(Online) ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Review Article*
Vol. 13, No. 1, April 2025, pp.263-280

Strategies to strengthen cybersecurity for business resilience in the digital age

Snizhana Sukachova[1,*], Larysa Gorodianska[2], Mykola Burmaka[3], Iryna Yanenkova[4], Ihor Tkach[5]
[1] Department of Economics and Business, Faculty of Economic Relations and Finance, State Biotechnological University, Ukraine
[2] Management of Foreign Economic Activity of Enterprises Department, Faculty of Economics and Business Administration, State Non-Commercial Company «State University «Kyiv Aviation Institute», Ukraine
[3] Department of International Management, Faculty of International Economics and Management, Kyiv National Economic University named after Vadym Hetman, Ukraine
[4] Digital Economy Sector, State Organization "Institute for Economics and Forecasting of the NAS of Ukraine", Ukraine
[5] Department of Information Systems in Management, Faculty of Economics, Ivan Franko National University of Lviv, Ukraine

*Corresponding author E-mail: stsn13@gmail.com

ABSTRACT

Globalization has transformed the way people live, work, and interact. In recent decades, businesses of all sizes have been profoundly impacted by the exponential advances in computer, network, and data storage technology. Virtually all industries, from the healthcare to the automotive sector, have integrated digital technologies into their work. This phenomenon is called digitalization, the drive to connect real-world objects and people virtually and digitally. Digitalization has unleashed new and exciting opportunities while also creating particular and unique threats and challenges. One such challenge, which has garnered significant attention, is cybersecurity. This paper serves as a primer for business professionals to gain a foundational understanding of cybersecurity. Businesses of all sizes and functions will need to establish a digital presence for their company. The inability to embrace digitalization will render many businesses obsolete. However, given the vulnerability of the digital sector to hacking attacks and having recognized that 60% of companies that undergo a significant cyberattack go under within six months, digital entrepreneurs must carefully deliberate on how to establish effective cyber-business strategies and models. Adopting a descriptive analysis method, this paper can be viewed as a primer for business professionals who need to consider the cybersecurity of their company, brand, or business models, as well as for students and researchers interested in the subject.

Keywords: Cybersecurity, Cyber threats, Digital transformation, Digitalization, Risk management, Data protection, Human resources management, Information systems security, Business strategy, Business sustainability

1. Introduction

This paper explores strategies to strengthen cybersecurity in businesses. While it primarily focuses on businesses, many of its points would also apply equally to public organizations, civil society, or private individuals. With evolutions in the political, economic, and societal spheres driven by the explosion of data and its digital transmission channels, the accompanying evolution of cyber threats to these spheres has brought the topic of cybersecurity to the forefront of global policy priorities. Cybersecurity policymakers' responses must be adapted and proportionate in a context shaped by the fluid evolution of threat actors and the changing objectives of their actions. Resilience demonstrates an entity's ability to protect and pursue its vital functions or missions for its stakeholders in the face of adversity.

Cybersecurity for business resilience thus requires a solid cyber risk management program, led from the top and supportive of a dynamic approach to the business, reassuring stakeholders and possible investors that a company's goals and strategies can be realized despite exposure to cyber threats. It reflects the ability to manage cybersecurity risk while aiming for long-term business success. Indeed, a too heavy focus on cybersecurity preparedness may deter forward-thinking risk-taking and lead to negative consequences, such as excessive and

redundant data protection. Successful business leaders know that risk-taking, supported by adequate investment and acceptable inherited business risk, can result in benefits worth realizing [1].

1.1. Defining cybersecurity and business resilience

Folorunso argued that cybersecurity and business resilience-building exercises are no longer optional for any institution [2]. From the latest high-profile incidents suffered by various organizations to cyber espionage conducted by sophisticated cyber actors, it is rare for a day to pass without reports of a newly discovered vulnerability or attack. The simple fact is that we are relying more on technology and are more interconnected. As everything, from power grids to transportation systems to global markets, relies heavily on networks, we are integrating them even more. As a result, the risks we face in this area have dramatically increased. A distinguished committee also made this point, advising that 'business and government must do more, sooner, if they are to have confidence and rigor in their responses'.

Cybersecurity encompasses protecting and responding to ongoing threats, as well as informing policy and research directions through public-private collaboration, security education, and basic research to deliver the necessary platforms. On the other hand, business resilience building describes the function that protects institutions from catastrophic events, always supports them and their customers, and facilitates faster recovery as soon as disruptions occur. It addresses the various domains that institutions face, presenting challenges such as natural disasters, technological failures, sophisticated attacks, and human errors. Business resilience and cybersecurity functions must be integrated into an entity's corporate governance framework, strategy, standards, and messaging, representing a significant component of its core operations [3].

1.2. Overview of cybersecurity in the digital age

Digital has become an integral part of our daily lives and has significantly transformed how we live, work, and govern. At every corner, the contribution of digital technologies, such as open data, the Internet of Things, artificial intelligence, and blockchain, drives various activities delivered through user-centered, convenient, and on-demand services to consumers and businesses. However, the benefits can only be realized if these services are secure, trustworthy, and resilient to potential harm. In the digital transformation process, as more business operations are integrated into the digital space, emerging risks pose a threat to digital security. When cybercrime strikes, it can have a damaging effect on business profitability and customer trust. Hence, businesses must prioritize cybersecurity as they operate in a dynamic and evolving cyber threat landscape. Businesses remain vulnerable to cyberattacks, and if attacked, they must also ensure that they can respond promptly, recover quickly, and maintain long-term security resilience. This report presents strategies that strengthen business cybersecurity by helping companies continuously monitor, review, and adapt their cybersecurity stance to ensure they operate in a secure environment [4].

1.3. Current cyber threat landscape

According to Radhi et al., the Information and Communications Technology (ICT) industry plays a pivotal role in supporting economic, social, and digital transformation [5]. The widespread digital connectivity has opened up new business opportunities, and a more efficient and secure digital environment has promoted economic growth. However, with ever-growing connectivity and the amount of information being transmitted through digital means, many 'black hat' organized crime groups (OCGs) have changed their focus from conducting physical crimes and drug trafficking to carrying out cyberattacks to extort businesses with sizeable returns.

Over the years, as the capabilities of cyber attackers have become increasingly advanced, and as businesses persist in not treating cybersecurity as a 'must-have', the total losses suffered from cyber threats have also increased significantly. Some 35% of small organizations believe their cyber resilience is inadequate, a proportion that has increased sevenfold since 2022. By contrast, the share of large organizations reporting insufficient cyber resilience has nearly halved [6]. Organizations and businesses must deploy cybersecurity measures; otherwise, they may face dire consequences if a successful cyber-attack is launched against them.

1.4. Importance of cybersecurity for business resilience

Cybersecurity is a matter of paramount importance for business. Proper knowledge, expertise, and support are crucial for achieving business resilience. The reliance on technologies and digital solutions places a premium on mitigating cyber risks and threats. Investments in cybersecurity should be no less significant than investments

in facilities, machinery and equipment, stock, services, and even the workforce. Given the significant societal trends in digitalization and artificial intelligence [7], enterprises should prioritize cybersecurity. Indeed, business continuity planning must consider typical natural disasters and political crises as challenges and cyber incidents [8]. The enterprise's core goals are protection of the business model, sustained success, and profitability. The digital age requires management insight in coping with risks and threats related to big data, cloud services, the Internet of Things, and connected, intelligent, autonomous systems. Every enterprise relies on technological and digital solutions, and the acceptance of cyber risks must be assessed in the context of the risk appetite of its board of directors and stakeholders. Achieving benefits and avoiding excessive costs in deploying advanced technologies requires businesses to consider, with urgency, consulting and obtaining advice from internal and external cyber experts in a process of continuous learning and understanding the implications of cyber risks on their resilience management. Small and medium-sized companies benefit from cost-effective outsourcing arrangements for cyber security [9].

1.5. Impact of cyber-attacks on business operations

The increasing use of digital technology creates opportunities for greater operational efficiency and cost savings, thereby boosting the competitiveness of businesses. However, the same technological evolution has spawned new measures that can easily penetrate poorly protected business information systems and inflict unquantifiable damage on organizations and their business partners. The cyber threat landscape has a common characteristic: there will always be targets for profit-motivated cyberattacks. The ease of conducting such attacks, often with minimal risk of detection and the potential for substantial profit if successful, creates additional concerns [10].

Similarly, Pavelea and Negrea are of the view that, despite the significant strides made in technology for detecting and responding to cyber threats, the expertise of those who operate these advanced systems has not yet entirely caught up with the arms race as they seek to stay one step ahead of cyber adversaries [11]. Human errors, business processes, and changes to technological controls and governance structures, whether intentional or not, continue to enable cyber adversaries to be successful. Recent reported high-profile cyber-attacks on businesses, many of which were a result of human errors or failures at their third-party vendors, clearly illustrate that the state of cybersecurity for businesses, especially for those who rely on external vendors to protect their core business operations, has not improved commensurately with the capability and technology in the market today.

2. Method

To delve into these matters, this paper employs a qualitative research method, as it allows for complex explorations of subjects like this one without reducing boundaries to those that can be quantified. When people refer to a research project as 'qualitative', they typically mean that the research is designed to reveal the target audience's range of behaviors, normative beliefs, values, and motivations drawn from direct accounts or quotes from the interviewees. This direction explores ways to utilize insights to understand issues better and, if relevant, refine survey research to obtain findings supported by lived experience. The exploratory method was therefore chosen to reveal how people think about and approach cybersecurity topics. Exploratory research employs a flexible research design that allows for consideration of a broad range of issues and trends, constraining or broadening them.

2.1. Method of data analysis

Descriptive analysis is then employed to gather data through interviews and literature reviews, which aid in understanding the problem and provide more significant insights. Analysis techniques enable us to categorize data more effectively into analytical and interpretive themes for presentation. This approach enables us to gain insight into real-world behaviors and organizational perceptions, thereby avoiding the creation of our typically bounded perceptions or an idealistic future. Finally, qualitative research is an inclusive methodological approach to determining what constitutes data. However, while this flexibility is a distinct strength, it also means that researchers must be aware that primary concerns, such as validity and reliability, cannot be guaranteed in the same way as they can with survey research or software-based inquiry.

2.2. Key components of a robust cybersecurity strategy

A comprehensive cybersecurity strategy is essential to a company's operational resilience. From enhancing business operations and fostering customer confidence to mitigating risks and creating a competitive edge,

cybersecurity protects firms from a myriad of disruptions and attacks. The demand for a robust and agile cybersecurity strategy has never been higher in a rapidly changing marketplace, with an increasing reliance on multiple interconnected technology platforms. Recent large-scale cyberattacks, along with the continued escalation of attacks on a company's core infrastructure and ethical business practices, have heightened the financial and reputational risks, drawing attention to board-level corporate governance issues [12].

On the other hand, the starting point in developing an effective cybersecurity strategy is for a company to acknowledge that no security solution is 100% secure and confront the new attack surface with clear goals and objectives in mind. The best security posture is achieved by implementing a holistic strategy with multiple layers of defense, requiring the commitment and vigilance of all stakeholders. The company must treat its cybersecurity posture as an enterprise-wide risk management challenge [13]. Senior management and the board of directors, with a comprehensive understanding of the company's risks and vulnerabilities, set the security strategy, allocate resources, foster an organizational culture that values security as a foundational principle, and determine the level of residual cybersecurity-related risk they are willing to accept. In corporate governance terms, the board of directors is responsible for setting the policies and standing as the final line of defense for overseeing the company's cybersecurity posture and ensuring fulfilment of the company's cybersecurity strategy.

2.3. Risk assessment and management

In the opinion of Ksibi, Jaidi, and Bouhoula, risk assessments and ongoing risk management are the foundation of any strong cybersecurity program [14]. However, companies must design and implement a dynamic approach to risk management that focuses on overall risk and the specific risks associated with particular assets and functions, prioritizing responses accordingly. However, they believe that the ability to change rapidly as emerging digital threats and potential vulnerabilities evolve is a critical part of ongoing risk management [15]. Although smaller companies are relatively newcomers to the digital marketplace, many already have a competitive advantage in transforming through complex digital infrastructure. When an attacker breaches such infrastructure, the potential risk is limited to the digital information necessary for the systems, not the loss of robust and valuable infrastructure. Such an approach mitigates the value of a successful attack.

A constructive approach to risk management considers the external threat environment, recognizing that cybercriminals, political activists, and hostile nation-states are often best positioned to delay new capabilities and are highly adaptable in utilizing them. Initial targets in fast-changing environments may not be easy to distinguish, partly due to the complex interdependencies evident throughout digital platforms and in sectors where smaller companies compete with established ones [16]. Nevertheless, companies require a disciplined risk management strategy that evolves in tandem with systems and infrastructure, adapting to their changing needs. Hartung argued that this approach would filter out projects that are not heavily involved in InfoSec initiatives, leverage available budgets and personnel effectively, and regularly manage emerging risks. Corporate boards and executives across various business sectors should monitor, learn from, and leverage the commentary, processes, and outputs of their mature company peers.

2.4. Technological solutions for cybersecurity

Developments in technologies have made it easier to automate cybersecurity tasks. Machine learning, computer vision, and natural language processing help detect malware and analyze threats. The public domain also contains substantial software businesses can use to protect their cybersecurity. Furthermore, although hardware-based security measures are costly, they can be a viable alternative for businesses involved in financial technology, cryptocurrency, and hardware production. The security challenges faced by AI developers are, in fact, self-imposed and driven by the need for competition. If they select the most efficient hardware available on the market, it is likely to be exposed to hackers ready to test its security privileges and capabilities. Apart from these tests, businesses also face an increased risk of security breaches as technology has become more vulnerable due to its increased connectivity [17]. Due to the highly interconnected nature of technological advancements in cybersecurity, new security measures are necessary to address increasingly sophisticated threats and frequently limited performance. Both chief executives and information security officers must realize that although advancing technologies optimize a company’s productive capacity, they come with substantial challenges to cybersecurity. Such misunderstandings can result in substantial information technology security breaches, leading to the business’s shutdown. Numerous measures can be adopted to overcome technological challenges, and businesses must keep pace with these developments. The interest is twofold: how industry and governments can support all those involved in today’s digital chain and how such processes can be automated securely.

2.5. Firewalls and intrusion detection systems

Firewalls keep unauthorized users out of private networks while allowing authorized users access to network resources. Some firewalls operate at the packet level, examining each packet that attempts to pass through the firewall according to a set of user-defined rules. Other firewalls operate at the application level. These so-called proxy firewalls provide enhanced security by examining the contents of data packets for specific characteristics relevant to the application being used. The security of the proxy firewall is enabled because data destined for the network protected by the firewall does not travel across the firewall in the traditional sense. The firewall receives or sends data on behalf of the original destination and verifies it before forwarding [18].

Intrusion detection systems are used to detect the presence of an actor who may be attempting to compromise the confidentiality, integrity, or availability of a resource. An intrusion is defined as any action attempting to compromise a system. An intrusion detection system searches for signatures of intrusions. These separate rules define what will be called offensive traffic. Intrusion detection systems are sometimes supplemented or replaced by intrusion prevention systems [19]. They continued that an intrusion prevention system can detect malicious network traffic and respond somehow. For example, the intrusion prevention system may block traffic from a hostile source. A limitation of a signature-based security approach, in general, is that prior experience is required to identify an intrusion signature. If changes in patterns of intrusion occur, the response time of an intrusion detection system might be delayed.

2.6. Human factors in cybersecurity

Whilst technology can boost what we do in cybersecurity, it should not be forgotten that behind all this IT equipment are the humans using and operating it. Addressing cybersecurity challenges requires a focus on human factors and end-user perspectives. There are highly skilled staff in workplaces who are likely to have better cybersecurity knowledge than general employees. They may also have roles and responsibilities that prescribe greater use of security behaviors.

Our insights reject overly simplistic panaceas about improving the state of individuals that abound in public policy and the cybersecurity literature, replacing them with a focus on organizations. These insights may be used to inform practice and guide future research in cybersecurity. In what follows, we first review the literature on cyber resilience before identifying existing knowledge gaps. We then present a research agenda to revisit the question: What must HRM do to achieve sustainable employee-driven cybersecurity capability? Considering this, Stowe and Nambiar opined that employee-driven cybersecurity capability is supported and reinforced by an HRM approach that takes account of these human dynamics, and we provide a strategic framework towards this end [20]. It aims to provide a means for organizations to lean forward, be assertive, and have their strategies and policies responsive to the dynamic changes that occur over time, including those related to employees and the workplace.

Considering this, Gorodianska opined that cyberattacks can lead to significant losses, fines, loss of customer and supplier trust, and other negative consequences that can destroy a business. Business owners should be aware of these threats and pay due attention to implementing a cybersecurity strategy and policy, as well as renewable economic resources, which requires predictive analysis [21]. The interaction between a person, as a key component of the enterprise's economic resource management system, and information and communication technologies requires planning measures to renew professional human competencies and overcome cyber threats, thereby strengthening business in the conditions of digitalization.

It is time for HRM to take the lead at the intersection of human resources and challenges in the digital age. Thus, just as there is a need to rethink overall HRM policies and strategies, it is also necessary to gain insights into how employees respond individually and collectively to security processes and cyber challenges, enabling compliance levels to be effectively monitored. The strategic roadmap we present can lead to a sustained employee-driven cybersecurity capability, a core area of concern in every organization that is more responsive to the digital age's challenges.

2.6.1. Employee training and awareness programs

Employee training and awareness are essential to any cybersecurity program, bolstering security measures. People in a company's workforce, from the board of directors to the sales staff, play a vital role in the security chain. For this reason, their knowledge and awareness of security issues is a company-wide concern. Training should be business-specific, with employees receiving essential information security instructions, familiarizing themselves with procedures in the event of a security incident, and being aware of their responsibilities in a

privacy-sensitive environment. This includes regular security-related reminders, emails, events, and encouragement to report incidents. The emphasis on employee awareness is to help ensure that security breaches originating within the sizable employee population are prevented wherever possible [22].

Employee training and awareness programs should not be a one-time effort. It is generally agreed that the existing paradigms on which security awareness programs are based either do not make intense enough demands or are inadequate in their own right. The perception of the importance of a security role among employees must be maintained through regular promotions of achievements, and the implications of significant events, such as data theft losses, must be emphasized. Security responsibilities, including who is responsible for them, are not always clear, and an ongoing review of the awareness training program will clarify these issues for staff. The consequences of different security risks for businesses must be understood at both a departmental and overall level, particularly in terms of how they may affect internal politics [23].

2.7. Regulatory compliance and cybersecurity

The legal and regulatory frameworks provide the foundation and guardians for the integrity of the sector and customer protection, ensuring that the deployment of digital services is fit for its purpose. Governments issue mandates for businesses to comply with so that the cybersecurity governance model begins at the organization's highest level. The challenge that organizations face involves ensuring that the compliance model is well articulated and integrates both governance and implementation processes that are purpose-built to protect the assets of the organization from executives to the customers, ultimately dampening the risks facing an organization, whether they are operational risks against the backdrop of the boardroom or the operational environment within the infrastructure tier. Melaku continued arguing that compliance with regulations is a key driver for many companies when they decide to invest in cybersecurity. Yet, for many, it can be seen as a box-ticking exercise [24].

Compliance with secrecy can be mandated by either regulators or individual audit firms. In some industries, individual risk managers implement complex privacy management policies, often falling short of rigor and severely lacking in addressing some significant compliance issues. By focusing on compliance over business priorities in these new areas, firms tend to view these security capabilities as a necessary cost, with no inherent need for improved efficiency or revenue generation that benefits customers.

2.7.1. GDPR and other data protection regulations

So, what about meeting international privacy standards such as those outlined in the General Data Protection Regulation or the numerous other regional, national, and industry regulations? Despite the evolving and growing nature of these regulations, they often complement each other, allowing firms to standardize their privacy compliance practices across vast geographies. Internally, this is beneficial as it enables the discovery of hidden standard policies and the removal of redundant ones. There is significant redundancy in the number of privacy and other security documents in the policy. However, taking this advantage overlooks any legal differences between various regulatory statements – this, after all, would seem to be in direct contrast with the legislation's letter and spirit. Accepting the suggestion for a lowest common denominator approach to compliance at face value seems unrealistic. Good cybersecurity policy should be driven by what is legally required of individuals rather than what the most cost-effective option dictates.

Beyond meeting regulatory needs, Tkachuk et al. believe that information assurance is about ensuring the appropriate level of confidentiality, integrity, and availability of information used in the context of the risks posed by the misuse of this information [25]. An essential part of an organization's understanding of the risks is identifying the applicable regulations – the fundamental lynchpin of compliance. But it's not just about meeting legal obligations. Compliance ensures the legality of business operations and facilitates clearly defined business operations

2.8. Incident response and business continuity planning

A coherent and well-articulated cybersecurity incident response plan is like a life vest on troubled waters for an organization. It provides clear directions on who to contact, what to contain, what to restore, and how to recover during a data emergency. This is especially important during a 'typical' business incident or a major national emergency. Lightweight, well-understood, and familiar with response protocols work far better than highly detailed plans and procedures where every scenario is meticulously scripted and carefully managed. Incident response plans and tabletop exercises are essential components of an organization's overall business resilience [26].

Big data and the ability to rapidly analyze and respond to cyber threats significantly improve an organization's ability to predict, prevent, detect, and respond to cyber incidents. By closely watching an organization's networks and paying close attention to network traffic, an organization can pre-empt and detect internal and external cyberattacks. It is no longer a question of whether a cybersecurity event will occur but of when that call will come, for indeed, it will. Organizations must become situationally aware to quickly detect and respond to these incidents or risk serious harm and loss. Awareness is now achieved through the increased use of products such as NetFlow, authentication logs, audit logs, firewalls, and Intrusion Detection Systems. Organizations must also conduct drills and exercises that include cyber events to better prepare for potential cyber incidents. These activities will help strengthen overall cybersecurity [27].

2.8.1. Developing an incident response plan

Staves et al. argued that time is critical when data are compromised, or a system fails irrevocably or goes down [28]. Establishing an incident management team and equipping them with the necessary knowledge and skills to respond decisively to incidents is a key element of cybersecurity resilience. The typical components of an incident response team are the legal representative, information security manager, public relations manager, customer service manager, data privacy manager, and potentially other stakeholder teams. When an incident threatens data, a network, a system, or an application, a series of activities should be taken. For example, define an incident response policy's who, what, and why. The team and its responsibilities should do this by defining an incident, i.e., what qualifies as an incident and who communicates cyber incident awareness knowledge to different departments or business units.

This is typically the security operations center if the company has it. After that, identify and assess the compliance and threats and how they can be seen and characterized. Finally, the action steps should be defined to increase knowledge of the contact points in the event of an unusual occurrence and to outline the measures that should be taken to protect internal or external confidentiality. Finally, this is the last step that should be taken, including the definition and frequency of response tests, such as tabletop exercises that cover testing, for example, antivirus systems, firewalls, and system access control compliance.

2.9. Integration of cybersecurity into a business strategy

The cybersecurity function cannot be the company's only bearer of cybersecurity. Businesses need to recognize it as a business imperative, and there is a need for the right culture throughout the broader business organization and the entire ecosystem to have proper cybersecurity in place. This requires raising awareness of the importance of cybersecurity at the board level, steering the cyber strategy in combination with expertise and coordinated action to enhance cybersecurity and incident response capabilities at every level within the organization, as well as with its suppliers, customers, and partners. Only if the message is reinforced throughout the company and the organization's ecosystem, from the business strategy shaping, leadership, and talent nurturing down to the execution level, together with attention to technological or process improvements, will businesses truly safeguard and be in firm control of this trinity: "People-Process-Technology" [29].

Arroyabe et al. also argued that many businesses do not consider security a key intermediate objective to align with overall corporate success [30]. Only companies in the energy and power sector seemingly recognize the critical importance of security to business turnover, the value of reputational protection, and the sustainable contributions that security can bring to their operational success. Other sectors appear to see security mainly as an obligation, the costs of which need to be limited or minimized.

To mainstream the perception of cybersecurity as a business differentiator, companies need to understand better the risks posed by cybersecurity vulnerabilities and consider them as significant financial exposures. The impact of share price and reputation does get the board's attention more directly, as the business sees them as an integrated objective. In contrast, brand and intellectual property are perceived as growth factors. Companies have already considered the impact of not having access to the brand, the intellectual property, or the identity used to share an asset. More and more customers are increasingly expecting companies to take active steps to protect their brand and information security, and they are voting with their feet accordingly. It is not just a big company issue; 50% of European SMEs expect it will be a matter of time before they face cybercrime.

2.9.1. Aligning cybersecurity with organizational goals

Corporate leadership and information security leaders must share business objectives to maintain alignment between business and information security programs. One way to establish this shared vision is through clear communication and an understanding of corporate goals. One approach is for corporate leadership to establish

strategic goals and for business leaders to establish performance objectives and critical success factors for individuals, business operating units, or the corporation. Security should create an annual plan with performance goals aligned with these performance objectives and success factors. Identifying and strengthening alignment at the appropriate organizational boundary levels enables the identification of cybersecurity requirements for people, processes, technology, and governance, which can support a business [31].

Maintaining core capabilities by managing cybersecurity risks, losses, and responses associated with cybersecurity failures should be a consistent and necessary measure to achieve key business success factors. Risk management is fundamentally about understanding business-threatened outcomes and related business success factors. A formal, universal, and consistent framework is necessary to build the highest level of leadership's risk management knowledge, understanding, and skills. It must be designed to support strategic thinking and release the intimate knowledge of the business operations in multiple contexts. Sensible convergence of business and risk management disciplines will provide the means for certifying relevant business outcomes and a practical, well-defined risk management strategy that fosters the successful ongoing performance of the business [32].

3. Results and discussion

3.1. SWOT analysis of cybersecurity in business

Businesses require appropriate cybersecurity advice, training, and expert guidance on methodologies for maximizing effectiveness and optimizing costs associated with creating and maintaining cybersecurity resilience. Security tools and techniques must complement the business's needs and the organization’s technology to be effective. IT risk, device, and data protection are imperative. Balancing the business's exposure to cybersecurity data breaches is critically essential. Non-functional behavioral compliance solutions educate employees and minimize exposure to phishing scams, cybersecurity failures, and cybersecurity attacks exploiting network and server vulnerabilities. Data breaches and cybersecurity issues may be managed and resolved proactively or reactively [33]. They believe cybersecurity exists to protect the business's enterprise data integrity, availability, and confidentiality. Technology is essential for protection and dramatically benefits from administrative security policies that support IT technology. Threats that exploit vulnerabilities are constant and inherent in any computer network's privacy and security, affecting communication for data. This poses a challenge to the progression of security constraints as data protection evolves and is effectively maintained against cybersecurity risks with a conservative margin.

3.2. Strengths: current cybersecurity capabilities

Across the modern digital economy, business strategies combine with technologies to produce ambitious commercial outcomes that deliver value to consumers and prosperity to investors and communities. The CEO-driven enterprise strategy focuses on robust financial performance and includes an expanded commitment to cybersecurity. Business leaders recognize the value at stake in protecting valuable digital assets, ensuring enterprise operations continuity, and demonstrating responsibility for protecting consumer privacy and interactions. The principles broadly accept that cybersecurity requires performance and maturity levels that are managed, measured, and scaled to foster business growth and maintain consumer trust.

An industry-driven discipline has evolved to manage threat landscapes and deliver robust and effective cybersecurity tools integrated into business operating environments. Cybersecurity stakeholders have formed an industry constituency of organizations, large and small, producing a portfolio of cybersecurity tools and practices suitable for various specialties, scales, and service levels. Whether a large enterprise, a regional service provider, or a small commercial enterprise, capable cybersecurity protection is available through options centered on a mix of in-house or outsourced tools and talent. Our healthcare organizations, operating with awareness of the value of their data, patients, and services, have strengthened their relative cybersecurity postures. As critical stakeholders in the healthcare business ecosystem, so have its myriad service providers, including insurance companies, pharmaceutical developers, and medical device manufacturers. Similar histories of successful and mature cybersecurity protections can be cited for other industry sectors.

3.3. Weakness: vulnerabilities and gaps in security

A critical point in common with the cases above is the weakness of current ICT systems against cybercrime. Business organizations are at risk if they neglect these facts. The number of types of digital information that is available has also increased. One crucial point is that new types of information serve as better collaboration

tools and are an increasingly important part of today's world. Organizations need to be repositories of knowledge and packets of intelligence about things needed for success.

Legitimate businesses have a legitimate need to collaborate. Illegal organizations also have a similar need to evade detection. The forensic readiness of an organization's information systems is vital in determining who gets apprehended and convicted, who effectively works together, and which organization is effectively protected against cybercrime. These are significant weaknesses in current systems.

A key point is that we only know the value of current gaps and weak points because attackers are aware of them. These are the logical results of attackers knowing our systems better than administrators. However, a system is poorly designed if the only way to identify gaps is by observing who gains access, regardless of protocol. If nobody can spot the gaps, that's good from the attackers' perspective. If we can't spot the gaps, we can't understand how an organization has been attacked.

Organizational readiness is a key point that determines many aspects of organizational success. This might be related to the competitive advantage angle. Another way attackers gain access is by identifying a system that is already failing and then leveraging the success of legitimate requests by masquerading.

3.4. Opportunities: emerging technologies and best practices

Network connections must be well-protected and resilient, so organizations across sectors and industries can continue operations in an emergency. Employees must have alternatives in terms of technology that can be used to connect networks and securely perform tasks when physical barriers prevent them from full access.

These technologies and processes include advanced remote capabilities, zero-trust architecture, secure access service edge, cloud-distributed denial-of-service protection, software-defined perimeters, network virtual appliances, access control measures, service meshes, and key-driven multi-factor authentication. Entities could protect the high availability and functionality of protected cloud services by leveraging various remote cloud-based managed security services. These can help combat typical cyber threats and provide a direct path back for businesses that an incident has endangered.

Cybersecurity professionals can differentiate between security and resilience by thinking of resilience as a martial arts opponent rather than a brick wall; instead of simply trying to stop what is coming at us, resilience requires us to absorb the hit and continue. In the digital age, lessons learned about cybersecurity and resilience underscore the importance of adopting a proactive, risk-based approach to securing networks and information.

These measures include strengthening relationships between the public and private sectors, supporting federal workforce development, integrating advanced technologies, utilizing service mesh security, and creating opportunities to enhance innovation and resilience while simultaneously adding value and avoiding redundancy [34]. Cyber threats appear to be in constant flux. As technology evolves in scope and character, systemic cyber vulnerabilities grow and merge, eliminating all risks and ensuring absolute security is unattainable.

3.5. Threats: rising cybercrime and regulatory challenges

In this digitally driven economy, cybersecurity issues have taken on boardroom importance. For many companies, their data is the most valuable asset and ensuring that their systems are as secure as possible is a crucial part of their business strategy. As IT continues to evolve and we see an increasing number of computerized devices and applications, the risk of cybercrime also rises [35].

Very few companies today have been hit by an IT security breach, including companies with the best security systems and strategies. Small businesses are more vulnerable to their size compared to larger companies. What risk do IT security issues represent? And what can be done to minimize problems and damage? The following is a collection of thoughts on relevant market factors, associated statistics [36] regarding the size and cost of the problem, and some brief best practice industry suggestions.

The Internet is a whole of hackers. Networks are often under attack; sometimes, you cannot feel secure in your home. Today, most business concerns revolve around keeping their networks secure. Risks associated with security breaches make Internet and computer security an industry growing due to the sheer need for security and a desire to survive hacking attempts. Internet security is the protection associated with computer security, computer networks, and the information and data stored and transmitted.

A variety of technologies exist to protect these assets. Many steps can be taken to protect company data; unfortunately, no protection can ever be 100% effective. Companies must be aware of the risks to their business

from external and internal threats, mainly when numerous cybercriminals target them. For companies providing security services, the 'outrage factor' can often be the main engine for promoting the importance of their services.

On the other hand, the procurement and responsiveness of companies towards the purchase of security software also involve several subsequent market factors, which are uniquely illustrated in a simple model (Figure 1).

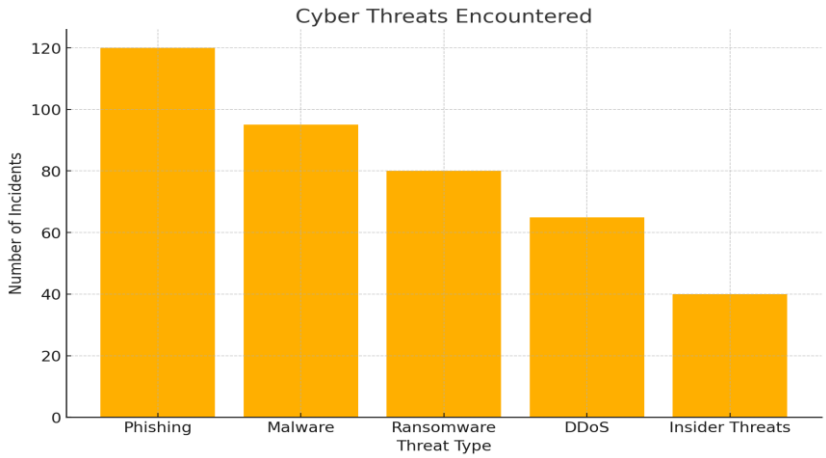

Figure 1. Cyber Threats

Source: from the cyber magazine highlights reports, 2025

This bar chart illustrates the frequency of various cyber threats that businesses encounter. This pie chart (Figure 2) shows the distribution of common cybersecurity vulnerabilities in organizations.

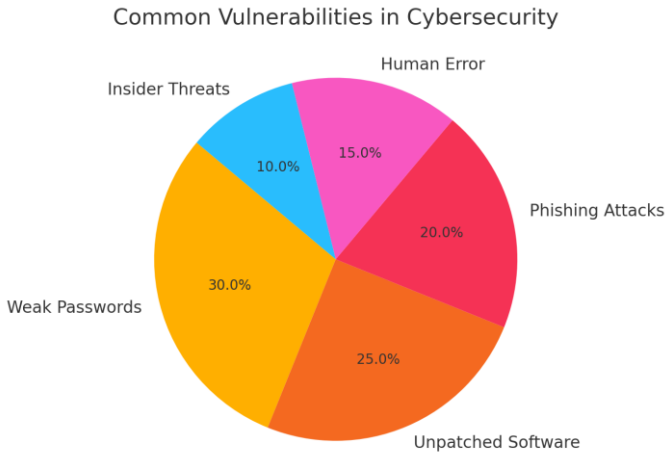

Figure 2. Common vulnerabilities

Source: Bitdefender report 2024, accessed February 21st, 2025

3.6. Strategies to leverage strengths in cybersecurity

Some strategies enable a strengthening of a company's cybersecurity intelligence work. Indeed, most companies today are becoming aware that their ability to respond promptly and efficiently to security threats is one of the most valuable aspects of their cybersecurity program. However, traditional vulnerability assessment methods can no longer detect the sophisticated and stealthy advanced persistent threats that lurk within the enterprise network and connect with the necessary information. This type of internal network attack has become increasingly targeted and difficult to locate; therefore, it is necessary to conduct cyber-intelligence operations to obtain accurate visibility of the company's cybersecurity status. The cyber-intelligence capability an organization acquires is measured by the degree of correlation of diverse types of data it produces, such as security information and event management outputs, network and host behavior analysis data, and static and dynamic malware analysis. It also includes reports of targeted attacks for forensic and network behavior

analysis, as well as strategic threat intelligence, among other types of data [37]. The number of tools required to gather sufficient information about security attacks can be overwhelming. Hence, we propose a series of strategies to implement before implementing specific intelligence tools. In the first step, clear definitions and standards must be produced to set measurable goals that can be followed and implemented during the migration process. This is indeed a must-have, given that correctly measuring the quality of a cyber-intelligence operation is a necessary step and a helpful guide in planning development and resource allocation. Hence, well-defined metrics are needed to indicate the security posture, time, and resources required to transition to a state-of-the-art security model implementation. The human factor needs a behavior change, and its effectiveness should be measured and tracked. The remaining intelligence capability requirements are associated with more specific optimization strategies, summarized next [38].

3.7. Implementing robust security infrastructure

Employees at the perimeter require access to applications and services housed in the private or hybrid cloud. Access must also be provided to frequently mobile employees, who may not be located securely in a business central or branch office. A robust security infrastructure, utilizing leading technologies from security vendors that continuously invest in their security platforms, will provide the most effective protection against the myriad of cyber threats faced by security teams and end users today. Technologies such as firewalls, web application firewalls, and secure web gateways can be hosted within the private network to protect against the increasing volume of web-based threats driven by the growth of public cloud services. Additional security technologies are needed at the perimeter to protect against threats such as Trojans and bots that web security technologies typically will not detect [39]. Endpoint security policies and mobile device management solutions will be utilized to protect both managed and unmanaged devices, enforcing security policies to mitigate the risk of data breaches. Businesses should invest in the people, security technologies, and processes needed today while also planning and investing in future security strategies. These strategies will provide optimal protection by integrating software and hardware capabilities with the continually evolving security platforms of leading security vendors. Faced with relentless attacks and data breaches causing a multitude of usually maverick and financially driven criminal activities, it is no longer a choice to protect and defend; it is a necessity for businesses to remain strong and resilient within the digital global marketplace of today and the continually evolving global digital economy of the future [40].

3.8. Enhancing data encryption and access controls

To Reddy and Ravindranath, securing data has become increasingly crucial due to the rise in cyberattacks and the growing volume of data generated daily [41]. Many business organizations encrypt data stored on the internet. However, not many consider implementing another level of encryption for their internal transmissions. Business organizations should encrypt data both at rest and in motion. When internal communications are stored in an encrypted format, any potential unauthorized party that may compromise data by leaving a device or attempting to decrypt the already encrypted data cannot make sense of it [42]. Data access should be controlled by setting user permissions to limit data exposure. As some users may not be aware of the data security protocols or understand how these protocols protect them, implementing automated access controls to deny access to files stored in local folders, shared folders on company networks, or collaboration sites is recommended. Furthermore, artificial intelligence or analytics for data use should also be applied to alert the IT department to any unusual changes made on the company network, allowing for immediate investigation [43].

3.9. Developing proactive threat intelligence and monitoring

Companies operate in a dynamic environment with cyber risks in today's interconnected business landscape. The rapidly evolving digital world is witnessing an increase in cyberattacks and threats posed by emerging technologies. Current cyberspace security efforts often rely on reactive responses or lack the coordination, agility, and collaboration necessary to mitigate threats effectively. Many existing strategies neither address the growing vulnerability of businesses to digital exploitation nor are they commensurate with emerging technologies and digital transformation. This deficiency could render redundant innovative digital solutions that

are yet to realize their potential, such as driverless operation and user-delivered instant transport. Chen et al. believe that building cybersecurity into all stages of system and software development, relying on artificial intelligence and machine learning, using cloud technology, implementing the Zero Trust Model, as well as monitoring 24 hours a day, seven days a week, can help companies transform reactive defenses into proactive protections [44]. This proactive approach pays off better by reducing maintenance overheads and increasing customer loyalty. Moreover, combining digital tools with expert knowledge to gather, analyze, and distribute cyber threat intelligence helps understand companies' risks, allowing for more informed strategic decisions. Efficient emergency planning is now in the hands of top management, whether agreed upon or shared with an appropriate department. Cybersecurity must be elevated to a strategic level to enable everyone familiar with it to leverage it to its fullest, ensuring resilience for the company during the era of digital disruption. This explored the potential of various initiatives, with valuable lessons for developing a supportive cybersecurity strategy perspective. A collaborative environment can help companies implement resilient security systems by assigning different stakeholders roles in implementing and monitoring these activities.

3.10. Key strategies to choose to overcome weakness

This paper argues that the strategies we recommend for strengthening cybersecurity and achieving business resilience are:

1. Identification of essential functions: Defining and identifying the essential functions and activities required to enable trade, as well as those essential for enterprise renewal purposes.
2. Prioritized delivery of products and services: prioritized delivery of essential products and services through the continued operation of key IT systems.
3. Adaptable, resilient, and sustainable: use adaptable, resilient, and sustainable security strategies integrated into multi-disciplinary plans.

3.11. Comparison with similar studies

Table 1 provides a detailed comparison of the manuscript titled "Strategies to Strengthen Cybersecurity for Business Resilience in the Digital Age" with studies conducted in cybersecurity.

Table 1. Comparison of findings with previous studies

Aspect	Manuscript Results	Relevant Studies	Comparison and Validation
Cybersecurity Importance	Highlights the importance of cybersecurity in ensuring business resilience, particularly in today's digital landscape.	[1], [3], [10]	The manuscript aligns with these studies, which emphasize the importance of cybersecurity for business continuity and growth.
Digital Transformation Impact	Highlights the opportunities and cybersecurity risks associated with digital transformation.	[8], [30]	The manuscript supports the finding that, although the benefits of digital transformation are well-documented, their realization demands solid cybersecurity countermeasures to mitigate potential risks.
Human Factors in Cybersecurity	It emphasizes the importance of human factors and the need for employee training and awareness programs.	[21], [47]	The manuscript supports these studies and highlights the critical role of human behavior and education in cybersecurity approaches.

Aspect	Manuscript Results	Relevant Studies	Comparison and Validation
Regulatory Compliance	Emphasizes the crucial need for GDPR and other data protection legislation compliance.	[29], [32]	The manuscript echoes these studies, providing details on how compliance is vital to the governance of cybersecurity.
Technological Solutions	Recommends machine learning, firewalls, intrusion detection systems, and other state-of-the-art technologies.	[5], [19]	The manuscript supports and promotes the integration of advanced technologies into cybersecurity.
Incident Response Planning	Stress on incident response and well-documented business continuity planning.	[28], [27]	This manuscript aligns with these works on the pivotal role of preparedness and response planning within the cybersecurity field.

The importance of cybersecurity in enhancing business resilience is well supported in the literature, as seen in the manuscript. Studies by A. Kanaan et al. [1] and S. Saeed [3] also review the literature related to secure E-business operations and continuous operation in the face of digital threats. The statement in the manuscript that digital transformation presents significant opportunities but also poses unique cybersecurity risks is supported by the work of I. Yanenkova and V. Nedelko [7] as well as S. Abdelkader et al. [39]. Such consensus underscores how vital it is for businesses to take cybersecurity into their own hands through a strategic approach to their digital transformation plans. The manuscript provides valuable insights into the importance of human factors in cybersecurity, highlighting the significance of employee training and awareness initiatives, as supported by the studies conducted by J. Stowe and R. Nambiar [20]. The studies further demonstrate that human behavior and training are foundational aspects of any solid cybersecurity approach. The manuscript focuses on data regulatory compliance, particularly regarding the GDPR, aligning with the findings of H. M. Melaku [24] and S. Tkachuk et al. [25]. Every organization must have cybersecurity governance aligned with relevant regulatory frameworks. Support for the manuscript's suggestion of utilizing advanced technologies, such as machine learning, firewalls, and intrusion detection systems, as mentioned by M. A. H. Radhi [5] and H. Attou et al. [19]. This suggests that advanced technologies need to be incorporated for improved cyber defense, as indicated by our studies. A. Staves et al. support the manuscript's emphasis on a well-defined incident response plan and business continuity planning [28]. This alignment further underscores the importance of planning and preparedness in effectively addressing cybersecurity incidents. Moreover, the study's top-level SWOT analysis may not be able to convey the nuanced details of cybersecurity issues and areas of potential. Further research may identify more granular and industry-based analyses with the potential for implementing actionable steps. Additionally, the more generalist nature of the manuscript may fail to meet some of the specific cybersecurity requirements within different sectors, such as healthcare or finance, which operate under their own regulatory and operational environments. Future work should explore more focused recommendations that consider industry-specific cybersecurity challenges and responses. Limited types of studies, such as longitudinal studies, can also help evaluate the long-term impact of cybersecurity strategies on business sustainability and resilience, providing insights into the effectiveness of various approaches over time.

Comparing the results of the manuscript with the existing and relevant studies, a firm agreement was observed in areas such as the need for cybersecurity, the impact of digital transformation on cybersecurity needs, the role and importance of human factors, and regulatory compliance. These results demonstrate the manuscript's accuracy and relevance to the current cybersecurity landscape. Yet, future research directions can be further improved to identify quantitative validations, industry-specific analyses, or longitudinal studies that will both strengthen the study's impact and provide actionable insights for business managers and policymakers.

3.12. Limitations of the study

The current research has some limitations. They are related to several aspects:

- *Qualitative Nature* of this research can restrict the generalizability of the results. Although qualitative methods can yield in-depth insights, they may not accurately reflect the extent of the cybersecurity problem in various sectors.
- *Weakness of the concept* is that Descriptive Analysis is used and this is not able to give a strong statistics validation. The conclusions of the current study would have been strengthened with more quantitative data.
- *SWOT Analysis:* while the SWOT includes a high-level overview of cybersecurity elements, it might fail to encompass the nuanced complexities of relating challenges and opportunities.
- *Sector-specific findings:* the research might not adequately account for the varied cybersecurity challenges faced by different sectors, including healthcare or finance, that have varying regulatory and operational frameworks.

3.13. Future research directions

Several directions are suggested by authors for future research. Firstly, quantitative studies could be conducted to validate and substantiate the findings with statistical evidence regarding the impact of cybersecurity measures on business resilience. The authors recommend analyzing industry-focused studies and examining cybersecurity issues related to various sectors, providing more contextual solutions. Perform longitudinal studies to analyze the enduring impact of cybersecurity strategies on sustainable and resilient businesses. Discuss the potential of new technologies, such as artificial intelligence [45], quantum computing, data processing with machine vision [46], blockchain, and biomedical engineering [47], in improving cybersecurity during data analysis and transfer. Regarding international comparisons, the authors plan to explore global cybersecurity practices and their effectiveness across various countries and regions to identify best practices and areas for improvement.

4. Conclusions

In conclusion, this paper highlights the importance of cybersecurity to business resilience, traces the trends of digital technology adoption, and discusses how these trends will increase business dependence on cyber systems [48]. It introduced the significant causes of cybersecurity vulnerability and the business drivers and motivators for cybersecurity [49]. Today, it is not just organizations that need their information to conduct business with others; it is also suppliers, dealers, shipping companies, banks, and investors [50]. Concerned with information security managers who wish to enhance their organization’s security commitment need to be able to contribute evidence of business benefits to this debate. Because an organization’s influence and impact on its employees are critical factors in determining commitment, its corporate culture has a significant influence. Socio-cognitive models that draw upon psychological theories, such as the Theory of Planned Behavior, which emphasizes the importance of attitudes, social norms, and perceived control, have gained recognition for explaining and predicting behavioral intentions within the technology adoption domain [51]. The following recommendations are presented in this paper. Assign ownership of cybersecurity: the organization should have the right person managing the cybersecurity of the company's cyber systems. The CSO should have a seat at the board level and participate in regular risk management meetings [52]. Employing a CSO can increase perceived risk ownership, leading to more assertive risk-reducing behavior. Given the diverse nature of security applications, such a holistic view and coordination of security incidents across different security bodies are crucial. This would imply close collaboration between the government and local law enforcement agencies. Governance, culture, and enforcement: empirical evidence indicates that organizational factors are among the primary causes of most security breaches. A cultural approach represents a more effective way to manage insider threats according to

practical implications. Physical and environmental control within the organization plays a vital role in preventing insider threats by effectively implementing technological mechanisms [53].

Declaration of competing interest

The authors declare that they have no known competing interests, financial or otherwise, in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

Author contribution

The contribution to the paper is as follows: S. Sukachova, L. Gorodianska: study conception and design; M. Burmaka: data collection; L. Gorodianska, I. Yanenkova, M. Burmaka: analysis and interpretation of results; I. Tkach: draft preparation. All authors approved the final version of the manuscript.

References

[1] A. Kanaan, A. M. Al-Hawamleh, M. Aloun, A. Alorfi, and M. A. Alrawashdeh, "Fortifying organizational cyber resilience: an integrated framework for business continuity and growth amidst escalating threat landscapes", *International Journal of Computing and Digital Systems*, vol. 17, no. 1, pp. 1-14, 2024.

[2] A. Folorunso, "Cybersecurity and its global applicability to decision making: a comprehensive approach in the university system", *Available at SSRN*, 4955601, 2024.

[3] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations", *Sensors*, vol. 23, no. 15, 6666, 2023.

[4] L. Judijanto, D. Hindarto, S. I. Wahjono, and N. Djunarto, "Edge of enterprise architecture in addressing cyber security threats and business risks", *International Journal Software Engineering and Computer Science (IJSECS)*, vol. 3, no. 3, pp. 386-396, 2023.

[5] M. A. H. Radhi, N. M. Hussien, and Y. M. Mohialden, "Reviewing organized cybercrime: a global perspective on cyber security", *Scientific Research Journal of Engineering and Computer Sciences*, vol. 3, no. 4, pp. 7-16, 2023.

[6] Global Cybersecurity Outlook 2025. *World Economic Forum*, 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

[7] I. Yanenkova, and V. Nedelko, "The key global trends in the development of digital technologies in 2025", *Electronic scientific journal "Efektyvna ekonomika"*, no 7, 2024.

[8] S. Atkins and C. Lawson, "An improvised patchwork: success and failure in cybersecurity policy for critical infrastructure", *Public Administration Review*, vol. 81, no. 5, pp. 847-861, 2021.

[9] D. Kosutic and F. Pigni, "Cybersecurity: investing for competitive outcomes", *Journal of Business Strategy*, vol. 43, no. 1, pp. 28-36, 2020.

[10] N. Sun, M. Ding, J. Jiang, W. Xu, X. Mo, Y. Tai, and J. Zhang, "Cyber threat intelligence mining for proactive cybersecurity defense: a survey and new perspectives", *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1748-1774, 2023.

[11] A. Pavelea, and P. C. Negrea, "A Comprehensive Analysis of High-Impact Cybersecurity Incidents: Case Studies and Implications", 121 p., 2024.

[12] V. Vakarov, K. Redko, M. Hodiashchev, S. Tkachuk, and V. Yemets, "Opportunities and threats for the strategic development of ukraine's economy until 2030", *Futurity Economics & Law*, vol. 4, no. 4, pp. 42-59, 2024.

[13] N. Rodinova, N. Pylypchuk, S. Domashenko, I. Havrylyuk, and A. Androsovych, "Ukrainian economy in the era of digital branding: Risks and opportunities", *Futurity Economics & Law*, vol. 4, no. 4, pp. 4-24, 2024.

[14] S. Ksibi, F. Jaidi, and A. Bouhoula, "A comprehensive study of security and cyber-security risk management within e-health systems: synthesis, analysis and a novel quantified approach", *Mobile Networks and Applications*, vol. 28, no. 1, pp. 107-127, 2023.

[15] K. Koshekov, K. Alibekkyzy, B. Toiganbayev, S. Belginova, T. Keribayeva, V. Tulaev, and A. Koshekov, "Formalization of risk management in the context of digital business transformation", *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 3, pp. 1428-1439, 2023.

[16] T. Hartung, "ToxAIcology – The evolving role of artificial intelligence in advancing toxicology and modernizing regulatory science", *Alternatives to Animal Experimentation (ALTEX)*, pp. 559-570, 2023.

[17] A. A. Mughal, "Building and securing the modern security operations center (SOC)", *International Journal of Business Intelligence and Big Data Analytics (IJBIBDA)*, vol. 5, no. 1, pp. 1-15, 2022.

[18] B. Singh and S. S. Cheema, "Next generation firewall and self authentication for network security", in *7th International Conference on Image Information Processing*, India, 22-24 November 2023, pp. 707-713.

[19] H. Attou, M. Mohy-eddine, A. Guezzaz, S. Benkirane, M. Azrour, A. Alabdultif, and N. Almusallam, "Towards an intelligent intrusion detection system to detect malicious activities in cloud computing", *Applied Sciences*, vol. 13, no. 17, 9588, 2023.

[20] J. Stowe, and R. Nambiar, "The future for frontline retail employees: exploring the intersection of employee-driven innovation and technology integration", Master's degree thesis, Dept. of Design in Strategic Foresight & Innovation, OCAD University, Toronto, Ontario, Canada, 2023.

[21] L. V. Gorodianska, "Predictive analysis of renewable economic resources", *Actual Problems of Economics*, vol. 145, no. 7, pp. 8-15, 2013.

[22] N. T. O. Abrahams, N. O. A. Farayola, N. S. Kaggwa, N. P. U. Uwaoma, N. A. O. Hassan, and N. S. O. Dawodu, "Cybersecurity awareness and education programs: a review of employee engagement and accountability", *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 100-119, 2024.

[23] N. A. C. Odimarha, N. S. A. Ayodeji, and N. E. A. Abaku, "Securing the digital supply chain: Cybersecurity best practices for logistics and shipping companies", *World Journal of Advanced Science and Technology*, vol. 5, no. 1, pp. 26-30, 2024.

[24] H. M. Melaku, "A dynamic and adaptive cybersecurity governance framework", *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 327-350, 2023.

[25] S. Tkachuk, S. Suprunenko, and S. Stender, "Regulatory challenges and consumer protection in the context of the growth of electronic money in Ukraine: a literature review", *Law, Business and Sustainability Herald*, vol. 3, no. 2, pp. 15-29, 2023.

[26] A. Basu, "International cyber incidents: on the question of public attribution", *Observer Research Foundation (ORF), Issue Brief*, no. 748, 20 p., 2024.

[27] S. Bag, P. Dhamija, S. Luthra, and D. Huisingh, "How big data analytics can help manufacturing companies strengthen supply chain resilience in the context of the COVID-19 pandemic", *The International Journal of Logistics Management*, vol. 34, no. 4, pp. 1141-1164, 2021.

[28] A. Staves, T. Anderson, H. Balderstone, B. Green, A. Gouglidis, and D. Hutchison, "A Cyber Incident response and recovery framework to support operators of industrial control systems", *International Journal of Critical Infrastructure Protection*, vol. 37, 100505, 2022.

[29] A. George, A. George, and T. Baskar, "Digitally immune systems: Building robust defences in the age of cyber threats", *Partners Universal International Innovation Journal*, vol. 1, no. 4, pp. 155-172, 2023.

[30] M. F. Arroyabe, C. F. A. Arranz, I. F. De Arroyabe, and J. C. F. De Arroyabe, "Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives", *Computers & Security*, vol. 141, 103826, 2024.

[31] F. Hoffmann and B. Withers, "Shared Values: Nutrients for learning", in *Learning Organizations*, J. Renesch, S. Chawla, Eds., UK: Productivity Press, pp. 463-476, 2024.

[32] A. Al-Momani, M. Sarram, S. Zighan, et al., "The influence of cybersecurity leadership on the resilience of Jordanian businesses: A study on the role of cybersecurity measures in entrepreneurial success", in *Business Analytical Capabilities and Artificial Intelligence-enabled Analytics: Applications and Challenges in the Digital Era*, vol. 2, Switzerland: Springer Nature, pp. 1-15, 2024.

[33] 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. 85701-85719, 2022.

[34] O. Dobrovolska, R. Sonntag, W. Ortmanns, I. Kadyrus, and T. Rudyanova, "Structural and comparative analysis of R&D funding impact on the level of innovation development: The empirical evidence of GII's leaders and Ukraine", *Innovative Marketing*, vol. 19, no. 4, pp. 310-322, 2023.

[35] S. R. Biedron, "Cybercrime in the digital age", Master's thesis, Centre for Criminology, Faculty of Law, University of Oxford, Oxford, England, 2024.

[36] V. Shvedun, and S. Khlamov, "Statistical modelling for determination of perspective number of advertising legislation violations", *Actual Problems of Economics*, vol. 184, no. 10, pp. 389-396, 2016.

[37] M. Paul, L. Maglaras, M. A. Ferrag, and I. Almomani, "Digitization of healthcare sector: A study on privacy and security concerns", *ICT Express*, vol. 9, no. 4, pp. 571-588, 2023.

[38] K. F. Hew, W. Huang, J. Du, and C. Jia, "Using chatbots to support student goal setting and social presence in fully online activities: learner engagement and perceptions", *Journal of Computing in Higher Education*, vol. 35, no. 1, pp. 40-68, 2023.

[39] S. Abdelkader, J. Amissah, S. Kinga, G. Mugerwa, E. Emmanuel, D. E. A. Mansour, M. Bajaj, V. Blazek, L. Prokop, "Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks", *Results in Engineering*, vol. 23, 102647, 2024.

[40] L. Li, "Reskilling and upskilling the future-ready workforce for industry 4.0 and beyond", *Information Systems Frontiers*, vol. 26, no. 5, pp. 1697-1712, 2022.

[41] P. R. S. Reddy, K. Ravindranath, "Enhancing secure and reliable data transfer through robust integrity", *Deleted Journal*, vol. 20, no. 1s, pp. 900-910, 2024.

[42] O. Yu. Guseva, I. O. Kazarova, I. Y. Dumanska, M. A. Gorodetskyy, L. V. Melnichuk, and V. H. Saienko, "Personal data protection policy impact on the company development", *WSEAS Transactions on Environment and Development*, vol. 18, pp. 232-246, 2022.

[43] S. Duggineni, "Impact of controls on data integrity and information systems", *Science and Technology*, vol. 13, no. 2, pp. 29-35, 2023.

[44] J. Chen, Z. Liu, X. Huang, C. Wu, Q. Liu, G. Jiang, Y. Pu, Y. Lei, X. Chen, X. Wang, K. Zheng, D. Lian, and E. Chen, "When large language models meet personalization: perspectives of challenges and opportunities", *World Wide Web*, vol. 27, 42, 2024.

[45] O. Yuryk, L. Holomb, L. Konovalova, V. Vivsyannuk, and Y. Tsekhmister, "Assessment of the impact of artificial intelligence technologies on the development of Ukrainian medicine in war conditions", *International Journal of Chemical and Biochemical Sciences*, vol. 24, no. 5, pp. 206-211, 2023.

[46] S. Khlamov, V. Savanevych, I. Tabakova, V. Kartashov, T. Trunova, and M. Kolendovska, "Machine Vision for Astronomical Images using The Modern Image Processing Algorithms Implemented in the CoLiTec Software", *Measurements and Instrumentation for Machine Vision*, pp. 269-310, 2024.

[47] Y. V. Tsekhmister, A. V. Chalyi, and K. A. Chalyy, "Teaching and Learning of Medical Physics and Biomedical Engineering in Ukrainian Medical Universities", *World Congress on Medical Physics and Biomedical Engineering*, IFMBE Proceedings, vol. 25, no. 12, 2009.

[48] O. Akimova, N. Zhydovska, T. Kuchmiiova, N. Kozitska, and I. Buriak, "Cyber protection of financial data in accounting: implementation and use of cryptographic techniques", *Economic Affairs*, vol. 69, no. 2, pp. 1041-1052, 2024.

[49] C. A. Rosario, S. R. Anan, and M. M. Alam "The human element in cybersecurity – bridging the gap between technology and human behaviour", INTE1130 Industry Awareness Project Final Report, RMIT University, Melbourne, Australia, 2023.

[50] O. Muliarevych, "Acceptance and shipping warehouse zones calculation using serverless approach", in *12th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece, 09-11 December 2022, pp 1-6.

[51] A. Panchenko, A. Voloshina, S. S. Sadullozoda, O. Boltyansky, and V. Panina, "Influence of the design features of orbital hydraulic motors on the change in the dynamic characteristics of hydraulic drives", in *5th International Conference on Design, Simulation, Manufacturing*, Poland, 7-10 June 2022, vol. 2, pp. 101-111.

[52] S. V. Kovalchuk, D. L. Kobets, and Ye. M. Zaburmekha, "Modeling the choice of strategies of marketing management of enterprise personnel", *Naukovyi Visnyk NHU*, no. 2, pp. 163-173, 2019.

[53] A. Bondar, H. Tolchieva, M. Bilyk, O. Slavkova, and V. Symonov, "The role of digitization in management and strategic decision-making in modern management", *Financial and Credit Activity Problems of Theory and Practice*, vol. 2, no. 55, pp. 214-227, 2024.