Security Evaluation of Industrial Organisations in an Isolated Region

Jules Martial Yin-belta Mbara*, Fehmi Jaafar†, Pierre Martin Tardif‡
*†Department of Computer Science and Mathematics (DIM),Quebec University at Chicoutimi Canada
Emails: julesmartialmbara@gmail.com, fjaafar@uqac.ca
‡SIMQG Department, Management School, University at Sherbrooke, Canada
Email: pierre-martin.tardif@usherbrooke.ca

***Abstract*—This paper presents the results of a cybersecurity audit conducted on thirty industrial SMEs located in a remote region of Eastern Canada. These firms face growing cyber threats while having limited access to security expertise and infrastructure. Using a mixed-method approach combining on-site technical assessments, structured interviews, and questionnaires, the study analyzes vulnerabilities through the TOE framework (Technological, Organizational, Environmental). Results show that 90% of companies lacked internal network segmentation, 80% were vulnerable to phishing attacks, and over 70% had no cybersecurity training or formal security policy. Based on these findings, we propose a set of low-cost and practical recommendations tailored to SMEs in isolated regions. These include awareness training, simple network protections, and internal policy development. The study highlights the urgent need for targeted cybersecurity strategies adapted to geographic and resource constraints, and contributes to both academic and operational understanding of how to improve cyber resilience in decentralized industrial ecosystems.**

Keywords— Cybersecurity, Industrial SMEs, Human factor, Field audit, Vulnerabilities, Law 25

I. Introduction

The cybersecurity of industrial systems has become a major global concern due to the massive integration of digital technologies into industrial processes [1]. These systems, encompassing manufacturing plants, energy distribution networks, and other critical infrastructures, are essential to the economic and social functioning of societies [2]. Their increasing interconnectivity, combining Information Technology (IT) and Operational Technology (OT), has optimized operations but also introduced significant vulnerabilities to cyber threats [3]. Cyberattacks targeting industrial environments can result in prolonged operational disruptions, financial losses, data breaches, and, in severe cases, threats to public safety [4, 5]. The attacks against the Colonial Pipeline in 2021 and Norsk Hydro in 2019 exemplify the devastating impact of cybersecurity breaches on industrial operations [6]. These incidents underscore the urgent need for robust cybersecurity practices adapted to industrial contexts. The situation is even more critical in remote regions where small and medium-sized enterprises (SMEs) play a vital role in the local economy. These companies sustain employment, contribute to regional supply chains, and maintain the economic fabric [7]. However, they often operate with limited financial resources, outdated technological infrastructures, and minimal access to specialized cybersecurity expertise [8]. Consequently, cybersecurity is frequently considered a secondary concern compared to immediate business priorities [9]. Emerging technologies, such as large language models, offer new opportunities for threat detection and cyber defense [10]. Nevertheless, vulnerabilities persist, particularly in smart industrial environments where the complexity of interconnected systems creates multiple attack vectors [4]. A detailed understanding of these vulnerabilities is critical to designing effective cybersecurity strategies for SMEs, especially those operating in isolated regions. This study addresses these challenges by conducting a field audit of industrial SMEs located in a remote region of Eastern Canada. The regional economy is primarily based on manufacturing, energy, and agri-food sectors, with enterprises typically employing between 10 and 50 employees. The geographic isolation exacerbates cybersecurity challenges by limiting access to specialized IT services and slowing the adoption of security best practices. In this paper, we are applying the TOE framework [11] to provide a holistic analysis of cybersecurity vulnerabilities. Building upon recent reviews on cybersecurity risks among SMEs [12, 13], the study combines on-site technical audits, structured interviews, and organizational assessments to build a comprehensive picture of the cybersecurity posture. The primary objective of this research is to identify the key cybersecurity vulnerabilities faced by SMEs in this isolated region [14, 15], by applyin a mixed-methods approach combining technical and qualitative assessments [16, 17], and then propose the practical recommendations tailored to the specific constraints of these enterprises [18]. By aligning with the TOE framework [11] and incorporating insights from industrial cybersecurity studies [19, 20], our goal is to contribute both academically and operationally to strengthening cybersecurity resilience among industrial SMEs operating in geographically isolated environments.

II. Background and Related Work

Cybersecurity encompasses the strategies, practices, and technologies aimed at protecting computer systems and digital data from unauthorized access, cyberattacks, and malicious threats [2]. In the industrial context, securing data and critical business processes is crucial for operational continuity and competitiveness [1]. The increased digitalization and intercon-

nectivity of modern industrial systems have amplified their exposure to cyber threats [4], resulting in severe operational and financial impacts [21]. Cyberattacks targeting industrial environments, such as the Colonial Pipeline attack in 2021 or the Norsk Hydro ransomware incident in 2019, have demonstrated the devastating consequences of such threats [22, 6]. These cases emphasize the urgent need for robust cybersecurity measures, especially for SMEs located in remote areas with limited resources [12]. Among the vulnerabilities identified in the literature, human factors remain critical. Studies have shown that human error is responsible for the majority of cybersecurity incidents [9]. Poor password practices, phishing susceptibility, and lack of employee awareness are among the leading causes [18, 3]. Additionally, outdated IT infrastructure and missing software updates expose companies to well-known and easily exploitable vulnerabilities [23, 8]. Environmental and organizational challenges further complicate cybersecurity for SMEs in isolated regions. Limited access to specialized expertise, low availability of advanced technological services, and non-compliance with regulations like Quebec's Law 25 contribute to increased risks [24, 25]. Emerging technologies, such as large language models for cybersecurity detection, offer new possibilities, yet industrial SMEs continue to face persistent network vulnerabilities [10, 4]. Furthermore, the need for systematic evaluation protocols, such as the Application Security Assessment Protocol (ASAP), becomes essential to assess and mitigate risks effectively [26]. To synthesize the key characteristics of cyberattacks affecting industrial SMEs, Table I summarizes the main attack types, their causes, and associated risks based on the ICS ATT&CK Matrix.

III. METHODOLOGY

This section presents the detailed methodological framework adopted in this study, based on a mixed-method approach that combines qualitative and quantitative techniques to assess cybersecurity vulnerabilities among industrial SMEs.

A. Methodological Approach

The research employed a mixed-method design, integrating empirical technical audits, structured questionnaires, and semi-structured interviews. Quantitative assessments were conducted through technical tools such as Nmap, Nessus, and Horizon3.ai to identify existing vulnerabilities in systems and networks [23]. SMEs were selected using stratified sampling, based on criteria such as company size (10-50 employees), sector (manufacturing, energy, agri-food), and geographical isolation (more than 100 kilometers from a major urban center) [12]. Qualitative data were collected through semi-structured interviews with managers, IT staff, and employees, complemented by questionnaires focusing on cybersecurity practices, risk awareness, and organizational culture [18]. Statistical analysis was conducted using SPSS, maintaining a confidence level of 95% for the results [27]. The overall methodological process is summarized in Figure 1, combining technical data collection with organizational and human factor analysis under the TOE framework [11].

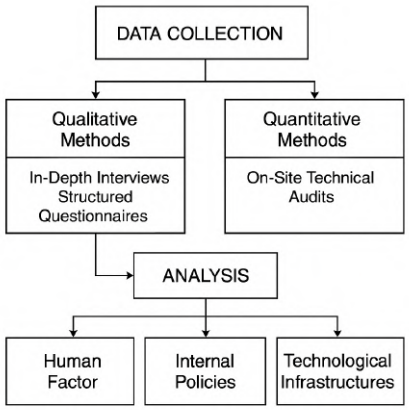

Fig. 1. Schematic representation of the methodological process combining technical audits, interviews, and the TOE framework

B. Justification of the Theoretical Framework

Several theoretical models have been proposed to study technology adoption and cybersecurity behaviors. The Technology Acceptance Model (TAM) introduced by Davis [28] emphasized perceived usefulness and ease of use but mainly focused on individual acceptance rather than organizational or environmental factors. The Unified Theory of Acceptance and Use of Technology (UTAUT) by Venkatesh et al. [29] expanded this view by integrating social influences and facilitating conditions but remained largely oriented towards user behavior without addressing technical vulnerabilities. Structural modeling approaches such as ISM [30] and causal analysis models like DEMATEL [31] provided valuable insights into interdependent decision-making but require formal structures and complex modeling efforts, making them impractical for resource-limited SMEs. More recent hybrid models combining TOE and TAM frameworks, such as the one proposed by Yadegaridehkordi et al. [32], aim to balance technical, organizational, and behavioral dimensions but are still in early empirical stages, especially for industrial contexts. Given these considerations, the TOE framework [11] remains the most appropriate choice for this study. It enables a structured analysis of technological infrastructures, organizational capabilities, and environmental constraints faced by industrial SMEs, providing a holistic view essential for understanding cybersecurity vulnerabilities in isolated regions.

C. Comparative Analysis of Cybersecurity Theoretical Frameworks

The principal cybersecurity frameworks evaluated for potential use in this study are summarized in Table II. The TOE framework was selected based on its suitability for capturing the complex interplay between technical, organizational, and environmental factors in SMEs.

TABLE I
SUMMARY OF CYBERATTACK TYPES, CAUSES, AND RISK IMPACTS IN INDUSTRIAL SMES (ADAPTED TO ICS ATT&CK MATRIX)

Ref [#]	Year	Attack Types (ICS ATT&CK Matrix)	Cause	Risk Impact
[9]	2020	Phishing, Credential Access, Data Leakage	Lack of training, Weak passwords	Employee manipulation, Data breach
[8]	2020	Ransomware, Initial Access Exploits	Outdated infrastructure	Operational shutdown, Data loss
[3]	2019	Insider Threats, Human Error, Unsecure Configurations	No security training, Mismanagement	Data theft, System compromise
[23]	2015	Control System Attacks, Network Intrusions	Unpatched ICS, Weak segmentation	Production disruptions, Safety incidents
[1]	2024	Remote Exploits, Protocol Abuse	Unsecured industrial protocols	Command hijacking, Critical failures
[2]	2002	General Cyberattacks, Risk Exposure	Underinvestment in cybersecurity	Severe financial loss, Reputational damage
[13]	2024	Phishing, Weak Credential Use	Lack of awareness programs	Social engineering success, Unauthorized access
[15]	2024	Compliance Failures, Data Exfiltration	Regulation gaps, Limited expertise	Legal penalties, Persistent vulnerabilities

TABLE II
COMPARATIVE ANALYSIS OF CYBERSECURITY THEORETICAL FRAMEWORKS FOR SMES

Framework	Key Objective	Main Limitations	Suitability
TAM [28]	Understand technology acceptance at individual level	Ignores organizational and environmental factors	Low
UTAUT [29]	Integrate behavioral, social, and facilitating conditions in technology adoption	Focused only on user behavior, not technical vulnerabilities	Low
ISM [30]	Structure complex decision relationships	Requires formal structures, unsuitable for small firms	Low
DEMATEL [31]	Analyze causal relationships among variables	High complexity and modeling effort required	Low
Hybrid TOE-TAM [32]	Combine technological, organizational, and behavioral dimensions	Limited validation in industrial SME contexts	Moderate
TOE [11]	Analyze technology, organization, and environment jointly	Older model, but robust and adaptable for SMEs	High

D. Data Collection Strategy

The data collection strategy was conducted in four sequential phases. First, a preliminary questionnaire was distributed to gather initial information about cybersecurity practices. Second, on-site technical audits were carried out using Nmap, Nessus, and Horizon3.ai tools to detect vulnerabilities in network infrastructures, systems, and applications [26]. Third, semi-structured interviews were conducted with company leaders and IT staff to identify organizational practices, incident management capabilities, and levels of employee awareness [3]. Finally, a post-audit evaluation was performed to monitor initial improvements and measure changes in cybersecurity posture. Data from all sources were categorized according to the TOE framework's three dimensions. This categorization allowed for a granular analysis of the vulnerabilities and risk factors specific to each technological, organizational, and environmental domain, enabling the development of targeted recommendations [11].

IV. RESULTS AND DISCUSSION

This section analyzes the cybersecurity audits conducted on thirty industrial SMEs located in a remote region [12]. The results are structured according to the TOE framework [11], combining technical findings and organizational observations.

A. General Cybersecurity Posture

The audits revealed a generally low cybersecurity maturity level across the SMEs. Approximately 60% had no formal security policies [33], and 50% operated obsolete IT infrastructures [23]. Vulnerability scanning showed that: - 90% lacked internal network segmentation [8] - 80% had unnecessary open ports [4] - 65% lacked properly configured firewalls [26] On the human side, 70% of SMEs experienced incidents due to employee mistakes [14]. Phishing attacks were the most prevalent, affecting 80% of firms [9]. Most employees had never received basic cybersecurity training prior to the audit [18]. These findings are summarized in Figure 2, illustrating the distribution of the most frequent vulnerabilities.

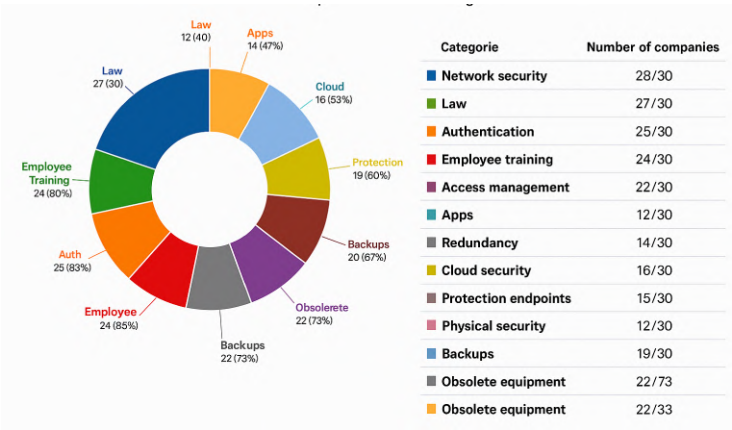

Fig. 2. Frequent cybersecurity vulnerabilities identified across 30 SMEs

B. Comparative Evaluation of Service Providers

Some SMEs had previously engaged local service providers for cybersecurity assessments. Two providers' performances were compared. The first provider performed manual audits and identified most technical vulnerabilities but did not assess human factors [16]. The second provider combined automated scans with awareness training, leading to better outcomes

in reducing human risks [30]. This comparison is shown in Figure 3, contrasting their effectiveness.

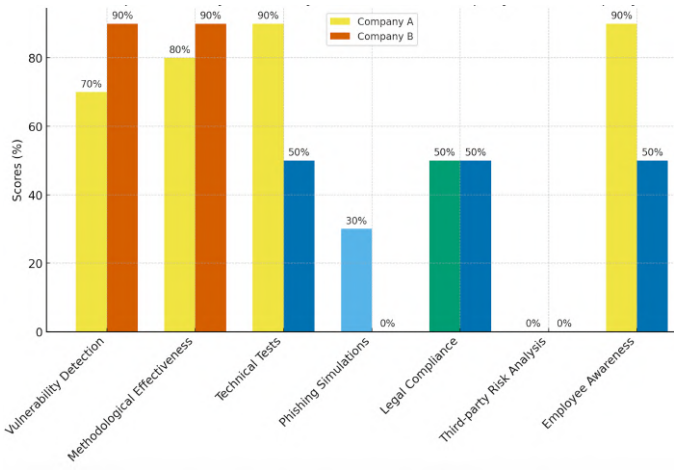

Fig. 3. Comparison of service providers' performance

C. Case Studies of Anonymized SMEs

Three representative SMEs are presented as case studies to highlight the measurable impacts of recommended corrective actions. - **SME A**: Implemented daily backups and password rotation after initially lacking basic controls [17] - **SME B**: Encrypted sensitive data and segmented networks, improving compliance with Québec's Law 25 [34] - **SME C**: Secured Wi-Fi access and separated networks, eliminating unauthorized connections [4] Figure 4 illustrates compliance improvements observed after interventions.

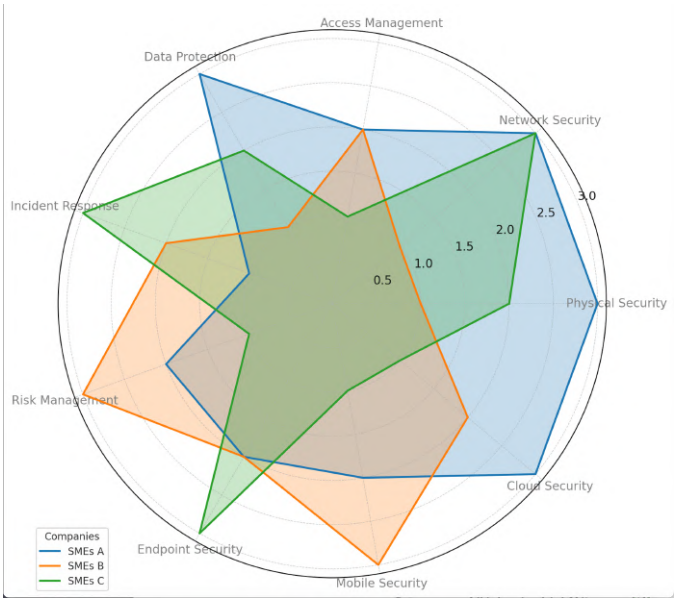

Fig. 4. Compliance levels before and after security improvements in 3 SMEs

D. Cross-Dimensional Analysis

Using the TOE framework, the main cybersecurity problems are categorized by technological, organizational, and human factors. Technological weaknesses include obsolete systems and poor segmentation [23]. Organizational gaps center around the absence of formal policies and lack of incident response capabilities [19]. Human errors remain a predominant risk due to insufficient awareness training [9]. Figure 5 shows the overall distribution of cybersecurity issues across SMEs. The

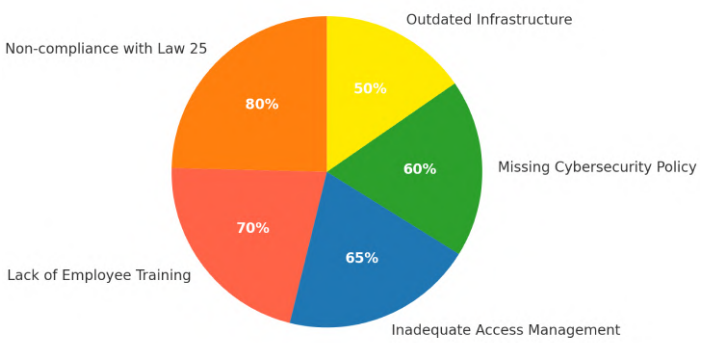

Fig. 5. Cybersecurity problems observed across audited SMEs

vulnerabilities identified are further categorized according to the TOE framework in Table II.

V. Recommendations

This study identifies several short-, medium-, and long-term actions to improve cybersecurity resilience among industrial SMEs in isolated regions. These recommendations are structured according to the TOE framework and are designed to be actionable, affordable, and realistic for SMEs with limited technical and financial resources. These actions are formulated based on the vulnerabilities observed and aligned with the TOE framework [11].

In the short term (0 to 3 months), companies should immediately address critical vulnerabilities through low-cost initiatives. It is crucial to establish a basic documented cybersecurity policy covering key aspects such as password management, data protection, and user access rights [33]. Password policies may enforce complexity requirements and mandate renewal every 90 days [21]. Implementing multi-factor authentication (MFA) on critical systems such as email and accounting software is essential to prevent credential theft [13]. Free or governmental cybersecurity awareness programs can be deployed internally to train employees on basic digital hygiene practices [18]. Regular and disconnected backups must also be set up to mitigate ransomware threats [23]. Networks can be hardened by closing unused ports and disabling obsolete services like SMBv1 [10].

In the medium term (3 to 6 months), SMEs should develop more structured cybersecurity initiatives. Formalizing an incident response plan with clear responsibilities and communication protocols is necessary to enable rapid responses to cyber incidents [19]. Networks should be segmented by functional units to contain lateral movement in case of compromise [8]. Updating obsolete infrastructures (operating systems, routers,

servers) should be prioritized to eliminate known vulnerabilities [22]. Bill 25 compliance must be systematically pursued through audits and the appointment of a part-time data protection officer to reduce regulatory exposure [34]. SMEs should also formalize cybersecurity clauses when contracting external IT providers [24] and designate an internal cybersecurity liaison officer among existing staff [35].

In the long term (6 to 12 months and beyond), sustainable measures must be implemented to ensure resilience. SMEs in isolated regions could benefit from the establishment of a shared regional cybersecurity resource hub to mutualize support and training services [20]. Investing in affordable automated threat detection tools such as Endpoint Detection and Response (EDR) systems will help SMEs proactively detect anomalies [36]. Partnerships with educational institutions to organize continuous cybersecurity awareness programs would also strengthen the cybersecurity culture over time [37].

Together, these measures provide a step-by-step path for SMEs to enhance their cybersecurity posture without requiring large investments or specialized expertise.

VI. Conclusion and Future Research Directions

This study conducted a comprehensive field analysis of cybersecurity vulnerabilities among thirty industrial SMEs operating in an isolated region. Using a rigorous mixed-method approach structured around the TOE framework [11], the results revealed significant weaknesses in technological infrastructures, organizational governance, and human factors. Technological audits showed that 50% of SMEs operated with outdated systems, and 90% had no internal network segmentation, greatly increasing exposure to cyberattacks [23, 8]. Organizationally, the absence of cybersecurity policies and training programs in 70% of companies indicated a lack of structured risk governance [33]. Human vulnerabilities, particularly related to phishing and poor password management, were also found to be major risk amplifiers, affecting more than 75% of the audited organizations [3, 9]. These findings confirm that cybersecurity challenges in industrial SMEs cannot be treated solely from a technical perspective; they require integrated responses that also consider organizational processes and local environmental constraints [15, 25]. Despite limited resources, some SMEs achieved significant improvements following basic technical and organizational corrections, demonstrating that even modest efforts can yield tangible results when properly targeted [38]. The comparison between two local cybersecurity service providers highlighted the trade-offs between manual customization and automation, emphasizing the need for tailored approaches rather than standardized solutions [24, 13]. Several research perspectives emerge from this work. First, it would be valuable to design and experimentally test low-cost cybersecurity solutions specifically adapted to SMEs with limited technological infrastructures [2]. Second, regional cooperation models could be explored to allow SMEs to share cybersecurity services and expertise [39]. Third, future studies should evaluate the effectiveness of AI-based phishing detection systems in decentralized and low-resource environments [10]. A longitudinal evaluation of behavioral changes following cybersecurity training initiatives would also provide valuable insights [18]. Finally, integrating cybersecurity incentives into local public policies could encourage a wider adoption of minimal protection measures among SMEs in isolated regions [40]. This article constitutes a foundational contribution to understanding the specific cybersecurity needs of industrial SMEs in remote areas and lays the groundwork for further scientific and operational advances toward a more resilient regional cybersecurity posture [5]. This study has several limitations. It focuses on a specific geographical area and a limited sample of thirty SMEs, which may affect the generalizability of the results. Some data were self-reported through interviews and questionnaires, which can introduce response bias. The study did not include real-time penetration tests or simulated attacks, and the long-term effectiveness of the proposed measures has not yet been assessed. Future research should address these aspects by expanding the study to other regions, using behavioral tracking, and evaluating results over time under realistic threat conditions.

Acknowledgment

The authors thank the Natural Sciences and Engineering Research Council of Canada (NSERC), the Mathematics of Information Technology and Complex Systems (MITACS) and the Desjardins Group (Mouvement Desjardins) for their financial support.

References

[1] Raza Ahmad, Sanjay Kumar, and Dhiren Patel. “Securing Industry 4.0: Assessing cybersecurity challenges and solutions”. In: *Computers in Industry* 156 (2024), p. 103933.

[2] Lawrence A. Gordon and Martin P. Loeb. “The Economics of Information Security Investment”. In: *ACM Transactions on Information and System Security* 5.4 (2002), pp. 438–457.

[3] Uchenna Daniel Ani, Hongmei He, and Ashutosh Tiwari. “Human factor security: evaluating the cybersecurity capacity of the industrial workforce”. In: *Journal of Systems and Information Technology* 21.1 (2019), pp. 2–35.

[4] Adnan Khan et al. “Exploring the Potential Network Vulnerabilities in the Smart Industrial Environment”. In: *IEEE Access* 12 (2024), pp. 106596–106612.

[5] Marco Gercke, Moses Mutemwa, and Dewald Sacks. “Cybersecurity threats experienced by small businesses”. In: *Security Journal* (2023).

[6] Dragos Inc. *2021 ICS Cybersecurity Year in Review*. Tech. rep. Dragos Inc., 2021.

[7] Maqsood Ahmed, Shahzad Khan, and Liaqat Ali. “The impact of cybersecurity on SMEs strategies through technological infrastructure”. In: *Journal of Industrial Policy and Development* 3.1 (2023), pp. 45–58.

[8] Thomas Williams, Jason Beale, and Steven Furnell. "Cyber security vulnerabilities in industrial control systems: Addressing the emerging challenges of Industry 4.0". In: *Computers & Security* 96 (2020), p. 101920.

[9] Steven Furnell and Jayesh N. Shah. "Home working and cyber security – an outbreak of unpreparedness?" In: *Computer Fraud & Security* 2020.8 (2020), pp. 6–12.

[10] Xiao Zhang et al. "Application of Large Language Models in Cybersecurity". In: *IEEE Access* 12 (2024), pp. 67242–67261.

[11] Louis G. Tornatzky and Mitchell Fleischer. *The Processes of Technological Innovation*. Lexington Books, 1990.

[12] Teresa Pereira, Henrique Santos, and João Martins. "Cybersecurity Risk Management in Small and Medium Enterprises: A Systematic Review of Recent Evidence". In: *International Journal of Information Security* 22.4 (2023), pp. 789–805.

[13] Yves Barlette, Annabelle Jaouen, and Pamela Baillette. "One size does not fit all: cybersecurity perspectives of SMEs". In: *Journal of Information Warfare* (2024).

[14] Marco Gercke, Katharina Krombholz, and Daniel Schatz. "Cybersecurity Resilience in SMEs: A Machine Learning Approach". In: *Journal of Computer Information Systems* (2023).

[15] Unal Tatar, Bilge Karabacak, and Adrian V. Gheorghe. "A Specialized Cybersecurity Risk Assessment Framework for SMEs". In: *Electronics* (2024).

[16] Peter Jones, Sarah Williams, and Thomas Brown. "Cybersecurity Challenges and Solutions for Small Businesses". In: *International Journal of Information Security* (2024).

[17] L. et al. Garcia. "Understanding Cybersecurity Frameworks and Information Security Standards". In: (2023).

[18] Karen Renaud and Jason R. C. Nurse. "Developing cybersecurity education and awareness programmes for SMEs". In: *Information and Computer Security* 32.1 (2024), pp. 1–15.

[19] John Smith, Robert Brown, and Michael Johnson. "Digital Transformation and Cybersecurity Challenges for Businesses". In: *Journal of Business Continuity & Emergency Planning* (2023).

[20] Thomas Johnson, Sarah Williams, and Wei Chen. "Interdisciplinary Approaches to Cybervulnerability Impact Assessment". In: *ACM CCS Proceedings* (2024).

[21] James Williams, Robert Thompson, and Michael Davis. "Digital transformation in SMEs: Identifying cybersecurity risks". In: *Journal of Business Research* (2024).

[22] Robert M. Lee, Michael J. Assante, and Tim Conway. "The Cybersecurity Landscape in Industrial Control Systems". In: *Proceedings of the IEEE* 104.5 (2016), pp. 1039–1057.

[23] Keith Stouffer et al. "Guide to Industrial Control Systems (ICS) Security". In: *NIST Special Publication* 800-82 (2015).

[24] Eli Rohn, Regner Sabillon, and Moses Dlamini. "Investigating the experiences of providing cybersecurity support to SMEs". In: *Computers & Security* 140 (2025), p. 101373.

[25] Ravi Sharma, Mark Johnson, and Dhiren Patel. "Cybersecurity needs for SMEs". In: *Issues in Information Systems* (2024).

[26] Michael Johnson, Rebecca Smith, and Anish Patel. "ASAP: Application Security Assessment Protocol". In: *IEEE Cybersecurity and Resilience Conference*. 2023, pp. 245–252.

[27] Arun Sukumar, Hannan Amoozad Mahdiraji, and Vahid Jafari-Sadeghi. "Cyber risk assessment for SMEs: Multilevel decision-making approach". In: ().

[28] Fred D. Davis. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology". In: ().

[29] Viswanath Venkatesh et al. "User Acceptance of Information Technology: Toward a Unified View". In: ().

[30] John N. Warfield. "Binary Matrices in System Modeling". In: *IEEE Transactions on Systems, Man, and Cybernetics* ().

[31] Emilio Fontela and André Gabus. *DEMATEL, Innovative Methods*. Technical Report. Geneva, Switzerland.

[32] Elaheh Yadegaridehkordi et al. "A Hybrid TOE-TAM Framework to Assess the Impact of Green IT Adoption on Sustainable Consumption Behavior". In: (2021).

[33] Adamu Garba and Aliyu Musa Bade. "An Investigation on Recent Cyber Security Frameworks". In: *International Journal of Computer Science and Information Security* ().

[34] René-Sylvain Bédard and Will Christodoulou. *Quebec's new Law 25 is the toughest privacy legislation in Canada. Here's why it matters*. https://cybersecurecatalyst.ca/quebecs-new-law-25-is-the-toughest-privacy-legislation-in-canada-heres-why-it-matters/.

[35] Mohammed Alharbi, Nancy Paterson, and Karen Renaud. "Revealing the realities of cybercrime in SMEs". In: *ACM Computing Surveys* (2024).

[36] Kapal Sharma, Anupam Joshi, and Bojan Klucaric. "A systematic review of current cybersecurity training methods". In: *ACM Computing Surveys* (2023).

[37] Skander Millequant. *Complete Guide on Data Protection in Quebec: A Deep Dive into Bill 25*. https://commissionnairesquebec.ca/en/decoding-bill-25/.

[38] Manuel Rodriguez, Carlos Garcia, and Elena Martinez. "Cybersecurity for Industry 5.0: trends and gaps". In: *Frontiers in Computer Science* (2024).

[39] Mohammed Alharbi, Nancy Paterson, and Karen Renaud. "Revealing the realities of cybercrime in SMEs". In: *Computers & Security* 138 (2024), p. 103598.

[40] Fred D. Davis. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology". In: *MIS Quarterly* 13.3 (1989), pp. 319–340.