International Journal of Computing and Digital Systems
2025, VOL. 17, NO.1, 1-14

http://dx.doi.org/10.12785/ijcds/1571023809

Fortifying Organizational Cyber Resilience: An Integrated Framework for Business Continuity and Growth Amidst an Escalating Threat Landscape

Anas Kanaan[1], Ahmad AL-Hawamleh[2], Mohammad Aloun[3], Almuhannad Alorfi[4] and Mohammed Abdalwahab Alrawashdeh[5]

[1]*Department of E-Business and Commerce, University of Petra, Amman, Jordan*
[2]*Department of E-Training, Institute of Public Administration, Riyadh, Saudi Arabia*
[3]*Department of Cyber Security, Irbid National University, Irbid, Jordan*
[4]*Department of Information Technology, King Abdul-Aziz University, Jeddah, Saudi Arabia*
[5]*Department of Administration and Finance, Queen Noor Civil Aviation Technical College, Amman, Jordan*

Received 23 April 2024, Revised 8 December 2024, Accepted 9 December 2024

Abstract: In the face of mounting cyber threats disrupting enterprises, this study emphasizes the critical role of organizational resilience in safeguarding business development and continuity. It proposes an integrated framework comprising proactive security policies, resilience testing, collaborative engagement, and the integration of emerging technologies. Employing a meticulous methodology blending literature analysis and framework development, the study identifies key components for a comprehensive cyber resilience framework. This analysis delves into evolving threat landscapes, digital ecosystems, resource constraints, and ethical obligations, surpassing established frameworks by emphasizing customization, collaboration, and proactive measures. The resulting framework is not only robust but also adaptable and ethical, offering strategic guidance for organizations seeking to embed cyber resilience within digital transformation initiatives. While acknowledging limitations and varying applicability based on organizational contexts, the study encourages further validation through field applications to enhance adaptability within diverse cybersecurity ecosystems. The practical implications extend to organizations aiming to fortify cybersecurity measures amid digital transformation. By addressing the dynamic nature of cyber threats and offering practical insights for implementation, the proposed framework supports innovation and growth. It provides a roadmap for organizations navigating the complexities of cybersecurity in the digital age, ensuring they remain resilient in the face of evolving threats. Ultimately, the study advocates for a proactive approach to cybersecurity, recognizing its pivotal role in sustaining business operations and fostering long-term success in today's interconnected world.

Keywords: Digital Age, Business Continuity, Sustainable Development, Evolving Threats, Cyber Resilience, Future Emerging Technologies.

1. Introduction

With the continual advancements in the field of information technology, organizations are increasingly faced with the challenges of the digital environment. The organizations are now exposed to a range of new cyberattacks, which are of great concern. However, this has also paved the way for further innovations and progress in the field [1]. These cyber risks range from impactful data breaches and cyber espionage to different kinds of advanced viruses [2]. The existence of such risks negatively impacts organizational growth. Resilience, which enables organizations to not only recover from threats but also continue routine operations under challenging conditions, is now recognized as an essential component of any organizational strategy [3].

The scale and potential impact of cyber threats on business development are profound, with real-world consequences that underscore the critical importance of robust cybersecurity measures. The frequency and severity of cyber threats have witnessed a significant surge in recent years, with a reported 105% increase in ransomware attacks alone [4]. The financial toll of these attacks is staggering, as cybercrime is estimated to cost businesses globally over $1 trillion annually by 2025 [5]. Furthermore, high-profile breaches, such as the SolarWinds incident in 2020, exemplify the far-reaching consequences of cyber threats

E-mail address: Anas.Kanaan@uop.edu.jo, alhawamleha@ipa.edu.sa, m.oun@inu.edu.jo, Aalorfi@kau.edu.sa, m.rawashdeh@qnac.edu.jo

on businesses and government entities, with sophisticated actors compromising sensitive data on an unprecedented scale [6].

These statistics underscore the practical relevance of understanding and mitigating cyber threats for business development. The reputational damage resulting from a cyberattack can be severe, eroding customer trust and confidence [7]. In a digitally connected landscape, where businesses rely heavily on technology for operations, innovation, and customer engagement, the potential disruption caused by cyber threats poses a direct threat to the continuity and progress of organizations [8]. As businesses increasingly embrace digital transformation and interconnected ecosystems, the need to comprehensively address cyber threats becomes not just a matter of compliance but also a strategic imperative for sustaining growth, safeguarding sensitive information, and maintaining a competitive edge in the modern business landscape [9]. In order to safeguard enterprises from cyber threats and lessen the effects of possible breaches, the idea of cyber resilience has gained popularity [10].

A proactive approach known as "cyber resilience" reduces vulnerabilities and guarantees quick recovery in the event of an attack [11]. It is a holistic strategy that encompasses comprehending the ecosystem of a firm, which includes its digital assets, personnel, operational procedures, and outside collaborations [12]. Risk evaluation, proactive threat monitoring, incident response planning, and encouraging a cybersecurity culture among staff members are all included in this. Exploring the cyber threat environment and organizational vulnerabilities, whether financial or political, brought on by hackers, criminal organizations, or hacktivists is necessary to understand cyber resilience [13], [14].

As businesses today manage enormous volumes of sensitive data, including customer information, intellectual property, and trade secrets, data protection is essential [15]. Theft of data may result in monetary and legal problems [16]. A multi-layered defensive strategy is needed to provide cyber resilience, including strong data security, encryption, access restrictions, and incident response procedures [17]. Additionally, it places a strong emphasis on data governance and legal compliance [18]. Data security not only preserves assets but also fosters confidence among stakeholders and clients [19].

This research endeavors to develop an actionable and adaptive cyber resilience framework aimed at securing business continuity and fostering progress in the face of escalating cyber threats. The study delves into the evolving cyber threat landscape and its impact on contemporary corporate resilience, seeking to equip organizations with effective strategies to defend their growth. With a focus on the critical importance of enhancing cyber resilience, the investigation provides insights into surviving cyberattacks and thriving in a digitally interconnected environment. By reviewing existing best practices and frameworks, the research aims to offer organizations a structured and adaptive approach to confront and mitigate the challenges posed by the evolving threat landscape. The outcome of this study is integral to ensuring the long-term viability and profitability of organizations as they leverage technology to enhance competitiveness and agility. The paper underscores the significance of establishing a close nexus between cybersecurity and business development for sustained organizational success.

This paper is structured as follows: Section 2 reviews the relevant literature on business development and cybersecurity frameworks. Section 3 presents the methodology for the study, detailing the framework development and literature selection process. Section 4 outlines the proposed framework for building cyber resilience, and Section 5 discusses the key challenges and considerations. Finally, Section 6 offers conclusions and recommendations for future research.

2. Literature Review

A. *Business Development's Role in Organizational Growth*

Business development is essential for an organization's expansion and long-term viability in the twenty-first century. It includes a range of approaches, programs, and projects intended to increase the impact, influence, and profitability of an organization [20], [21]. This extends past sales and marketing to embrace any endeavors that aid in the expansion and development of a business. Business development is crucial for organizational existence and serves as a reaction to market conditions [22], [23]. In order to explore unknown territory and set the route for long-term success, it seeks to recognize and take advantage of new possibilities, such as market segments, alliances, or emerging technology [24]. Effective business development activities help organizations reach untapped markets, generate new income streams, and stay one-step ahead of the competition. Business development helps companies negotiate the challenges of the twenty-first century, including the fast expansion of technology, globalization, and shifts in customer preferences [25], [23].

A vital component of an organization's strategy, sales, marketing, and innovation is business development, which links its strategic goal to operational implementation [26]. It entails looking for business opportunities, forming partnerships, and developing value propositions that appeal to partners and clients [27], [28]. Professionals in business development play the role of catalysts, coordinating cross-functional initiatives to match organizational objectives with market realities. They are essential to organizational flexibility as well, enabling businesses to change course and react to shifting market conditions [29]. Business development nowadays includes encouraging innovation in goods, services, and internal procedures in addition to looking for new markets and income sources [30]. They locate holes in the market and create plans to fill them, ensuring that businesses are competitive and flexible. Faced

with the constantly changing difficulties offered by the digital economy of the twenty-first century, this capacity for innovation and adaptation is crucial [31], [32].

B. Cybersecurity in Business Development

By integrating digital technology and the internet, the digital era has profoundly changed the growth of businesses. However, this quick digitalization has also brought forth new difficulties, notably in cybersecurity [33], [34]. Organizations must embrace digital transformation in order to increase their efficiency and competitiveness while also coping with the constantly changing cyber threat scenario [35]. Nowadays, businesses must incorporate digital technologies to be competitive in a globally networked environment [36]. While technology presents chances for development and innovation, it also generates weaknesses that businesses must deal with [37], [38]. The main issue is how to make use of modern technology while maintaining the availability, confidentiality, and integrity of data [39], [34]. This demonstrates the value of cybersecurity in the digital era since it is crucial to protecting business development.

Because of how interconnected businesses are becoming in the digital era, cybersecurity is essential for business development. Through digital interfaces, these enterprises are linked to stakeholders, partners, suppliers, and clients. The attack surface grows as cyber threats do as well [40], [34]. Beyond financial losses, brand reputation, consumer trust, and legal implications are all affected by cyberattacks [41]. The evolving cyber threat scenario has a direct impact on the resilience and ongoing success of business development [42]. Because of this, cybersecurity is not only a technological issue but also a strategic and operational necessity that must be considered while developing an organization.

The contemporary cyber threat landscape is complex and multidimensional, with a variety of adversaries, including cybercriminals out for financial gain and hacktivists motivated by ideology [43], [44], [45]. These dangers employ a variety of strategies, such as social engineering, ransomware, and advanced persistent threats [44]. Cyberattacks have serious repercussions, including financial losses, regulatory fines, and reputational harm. Data theft or loss can have disastrous effects in the digital age. For enterprises to successfully traverse the digital era, a thorough understanding of the changing cyber threat landscape is essential [46].

C. Cybersecurity Frameworks

Established cybersecurity frameworks play a crucial role in guiding organizations toward robust security postures and effective risk management. The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a widely recognized and influential standard in the field. It provides a comprehensive approach to managing and improving cybersecurity risk across critical infrastructure sectors [47]. NIST's framework comprises five key functions: Identify, Protect, Detect, Respond, and Recover. These functions serve as the foundation for organizations to assess and enhance their cybersecurity capabilities. The framework encourages a risk-based approach, emphasizing the importance of continuous improvement and adaptability to evolving cyber threats [48]. With its voluntary and flexible nature, the NIST Cybersecurity Framework has become a benchmark for organizations aiming to establish a resilient cybersecurity posture [49].

ISO 27001, developed by the International Organization for Standardization (ISO), is another prominent cybersecurity framework that focuses on information security management systems (ISMS). ISO 27001 provides a systematic and risk-based approach to managing sensitive information, ensuring its confidentiality, integrity, and availability [50]. This internationally recognized standard encompasses a wide range of controls and best practices, covering areas such as information asset management, human resource security, and incident management. ISO 27001 is particularly valuable for organizations seeking formal certification, demonstrating their commitment to information security to clients, partners, and regulatory bodies [51]. The framework's emphasis on continual improvement aligns with its goal of adapting to emerging threats and technology advancements. ISO 27001 serves as a comprehensive guide for organizations across various industries, emphasizing the need for a structured and disciplined approach to safeguarding information assets [52].

The Cybersecurity Framework developed by the Center for Internet Security (CIS) is a practical and actionable framework designed to help organizations of all sizes bolster their cybersecurity defenses [53]. The CIS framework provides a set of best practices, known as the Critical Security Controls (CSC), which are prioritized guidelines to mitigate the most prevalent and damaging cyber threats [54]. The framework is structured into three implementation groups based on an organization's size, resources, and risk profile, offering scalability and flexibility. The 20 Critical Security Controls cover areas such as inventory and control of hardware assets, data protection, and secure configuration. The CIS framework is renowned for its practicality, offering a roadmap for organizations to enhance their security posture incrementally [55]. It is particularly beneficial for organizations seeking a pragmatic and systematic approach to improving their cybersecurity defenses, making it accessible for both large enterprises and smaller entities with limited resources.

In conclusion, these frameworks collectively underscore the importance of a proactive and strategic approach to cybersecurity, reflecting the dynamic nature of cyber threats and the need for continuous improvement and adaptation. Organizations can leverage these established frameworks as foundational pillars in their cybersecurity strategies, tailoring their implementation to align with specific business needs and risk profiles.

3. Methodology

This study adopts a structured, multi-step approach to develop a comprehensive cyber resilience framework aimed at ensuring business continuity and growth in the face of escalating cyber threats. The methodology integrates rigorous literature selection, framework development, and validation processes. The following sections provide a detailed account of each phase:

A. Literature Selection

The literature selection process was driven by the objective of understanding both theoretical and practical aspects of cyber resilience. The criteria for selecting literature included:

- Relevance to Cyber Resilience: Peer-reviewed articles, conference proceedings, and industry reports were included based on their focus on cybersecurity, resilience strategies, and business continuity in the digital era.
- Date of Publication: Only sources published within the last 10 years were considered to ensure the inclusion of the most recent insights into emerging technologies and evolving threat landscapes.
- Credibility: Preference was given to established journals (such as IEEE, Springer, Emerald, and Elsevier), authoritative reports (NIST, ISO, CIS frameworks), and government publications on cybersecurity.
- Geographic and Sectoral Diversity: Studies from diverse geographic regions and industries (e.g., finance, healthcare, and public sector) were selected to ensure that the proposed framework is adaptable across different organizational contexts.

A total of 150 sources were initially reviewed, and after applying the above criteria, 90 articles, reports, and frameworks were deemed relevant for inclusion in the final analysis.

B. Framework Development

The development of the cyber resilience framework involved a synthesis of key concepts, strategies, and best practices derived from the literature. This was achieved through a two-step process:

- Thematic Analysis: The selected literature was systematically analyzed to identify recurring themes and strategies related to organizational resilience, threat landscapes, and emerging cybersecurity trends. This qualitative analysis helped in isolating critical components such as proactive policies, resilience testing, collaboration, and the integration of new technologies.
- Component Integration: Following the thematic analysis, the framework's core components were defined. These include proactive security policies, resilience testing, collaborative engagement, and the integration of emerging technologies. The components were integrated to form a holistic, adaptable approach, with each element designed to address specific aspects of cyber resilience (e.g., prevention, detection, response, and recovery).

C. Validation and Testing

The validation of the proposed cyber resilience framework was conducted through Comparative Analysis with Existing Frameworks. This approach aimed to assess the robustness, comprehensiveness, and adaptability of the new framework by benchmarking it against widely recognized and established cybersecurity frameworks. The comparison focused on identifying areas of alignment, improvement, and innovation. The following key frameworks were used for this analysis:

- NIST Cybersecurity Framework: the NIST framework is known for its five core functions: Identify, Protect, Detect, Respond, and Recover. Our proposed framework aligns with these functions but extends beyond them by emphasizing customization based on organizational context and collaborative engagement with external stakeholders. While NIST provides a flexible, risk-based approach, our framework further integrates proactive measures and emerging technologies such as AI and blockchain for dynamic threat detection and response.
- ISO/IEC 27001: ISO 27001 focuses on establishing and maintaining an Information Security Management System (ISMS), ensuring the confidentiality, integrity, and availability of information. In contrast, our framework incorporates resilience testing as a core component, which includes not only information security but also business continuity and disaster recovery measures. The comparison highlighted that the proposed framework builds on ISO 27001's systematic approach by embedding continuous resilience drills and proactive planning for evolving threats.
- CIS Critical Security Controls (CSC): the CIS framework provides a set of prioritized actions to mitigate cyber threats, particularly aimed at small to medium-sized organizations. Our framework aligns with this practical approach but is designed to be scalable for organizations of various sizes and complexities. While CIS emphasizes basic hygiene measures, the proposed framework incorporates advanced strategies like threat intelligence sharing and quantum-resistant encryption, positioning it for both current and future cybersecurity challenges.

Through this comparative analysis, it was observed that the proposed cyber resilience framework offers a more

holistic and adaptive approach. It complements and enhances established frameworks by focusing on:

- Proactive security measures that go beyond compliance.
- Resilience testing to ensure organizations are prepared for a wide range of threats.
- Collaboration and emerging technologies to address the rapidly changing threat landscape.

This validation method demonstrated that while existing frameworks provide strong foundations, the proposed framework offers additional layers of flexibility and innovation, making it particularly suitable for organizations navigating complex and evolving cybersecurity environments.

4. Building Cyber Resilience

In the dynamic landscape of contemporary cybersecurity, the cornerstone is cyber resilience, a strategic approach encompassing an organization's ability to anticipate, endure, recover from, and respond to adverse circumstances and cyberattacks [56]. This comprehensive strategy acknowledges the inevitability of breaches and disruptions, ensuring the organization's continuous operation even in the aftermath of a successful cyberattack [57]. Cyber resilience goes beyond the pursuit of perfect security, recognizing the need for readiness against sophisticated cyber threats and unforeseen incidents [58]. To navigate the ever-changing threat landscape, organizations must proactively plan for resilience, minimizing risk exposure, enhancing threat detection and response, and mitigating the impact of cyber events [59], [60].

Prolonged downtime, financial losses, and erosion of customer trust are the perils organizations face without resilience [61]. A bespoke strategy for cyber resilience, tailored to the operating environment, industry regulations, and specific threats, is essential [62], [63]. Proactive and collaborative best practices, such as staying abreast of the cyber security landscape and working with external entities, are vital for effective cyber resilience [10]. Disaster recovery and business continuity planning play interconnected roles in ensuring data and systems are secure and facilitating business resumption post-cyberattack [64]. Regular testing and simulations assess the efficacy of these strategies and the organization's readiness to face a cyber disaster.

In this study, the Building Cyber Resilience content is structured into several key components, each addressing critical aspects of fortifying an organization's digital infrastructure. Firstly, "Determine Strategies for Safeguarding Business Development" outlines proactive measures for cybersecurity, emphasizing the implementation of robust cybersecurity strategies, the development of comprehensive incident response plans, and the exploration of collaborative approaches to cybersecurity. Following this, the content delves into "Challenges and Considerations," addressing the identification of common challenges in implementing cybersecurity measures for business development. Furthermore, it explores the legal and ethical considerations associated with protecting sensitive data and customer information. The subsequent part of the content explores "Future Trends and Technologies," providing insights into emerging technologies that can contribute to enhanced cyber resilience. Finally, it leads up to the proposed framework, culminating in a cohesive and strategic approach to building cyber resilience within the broader context of business development.

A. Strategies for Safeguarding Business Development

1) Proactive Cybersecurity Measures

Organizational success in the digital era requires protecting business development from cyber threats. Cyber resilience requires proactive cybersecurity measures, including risk assessment and management, training for employees, and strong security policies and procedures, as shown in Figure 1.

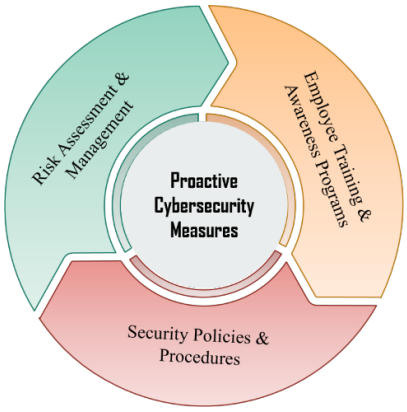

Figure 1. Proactive cybersecurity measures

Risk Assessment and Management entails systematically assessing and managing cybersecurity risks and vulnerabilities. This approach identifies infrastructure flaws and ranks risks by effect [65]. Risk avoidance, reduction, transfer, and acceptance must be implemented to minimize risks. A cybersecurity investment must match the risks [66]. Organizations must create and test security breach response strategies using simulations. Risk management techniques should alter with the threat landscape to ensure continual evaluation, adaptation, and improvement.

Employee training and awareness programs are critical in cybersecurity because they serve as the first line of defense against cyberattacks [67]. Employees are the first line of protection against phishing and social engineering assaults since they handle data, engage with customers, and use technology. Training should address a variety of cyber threats, including how to create secure passwords, spot questionable communications, in addition, appreciate the need for routine software upgrades. There should also be policies on the use of mobile devices, remote work, and data management. These initiatives promote a cybersecurity

culture in which all staff members take security seriously [68]. Beyond basic training, regular updates, simulated phishing drills, and real-time threat notifications should all increase cybersecurity awareness [69], [70]. Employees who have received training in threat detection and response can act as extra sensors in a larger cybersecurity plan, improving the organization's overall cyber resilience.

Security policies and procedures are crucial for a proactive cybersecurity strategy [71]. They describe the organization's cybersecurity strategy and specify roles, duties, and objectives [71]. These policies should cover all aspects of data management, network access, incident response, and supplier relationships. They should be well-documented, easily accessible, and consistently enforced. Procedures serve as a guide for the implementation of security measures like patch management, access control, incident reporting, and data encryption [72]. They ought to reduce weaknesses and make sure that threats or breaches are dealt with quickly. To prevent legal repercussions and strengthen the organization's cybersecurity posture, compliance with standards and laws is crucial [72]. In order to improve the organization's security posture over time, enforcement should be ongoing and incorporate feedback, threat information, and incident response data.

In general, a thorough approach to proactive cybersecurity measures is required for 21st-century business development, including risk assessment, employee-training programs, and the development of security policies. These components serve as the building blocks of a robust framework that can survive the shifting difficulties of the cyber threat landscape of the digital era.

2) Developing an Incident Response Plan

Developing an Incident Response Plan is an essential component of any organization's cybersecurity strategy. In today's interconnected digital landscape, the threat of cyberattacks and security incidents looms large, making it imperative for businesses to be prepared to effectively respond to such events [55]. An Incident Response Plan outlines the procedures, protocols, and strategies to follow when a security incident occurs, guiding organizations through the process of detecting, containing, mitigating, and recovering from incidents in a timely and coordinated manner. This introduction sets the stage for the subsequent steps involved in crafting a comprehensive Incident Response Plan, emphasizing the critical role it plays in safeguarding an organization's assets, reputation, and continuity of operations, as shown in Figure 2.

Assessing the severity of the issue is the initial step in developing an effective Incident Response Plan. This involves assessing the extent of the incident's impact on the organization's assets, systems, and data. By understanding the severity level, response efforts can be prioritized accordingly, ensuring resources are allocated where they are most needed and enabling a focused response to mitigate the incident's effects swiftly.

Figure 2. Incident Response Plan

Taking rapid action is paramount to minimize the impact of the incident and prevent it from escalating further. Once the severity is determined, immediate steps must be taken to contain and mitigate the incident. This may involve activating predefined response procedures, deploying security controls to halt the attacker's progress, and initiating communication channels to notify relevant stakeholders.

Organizing a coordinated response is essential to ensure that all necessary parties are involved and working together effectively. This step involves assembling the Incident Response Team, assigning roles and responsibilities, and establishing communication channels for seamless coordination. By fostering collaboration among team members and stakeholders, the organization can respond more efficiently and effectively to the incident.

Developing an incident playbook for cyber events entails creating detailed procedures and protocols tailored to different types of cyber incidents. This playbook serves as a guide for the Incident Response Team, providing step-by-step instructions on how to respond to specific threats and vulnerabilities. By having predefined procedures in place, the organization can streamline its response efforts and ensure consistency in its approach to handling cyber events.

Isolating the impacted systems is a crucial step to prevent the spread of the incident and minimize further damage. This involves implementing measures to quarantine affected systems, such as disconnecting them from the network or disabling compromised accounts. By isolating the impacted systems, the organization can contain the incident and prevent it from spreading to other parts of the network.

Gathering information is vital for understanding the nature and scope of the incident, as well as for supporting subsequent investigation and analysis. This step involves collecting relevant data, such as logs, network traffic, and system configurations, to determine how the incident occurred and what actions were taken. By gathering comprehensive information, the organization can make informed decisions and effectively respond to the incident.

Initiating the recovery process entails restoring affected systems and services to normal operation after containing and mitigating the incident. This includes tasks such as data restoration from backups, applying patches to secure vulnerabilities, and conducting post-incident testing to ensure system functionality. Promptly initiating recovery minimizes downtime, enabling the organization to resume normal business operations swiftly.

In conclusion, a well-developed incident response plan is not merely a document but a proactive cybersecurity strategy capable of significantly mitigating the impact of security incidents on an organization. By adhering to the steps outlined in this plan, organizations can effectively safeguard their assets and ensure business continuity amidst cyber threats. Regular testing, training, and refinement are essential to maintain the plan's effectiveness and alignment with evolving cybersecurity challenges. With a robust Incident Response Plan in place, organizations can respond promptly and decisively to security incidents, minimizing disruption, safeguarding sensitive data, and upholding stakeholder trust.

3) Collaborative Approaches to Cybersecurity

Organizations must adopt cooperative cybersecurity methods in the twenty-first century to safeguard their businesses' development. Because of the interconnectedness of the digital world, businesses frequently encounter the same vulnerabilities and threats. Collaboration with outside parties, business rivals, and governmental organizations can improve cybersecurity posture and attack response [73], [55]. In order to identify and mitigate new risks, technology suppliers, cybersecurity companies, and industry associations may have access to the most recent threat information, security tools, and knowledge. These alliances may also make it possible for real-time information on current threats, weaknesses, and attack patterns to be exchanged.

Working together on cybersecurity initiatives might help reveal shared risks and industry standards for a certain business or area. Industry-specific information-sharing and analysis centers (ISACs) make it easier for companies in certain industries to share threat data and security procedures [74]. Governmental institutions and law enforcement groups are also essential to these initiatives. To improve national and international cybersecurity resilience, public-private collaborations are being established more often. These partnerships give groups access to crucial resources, legal defense, and intelligence. However, issues like privacy, trust, and information sharing are problems that collaborative cybersecurity techniques must also deal with. Clear legal frameworks, trust-building strategies, and strong information-sharing agreements are crucial for navigating these difficulties [75]. A collaborative strategy may significantly increase an organization's capacity to defend against cyber threats and adapt to the digital world, ensuring business development in the twenty-first century.

B. Future Trends and Technologies

Cybersecurity must constantly innovate and adapt to the changing cyber threat scenario. Businesses need to be on the lookout for and open to new technologies like Artificial Intelligence (AI) and Machine Learning (ML), which can handle enormous volumes of data and spot patterns that may be challenging for human analysts. Threat detection, response, anomaly detection, and automation of regular security duties are all improved by these technologies [76], [77]. Their substantial implications for corporate growth are significant because they give firms the ability to strengthen defences and react swiftly to challenges, reducing the danger of disruption. An appropriate solution to the changing threat scenario is integrating AI, ML, Blockchain, zero trust architecture, or quantum-resistant encryption into the cybersecurity strategy, as shown in Figure 3.

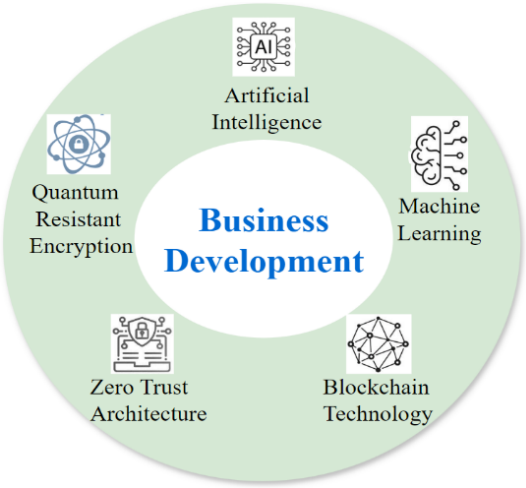

Figure 3. Emerging Cybersecurity Technologies

Blockchain technology, which is linked to cryptocurrencies, has the potential to completely change how data is protected because it is decentralized, cannot be changed, and is protected by cryptography [78]. To safeguard data integrity, improve supply chain security, and provide clear transaction records, it may be applied to corporate growth [78]. Organizations may utilize Blockchain to foster security and trust, fostering development and dependability in the digital era. This trend toward security-enhancing solutions denotes a move toward digital ecosystems that are more robust.

According to the cybersecurity paradigm known as Zero Trust Architecture, all organizations accessing an organization's systems and resources must continuously verify them,

regardless of where they are located. This strategy lessens exposure to internal dangers and outside cyberattacks [79]. It is consistent with how company growth is changing, as remote work and cloud services reduce the use of conventional network perimeters. The Zero Trust paradigm places a strong emphasis on the need to move away from perimeter-centric security approaches and toward more flexible and adaptive security postures.

Despite being in its infancy, Quantum-Resistant Encryption has the potential to undermine current cybersecurity procedures by weakening encryption techniques [80]. To combat this danger, however, quantum-resistant encryption methods are being developed [80], [81]. Employing encryption techniques that can survive quantum assaults will help organizations be ready for the quantum era and ensure data security and continued business operations. This change is essential for maintaining data privacy and adjusting to the changing cybersecurity environment.

In conclusion, new cybersecurity technologies are being investigated to improve data security and resilience against developing threats. These technologies include AI, ML, Blockchain, zero-trust architecture, and quantum-resistant encryption. These developments promote trust, dependability, and agility in the digital era, protecting sensitive data and client information while also promoting corporate success.

C. Proposed Framework for Building Cyber Resilience

As illustrated in Figure 4, the proposed framework for this paper revolves around the crucial idea of cyber resilience in today's cybersecurity, highlighting an organization's capacity to foresee, recover from, and react to cyberattacks while preserving sensitive data, vital operations, and continuous business continuity. Given the working context of the company, industry regulations, and unique threat landscapes, a customized approach is required. Enhancing cyber resilience requires proactive and cooperative methods that include risk assessment, employee training, and strong security policies to protect business development and keep a competitive edge in the ever-changing digital landscape. An incident response plan functions as a guide for locating, managing, and lessening the effects of security breaches in order to minimize business interruptions and increase customer trust. Experts, rivals in business, and governmental organizations can work together to improve cybersecurity posture and attack response through collaborative cybersecurity initiatives. To guarantee business safeguarding and growth in the twenty-first century, however, issues including evolving cyber threats, the complexity of digital ecosystems, a lack of cybersecurity awareness, and resource constraints must be methodically handled. Looking ahead, emerging trends and technologies such as Artificial Intelligence (AI), Machine Learning (ML), Blockchain, zero-trust architecture, and quantum-resistant encryption play a pivotal role in fortifying cybersecurity, fostering trust, reliability, agility, and serving as powerful techniques for protecting sensitive data and customer information, and ultimately encouraging the growth of businesses.

5. Challenges and Considerations

A. Cybersecurity Challenges in Business Development

This study addresses four primary challenges observed when implementing cybersecurity measures for business development: the evolution of cyber threats, the complexity of modern digital ecosystems, a lack of comprehensive cybersecurity awareness and expertise, and resource allocation and budget constraints, as shown in Figure 5. These challenges are crucial to address in order to safeguard and foster business development in the 21st century.

Evolution of cyber threats: The dynamic nature of cyber-attacks is a constant challenge for organizations operating in the current digital world [82]. Cybercriminals are always coming up with new ways to get around cybersecurity measures. This calls for constant vigilance and adaptability in cybersecurity strategies. Achieving a balance between strengthening digital defences against evolving threats and promoting innovation and expansion inside the organization is crucial. To tackle this, organizations must understand emerging cyberthreats including polymorphic malware, advanced persistent threats (APTs), and zero-day vulnerabilities [83]. These threats often exhibit extreme complexity, making it necessary to have excellent threat intelligence capabilities and anticipate possible attack vectors targeting certain industries or organizations.

To be able to respond to new threats, organizations must promote a culture of continual learning and development within their cybersecurity teams [84], [85]. In order to take preventative action in the face of changing cyber dangers, this entails encouraging an anticipatory attitude rather than a reactive one [57]. Interacting with external stakeholders, such as industry colleagues, cybersecurity forums, and governmental organizations, makes it easier to gain insights into the shifting threat landscape.

Investing in technology that can dynamically detect and respond to threats, like advanced machine-learning algorithms, artificial intelligence, and behavior-based analytics, can help companies find and stop new threats faster and more accurately than ever before [86]. Businesses must manage the continual change of the cyber threat landscape through accurate threat intelligence, dynamic adaptive approaches, and a culture of cybersecurity resilience since it is not an issue that can be totally eliminated [46]. Businesses can traverse the complicated digital ecosystem with confidence and guarantee that their pursuit of company expansion stays unwavering in the face of a constantly changing cyber threat scenario by promoting security and innovation.

Complexity of Modern Digital Ecosystems: Due to the complexity of modern digital ecosystems, organizations confront a substantial problem in increasing cybersecurity measures for business development [87]. Inherent security

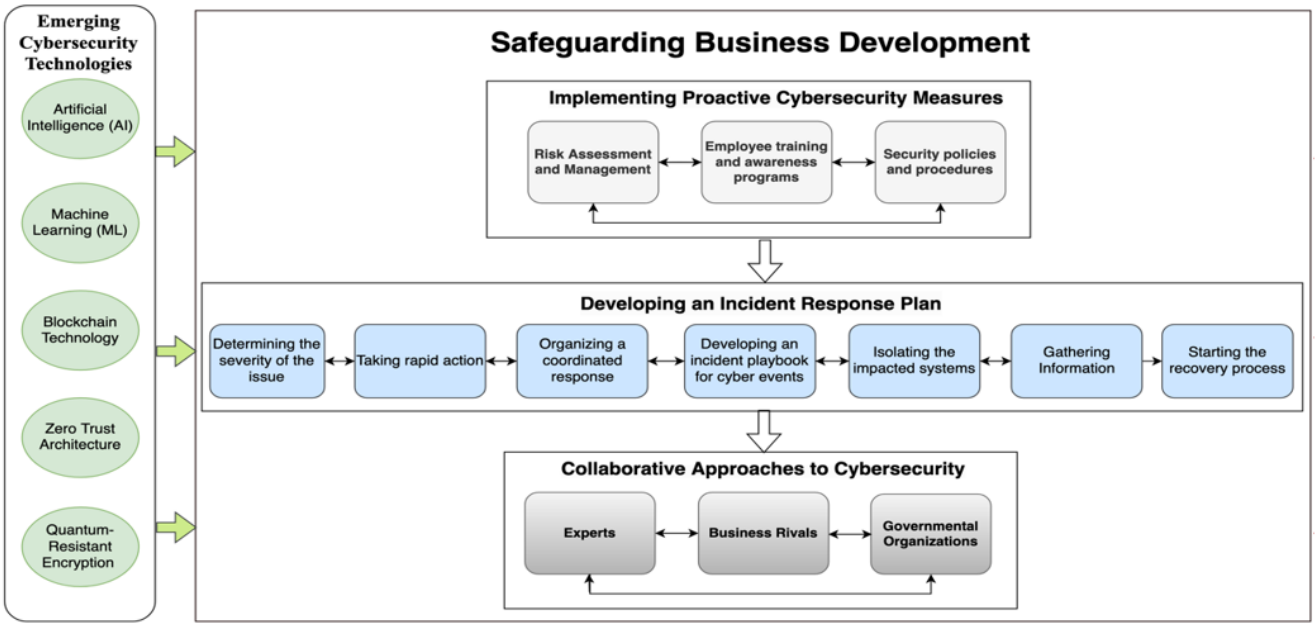

Figure 4. Proposed Framework for Cyber Resilience

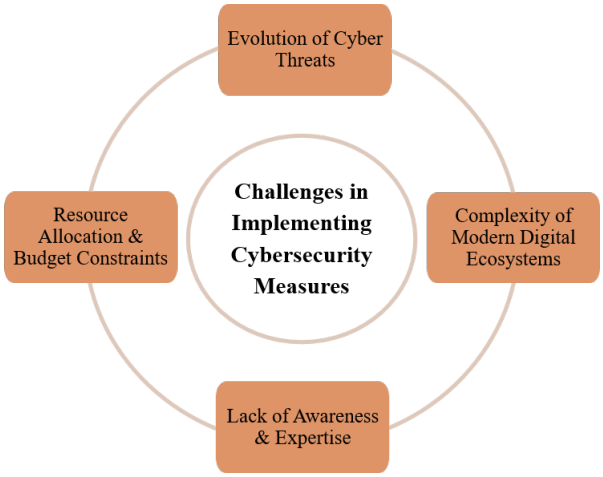

Figure 5. Primary challenges in implementing cybersecurity measures

flaws are introduced by these networks of networked systems, cloud services, and third-party suppliers. Technical know-how and a thorough comprehension of supply chain dynamics are needed for this. The prevalence of Internet of Things (IoT) devices adds another level of complexity because each one might be a point of entry for harmful cyberattacks, highlighting the continual and complicated nature of the cybersecurity problem that enterprises must deal with [88].

Organizations should carry out a thorough assessment of their interconnected systems and services in order to successfully safeguard their digital ecosystems. This aids in locating possible weak points and vulnerabilities, providing a focused, risk-based approach to the protection of digital assets [89]. Strong access restrictions, encryption techniques, and identity management tools should all be part of a multifaceted strategy [90]. This guarantees that private information is protected and that only authorized individuals may access vital systems. In these complex contexts, robust incident response strategies may also be created and quickly implemented in the event of a breach.

Furthermore, in contemporary digital ecosystems, it is vital to manage third-party interactions and supply chain security. To guarantee that security criteria are followed, organizations must create strict vendor management and evaluation methods. Regular audits can find weaknesses and reduce hazards. A thorough security system that includes device authentication, data encryption, and ongoing monitoring for breach signals is required due to the growth of IoT devices. Organizations may reduce the risks brought on by this level of complexity by addressing these particular difficulties within the digital ecosystem.

Lack of Awareness and Expertise: The absence of thorough cybersecurity awareness and experience within enterprises is a very human-centric problem [91]. Even though training and awareness campaigns are crucial, it might be difficult to guarantee that staff members regularly follow accepted security best practices. The persistence of social engineering and phishing attempts highlights how crucial it is to keep a watchful staff [92]. Organizations need to develop a ubiquitous cybersecurity culture in which everyone in the workforce shares responsibility for security.

Organizations must understand that cybersecurity aware-

ness entails behavioral change in addition to knowledge gain. Employees must be aware of the hazards and recommended procedures and incorporate them into their everyday work activities. It is critical to foster a culture where cybersecurity is viewed as crucial to company success. Due to the ongoing evolution of cyber risks, ongoing education is also essential. Organizations should offer continuous training programs that change as the threat environment changes. Employees can notice and react to genuine threats more quickly and efficiently if regular simulations of security breaches are conducted.

Additionally, fostering a cybersecurity culture requires encouraging shared responsibility and accountability among all staff members. As a result, strong protection against cyberattacks is created. In order to promote cybersecurity awareness, transparency and open communication are essential. Employees should not be afraid to report possible security problems because they will not face punishment. As a result, businesses can handle security concerns, look into breaches, and put preventative measures into place swiftly.

Resource Allocation and Budget Constraints: The primary obstacles to implementing reliable cybersecurity for corporate development are insufficient resource allocation and budget constraints [93]. Effective cybersecurity measures require a substantial financial commitment to implement and maintain, but businesses sometimes have conflicting priorities for their limited resources [93], [55]. Organizations must balance investments in security with other operational and strategic efforts; therefore, it is imperative that they make educated judgments regarding resource allocation. The complexity of cybersecurity decision-making is highlighted by this difficulty since resource allocation directly affects an organization's capacity to safeguard its digital assets and foster commercial expansion.

Organizations must have a thorough awareness of their unique demands and any potential dangers in order to address the complexity of cybersecurity. This entails evaluating the potential threat environment, comprehending the financial effects of breaches, and setting investment priorities appropriately [94]. Organizations must take a proactive stance, foresee possible threats, and be adaptable with their resource allocation. This might entail looking at managed security services, outsourcing possibilities, and risk-sharing arrangements with cybersecurity partners. By highlighting the long-term advantages of security investments, return on investment analysis may be included to help support resource allocation choices. Overall, firms must overcome this obstacle by maintaining knowledgeable, adaptable, and creative financial cybersecurity plans.

6. Discussion

The paper delves into a comprehensive exploration of the contemporary digital business landscape, underscoring its intricate relationship with cybersecurity. In the current competitive marketplace, the pursuit of business development is pivotal for organizational growth and sustainability. Beyond traditional sales and marketing endeavours, expansion, innovation, and diversification involve leveraging data analytics, cloud computing, and online platforms, necessitating a careful balance to harness the potential of the digital era while safeguarding data integrity, confidentiality, and system availability.

Recognizing the indispensable role of cybersecurity in safeguarding brand reputation, consumer trust, and business continuity, the paper underscores the importance of integrating cybersecurity into the core of organizational growth strategies. Central to this discussion is the concept of "cyber resilience," a holistic strategy focusing on an organization's ability to foresee, endure, recover from, and adapt to adverse circumstances, including cyberattacks. Cyber resilience is deemed essential for mitigating risks and ensuring swift recovery in an environment where absolute security is an elusive goal.

Practically, our proposed framework presents a holistic and adaptive approach to cybersecurity, centring on the pivotal concept of cyber resilience. In comparison to established frameworks such as the NIST Cybersecurity Framework, ISO 27001, and the Cybersecurity Framework by the Center for Internet Security (CIS), our framework distinguishes itself through a heightened focus on customization, collaboration, and the strategic integration of emerging technologies.

While the NIST Cybersecurity Framework provides a robust structure for managing and reducing cybersecurity risk, our framework complements this by emphasizing the need for tailored solutions that align with an organization's unique context, industry regulations, and specific threat landscapes.

Similarly, in contrast to ISO 27001, which offers a systematic approach to information security management, our framework extends beyond traditional security measures. It encourages proactive security policies, resilience testing, and collaborative engagement, recognizing the importance of not only preventing breaches but also ensuring organizations can effectively respond and recover in the face of cyber threats. The collaborative element, including partnerships with experts, business rivals, and governmental organizations, enhances the framework's adaptability and responsiveness.

In comparison to the Cybersecurity Framework by the Center for Internet Security (CIS), known for its actionable and prioritized best practices, our framework aligns by incorporating practical strategies. However, it goes further by explicitly addressing customization, collaboration, and the integration of emerging technologies as essential components of a comprehensive cybersecurity strategy. The emphasis on wider validation through field applications acknowledges the dynamic nature of cyber threats and the need for continuous refinement based on real-world scenarios.

Furthermore, our framework stands out by recognizing the role of emerging technologies, such as Artificial Intelligence (AI), Machine Learning (ML), Blockchain, zero-trust architecture, and quantum-resistant encryption, in fortifying cybersecurity. This forward-looking approach positions our framework as not only responsive to current challenges but also as a guide for navigating the complexities of the cybersecurity landscape in the future.

7. Conclusion and Future Research

The proposed integrated cyber resilience framework can guide enterprises in sustaining business development initiatives amidst escalating cyber disruptions and uncertainty. The research addresses a critical need for organizational preparedness and responsiveness to mitigate cyber threats while progressing digitalization. As a conceptual foundation developed through extensive literature analysis, experiential validation by security practitioners and testing across diverse organizational setups can further enrich the framework. Areas for additional investigation include quantified models integrating resilience metrics tailored to industry ecosystems, detailed cost-benefit trade-offs for decision support, and standardized maturity assessment tools.

References

[1] W. He, Z. J. Zhang, and W. Li, "Information technology solutions, challenges, and suggestions for tackling the covid-19 pandemic," *International journal of information management*, vol. 57, p. 102287, 2021.

[2] V. Vasani, A. K. Bairwa, S. Joshi, A. Pljonkin, M. Kaur, and M. Amoon, "Comprehensive analysis of advanced techniques and vital tools for detecting malware intrusion," *Electronics*, vol. 12, no. 20, p. 4299, 2023.

[3] T. Hussain, R. Edgeman, and M. N. AlNajem, "Exploring the intellectual structure of research in organizational resilience through a bibliometric approach," *Sustainability*, vol. 15, no. 17, p. 12980, 2023.

[4] F. Teichmann, S. R. Boticiu, and B. S. Sergi, "The evolution of ransomware attacks in light of recent cyber threats. how can geopolitical conflicts influence the cyber climate?" *International Cybersecurity Law Review*, vol. 4, no. 3, pp. 259–280, 2023.

[5] D. N. Panteleev, "Cybersecurity for the stimulation of entrepreneurship development in the digital economy markets," in *Anti-Crisis Approach to the Provision of the Environmental Sustainability of Economy*. Springer, 2023, pp. 263–271.

[6] D. P. Möller, "Ransomware attacks and scenarios: Cost factors and loss of reputation," in *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*. Springer, 2023, pp. 273–303.

[7] G. Assenza, L. Faramondi, G. Oliva, and R. Setola, "Cyber threats for operational technologies," *International Journal of System of Systems Engineering*, vol. 10, no. 2, pp. 128–142, 2020.

[8] A. Asgary, A. I. Ozdemir, and H. Özyürek, "Small and medium enterprises and global risks: evidence from manufacturing smes in turkey," *International Journal of Disaster Risk Science*, vol. 11, pp. 59–73, 2020.

[9] W. K. Chong and N. Patwa, "The value of integrity: Empowering smes with ethical marketing communication," *Sustainability*, vol. 15, no. 15, p. 11673, 2023.

[10] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience," *Sensors*, vol. 23, no. 16, p. 7273, 2023.

[11] M. J. Lees, M. Crawford, and C. Jansen, "Towards industrial cybersecurity resilience of multinational corporations," *IFAC-PapersOnLine*, vol. 51, no. 30, pp. 756–761, 2018.

[12] A. Salvi, P. Spagnoletti, and N. S. Noori, "Cyber-resilience of critical cyber infrastructures: Integrating digital twins in the electric power ecosystem," *Computers & Security*, vol. 112, p. 102507, 2022.

[13] A. Hawamleh, A. S. M. Alorfi, J. A. Al-Gasawneh, and G. Al-Rawashdeh, "Cyber security and ethical hacking: The importance of protecting user data," *Solid State Technology*, vol. 63, no. 5, pp. 7894–7899, 2020.

[14] N. H. Al-Kumaim and S. K. Alshamsi, "Determinants of cyberattack prevention in uae financial organizations: assessing the mediating role of cybersecurity leadership," *Applied Sciences*, vol. 13, no. 10, p. 5839, 2023.

[15] A. Ahmad, S. B. Maynard, K. C. Desouza, J. Kotsias, M. T. Whitty, and R. L. Baskerville, "How can organizations develop situation awareness for incident response: A case study of management practice," *Computers & Security*, vol. 101, p. 102122, 2021.

[16] A. Al-Harrasi, A. K. Shaikh, and A. Al-Badi, "Towards protecting organisations' data by preventing data theft by malicious insiders," *International Journal of Organizational Analysis*, vol. 31, no. 3, pp. 875–888, 2023.

[17] L. F. Ilca, O. P. Lucian, and T. C. Balan, "Enhancing cyber-resilience for small and medium-sized organizations with prescriptive malware analysis, detection and response," *Sensors*, vol. 23, no. 15, p. 6757, 2023.

[18] G. Mott, J. R. Nurse, and C. Baker-Beall, "Preparing for future cyber crises: lessons from governance of the coronavirus pandemic," *Policy Design and Practice*, vol. 6, no. 2, pp. 160–181, 2023.

[19] M. Anshari, M. Syafrudin, N. L. Fitriyani, and A. Razzaq, "Ethical responsibility and sustainability (ers) development in a metaverse business model," *Sustainability*, vol. 14, no. 23, p. 15805, 2022.

[20] T. J. Marion and S. K. Fixson, "The transformation of the innovation process: How digital tools are changing work, collaboration, and organizations in new product development," *Journal of Product Innovation Management*, vol. 38, no. 1, pp. 192–215, 2021.

[21] M. O. Al Shbail, Z. Jaradat, A. Al-Hawamleh, A. Hamdan, and A. M. Musleh Alsartawi, "Enhancing audit quality in non-big 4 firms: the role of remote auditing and audit staff capabilities," *Journal of Financial Reporting and Accounting*, 2024.

[22] M. Azeem, M. Ahmed, S. Haider, and M. Sajjad, "Expanding competitive advantage through organizational culture, knowledge sharing and organizational innovation," *Technology in Society*, vol. 66, p. 101635, 2021.

[23] Z. Jaradat, A. M. AL-Hawamleh, and M. Altarawneh, "Investigating the impact of technological orientation and innovation orientation

on the sustainability and development the industrial sector," *Competitiveness Review: An International Business Journal*, 2024.

[24] C. Fjäder, "Emerging and disruptive technologies and security: considering trade-offs between new opportunities and emerging risks," in *Disruption, Ideation and Innovation for Defence and Security*. Springer, 2022, pp. 51–75.

[25] R. V. B. Quintero and F. B. Quintero, "Fintech and consumer expectations: A global perspective," *IEEE Technology and Engineering Management Society Body of Knowledge (TEMSBOK)*, pp. 21–52, 2023.

[26] M. M. Moughari and T. U. Daim, "Developing a model of technological innovation for export development in developing countries," *Technology in Society*, vol. 75, p. 102338, 2023.

[27] A. M. Alhawamleh and A. Ngah, "Knowledge sharing among jordanian academicians: A case study of tafila technical university (ttu) and mutah university (mu)," in *2017 8th International Conference on Information Technology (ICIT)*. IEEE, 2017, pp. 262–270.

[28] M. Donner and H. de Vries, "How to innovate business models for a circular bio-economy?" *Business Strategy and the Environment*, vol. 30, no. 4, pp. 1932–1947, 2021.

[29] A. Hanelt, R. Bohnsack, D. Marz, and C. Antunes Marante, "A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change," *Journal of management studies*, vol. 58, no. 5, pp. 1159–1197, 2021.

[30] R. Yuana, E. A. Prasetio, R. Syarief, Y. Arkeman, and A. I. Suroso, "System dynamic and simulation of business model innovation in digital companies: An open innovation approach," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 7, no. 4, p. 219, 2021.

[31] T. Ciarli, M. Kenney, S. Massini, and L. Piscitello, "Digital technologies, innovation, and skills: Emerging trajectories and challenges," *Research Policy*, vol. 50, no. 7, p. 104289, 2021.

[32] Z. Jaradat, A. AL-Hawamleh, and A. Hamdan, "Examining the integration of erp and bi in the industrial sector and its impact on decision-making processes in ksa," *Digital Policy, Regulation and Governance*, 2024.

[33] C. Ancillai, A. Sabatini, M. Gatti, and A. Perna, "Digital technology and business model innovation: A systematic literature review and future research agenda," *Technological Forecasting and Social Change*, vol. 188, p. 122307, 2023.

[34] A. M. AL-Hawamleh, "Securing the future: Framework fundamentals for cyber resilience in advancing organizations," *Journal of System and Management Sciences*, vol. 14, no. 10, pp. 130–150, 2024.

[35] A. Díaz, L. Guerra, and E. Díaz, "Digital transformation impact in security and privacy," in *Developments and Advances in Defense and Security: Proceedings of MICRADS 2021*. Springer, 2022, pp. 61–70.

[36] C. Ge, W. Lv, and J. Wang, "The impact of digital technology innovation network embedding on firms' innovation performance: the role of knowledge acquisition and digital transformation," *Sustainability*, vol. 15, no. 8, p. 6938, 2023.

[37] N. Suchek, C. I. Fernandes, S. Kraus, M. Filser, and H. Sjögrén, "Innovation and the circular economy: A systematic literature review," *Business Strategy and the Environment*, vol. 30, no. 8, pp. 3686–3702, 2021.

[38] A. Kanaan, A.-H. Ahmad, A. Alorfi, and M. Aloun, "Cybersecurity resilience for business: A comprehensive model for proactive defense and swift recovery," in *2024 2nd International Conference on Cyber Resilience (ICCR)*. IEEE, 2024, pp. 1–7.

[39] S. A. Hamad, Q. Z. Sheng, W. E. Zhang, and S. Nepal, "Realizing an internet of secure things: A survey on issues and enabling technologies," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1372–1391, 2020.

[40] U. P. D. Ani, H. He, and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective," *Journal of Cyber Security Technology*, vol. 1, no. 1, pp. 32–74, 2017.

[41] S. Perera, X. Jin, A. Maurushat, and D.-G. J. Opoku, "Factors affecting reputational damage to organisations due to cyberattacks," in *Informatics*, vol. 9, no. 1. MDPI, 2022, p. 28.

[42] A. Garcia-Perez, J. G. Cegarra-Navarro, M. P. Sallos, E. Martinez-Caro, and A. Chinnaswamy, "Resilience in healthcare systems: Cyber security and digital transformation," *Technovation*, vol. 121, p. 102583, 2023.

[43] J. Al-Gasawneh, A. Al-Hawamleh, A. Alorfi, and G. Al-Rawashde, "Moderating the role of the perceived security and endorsement on the relationship between per-ceived risk and intention to use the artificial intelligence in financial services," *International Journal of Data and Network Science*, vol. 6, no. 3, pp. 743–752, 2022.

[44] A. M. AL-Hawamleh, "Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 2, 2023.

[45] A. Kanaan, A. AL-Hawamleh, A. Abulfaraj, H. Al-Kaseasbeh, and A. Alorfi, "The effect of quality, security and privacy factors on trust and intention to use e-government services," *International Journal of Data and Network Science*, vol. 7, no. 1, pp. 185–198, 2023.

[46] J. Kotsias, A. Ahmad, and R. Scheepers, "Adopting and integrating cyber-threat intelligence in a commercial organisation," *European Journal of Information Systems*, vol. 32, no. 1, pp. 35–51, 2023.

[47] B. Krumay, E. W. Bernroider, and R. Walser, "Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the nist cybersecurity framework," in *Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings 23*. Springer, 2018, pp. 369–384.

[48] H. I. Kure, S. Islam, and H. Mouratidis, "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection," *Neural Computing and Applications*, vol. 34, no. 18, pp. 15 241–15 271, 2022.

[49] S. J. Shackelford, A. A. Proia, B. Martell, and A. N. Craig, "Toward a global cybersecurity standard of care: Exploring the implications of the 2014 nist cybersecurity framework on shaping reasonable national and international cybersecurity practices," *Tex. Int'l LJ*, vol. 50, p. 305, 2015.

[50] S. A. R. Mortazavi and F. Safi-Esfahani, "A checklist based evalua-

tion framework to measure risk of information security management systems," *International Journal of Information Technology*, vol. 11, no. 3, pp. 517–534, 2019.

[51] M. Podrecca, G. Culot, G. Nassimbeni, and M. Sartor, "Information security and value creation: The performance implications of iso/iec 27001," *Computers in Industry*, vol. 142, p. 103744, 2022.

[52] K. Beckers and K. Beckers, "Supporting the establishment of a cloud-specific isms according to iso 27001 using the cloud system analysis pattern," *Pattern and Security Requirements: Engineering-Based Establishment of Security Standards*, pp. 299–392, 2015.

[53] M. Domínguez-Dorado, J. Carmona-Murillo, D. Cortés-Polo, and F. J. Rodríguez-Pérez, "Cybertomp: A novel systematic framework to manage asset-focused cybersecurity from tactical and operational levels," *IEEE Access*, vol. 10, pp. 122 454–122 485, 2022.

[54] S. Paz, "Cybersecurity standards and frameworks," *IEEE Technology and Engineering Management Society Body of Knowledge (TEMS-BOK)*, pp. 397–416, 2023.

[55] A. AL-Hawamleh, "Cyber resilience framework: Strengthening defenses and enhancing continuity in business security," *International Journal of Computing and Digital Systems*, vol. 15, no. 1, pp. 1315–1331, 2024.

[56] H. Tran, E. Campos-Nanez, P. Fomin, and J. Wasek, "Cyber resilience recovery model to combat zero-day malware attacks," *computers & security*, vol. 61, pp. 19–31, 2016.

[57] A. Annarelli, F. Nonino, and G. Palombi, "Understanding the management of cyber resilient systems," *Computers & industrial engineering*, vol. 149, p. 106829, 2020.

[58] B. Dupont, C. Shearing, M. Bernier, and R. Leukfeldt, "The tensions of cyber-resilience: From sensemaking to practice," *Computers & Security*, vol. 132, p. 103372, 2023.

[59] S. Altaha and M. H. Rahman, "A mini literature review on integrating cybersecurity for business continuity," in *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. IEEE, 2023, pp. 353–359.

[60] A. M. Al-Hawamleh, "Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the ksa," *Digital Policy, Regulation and Governance*, vol. 26, no. 3, pp. 317–336, 2024.

[61] J. Adekola and D. Clelland, "Two sides of the same coin: Business resilience and community resilience," *Journal of Contingencies and Crisis Management*, vol. 28, no. 1, pp. 50–60, 2020.

[62] B. Keys and S. Shapiro, "Frameworks and best practices," *Cyber Resilience of Systems and Networks*, pp. 69–92, 2019.

[63] Z. Jaradat, A. Al-Hawamleh, M. O. Al Shbail, and A. Hamdan, "Does the adoption of blockchain technology add intangible benefits to the industrial sector? evidence from jordan," *Journal of Financial Reporting and Accounting*, 2023.

[64] R. Al-Husain, "Promoting sustainability in kuwait: An exploratory study of disaster management preparedness and resilience in state organizations," *Sustainability*, vol. 15, no. 13, p. 10066, 2023.

[65] M. Shokry, A. I. Awad, M. K. Abd-Ellah, and A. A. Khalaf, "When security risk assessment meets advanced metering infrastructure: Identifying the appropriate method," *Sustainability*, vol. 15, no. 12, p. 9812, 2023.

[66] M. Dinkova, R. El-Dardiry, and B. Overvest, "Should firms invest more in cybersecurity?" *Small Business Economics*, pp. 1–30, 2023.

[67] S. von Solms, J. du Toit, and E. Kritzinger, "Another look at cybersecurity awareness programs," in *International Symposium on Human Aspects of Information Security and Assurance*. Springer, 2023, pp. 13–23.

[68] A. Alyami, D. Sammon, K. Neville, and C. Mahony, "The critical success factors for security education, training and awareness (seta) program effectiveness: a lifecycle model," *Information Technology & People*, vol. 36, no. 8, pp. 94–125, 2023.

[69] M. Domínguez-Dorado, F. J. Rodríguez-Pérez, J. Carmona-Murillo, D. Cortés-Polo, and J. Calle-Cancho, "Boosting holistic cybersecurity awareness with outsourced wide-scope cybersoc: A generalization from a spanish public organization study," *Information*, vol. 14, no. 11, p. 586, 2023.

[70] A. AL-Hawamleh, "Exploring the satisfaction and continuance intention to use e-learning systems: An integration of the information systems success model and the technology acceptance model," *International journal of electrical and computer engineering systems*, vol. 15, no. 2, pp. 201–214, 2024.

[71] A. Mishra, Y. I. Alzoubi, M. J. Anwar, and A. Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations," *Computers & Security*, vol. 120, p. 102820, 2022.

[72] J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Future generation computer systems*, vol. 92, pp. 178–188, 2019.

[73] C. Del-Real and A. M. Díaz-Fernández, "Understanding the plural landscape of cybersecurity governance in spain: a matter of capital exchange," *International Cybersecurity Law Review*, vol. 3, no. 2, pp. 313–343, 2022.

[74] J. M. Salomon, "Public-private partnerships and collective cyber defence," in *2022 14th International Conference on Cyber Conflict: Keep Moving!(CyCon)*, vol. 700. IEEE, 2022, pp. 45–63.

[75] M. Metcalfe, J. Nager, and C. S. Hacker, "Trust framework for data sharing between industry and government," in *2023 Integrated Communication, Navigation and Surveillance Conference (ICNS)*. IEEE, 2023, pp. 1–9.

[76] L. Rosa, T. Cruz, M. B. De Freitas, P. Quitério, J. Henriques, F. Caldeira, E. Monteiro, and P. Simões, "Intrusion and anomaly detection for the next-generation of industrial automation and control systems," *Future Generation Computer Systems*, vol. 119, pp. 50–67, 2021.

[77] Z. Jaradat, A. AL-Hawamleh, M. Altarawneh, H. Hikal, and A. Elfedawy, "The interplay between intellectual capital, business intelligence adoption, and the decision to innovate: evidence from jordan," *International Journal of Computing and Digital Systems*, vol. 15, no. 1, pp. 1375–1389, 2024.

[78] E. Politou, F. Casino, E. Alepis, and C. Patsakis, "Blockchain mutability: Challenges and proposed solutions," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, pp. 1972–1986, 2019.

[79] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (zta): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57 143–57 179, 2022.

[80] G. N. Brijwani, P. E. Ajmire, and P. V. Thawani, "Future of quantum computing in cyber security," in *Handbook of Research on Quantum Computing for Smart Environments*. IGI Global, 2023, pp. 267–298.

[81] A. M. Alhawamleh, "Advanced spam filtering in electronic mail using hybrid the mini batch k-means normalized mutual information feature elimination with elephant herding optimization technique," *International Journal of Computing and Digital Systems*, vol. 13, no. 1, pp. 1–1, 2023.

[82] H. Saleous, M. Ismail, S. H. AlDaajeh, N. Madathil, S. Alrabaee, K.-K. R. Choo, and N. Al-Qirim, "Covid-19 pandemic and the cyberthreat landscape: Research challenges and opportunities," *Digital communications and networks*, vol. 9, no. 1, pp. 211–222, 2023.

[83] A. Sharma, B. B. Gupta, A. K. Singh, and V. Saraswat, "Advanced persistent threats (apt): evolution, anatomy, attribution and countermeasures," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 7, pp. 9355–9381, 2023.

[84] W. Al Omari, N. Mai, H. S. Hin, and A. Al Hawamleh, "Enhancing learning process by applying cooperative learning supported with augmented reality environment," *International Journal*, vol. 10, no. 4, pp. 68–75, 2023.

[85] A. AL-Hawamleh, E. Abdelatie, W. Al Omari, A. Kanaan, M. Aloun, and A. Alshawawreh, "Toward sustainable e-learning: Visionary insights, innovative strategies, and practical recommendations for the future," *International Journal of Computing and Digital Systems*, vol. 16, no. 1, pp. 1–14, 2024.

[86] N. Mohamed, J. Al-Jaroodi, I. Jawhar, and N. Kesserwan, "Data-driven security for smart city systems: Carving a trail," *IEEE Access*, vol. 8, pp. 147 211–147 230, 2020.

[87] H. Susanto, L. F. Yie, D. Setiana, Y. Asih, A. Yoganingrum, S. Riyanto, and F. A. Saputra, "Digital ecosystem security issues for organizations and governments: Digital ethics and privacy," in *Web 2.0 and cloud technologies for implementing connected government*. IGI Global, 2021, pp. 204–228.

[88] A. Djenna, S. Harous, and D. E. Saidouni, "Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure," *Applied Sciences*, vol. 11, no. 10, p. 4580, 2021.

[89] P. G. George and V. Renjith, "Evolution of safety and security risk assessment methodologies towards the use of bayesian networks in process industries," *Process Safety and Environmental Protection*, vol. 149, pp. 758–775, 2021.

[90] M. Kianpour, S. J. Kowalski, and H. Øverby, "Systematically understanding cybersecurity economics: A survey," *Sustainability*, vol. 13, no. 24, p. 13677, 2021.

[91] N. Poehlmann, K. M. Caramancion, I. Tatar, Y. Li, M. Barati, and T. Merz, "The organizational cybersecurity success factors: an exhaustive literature review," *Advances in Security, Networks, and Internet of Things: Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20*, pp. 377–395, 2021.

[92] C. S. Babu, P. A. Simon, and S. B. Kumar, "The future of cyber security starts today, not tomorrow," in *Malware Analysis and Intrusion Detection in Cyber-Physical Systems*. IGI Global, 2023, pp. 348–375.

[93] A. Chidukwani, S. Zander, and P. Koutsakis, "A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations," *IEEE Access*, vol. 10, pp. 85 701–85 719, 2022.

[94] S. Armenia, E. Ferreira Franco, F. Nonino, E. Spagnoli, and C. M. Medaglia, "Towards the definition of a dynamic and systemic assessment for cybersecurity risks," *Systems research and behavioral science*, vol. 36, no. 4, pp. 404–423, 2019.