Section of the conference: Computer science, computing and automation

Sekcja konferencji: Informatyka, obliczenia i automatyzacja

How to cite: Hossain, M. R., & Yassar, I K M S. (2025). AI-integrated IT framework for cyber resilience in SMEs. *World Conference on Emerging Science, Innovation and Policy 2025*. Futurity Research Publishing. https://doi.org/10.5281/zenodo.16595831

AI-Integrated IT Framework for Cyber Resilience in SMEs

Muhammad Riyaz Hossain[1], I K M Saameen Yassar[2]

[1]MBA, Assistant Operation Manager, Ayaz Group LLC

[2]Master of Information Technology, Washington University of Science and Technology VA 22314

Accepted: July 8, 2025 | **Published**: July 20, 2025 | **Language:** English

Abstract: U.S. and Western-economies small and medium-sized businesses (SMBs) in general face a rising number of cyber breaches because of resource shortages and technical constraints. The study proposes an AI-infused IT framework through a phased approach for raising cyber resilience of SMEs within levels of awareness, detection, response, and continuous improvements. Keeping in mind the detection shortcomings, workforce training, and governance-related issues, this model leverages low- cost AI tools while complementing the NIST Cybersecurity Framework. The modular nature of the framework allows optionality in implementation, granting SMEs the choice to ramp up their defenses in a cost-effective way. Future research will validate the framework in practical surroundings, and it will quantify how it constellates into the cyber readiness of SMEs.

Keywords: AI, cybersecurity, SMEs, resilience, NIST framework, and threat detection.

1. Introduction

More than 90% of the U.S. companies are SMEs and have gradually become cushioned targets for

cyber assaults because of barely-there IT budgets, an absence of experience, and premature strategies with little or no testing. The reality is that SMEs are often the ones who cannot even withstand low-level cyber incidences; they actually could not have an incident response plan; only 19% of companies in the UK do by their own admission (Iqbal & Abbas, 2025). They have essentially become sitting ducks for any party wishing to extort money from them since they have almost no resources to implement security defenses or mechanisms. It really is a powerful situation with cyber-criminals, enabled increasingly by artificial intelligence (AI), i.e., automated phishing and deepfake forging, on one side and using AI to strengthen their defenses on the other. Hence, an AI-powered IT framework for cyber resilience can support SMEs quite proactively in detecting, responding to, recovering from, and preventing threats with a scratch of limited resources (Lani & Abbas, 2025).

2. Analysis of Recent Research & Publications

2.1 Cybersecurity Gaps in SME

Small- to medium-sized enterprises are extremely sensitive to cyber threats, with all sorts of gaps still present in cybersecurity modifications and resources. According to a systematic review by (Chaudhary, et al., 2023), SMEs are considered mostly "unaware, unfunded, and uneducated" in regards to their own exposure to cyber risk. A distinct view is given by the Data Breach Investigations Report of 2023 by Verizon, noting that 43 percent of all attacks globally are targeted at SMEs while most small enterprises do not have cybersecurity policies or incident responses. Being economic backbones in the West, such as American and European, the SMEs sometimes still stay in the clutches of obsolete, inefficient security measures that leave them exposed to classic and modern forms of attack such as AI-generated phishing attacks. More than 50 percent of SMEs view cybersecurity as an issue of secondary importance in Europe, according to (Button et al., 2025). This reflects a lack of awareness and the lack of resources dedicated to cybersecurity initiatives. These considerations then instill a very great urge for scalable and cost-effective solutions meant for SMEs.

2.2 AI Challenges for SMEs

Artificial intelligence posits a strengthening force in the SME cybersecurity domain; nevertheless, very few are adopting AI because of some barriers. A study highlighted by (Lu et al., 2022) mentioned in SpringerLink several challenges, such as cost of implementation, availability of high-quality data for training, and technical immaturity of SME infrastructures. Further to this, many small- and medium-enterprise leaders remain AI illiterate and hence cannot effectively decide upon or deploy AI solutions. (Iyelolu et al., 2024) on ResearchGate also pointed out lack of experts and the perception that AI systems are far too sophisticated for smaller entities. However, stepwise, low-cost integration solutions have been floated to overcome these barriers, with the emphasis laying on SaaS-based AI tools and workforce training as a practical beginning for SMEs in the US-Western European context.

2.3 AI-Powered Resilience Frameworks

AI-assisted resilience frameworks have recently been put forth as promising avenues to boost SME cyber resilience. An important piece of work from Rotterdam University (Sundaramurthy et al., 2022) proposes the use of generative AI to automate threat-intelligence sharing in order to simplify complex information for non-technical SME personnel. In a similar vein, adaptive AI-driven training modules have previously been developed to build workforce resilience by focusing on specific skill gaps of the individual, as described by (Aldoseri et al., 2025). These approaches focus not only on empowering the technologists but on empowering the employees-a key factor in Western regulatory regimes which emphasize human-centered cybersecurity approaches, such as under GDPR or CCPA.

2.4 Integrated Framework Potential

The integration of AI into IT systems for SMEs shows great possibilities of creating a very resilient system getting to anticipate, resist, and recover from cyber incidents. According to (Hassan et al., 2023), organizational readiness, including AI literacy and social capital, is vital for the successful adoption. Adaptive AI solutions give SMEs the power to keep watch continuously and enable automated responses. This aligns with those frameworks sponsored by the U.S. National Institute of Standards and Technology (NIST). Such understanding indicates that AI-integrated resilience frameworks can bolster SMEs to apply a cost-effective phased approach to strengthening their defense mechanisms, thereby making cyber resilience feasible for otherwise resource-constrained organizations.

3. Purpose of the Article

The paper aims to propose an AI-integred IT framework hypothetical, yet promising for SMEs in the U.S. and other Western contexts to build their cyber-resilience on ever-so-cheap and incremental steps. Increasing cyber threats to SMEs thus demand exploiting AI to automate threat detection, speed up incident response, and improve workforce skills. The first goal is mapping the existing cybersecurity and AI adoption challenges in Western SMEs, including constraints such as lack of financial resources or technical know-how or awareness of AI's potential in cybersecurity. The second goal relates advances in AI-based threat detection and response and workforce training by identifying inexpensive and scalable AI solutions suitable for an SME environment. The third goal is designing a phased resource-sensitive framework based on the NIST Cybersecurity Framework (CSF) principles, which allows SMEs to start small with the adoption of AI tools and build the resilience incrementally over time. At last, this article seeks to evaluate the framework's effectiveness and adoption ease to ensure it fits the operational realities of SMEs and provides viable pathways for these enterprises to produce adaptive defenses enhanced with AI against evolving threats in the Western digital land.

4. Research Result

The SME-AI Resilience Framework (SAIRF) is a wide-ranging, model encompassing four full phases, resulting in an application that integrates AI effectively within small- and medium-sized enterprises

(SMEs). In theory, this allows it to become more cyber-resilient. The framework takes into consideration the big challenges an SME faces, such as an extremely restrictive budget, a lack of internal expertise, ever-changing cyber threats-and so on-and presents solutions that shine in cases requiring scalability, cheap solutions, and conformity with recognized cybersecurity standards, including the NIST Cybersecurity Framework (CSF) (Vihaan & Adrian, 2025).

Phase 1: Awareness and Baseline facilitates the establishment of cybersecurity baselines through lightweight risk assessments designed for the SME context. The risk assessments use accessible yet user-friendly tools, so an SME understands its current risk posture without requiring heavy technical resources (Fernandez de Arroyabe et al., 2024). Simultaneous AI-based employee training is implemented, using adaptive learning modules with phishing simulation in order to increase employee awareness and preparedness as the human factor sometimes can result in security breaches. Management is introduced into viewing AI-augmented cyber intelligence tools, such as generative AI bots, to feed them with a less technically overwhelming alert perspective thus encouraging them to decide and work on cybersecurity priorities (Thomas, 2024).

Phase 2: Detection & Monitoring sees the deployment of inexpensive AI-assisted anomaly detection solutions. Such solutions are usually delivered as SaaS tools observing the network traffic and the activity on endpoints for unusual patterns that might constitute a security incident. Thanks to generative AI, alerts are automatically summarized into reports digestible to non-technical staff, ensuring quick comprehension and response along the whole organization (Carayannis et al., 2024).

Phase 3: Response and Recovery, involves setting simple yet effective incident response plans that are supported by AI. These plans simulate workflows for the containment, mitigation, and recovery phases of a cyber event. The security posture of the organization is trained and tested with weaknesses in response responses identified utilizing AI simulation drills for ransomware attack scenarios (Fidel- Anyana et al., 2025).

Phase 4: Continuous Improvement revolves around quarterly updates of AI-enhanced threat intelligence, with generative AI analysis providing current threat information to SMEs. Workforce training modules are dynamically adapted corresponding to identified skill gaps to keep employee competencies in tune with the threat landscape. The governance structure within this phase is mapped against the NIST CSF functions - Identify, Protect, Detect, Respond, and Recover - to ensure a formalized and ongoing solicitation of resilience improvements (Jackson, 2024).

4.2 Framework Advantages

Benefits of the SAIRF model for SMEs include:

Cost-effectiveness: By employing lightweight SaaS solutions and letting SMEs tap into free and regionally funded cybersecurity resources, this framework works to reduce the financial roadblocks that normally prevent SMEs' efforts in cybersecurity (Eberhardsteiner, 2024).

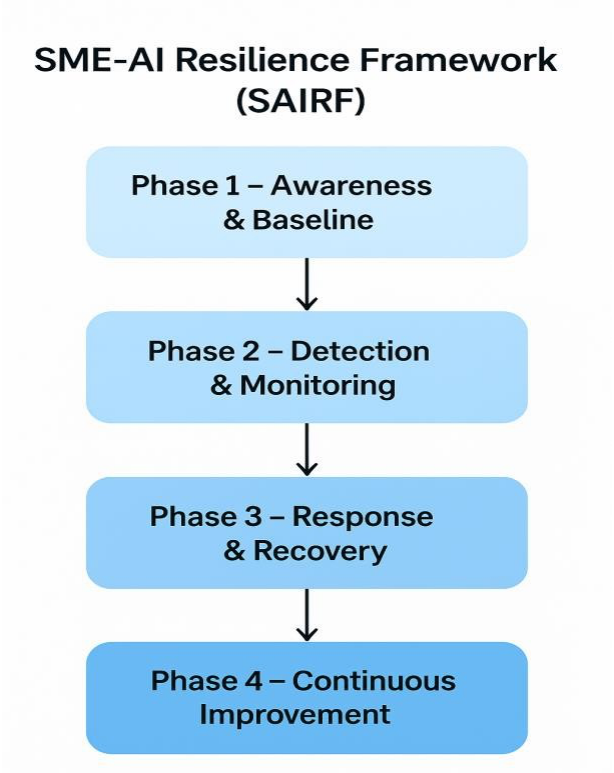
Scalability: This modular, phased process allows the SME to take up elements of the framework depending on its maturity and available funds. Organizations slowly build capabilities on their own without requiring cash resources that are scarce (El Shenawy et al., 2025).

AI Empowerment: The use of AI enhances technical detection-and-response abilities beyond providing clarity of communications and sufficiently training the workforce. Automated, adaptive alerts and training reduce human-induced risk and foster improved cyber hygiene (Ode et al., 2025).

Standards-Aligned: Aligning the framework with the NIST CSF ensures that SMEs are working with a recognized and thorough guide to cybersecurity, thus encouraging on-time compliance and raising confidence from stakeholders (Fernandez de Arroyabe et al., 2024).

Figure 1

SME-AL Resilience Framework (SAIRF



4.3 Illustrative Case Study (Hypothetical)

Consider another case of a hypothetical software SME in the United States, employing approximately 50 people, which embarked on SAIRF starting with Phase 1 as show in figure 4.2. In their risk assessment, they used freeware available online to ascertain their baseline cybersecurity posture. After this, they started the rollout of AI-powered adaptive employee training programs complemented with

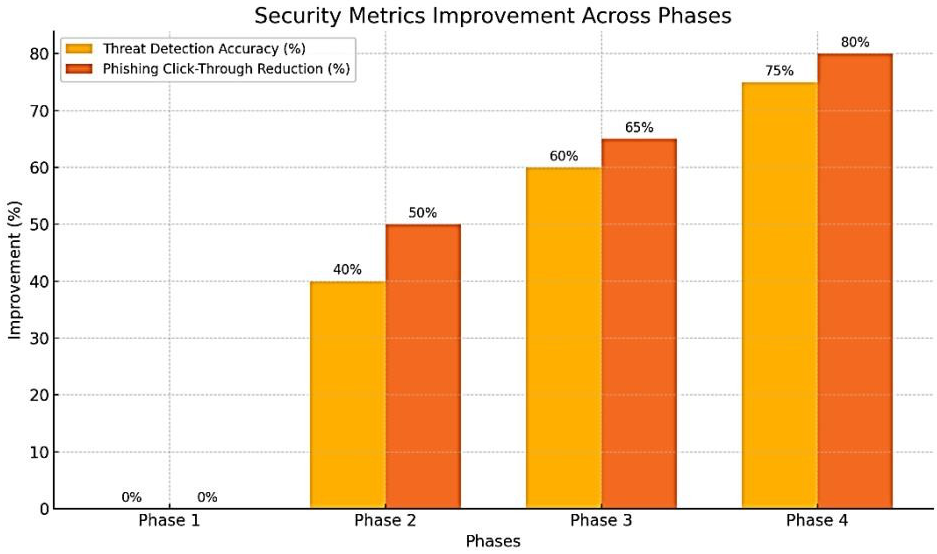
industry-specific phishing simulations (Carayannis et al., 2025).

Once Phase 1 has been successfully completed, a decision is made by this SME to move into Phase 2 by subscribing to an AI anomaly detection SaaS that is priced at $300 on a monthly subscription basis. The system monitors network traffic and end points on an ongoing basis, giving a warning of suspicious activity. The generative AI in the tool takes a shortcut by summarizing security alerts to layman reports for non-technical staff so that they can fast understand and act upon the matter (Pemmasani, 2023). plans and ransomware simulation drills that enhance the recovery time objectives (RTO) and containment strategies of the company (Hokmabadi et al., 2024).

While in Phase 4, quarterly updates based on generative AI analyses keep the SME abreast of ever-changing threats, and workforce training modules are being amended to remediate the newly-discovered vulnerabilities. Governance adapted by NIST CSF assures the continuous enhancement of policy and procedures.

Figure 2

Security Metrics Improvement across phases



5. Conclusion

Given their limited resources and growing attacks' sophistication, the risk of cyber-attacks remains high and above average for SMEs. Nevertheless, AI offers scalable and low-cost tools for detection, response, training, and governance. SAIRF contains a phased, AI-Powered roadmap tied to NIST CSF the idea is to bring SMEs cyber resilience in a gradual way at the least investment yet highest impact. Future steps include piloting the SAIRF on diverse SMEs across the United States and Europe, determining the ROI, assessing resilience incrementally over time, and investigating regulatory incentives that can aid its adoption. The use of AI-driven IT resilience infrastructure will strengthen SMEs' resilience gap and allow them to confidently operate in an ever-evolving threat landscape.

References

Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2024). A framework for building resilience through innovation and process optimization in AI-powered digital transformation. In M. A. Badar, R. Gupta, P. Srivastava, I. Ali, & E. A. Cudney (Eds.), *Handbook of digital innovation, transformation, and sustainable development in a post-pandemic era*(pp. 3–33). CRC Press. https://doi.org/10.1201/9781003438748-2

Button, D. J., Ophoff, J., Irons, A., & McDonald, S. (2025). Mind the gap: Exploring perceptions of cyber security in the SME context. *Information & Computer Security*. Advance online publication. https://doi.org/10.1108/ICS-02-2025-0047

Carayannis, E. G., Dumitrescu, R., Falkowski, T., & Zota, N.-R. (2024). Empowering SMEs: Harnessing the potential of Gen AI for resilience and competitiveness. *IEEE Transactions on Engineering Management, 71*, 14754–14774. https://doi.org/10.1109/TEM.2024.3456820

Carayannis, E. G., Dumitrescu, R., Falkowski, T., Papamichail, G., & Zota, N.-R. (2025). Enhancing SME resilience through artificial intelligence and strategic foresight: A framework for sustainable competitiveness. *Technology in Society, 81*, 102835. https://doi.org/10.1016/j.techsoc.2025.102835

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review, 50*, 100592. https://doi.org/10.1016/j.cosrev.2023.100592

Eberhardsteiner, L. (2024). *Adopting AI in SMEs: Development of a framework for adopting AI in SMEs with a focus on security and privacy concerns* [Doctoral dissertation, Johannes Kepler University Linz]. JKU ePUB. https://epub.jku.at/obvulihs/content/titleinfo/11427103

El Shenawy, A. S., Khourshed, N. F., Ragheb, M. A., & Beshr, M. H. (2025). Integration of Industry 4.0 and Lean Six Sigma: Critical success factors for overcoming socioeconomic challenges in the telecommunication sector. *SocioEconomic Challenges, 9*(1), 80–100. https://doi.org/10.61093/sec.9(1).80-100.2025

Fernández de Arroyabe, J. C., Arroyabe, M. F., Fernández, I., & Arranz, C. F. A. (2024). Cybersecurity resilience in SMEs: A machine learning approach. *Journal of Computer Information Systems, 64*(6), 711–727. https://doi.org/10.1080/08874417.2023.2248925

Fidel-Anyana, I., Onus, E. G., Mikel-Olisa, U., & Ayanbode, N. (2025). AI-driven cybersecurity frameworks for SME development: Mitigating risks in a digital economy. *International Journal of Multidisciplinary Research and Growth Evaluation, 6*(1), 982–988. https://doi.org/10.54660/.IJMRGE.2025.6.1.982-988

Hassan, Y. G., Collins, A., Babatunde, G. O., Alabi, A. A., & Mustapha, S. D. (2023). AI-powered cyber-physical security framework for critical industrial IoT systems. *Machine Learning, 27*.

Hokmabadi, H., Rezvani, S. M., & de Matos, C. A. (2024). Business resilience for small and medium enterprises and startups by digital transformation and the role of marketing capabilities—A systematic review. *Systems, 12*(6), 220. https://doi.org/10.3390/systems12060220

Iqbal, J., & Abbas, A. (2025). Cybersecurity and AI synergy for SME resilience and economic equality[Unpublished manuscript].

Iyelolu, T. V., Agu, E. E., Idemudia, C., & Ijomah, T. I. (2024). Driving SME innovation with AI solutions: Overcoming adoption barriers and future growth opportunities**.** *International Journal of Science and Technology Research Archive, 7*(1), 36–54. https://doi.org/10.53771/ijstra.2024.7.1.0055

Jackson, M. (2024, November). Empowering SMEs through digital transformation: Harnessing AI and cybersecurity for long-term success

Lani, K., & Abbas, N. (2025). Data-driven AI solutions for strengthening SME resilience in cyber risk environments [Unpublished manuscript].

Lu, X., Wijayaratna, K., Huang, Y., & Qiu, A. (2022). AI-enabled opportunities and transformation challenges for SMEs in the post-pandemic era: A review and research agenda**.** *Frontiers in Public Health, 10*, 885067. https://doi.org/10.3389/fpubh.2022.885067

Ode, E., Awolowo, I. F., Nana, R., & Olawoyin, F. S. (2025). Social capital and artificial intelligence readiness: The mediating role of cyber resilience and value construction of SMEs in resource-constrained environments**.** *Information Systems Frontiers*. Advance online publication. https://doi.org/10.1007/s10796-025-10608-z

Pemmasani, P. K. (2023). National cybersecurity frameworks for critical infrastructure: Lessons from governmental cyber resilience initiatives**.** *International Journal of Acta Informatica, 2*(1), 209–218. https://www.yuktabpublisher.com/index.php/IJAI

Sundaramurthy, S. K., Ravichandran, N., Inaganti, A. C., & Muppalaneni, R. (2022). AI-powered operational resilience: Building secure, scalable, and intelligent enterprises. *Artificial Intelligence and Machine Learning Review, 3*(1), 1–10.

Thomas, C. (2024, November). Digital transformation for SMEs: Leveraging AI and cybersecurity for sustainable growth [Unpublished manuscript].

Vihaan, A., & Adrian, G. (2025). AI-integrated business intelligence: Safeguarding SMEs in the digital market [Unpublished manuscript].