

# A Framework for Building a Secure, Resilient and AI-based Digital Future for SMEs

Angel Jimenez-Aranda<sup>\*,†</sup>, Tarek Gaber<sup>†</sup>, Yun Chen<sup>†</sup> and Mirage Islam<sup>†</sup>

*The University of Salford, 43 Crescent, Salford M5 4WT, United Kingdom*

## Abstract

The rapid adoption of artificial intelligence (AI) by small and medium-sized enterprises (SMEs) presents both new opportunities and significant cybersecurity challenges. While AI offers powerful tools for enhancing cyber defence, it also introduces vulnerabilities that attackers can exploit. However, a clear gap remains in understanding the dual role of AI, as a solution to enhance cybersecurity and as a potential source of new security vulnerabilities in its own applications. This paper presents a novel framework designed to explore and strengthen the interconnection between AI adoption and cybersecurity preparedness in SMEs. The framework takes a multi-faceted approach to raise awareness, build organisational capacity, and enhance resilience against emerging threats. A distinguishing feature of the framework is its commitment to inclusivity, aligning with United Nations goals to increase diversity in the STEM workforce, particularly by encouraging the participation of women in AI and cybersecurity, highlighting role models, and fostering a more diverse and inclusive ecosystem. By integrating technical, organisational, and behavioural dimensions, the framework promotes responsible AI adoption while supporting broader national priorities. The findings offer practical insights and reinforce the growing need for targeted support mechanisms to ensure SMEs can confidently and securely embrace AI technologies.

## Keywords

AI, Cybersecurity, SMEs, Secure AI, Digital Transformation.

## 1. Introduction

Artificial intelligence (AI) is reshaping industries across the globe, offering transformative potential for productivity, decision-making, and innovation. Its adoption is no longer confined to large corporations, and small and medium-sized enterprises (SMEs) are increasingly embedding AI into their operations, from customer service chatbots to predictive analytics in logistics and finance [1, 2]. However, this technological shift is not without risk. As AI systems become more pervasive, concerns increase about their security, robustness, and trustworthiness [3, 4]. For SMEs in particular, often operating with constrained resources and limited technical expertise, these risks are amplified.

The cybersecurity landscape is evolving rapidly alongside AI. Attackers are now exploiting vulnerabilities in AI systems, such as adversarial machine learning, data poisoning, and model inversion [5, 6]. At the same time, AI is being used defensively to enhance cybersecurity practices, enabling anomaly detection, threat intelligence, and dynamic response capabilities [7]. This dual role of AI, both as a potential threat vector and a security tool, creates what we term the "AI-Cyber Nexus": a critical connection at which the future of secure digital transformation is being negotiated.

Despite growing recognition of the risks and opportunities associated with AI, SMEs remain underserved in cybersecurity discourse and support. Studies show that SMEs often underestimate their exposure to cyber threats, lack formal risk assessments, and struggle to implement even basic

---

*2nd Workshop on Education for Artificial Intelligence (edu4AI 2025, <https://edu4ai.di.unito.it/>), Co-located with ECAI 2025, the 28th European Conference on Artificial Intelligence which will take place on October 26, 2025 in Bologna, Italy*

\* Corresponding author.

† These authors contributed equally.

✉ a.jimenez-aranda@salford.ac.uk (A. Jimenez-Aranda); t.m.a.gaber@salford.ac.uk (T. Gaber); y.chen@salford.ac.uk (Y. Chen); m.a.k.r.islam@salford.ac.uk (M. Islam);

ORCID 0000-0002-8913-8668 (A. Jimenez-Aranda); 0000-0003-4065-4191 (T. Gaber); 0000-0001-5123-1624 (Y. Chen); 0009-0008-1440-343X (M. Islam);



© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

cybersecurity controls [8, 9]. When it comes to AI, these challenges are further complicated by a lack of clarity around regulation, best practices, and ethical standards [10, 11]. This results in a widening knowledge gap that can undermine trust, resilience, and competitiveness.

In response to these challenges, this study introduces a novel framework aimed at examining and reinforcing the relationship between the adoption of artificial intelligence (AI) and cybersecurity readiness within SMEs. The proposed framework adopts a comprehensive approach that emphasises awareness-raising, capacity building, and the strengthening of organisational resilience in response to evolving cyber threats for AI and of AI. An important dimension of the framework is its inclusive orientation, which aligns with broader national and United Nations objectives to diversify the STEM workforce. In particular, it seeks to promote greater female participation in AI and cybersecurity by showcasing role models and cultivating a more inclusive and representative professional environment. As a case-study in Greater Manchester, UK, a region recognised for its dynamic SME ecosystem, the framework was evaluated to support SMEs in navigating the dual challenge of AI adoption and cybersecurity preparedness.

## 2. Methodology

The development of the AI-Cyber Nexus framework was informed by insights and lessons learned from earlier regional initiatives, such as the Cyber Foundry and AI Foundry programmes. These previous initiatives provided valuable understanding of the needs, barriers, and capabilities of SMEs adopting digital technologies. However, neither addressed the specific risks and opportunities arising from the convergence of AI and cybersecurity. The AI-Cyber Nexus framework sought to fill this gap by integrating key themes from both fields and applying them across four practical dimensions: Awareness and Engagement, Skills and Capability Development, Hands-on Support and Expert Guidance, and Inclusivity. The framework was operationalised through a series of targeted interventions delivered over a three-month period, from January to March 2025.

The framework was shaped and refined through ongoing engagement activities with SMEs, which served both to validate its relevance and to ensure its implementation addressed real-world challenges. Particular attention was given to reaching underserved groups and sectors traditionally underrepresented in the digital economy.

Collaboration was central to this initiative. The delivery team worked closely with local business networks, innovation hubs, AI and cybersecurity experts, and academic partners to ensure relevance and legitimacy. Partnerships with regional organisations extended the project's reach and ensured that messaging aligned with the existing SME support ecosystem.

The engagement activities were delivered through four main strands. First, a series of interactive workshops—conducted both in-person and online—focused on practical topics such as AI risks, cybersecurity for non-specialists, and responsible AI deployment. These sessions featured real-world examples and facilitated peer discussion to make the material accessible and engaging for SMEs. Second, a suite of digital training materials, including animated videos, was made available via an open-access platform. These resources included concise explanations, infographics, and checklists tailored for time-constrained business owners and managers. Third, a podcast series was produced, featuring interviews with industry leaders, cybersecurity experts, and AI thought leaders. These episodes offered SMEs valuable insights into practical applications, emerging challenges, and opportunities at the intersection of AI and cybersecurity. Available across multiple platforms (Spotify, Apple Podcasts, YouTube), the podcasts provided a flexible and accessible way for busy professionals to stay informed. Finally, SMEs were offered personalised advice through one-to-one consultancy sessions with the project team. These confidential sessions created a safe space for organisations to explore questions about AI adoption, regulatory compliance, and digital security without fear of judgment or exposure.

This flexible and modular structure enabled SMEs to engage with the initiative at varying levels of intensity, depending on their specific needs, interests, and availability.

### 3. Framework Overview

The AI-Cyber Nexus introduced a holistic framework grounded in practical experience and informed by sustained engagement with regional SME ecosystems. The framework, as illustrated in Figure 1, is structured around four interconnected dimensions: Awareness and Engagement, Skills and Capability Development, Hands-on Support and Expert Guidance, and Inclusivity and Diversity. Together, these dimensions offer a structured yet flexible approach to supporting SMEs in adopting AI responsibly, building cyber resilience, and ensuring equitable access to the benefits of digital innovation.

The *Awareness and Engagement* dimension focuses on raising awareness of both the opportunities and risks associated with AI and cybersecurity across the full spectrum of SMEs. Activities such as workshops, webinars, and community engagement events are used to demystify complex technologies and improve visibility among traditionally underserved groups. The emphasis is on developing inclusive messaging and engagement strategies that resonate with a diverse SME audience.

*Skills and Capability Development* addresses the significant skills gap in AI and cybersecurity as reported by UK government in [12]. This was done by supporting the creation of accessible and informal learning pathways tailored to SMEs with varying levels of digital maturity. It includes practical training, modular learning resources, and opportunities for hands-on exploration of relevant tools and techniques. The content is designed to be inclusive and relevant, regardless of the SME's size, sector, or technical background.

The third dimension, *Hands-on Support and Expert Guidance*, as proven in [13] provides contextualised, on-demand support through expert clinics, sector-specific advice, and one-to-one consultancy. This ensures that SMEs are not left to navigate the complexities of secure AI adoption in isolation but are supported through trusted, personalised guidance.

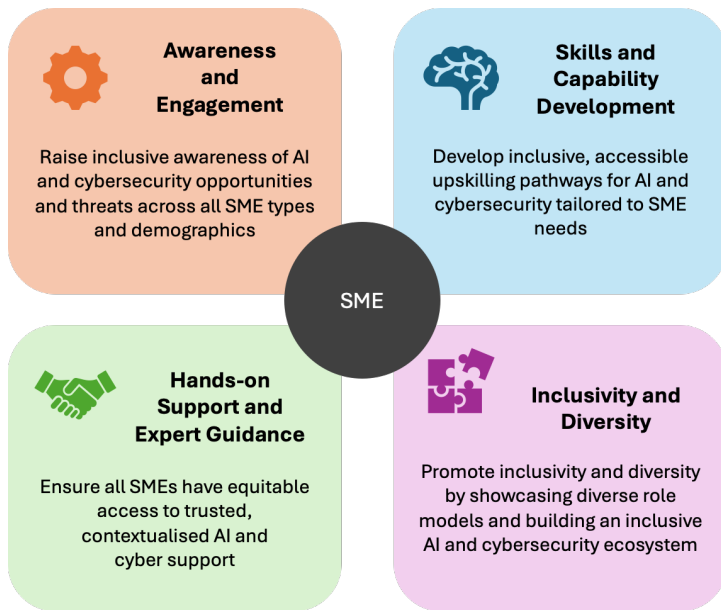


Fig 1. AI-Cyber Nexus Framework

The final dimension, *Inclusivity and Diversity*, is embedded throughout the entire framework and also functions as a standalone focus area. It aims to reduce structural barriers to digital participation by actively involving underrepresented groups, including women- and minority-led SMEs [14]. Activities include showcasing diverse role models in AI and cybersecurity, building inclusive networks, and designing interventions that reflect the lived experiences of a broader range of SME leaders. This approach supports the creation of a more equitable innovation ecosystem and aligns with national efforts to improve diversity in STEM and digital sectors.

Figure 1 presents a visual representation of the framework, positioning the SME at the centre, surrounded by the four dimensions. The design reflects the iterative and interconnected nature of the framework, where inclusivity and diversity are not treated as a separate strand but are integrated into every activity. It highlights the reinforcing relationships that drive awareness, build skills, enable informed action, and promote equity.

The framework is closely aligned with key UK government priorities, including the National AI Strategy (2021), the National Cyber Strategy (2022), and the UK Digital Strategy (2022) as well as international initiatives such as the US National Artificial Intelligence Initiative Act (2020), the EU

Strategy for Artificial Intelligence (2021), Canada's Pan-Canadian AI Strategy (2017), and Australia's AI Action Plan (2019)". It supports strategic objectives such as improving cyber resilience among SMEs, scaling the responsible adoption of AI, and increasing diversity across the digital and tech sectors. By taking a regional, inclusive, and practice-led approach, the AI-Cyber Nexus framework contributes meaningfully to the national goal of fostering a secure, innovative, and equitable digital economy.

## 4. Discussion and Results

The framework was evaluated by case-study in Greater Manchester, UK. This region was selected as it is recognised for its dynamic SME ecosystem. All project materials (including workshops, training resources, video and audio podcasts, and consultancy information) were made freely available via the project's dedicated website: <https://aicybernexus.salford.ac.uk>. The website functioned as a central hub for SMEs, allowing them to explore and download resources at their convenience. To enhance accessibility and ongoing engagement, the site also included interactive features such as feedback forms, event registrations, and updates on upcoming support opportunities. The site remains publicly accessible after the pilot, serving as a lasting legacy of the project.

The AI-Cyber Nexus framework yielded important insights into the current state of AI adoption and cybersecurity preparedness among SMEs in Greater Manchester. While the engagement activities were not designed to generate formal research data, they provided a rich source of qualitative evidence. Through workshops, briefing sessions, drop-in clinics, and informal discussions with SME owners, advisors, and ecosystem partners, the project team identified recurring concerns, knowledge gaps, and areas of opportunity. These findings directly influenced the development and refinement of the support activities, helping to ensure that the framework's four dimensions remained aligned with the lived experiences of SMEs.

One of the most striking insights emerged within the Awareness and Engagement dimension: a consistently low baseline understanding of how AI technologies can themselves pose cybersecurity risks. While many participants had some familiarity with using generative AI tools or business automation software, there was little awareness of issues such as adversarial attacks, data poisoning, or vulnerabilities in AI models. As in prior studies [8], many SMEs assumed that third-party, cloud-based AI tools were secure by default, an assumption that persists despite growing concern among cybersecurity experts about black-box models and supply chain risks [3, 9].

Relatively few SMEs (less than 3%) had considered the opportunities for using AI to enhance their cybersecurity posture. While some expressed interest in AI applications for threat detection, phishing prevention, or endpoint monitoring, this was often theoretical. Practical adoption was constrained by barriers identified under the Skills and Capability Development and Hands-on Support dimensions, specifically cost, complexity, and lack of clear, tailored guidance. Participants repeatedly expressed a desire for lightweight, explainable AI tools that could be integrated into existing systems with minimal disruption. Aligned with the findings of a previous study [15], this suggests a clear opportunity for innovation and targeted support and the development of simple, affordable, and trustworthy AI-enabled solutions designed specifically for the SME context.

The project also highlighted the challenges of digital maturity for the majority of participating SMEs. Even where appetite for innovation existed, foundational practices such as cybersecurity risk assessments, regular staff training, or data governance frameworks were often lacking. This presented a challenge for engaging with more advanced topics such as AI security or regulation readiness. 50% of SMEs expressed concern about potential non-compliance, particularly in relation to upcoming AI directives. These concerns reinforced the importance of demystifying AI and cybersecurity, central aims of the Awareness and Skills dimensions of the framework, and providing SMEs with a low-risk, practical entry point into these critical conversations.

A recurring theme across all engagement strands was the issue of internal capacity. Time, expertise, and resource constraints limited many SMEs' ability to engage with fast-evolving digital

technologies. When support was delivered through the Hands-on Support and Expert Guidance dimension, such as one-to-one consultancy sessions, it created a trusted environment for SMEs to explore their questions, however basic, without fear of judgement or exposure. This trust-based approach also facilitated participation from underrepresented groups, fulfilling the goals of the Inclusivity and Diversity strand. For example, several women and minority-led SMEs noted that the inclusive, jargon-free format of workshops and podcasts made them feel more comfortable joining the discussion and asking questions.

Overall, the participatory approach of the AI-Cyber Nexus framework proved highly effective in building trust, fostering dialogue, and enhancing engagement. The flexible, modular structure of the framework enabled SMEs to participate at varying levels of intensity, depending on their needs and availability. Participants expressed strong interest in future collaboration, including continued access to support materials and follow-up programmes. These findings demonstrate the value of regional, practice-led initiatives that go beyond awareness-raising to build real capability, reduce structural barriers, and equip SMEs for a secure and inclusive digital future.

## **5. Conclusion**

The AI-Cyber Nexus framework represents a timely and practical response to the growing need for targeted, inclusive support at the intersection of artificial intelligence and cybersecurity within the SME landscape. Drawing on lessons from earlier initiatives and informed by real-world engagement across Greater Manchester, as a case-study, the framework addresses not only the technical and operational challenges SMEs face, but also the broader structural barriers to participation, resilience, and innovation.

Greater Manchester was selected as the pilot region due to its strong history of innovation support and active SME base. Its diversity, both in terms of business sectors and communities, provided a valuable testbed for examining how inclusive and responsive the framework could be in practice. Insights gained from the regional implementation offer important lessons for broader adoption and replication across other UK regions.

By organising its interventions around four key dimensions (Awareness and Engagement, Skills and Capability Development, Hands-on Support and Expert Guidance, and Inclusivity and Diversity) the framework provides a comprehensive approach to enabling responsible AI adoption and strengthening cyber readiness. Its emphasis on accessibility, equity, and responsiveness ensures that SMEs are not only better equipped to adopt emerging technologies securely, but are also supported in ways that reflect their unique contexts and needs.

While the framework does not claim to be exhaustive, its initial implementation has demonstrated the value of an integrated, inclusive model for digital transformation and AI adoption. The findings suggest that a combination of tailored support, practical learning opportunities, and attention to diversity can significantly enhance SMEs' readiness to navigate the dual opportunities and risks of AI and cybersecurity.

Looking ahead, there is significant potential to adapt this framework across different sectors by tailoring its approach to their specific digital maturity, risk profiles, and operational challenges. The framework could also strengthen connections with national digital and innovation strategies. Further work is needed to deepen the evidence base, refine delivery mechanisms, and explore long-term impact. Nonetheless, the AI-Cyber Nexus contributes to the ongoing efforts to ensure that no SME is left behind in the rapidly evolving digital economy.

## **Acknowledgements**

This initiative was made possible through funding and support from the UK Department for Science, Innovation and Technology and InnovateUK as part of the Cyber Local Programme.

## Declaration of Generative AI

During the preparation of this work, the authors used GPT-4 in order to: Grammar and spelling check. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

## References

- [1] OECD, The Digital Transformation of SMEs, OECD Studies on SMEs and Entrepreneurship (2021). [Online]. Available: doi:10.1787/bdb9256a-en
- [2] UK Government, National AI Strategy, Department for Digital, Culture, Media and Sport (2021). [Online]. Available: <https://www.gov.uk/government/publications/national-ai-strategy>
- [3] M. Brundage, S. Avin, J. Clark, et al., The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, Future of Humanity Institute, University of Oxford (2018).
- [4] R. Binns, "On the apparent conflict between individual and group fairness," Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (2021).
- [5] B. Biggio, F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," Pattern Recognition, vol. 84, pp. 317–331 (2018). doi:10.1016/j.patcog.2018.07.023.
- [6] N. Papernot, P. McDaniel, I. Goodfellow, et al., "Practical Black-Box Attacks against Deep Learning Systems using Adversarial Examples," arXiv preprint, arXiv:1602.02697 (2016).
- [7] F. Sharmeen, A. Sami, S. Khan, et al., "Artificial Intelligence for Cybersecurity: A Systematic Mapping Study," Computers & Security, vol. 127, p. 102697 (2023). doi:10.1016/j.cose.2023.102697.
- [8] ENISA, Cybersecurity for SMEs, European Union Agency for Cybersecurity (2020). [Online]. Available: <https://www.enisa.europa.eu/publications/cybersecurity-for-smes>
- [9] NCSC, Cyber Security Small Business Guide, National Cyber Security Centre (2023). [Online]. Available: <https://www.ncsc.gov.uk/collection/small-business-guide>
- [10] L. Floridi, J. Cowls, "A Unified Framework of Five Principles for AI in Society," Harvard Data Science Review, vol. 1, no. 1 (2019). doi:10.1162/99608f92.8cd550d1.
- [11] European Commission, Proposal for a Regulation on Artificial Intelligence (AI Act), COM/2021/206 final (2021).
- [12] Department for Digital, Culture, Media & Sport. (2023). UK cyber security skills in the labour market 2023. <https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2023>
- [13] Bhalerao, K., Kumar, A., Kumar, A., & Pujari, P. (2022). A study of barriers and benefits of artificial intelligence adoption in small and medium enterprise. Academy of Marketing Studies Journal, 26(1). Allied Business Academies.
- [14] Carter, S., Mwaura, S., Ram, M., Trehan, K., & Jones, T. (2015). Barriers to ethnic minority and women's enterprise: Existing evidence, policy tensions and unsettled questions. International Small Business Journal: Researching Entrepreneurship, 33(1), 49–69. doi:10.1177/0266242614556823
- [15] Lyons, J. B., Meisner, C., & Bharati, P. (2024). Explainable AI for small and medium enterprises: Enabling trustworthy and context-aware adoption. Journal of Small Business Management. Advance online publication. doi:10.1080/00472778.2024.2379999