventional business hours may find themselves operating at a disadvantage against threats that develop around the clock.

Yet the discussion was not solely pessimistic. AI can also strengthen defence, helping security teams analyse information, identify patterns, prioritise incidents and respond more quickly. The central question is how organisations can harness those capabilities without introducing new risks.

A recurring warning was that adopting AI without sound security foundations may simply accelerate existing weaknesses. Effective cyber defence still depends on good information management, access controls, secure systems, clear processes and the ability to respond when something goes wrong.



The human factor remains central

The roundtable challenged the idea that cyber security is primarily a technical problem. Many attacks exploit trust, familiarity and the desire to be helpful: an employee may respond to an apparently genuine request, a help desk may reset a password without adequate verification, or a supplier may introduce a new AI tool without the customer understanding what information it can access.

The growth of AI-generated fraud makes awareness more important, but also more difficult. Traditional warning signs such as poor spelling, awkward phrasing or implausible messages may no longer be reliable.

Our delegates discussed the role of behavioural signals and layered protections in detecting suspicious activity. In financial services, for example, patterns of device use, payment behaviour and the circumstances surrounding a transaction can help identify potential fraud.

For employers, the challenge is to make cyber awareness relevant to the whole workforce, not only technical staff or office-based employees. People with limited access to computers may still handle sensitive information, use digital services or be targeted through personal devices.

The discussion emphasised the importance of accessible education, practical examples and a culture in which staff feel able to question unusual requests and report mistakes without embarrassment.





SMEs need practical support, not just warnings

A particularly strong theme was the vulnerability of small and medium-sized enterprises. Large organisations may have dedicated security teams, specialist advisers and formal governance structures. Many smaller businesses do not.

Yet their exposure can be significant. A cyber incident may interrupt operations, compromise customer information, undermine trust or threaten the viability of a business. Smaller suppliers can also become an entry point into larger organisations and supply chains.

Delegates argued that the core principles of cyber security apply across organisations, regardless of size. The difficulty is deciding what to prioritise, finding the resources to implement it and understanding where to seek help.

Basic measures including secure access, reliable backups, appropriate verification procedures and sound management of systems and suppliers remain essential. But compliance or certification alone should not be mistaken for comprehensive resilience. Organisations need to understand the risks that remain and prepare for the possibility that preventive measures will fail.

The conversation pointed to a role for regional networks, business support organisations and specialist cyber resilience services in helping SMEs build confidence and capability. Sharing practical lessons from incidents, rather than relying exclusively on high-level guidance, could make support more useful and actionable.

There was also concern about the difficulty of reporting cyber crime and accessing effective assistance after an incident. For smaller businesses, timely advice and a clear route to recovery can be as important as prevention.

Resilience means being able to recover



The discussion moved beyond the question of how to stop attacks to consider what happens when disruption occurs.

Cyber resilience requires organisations to understand which services are critical, how they would continue operating during an incident and how quickly they could restore essential systems. Backups, business continuity arrangements, incident response plans and tested recovery processes may appear unglamorous, but they can determine whether an organisation survives a serious disruption.

Delegates noted that cyber incidents can quickly become wider operational and governance issues. An outage may affect payments, public services, supply chains or the ability of staff to do their jobs. Decisions about technology risk therefore need to involve senior leadership and boards, rather than being treated solely as the responsibility of IT teams.

The growing use of AI also introduces questions about third-party dependencies, data access and the oversight of automated systems. Organisations need to know what tools are being used, what information they can reach, and what safeguards apply when systems or suppliers change.

The message was clear: prevention remains important, but it cannot guarantee safety. Preparedness, response and recovery must be part of the same resilience strategy.

Responsible AI adoption requires clear governance

Alongside cyber threats, our delegates explored the risks associated with AI inside organisations.

AI tools can expose information that was previously difficult to find or combine, particularly where existing permissions and data-sharing arrangements are poorly managed. The rapid adoption of workplace assistants and other AI applications can therefore reveal weaknesses in information governance.

The discussion highlighted the importance of distinguishing between different AI systems and use cases. A tool used to support routine administration raises different questions from one making consequential decisions or operating in a safety-critical environment.

Delegates considered the need for proportionate governance, human oversight and clear accountability. They also raised concerns about bias, over-reliance on generated outputs and the possibility that AI-produced material could be mistaken for reliable evidence.

The aim should not be to reject innovation, but to adopt it deliberately: understand the purpose of a system, assess its risks, protect the information it uses and retain appropriate human responsibility for its outcomes.



Education, skills and regional capacity



The roundtable returned repeatedly to the question of who is responsible for preparing people for the changing digital landscape.

Businesses have a responsibility to equip their employees, but our delegates questioned whether education can be left to individual employers particularly when many SMEs lack the capacity to provide it. Public services, schools, colleges, universities, business networks and specialist organisations all have a part to play.

The Midlands has significant strengths in technology, manufacturing, automotive research, financial services and higher education. These capabilities offer opportunities to develop and apply AI, strengthen cyber security and support innovation across the region.

However, delegates raised concerns about the future skills pipeline, the availability of specialist expertise and the challenge of retaining talent. Education needs to keep pace with technological change, while providing routes into digital and cyber careers for people with different backgrounds and levels of prior experience.

The discussion also recognised that digital confidence is a wider social issue. People need the knowledge to use technology safely, question suspicious communications and understand the implications of sharing personal or organisational data.

Regulation, responsibility and the public interest

The event explored whether existing governance and regulatory approaches are keeping pace with AI's development.

Delegates raised questions about accountability when AI systems cause harm, the appropriate level of oversight for different applications, and the balance between encouraging innovation and protecting people and organisations.

There was no simple consensus on the right regulatory model. Some contributions emphasised the risks of moving too slowly; others warned against rules that could constrain beneficial innovation or fail to reflect the very different uses of AI.

A key consideration was proportionality. The risks associated with a routine productivity tool are not the same as those associated with systems that influence high-stakes decisions or operate in safety-critical settings. Governance needs to reflect those differences while making responsibilities understandable to organisations with limited resources.

The discussion also connected AI adoption to broader questions about infrastructure, energy, data and the UK's ability to develop and retain technological capability.



Turning discussion into regional action



The roundtable concluded with a focus on what the Centre for the New Midlands and its wider network could contribute.

The discussion suggested several practical priorities for the region:

- Make cyber guidance accessible to SMEs. Translate technical advice into clear, manageable steps and help businesses identify trusted sources of support.
- Strengthen regional knowledge-sharing. Encourage organisations to share lessons from incidents and near misses, helping others prepare and recover.
- Promote resilience alongside prevention. Support businesses and public services to test arrangements, protect critical operations and plan for recovery.
- Build digital and AI literacy. Connect employers, educators and community organisations to provide relevant learning for people across the workforce and wider public.
- Encourage responsible adoption. Help organisations understand AI tools, manage data and supplier risks, and maintain appropriate human oversight.
- Bring regional experience into policy discussions. Ensure that the realities facing Midlands businesses, public services and communities inform debates about skills, regulation, infrastructure and innovation.

The conversation underlined that the Midlands' readiness for AI will depend on more than access to new technology. It will require strong foundations, informed people, practical support and a willingness to learn collectively.

AI presents genuine opportunities to improve productivity, strengthen cyber defence and create new capabilities. But those benefits will be realised most effectively when organisations understand the risks, prepare for disruption and retain responsibility for the systems they use.

Our delegates

Guest	Role	Organisation
Adriana Klincova	Legal Director	Anthony Collins Solicitors
Andrew Horkan	Chief Executive Officer	Cyber Tzar
Chris Smith	Founder and CEO	Centre for the New Midlands CIC
Clare Golby	Digital Transformation Manager	Coventry & Warwickshire Chamber of Commerce
Dean Harris	Director of Digital, Data and Technology	whg
Dominic Osborne	Associate Technical Director	Arcadis
Dr Eman Al-Hillawi	CEO	Entec Si Ltd
Frazer Dawkins	Oracle Account Executive	Oracle
Gary Wills	Founder and Talent Partner	Talent Today
Martin Sadler	Director - Digital Technology Services (DTS)	Birmingham City Council
Matt Whelan	Senior Associate	Trowers & Hamlins LLP
Mike Leonard	Special Sergeant	West Midlands Police
Rich Bishop	Director	withdigital
Ruhail Rana	Head of School - Digital and Computing	South and City College Birmingham
Sarah Onions	Business Manager	MIGSO PCUBED
Sarah Windrum	Head of Cluster Development	HORIBA MIRA / MIRA Tech Park
Scott Thorpe	Cyber Security Director	
Steve Cotton	Advisor	Socitm
Sue Walnut	Director of Technology	West Midlands Combined Authority
Sunny Vara	Founder & CEO	Cybercy Group
Tejal Kaur	Fraud and Identity SME	Feedzai

Centre for the New Midlands

Creating a ‘better’ West Midlands

The-New-Midlands

TheNewMidlands

