Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment

Technovation 143 (2025) 103219

Contents lists available at ScienceDirect

Technovation

journal homepage: www.elsevier.com/locate/technovation

Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment

Kuldeep Singh [a], Sheshadri Chatterjee [b], Marcello Mariani [c,d,*], Samuel Fosso Wamba [e]

[a] School of Management, Gati Shakti Vishwavidyalaya, Vadodara, 390004, India
[b] Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, Kharagpur, India
[c] Henley Business School, University of Reading, United Kingdom
[d] University of Bologna, Italy
[e] TBS Business School, 1 Place Alphonse Jourdain, TOULOUSE, 31068, France

ARTICLE INFO

Keywords:
Cybersecurity resilience
Innovation capability
Governance efficacy
Sustainable business excellence

ABSTRACT

Data and information systems are valuable, rare, and often inimitable resources for any organization willing to innovate its products, processes, and business models, with the ultimate goal of gaining a competitive edge in a digital world. Data and information systems are also valuable and rare resources when organizations interact with each other within their ecosystems as data flows are deployed conjointly by organizations to achieve innovation and performance outcomes for their ecosystem. As such data and information systems within organizations, interorganizational relationships and ecosystems need to be protected. For this reason, organizations are required to strengthen their cybersecurity systems. This seems a necessary precondition to assist organizations and ecosystems to innovate their products, processes, and business models especially during times of dramatic changes (such as wars or pandemics) that can pose threats to organizational and ecosystem data protection. Accordingly, cybersecurity resilience allows to address those threats triggered by dramatic changes. In this light, this study aims to investigate how components of cybersecurity resilience can influence organizations' innovation capabilities and ultimately sustainable business excellence as well as the moderating influences of macroeconomic policies and regulations. By building on a cross-sectional research design we found that cybersecurity resilience positively influences innovation capabilities that in their turn positively influence sustainable business excellence. We also find that macroeconomic policies and regulations moderate the relationship between government efficacy and sustainable business excellence.

1. Introduction

Cybersecurity resilience has become vital for many existing essential services, such as emergency services, banking systems, water management systems, electric power grids, and navigation systems for air and sea travel (Dalal et al., 2022; A. Mishra et al., 2022). Information systems (IS) literature more broadly has pointed out that cybersecurity resilience might be conducive to enhanced performance in the guise of business excellence (Slapničar et al., 2022; Taherdoost, 2022). It is not a case that an increasing number of reports have stressed that it is critical for organizations to develop solid cybersecurity systems in the guise of infrastructure and data protection mechanisms since they allow organizations to survive in the existing turbulent economic environment, also in light of digital transformation that is making cybersecurity increasingly important for organizational operations and performance (Dupont, 2019; Mhlanga, 2020; D'Ambra et al., 2022; Mariani and Borghi, 2019; Ranjan et al., 2022). Extant studies have also highlighted that cybersecurity resilience is as relevant as cybersecurity as it allows organizations to survive over time and maintain and cultivate a sustainable advantage. More specifically, cybersecurity resilience is not a monolithic construct, but it consists of different components such as compliance, risk management, and the efficacy of incident response

This article is part of a special issue entitled: Ecosystems for a sustainable world published in Technovation.

* Corresponding author. Henley Business School, University of Reading, United Kingdom.
E-mail addresses: kuldeep@gsv.ac.in (K. Singh), sheshadri.academic@gmail.com (S. Chatterjee), m.mariani@henley.ac.uk (M. Mariani), s.fosso-wamba@tbs-education.fr (S.F. Wamba).

https://doi.org/10.1016/j.technovation.2025.103219
Received 23 April 2024; Received in revised form 22 February 2025; Accepted 4 March 2025
Available online 9 March 2025

(Schmitz-Berndt, 2023). All these components are critical to enable organizations navigating a competitive digital, physical and phygital environment to cope with uncertainty and to safeguard and protect data which are valuable, rare, inimitable, and non-substitutable resources for individual organizations and for organizational ecosystems (Cram and D'Arcy, 2023; Melaku, 2023).

Consequently, strengthening cybersecurity systems seems a necessary precondition to assist organizations and ecosystems to enhance their individual and collective innovation capabilities to innovate (singularly or collectively) their products, processes, and business models.

During times of dramatic changes such as pandemics, global warming, and severe warfare that can pose threats to organizational and ecosystem data protection, cybersecurity and cybersecurity resilience become of paramount importance to minimize the risks related to the aforesaid dramatic changes. For instance, in recent and ongoing wars in Eastern Europe and Russia as well as the Middle East, cyber-attacks have been deployed as a tactical war weapon to disrupt businesses and their operations (Biller and Schmitt, 2019). By protecting essential and confidential business data, cybersecurity initiatives – taken at both the organizational and the inter-organizational and ecosystem levels – are aimed at avoiding the disruption of organizational activities and operations.

Extant studies have examined how global warming, warfare, pandemics, and rapid technological advances like 'deep-tech' innovation have reshaped business operations (Granstrand and Holgersson, 2020; Jarjoui and Murimi, 2021; Xu and Mahenthiran, 2021; Audretsch et al., 2022). While 'deep-tech' innovation can curb unhealthy competition, it may also widen the economic divide among nations and communities, making the world less sustainable (Granstrand and Holgersson, 2020; Vittori et al., 2022; Cosenz et al., 2023).

That said, all these studies did not explicitly discuss and analyse if and how cybersecurity resilience (and its components) influence organizational innovation capabilities (Hodapp and Hanelt, 2022; Ranjan et al., 2023; Safitra et al., 2023) and ultimately impact on sustainable business excellence (Felício et al., 2022; Wiertz et al., 2004). This is very surprising as in an increasingly digital world, organizations increasingly rely on data (Jossen, 2017; Economist, 2017), information systems and digital and interconnected technologies to gain a competitive advantage, and in so doing they also face higher exposure to various cyber threats that can severely impair their operations and performance (Al-Sartawi and Razzaque, 2020; Chaudhuri et al., 2022b; Gutiérrez Ponce et al., 2023; Giovando et al., 2023 Melaku, 2023). To summarize, we do not know if cybersecurity and more specifically cybersecurity resilience constitutes a suitable means of protecting an innovation ecosystem's data, data flows, and information systems and if this can enhance innovation capabilities and ultimately firm performance.

To bridge this research gap, this work leverages on the Resource-Based View (RBV) (Barney, 1991) and the Institutional Theory (DiMaggio and Powell, 1983) as well as cybersecurity studies (Al-Sartawi and Razzaque, 2020; Smaili et al., 2023) to address this focal research question:

RQ: How can the components of organizational cybersecurity resilience influence the innovation capabilities and the performance (i.e. sustainable business excellence) of organizations that belong to an innovation ecosystem and what is the role of macroeconomic policies and regulations in this context?

The above RQ has been addressed by analysing the responses of 359 respondents of companies belonging to an innovation ecosystem in India. A theoretical model has been developed by building on both the resource-based view (RBV) (Barney, 1991) and the institutional theory (DiMaggio and Powell, 1983). This model has been validated deploying the PLS-SEM technique. Interestingly, the combination of the resource-based view (RBV) (Barney, 1991) and institutional theory (DiMaggio and Powell, 1983) is relevant as none of the two theories, alone, can explain how the multiple components of cybersecurity resilience influence innovation capabilities, government efficacy, and sustainable business excellence of the organizations under the moderating influence of macroeconomic policy and regulations.

We found that cybersecurity resilience, through its components - cybersecurity compliance, cybersecurity risk management, and incident response effectiveness – positively influences innovation capabilities that eventually influence performance in the guise of organizational sustainable business excellence, as defined in extant literature (Felício et al., 2022; Wiertz et al., 2004), under the moderating influence of macroeconomic policies and regulations.

The topic that we cover in this study is important for the following reasons. First, through the study, we identify three salient and specific components of cybersecurity resilience which influence innovation capabilities within innovation ecosystems. Second, we highlight that some intermediate factors like innovation capabilities and government efficacy can facilitate the relationship between cyber security resilience and performance in the guise of organizational sustainable business excellence. Third, the study is among the first (if not the first) to analyse the impact of macroeconomic policies and regulations as a moderating variable that can facilitate the understanding of the relationship between cybersecurity resilience, innovation capabilities, government efficacy and organizational sustainability.

2. Background studies

2.1. Review of literature

The field of cybersecurity has traditionally prioritized protection against malicious attacks. Cybersecurity helps to protect data of organizations which are valuable, rare, inimitable, and non-substitutable (VRIN) resources (Lees et al., 2018; Lee, 2021). However, over the last decade, the concept of cyber resilience has come to the forefront as a vital component of effectively managing digital risks. Initial cybersecurity standards focused on safeguarding the internal boundaries of a system via firewalls, etc. By contrast, cyber resilience stresses enabling organizations to adequately prepare for, endure, and recover from inevitable security violations (Saeed et al., 2023a). This shift acknowledges the impracticality of perfect prevention and underscores the need for businesses to minimize fallout when incidents transpire. The pioneering study by Saeed et al. (2023) first delineated resilience from standard security, emphasizing that cyber systems must have adaptive capacities to withstand, respond to, and rebound from disruptions. The National Institute of Standards and Technology (NIST) in the U.S. subsequently characterized cyber resilience as the ability to forecast, tolerate, recuperate from, and adapt to adverse cyber events (Alexander and Panguluri, 2017; Chaudhuri et al., 2022a). Since information security comprises both digital and physical security, academia has strived to refine resilience assessment methods, models, and tools. It is pertinent to mention here that robust cybersecurity helps the organizations to use their data in an effective manner helpful to innovate their products, processes, and business designs (Saeed et al., 2023a).

Research has uncovered various dimensions and indicators for an organization's capacity to overcome cyber risks. Lees et al. (2018) devised a benchmark assessment to evaluate security approaches that we consider to safeguard most type of cyber domain. Rajapathirana and Hui (2018) stated one resilience approach as a key part of innovation ability to recover and regenerate what was lost. Furthermore, Jarjoui and Murimi (2021) showed resilience measures which can enhance risk identification and response efficacy. Ekelund and Iskoujina (2019) demonstrated cyber resilience in terms of operational and financial performance benefits if aligned with organizational outcomes. These findings confirm that in addition to conventional security, resilience is vital for corporate survival amidst changing technology and expectations (Sheshadri et al., 2022; Demetris et al., 2022). In case of any untoward apocalyptic situation, when dramatic changes take place in organizations, cybersecurity measures become very relevant since it

requires cybersecurity resilience to adequately address such dramatic changes (Alexander and Panguluri, 2017). However, expansion in technological integration in business operations can expose firms to significant cyber risks that can affect their performance, because technological breaches can instantly disrupt operations, erode stakeholder trust, and impose substantial recovery expenses (Xu and Mahenthiran, 2021; Viardot et al., 2023). Therefore, it is always a good idea to invest in cybersecurity resilience and it is increasingly imperative for maintaining organizational excellence despite unavoidable threats. In this research we explored cybersecurity resilience through three central pillars: cybersecurity compliance, effective risk management, and incident response effectiveness. Cyber security and cyber compliance are equally important and protect the institutes' internal rules, processes and behaviors adhering to external cybersecurity standards and best practices (Taherdoost, 2022). It provides a critical resilience baseline as it incorporates fundamental capabilities like access control, data security, and vulnerability management with well-known standards such as ISO 27001, NIST, and PCI DSS. Choo et al. (2021), stated that cyber risk management entails the continuous process of identifying, evaluating, and mitigating information security risks. This encompasses methodical approaches to detect major exposures and implement varied administrative, technical and physical controls to avert, identify and address threats. Be it mentioned here that cybersecurity measures play a critical role in organizations since it can protect data allowing the organizations to do businesses successfully with their partners who are often part of their business ecosystems (Viardot et al., 2023). Besides, organizational data protection is essential since it helps to improve innovative ecosystems to develop products, processes, and business model innovations (Melaku, 2023).

Ongoing assessment and mitigation of cyber threats compound resilience advantages. An effective incident response is defined as the ability to swiftly detect breaches, coordinate actions, minimize damage, eliminate vulnerabilities and restore normal operations (Jarjoui and Murimi, 2021; Meszaros and Buchalcevova, 2017; Audretsch et al., 2022 et al., 2022). The capacity to recognize, react to, and remediate events expeditiously demonstrates cyber resilience. As per Lattanzio & Ma (2023), innovation means the ability to deliver substantial new processes, products, services, business models or marketing methods conferring competitive edge. Under the resource-based view, rare and inimitable assets like cybersecurity capabilities promote innovation by safeguarding intellectual property and sensitive information; enabling data exchange and transparency vital for innovation; and releasing funds otherwise spent on breach costs for more R&D investment (Kosutic and Pigni, 2022). Advanced cyber governance mechanisms like zero-trust architecture and multifactor authentication also impart economic upsides. Elevated innovation capacities boost governance effectiveness, defined as an organization's aptitude for direction-setting, evaluation, risk management, accountability, transparency, ethics and fairness fundamental to robust operations and leadership (Dupont, 2019; Lattanzio and Ma, 2023; Melaku, 2023; Garcia-Perez et al., 2023). Furthermore, creative problem solving and programming concepts can support emerging risk identification, while innovative solutions increase operational openness. Basically, innovation leads to more resilient and vigilant governance systems through shared relationships. Finally, innovative abilities with efficient governance help to achieve sustainable business value. Innovation facilitates the adoption of newer cybersecurity capabilities, products and services to satisfy changing business needs. Also, robust governance ensures ethical conduct, transparency, accountability and seamless translation of ideas into tangible outcomes. These cumulative benefits manifest in balanced scorecards and triple bottom lines which serve as benchmarks for sustainable excellence.

2.2. The resource-based view theory

The Resource-Based View (RBV) theory considered one of the most influential views in management history (Lockett et al., 2009), traces its roots to the seminal works of different scholars (Connor, 2002; Obitade, 2019; Salimath and Philip, 2020). The central tenet posits that sustained competitive advantage arises from a firm's ability to acquire and control valuable, rare, inimitable, and non-substitutable resources and capabilities (Grant, 1991; Park et al., 2017; Chatterjee et al., 2021). Park et al. (2017) defines a firm's resources as encompassing all assets, capabilities, organizational processes, firm attributes, information, and knowledge controlled by the firm, enabling the development and implementation of strategies to enhance efficiency and effectiveness. It is pertinent to mention here that while earlier views considered strategic investments which deter market entry as well as raise prices as critical factors to ensure firms' competitiveness, RBV possesses an intra-firm focus since it can successfully explain how firms can achieve a competitive advantage by aptly deploying firm-specific inhouse resources (Teece et al., 1997; Wójcik, 2015).

This study adopts the Resource-Based Theory (RBT) as its guiding framework, introduced by Jay Barney in 1991, which posits that a company's internal resources and capabilities form the basis for attaining a competitive advantage (Borchert, 2008; Elia et al., 2021). Cavusoglu et al. (2015) argued for the applicability of the RBV in framing information security investments, citing the dual nature of IT resources as both non-security (e.g., IT systems, data, processes) and security resources (e.g., firewalls, security knowledge). The RBV has been utilized in the information systems literature, as seen in the works of Cavusoglu et al. (2015) and Borchert (2008), addressed issues like organizational size, security breaches, and its link to security investments. The VRIN qualities—valuable, rare, unique, and non-substitutable—emphasize the potential of resources and forces to generate significant value and outperform rivals over time. This underscores the importance of examining cybersecurity technologies to enhance resilience. The integration of governance, finance, infrastructure, technology, training, and staff promotes competencies such as cyber-compliance, risk management, and incident response, crucial for addressing digital risks and vulnerabilities in organizational ecosystems.

The RBV framework has a longstanding presence in the field of IT systems, with scholars like Hoskisson et al. (2018) and Weishäupl et al. (2018) who viewed IT and cybersecurity capabilities as organizational capacities influencing competitive advantage. Configurations of cybersecurity capabilities vary across companies, impacting organizational performance. Resource Based Theory (RBT) enhances governance effectiveness, acting as a crucial intermediary capacity through cyber-enabled innovation capabilities. Investments in cyber technology stimulate innovation, contributing to improved governance. RBT acknowledges the need to evaluate institutional norms and laws as external factors impacting sustainable business excellence outcomes (Connor, 2002). underscores the mutual benefits of coordinated governance and innovation, with their effective combination driving excellence while inadequate coordination hampers growth. This perspective views companies as open systems influenced by internal capabilities and external circumstances. In this context, cybersecurity in organizations emerges as a protective measure for IT systems, involving a set of measures, strategies, organizational processes, and procedures to mitigate risks and vulnerabilities. The configuration of these cybersecurity capabilities encompasses both operational and strategic organizational aspects (Borchert, 2008; Grant, 1991; Salimath and Philip, 2020; Weishäupl et al., 2018).

2.3. Institutional theory

Institutional Theory, a sociological perspective exploring how formal and informal norms and structures influence behaviors within organizations and institutions, complements the Resource-Based Theory in understanding the intricate dynamics of cybersecurity, governance, and organizational sustainability. While the Resource-Based Theory emphasizes internal capabilities as the driver of competitive advantage,

Institutional Theory posits that external environments shape internal structures, behaviors, and outcomes. Rooted in social science disciplines like ethnography, political science, anthropology, phenomenology, and organization studies, Institutional theory, as articulated by DiMaggio and Powell (1983), asserts that organizations tend to converge towards similar practices and behaviors over time. van Rijmenam and Logue (2021) elaborate on how organizations are significantly influenced by institutional environments, dictating legitimate and successful organizational appearances and behaviors while constraining decision makers' ability to conceive and implement certain types of organizational change. Institutional pressures from social, cultural, and regulatory institutions drive businesses to conform to standards, gaining legitimacy and vital resources for sustained growth. This alignment with established conventions, expectations, and regulations enriches the study by illustrating how broad cybersecurity policies, benchmarks, and legislation impact organizational strategies and decision-making. Formal institutions, including comprehensive cyber laws and breach notification mandates, and informal norms emphasizing transparency and accountability in managing cyber risks, exert coercive, mimetic, and normative drivers for companies to adopt cyber compliance. Institutional Theory posits that the quest for legitimacy is a primary driver of organizational behavior, surpassing efficiency considerations. This idea aligns with the argument that institutional pressures lead top managers to make strategic decisions similar to those of other reference organizations in their industry. Ording et al. (2022) highlighted how institutional pressures related to Information System (IS) security influence senior management's beliefs and participation in IS security initiatives. Moreover, Institutional Theory expands the Resource-Based framework by emphasizing how external cybersecurity structures influence internal governance orientations, covering responsibility, ethics, risk management, and leadership. This argument posits that organizational responses to institutional expectations are closely tied to and interwoven with culture. Organizations, in order to gain cognitive legitimacy, conform to taken-for-granted expectations set by institutional constituencies. In essence, organizations react to pressures from these constituencies, aligning with regulations, norms, values, beliefs, and expectations to secure legitimacy (DiMaggio and Powell, 1983; Hsu et al., 2012; Ording et al., 2022; Wang et al., 2021). Governance, encompassing policies, roles, and procedures, is under external oversight, with Institutional Theory reinforcing the notion that macro-level cyber regulations and expectations influence internal adoption of cyber compliance. This shift transforms boards, executives, and units into vigilant and resilient stewards, shaping robust governance linked to sustainable excellence. Within the realm of Institutional Theory, a key focus revolves around legitimacy applied within an organizational context, signifying the perception or assumption that entity actions align with socially constructed norms, values, beliefs, and definitions. Previous research has delved into both macro and micro applications of legitimacy, exploring how companies gain and maintain legitimacy as a whole and examining individual employee perspectives. Recognizing the limitations of even the most capable state to independently anticipate and fend off all cyber-attacks, cooperation becomes a critical aspect. Cybersecurity governance as such is seen as voluntary collaborative actions that ensure the accessibility, authenticity, reliability, and secrecy of digital information transmitted across cyberspace. In addition, Institutional Theory is crucial as we assess public cyber policies and norms as moderating variables that impact sustainable business excellence. The evaluation assesses the alignment or resistance of external pressures with the internal governance efficiencies required to adopt innovation and achieve balanced performance. Institutions that enable additional initiatives and governance mechanisms prioritize exceptional quality which can attain institutional synergy (Galati et al., 2021; Chatterjee et al., 2022; Mariani, 2018; Mariani et al., 2023). In contrast, institutions that are not compatible with this create internal conflicts. This adverse situation can impede the ability to maintain effective leadership and further progress. The assessment of institutional cyber norms is considered crucial since it acts as a factor that influences the paths taken by organizations.

3. Development of hypotheses and conceptual model

3.1. Cybersecurity resilience and innovation capabilities

The acknowledgment of innovation through cyber resilience as a sustainable and competitive enabler is widespread among both industry professionals and academics. However, the understanding of innovation management and practice remains fragmented, misunderstood, and untamed by practitioners and researchers. The innovation capability of an organization is directly influenced by its cybersecurity posture, particularly as digitalization becomes more pervasive across operations, products, and business models (Li and Liu, 2021). Cyber resilience creates an environment conducive to creativity and change, ensuring robust protection against various threats. This safeguarding of innovative efforts and financial investments from potential disruptions emphasizes that innovation cannot occur within a vacuum. It is impacted by a range of external contextual factors, in addition to internal considerations such as strategy and culture, resources and skills, leadership, organizational structure, and external linkages (Chatterjee et al., 2023). Advancing cybersecurity compliance, risk management, and incident response efficacy becomes vital for establishing a solid foundation and headroom for persistent innovation. This can be achieved through three central mechanisms. Firstly, stringent adherence to cybersecurity policies, controls, and best practices necessitates gathering security intelligence, enforcing access rules, securing data and system backups, implementing testing protocols, and internalizing continuity habits. Collectively, these actions constitute a sturdy compliance-based foundation (Von Solms and Van Niekerk, 2013). This multi-layered security approach, coupled with ingrained vigilance, frees up organizational resources for future initiatives, eliminating encumbrances that could hinder idea generation, strategic risk-taking, and new undertakings crucial for innovation. Cybersecurity is positioned as a strategy of preventive action, allowing for technological growth, advancement, and innovation. Resilience in cybersecurity is reflected in various fields, particularly through cooperative or global cybersecurity strategies.

The need for a joined cooperative strategic and operational capacity is crucial. Deploying specialized assessments, audits, and strategies to tackle cyber risks promotes persistent awareness, knowledge acquisition, and continuous improvement within the company (Kriaa et al., 2019; Sheshadri, 2021). Proactively uncovering and mitigating vulnerabilities instills organizational instincts for detecting issues, comprehending root causes, and delivering solutions — all critical drivers for innovation. The real cost of cybercrime is often overlooked, stemming from delayed or lost technological innovation. This issue arises partly from how thoroughly companies screen technological investments for their potential impact on the cyber-risk profile. From a macro-economic standpoint, Information and Communication Technology (ICT) innovations have direct and indirect effects on firm performance, emphasizing the strategic role of CIOs in delivering new innovations empowered by technology. Strategizing and drilling for rapidly identifying, containing, eradicating, and recovering from unforeseen breaches bolsters confidence in effectively handling unanticipated disruptions. Extensively tested response systems provide assurance that incidents can be swiftly remediated with minimal fallout, enabling innovative efforts to progress without major concerns. This resilience permits greater flexibility in exploring technological frontiers and pioneering business models, knowing that crises can be aptly and efficiently resolved.

Therefore, this study hypothesizes.

H1. Cybersecurity compliance has a significant positive effect on an organization's innovation capability.

H2. Cybersecurity risk management has a significant positive effect on an organization's innovation capability.

H3. Cybersecurity incident response effectiveness has a significant positive effect on an organization's innovation capability.

3.2. Cybersecurity resilience and governance efficacy

An effective cybersecurity strategy reinforces the necessary governance competencies to steer strategic decision-making, oversee operations, monitor risks and uphold responsible standards integral to overall corporate wellbeing (Michalec et al., 2022a; Renaud et al., 2019). Stringent cyber compliance guidelines place pressures on oversight processes and leadership skills by instituting rules around access rights, change control, vendor selection, business continuity planning and internal audits encompassing people, processes and technology (Al-Sartawi and Razzaque, 2020; Ranjan et al., 2021; Naseer et al., 2021; Melaku, 2023). The expanding need for round-the-clock data and network security brings heightened cyber-related discussions in boardrooms, executive performance reports and policy updates to meet enlarged due diligence requirements (Michalec et al., 2022a). Herein, pursuing compliance with external information security regulations and benchmarks precipitates organizational governance transformation—prioritizing, allocating resources towards and monitoring cyber risk mitigation as fiduciary and ethical imperatives. Institutionalizing cyber risk management programs augments corporate governance infrastructure by identifying risks across units and recalibrating controls to avoid, divert or minimize incidents (Smaili et al., 2023; van Rijmenam and Logue, 2021). Conducting regular assessments, audits and control upgrades helps construct robust governance to systematically pinpoint and address emerging vulnerabilities, comprehend underlying reasons and implement remedies. Governance now aligns more closely with the iterative cadence of cyber risk treatment—anticipating new vulnerability sources and proactively resolving them before fallout intensifies. Thus, risk intelligence fulfills the demands for vigilance imposed on responsible and transparent leadership. Additionally, devising and drilling cyber breach response instills concrete incident management playbooks for directors and executives to demonstrate crisis leadership around critical systems disruptions (Michalec et al., 2022a; Park et al., 2017; Sheshadri, 2019). Evaluating the ability to swiftly detect and respond to events ensures adequate preparedness to steer through uncertainty. Investigating, remediating, recovering and adapting to breach consequences hones long-term capacities to alter policies, procedures, technology and staff to mitigate further harm. Therefore, resilience preparation signifies governance readiness to navigate unexpected contingencies, which is vital for stakeholder confidence.

Therefore, this study hypothesizes.

H4. Cybersecurity compliance has a significant positive effect on an organization's governance efficacy.

H5. Cybersecurity risk management has a significant positive effect on an organization's governance efficacy.

H6. Cybersecurity incident response effectiveness has a significant positive effect on an organization's governance efficacy.

3.3. Cybersecurity resilience and sustainable business excellence

Sustainable business excellence denotes overall long-term corporate health and performance based on balancing financial returns with societal consequences (Sahu et al., 2020). As cyber threats escalate, cyber resilience attained through compliance, risk management and response capacities can enable this. These three pillars contribute to comprehensive balanced outcomes. Implementing extensive data, application, host and network security fulfils legal, industry and internal cyber compliance dictates, safeguarding foundational IT infrastructure that operationalizes functions (Bredt, 2019; Sulich et al., 2021). Cyberattacks globally have a detrimental impact on enterprise performance. Despite increased investments in cybersecurity to prevent such attacks, there is a scarcity of studies on the factors affecting overall cybersecurity adoption and awareness within organizations. Basic cyber hygiene measures, including enforcing device encryption, access rules, system patches, and credentials hygiene, play a crucial role in maintaining system integrity and availability, thereby supporting favorable business outcomes. This cyber hygiene eliminates obstacles to continuity, preventing unexpected disruptions that may occur in the absence of robust compliance. Rigorous cyber risk monitoring, audits, and control updates through formal risk programs enhance companies' understanding of emerging dangers, allowing proactive measures to address potential threats (Sahu et al., 2020). Cybersecurity not only protects against attacks but also has the potential to improve an organization's reputation, core competency, and overall performance. Marketers recognize the importance of addressing cybersecurity risks to carry out marketing activities effectively (Mishra, 2023). Businesses relying on digital services consistently identify cybersecurity as a significant challenge for growth and productivity (Dube and Mohanty, 2021; Vrontis et al., 2022). Consistent addressing weaknesses through regular risk management enables organizations to adapt corporate strategies and offerings in response to evolving customer needs and market conditions, leveraging secure digital platforms. Ongoing, future-focused cyber risk management is crucial for preserving excellence and supporting business operations. To counter the escalating cyber threats, organizations must elevate their current strategic cybersecurity management and pivot towards achieving cybersecurity excellence in their day-to-day activities. Cybersecurity, as a global phenomenon, presents a multifaceted socio-technical challenge for governments, necessitating the active participation of individuals (Singh and Alshammari, 2020). Despite being one of the most critical issues faced by governments today, public awareness and visibility regarding cybersecurity remain low. While the term is widely recognized, the urgency and behaviour of individuals do not necessarily reflect a high level of awareness. Building cyber resilience emerges as a pivotal strategy to reduce disruptions and fallout from frequent cyber-attacks, particularly for unprepared companies lacking swift response plans. This approach facilitates persistent quality improvement grounded in balanced assessments. Ensuring the accessibility, efficacy, and utilization of IT infrastructure is crucial to support business operations within a company. Organizations need to carefully consider IT infrastructure, capacity, and investment when determining cybersecurity resilience, emphasizing a comprehensive and proactive approach to safeguard their digital assets. An effective cyber resilience practice goes beyond technology and infrastructure; it must incorporate people, processes, and technologies to manage risks effectively and achieve greater firm performance (Bredt, 2019; Kure et al., 2022; Sahu et al., 2020; Siachou et al., 2022). Mature cybersecurity management within organizations involves well-defined processes governing the confidentiality, integrity, and availability of information within the cybersecurity resilience framework (See Fig. 1). Such processes contribute to sustainable business excellence by ensuring that operations are robust and resilient against breaches and attacks.

Therefore, this study hypothesizes.

H7. Cybersecurity compliance has a significant positive effect on an organization's sustainable business excellence.

H8. Cybersecurity risk management has a significant positive effect on an organization's sustainable business excellence.

H9. Cybersecurity incident response effectiveness has a significant positive effect on an organization's sustainable business excellence.

3.4. Mediation of governance efficacy

Given the escalating awareness of cybersecurity breaches and associated policies, research on the impact of cybersecurity risks on corporate decisions is gaining prominence (Cavelty and Wenger, 2022;

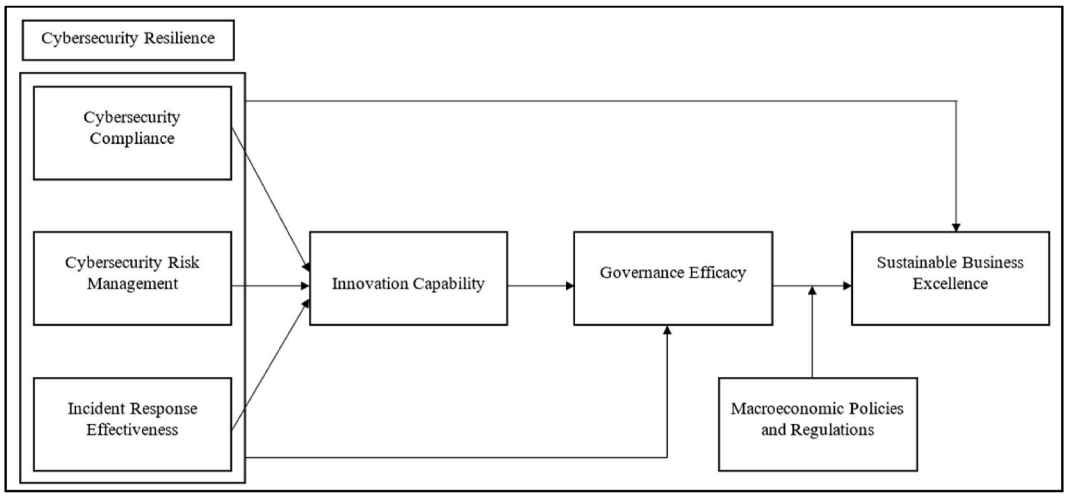

Fig. 1. The proposed conceptual framework.

Michalec et al., 2022b). However, existing studies often concentrate on the post-event repercussions of data breaches, wherein breached firms are compelled to increase precautionary savings, consequently reducing cash available for innovation endeavors. The governance of digital technologies revolves around infrastructural control points, intricately weaving together technical and economic efficiency with considerations of human and societal values (Dehghani et al., 2023). If cybersecurity risks influence innovation through the risk-taking channel, the effect on innovation should be more pronounced for firms less tolerant to risk. The complexity of governing software systems is significantly influenced by the growing number and sophistication of cyber threats to both open and closed system architectures. Despite concerns, there is scant evidence supporting a government takeover of internet governance in the name of security, making the discourse on the 'global war' or 'battle' over cybersecurity governance somewhat perplexing. Weak awareness of potential risks often results in vulnerabilities in software projects, which could threaten the product's integrity across its entire lifecycle. Nevertheless, cyber capabilities play a significant role as they encourage innovation and governance systems that lead to successful outcomes over time (Selimoglu and Saldi, 2023; Sun et al., 2021). This is important since innovation is a crucial element to improve the competitiveness and long-term development of organizations. Attaining a high level of cyber compliance maturity, consistently addressing risks, and implementing response plans foster an environment that is favorable for innovative problem-solving and effective change management. Resilience fosters a sense of psychological security among workers, enabling them to confidently present innovative ideas, and encourages their interest and research in state-of-the-art technologies that are essential for developing innovative and revolutionary products. The European Union's proposal for a formal regulation to establish a European cybersecurity industrial, technical, and research competence center highlights the significance of resilience in fostering innovation in response to changing consumer demands. Effective regulatory supervision is necessary to transform prospects into concrete market results while minimizing risks (Melaku, 2023; Selimoglu and Saldi, 2023). Effective implementation of innovative ideas at scale, while ensuring compliance, is facilitated by robust governance that includes leadership, accountability, ethical principles, and openness. Better governance via cyber rules and rigorous response testing provides a foundation for careful acceptance of the business opportunities brought by modernization. The combination of resilience, creativity, and governance expertise enables unhindered innovation on digital platforms. In today's context, it is crucial to achieve consistent excellence by implementing responsible innovation, which is facilitated by resilient governance. Cyber resilience not only strengthens long-term achievement but also improves the ability to innovate and manage effectively. It offers essential support for both financial and social advancement that is crucial for long-term achievement. The fast growth of cyberspace, particularly the Internet, has driven commercial and social exchanges beyond national boundaries via technology. The acknowledgment of the interaction between different entities and components in the cyber ecosystems, together with the complex nature of cyber resilience, has led to the concept of co-production of cyber resilience. Accordingly, the following hypothesis is developed.

H10. An organization's governance efficacy positively mediates the effect of innovation capability uplifted by cybersecurity compliance, risk management and incident response effectiveness on its sustainable business excellence.

3.5. *Moderating effect of macroeconomic policies and regulations*

In today's world, cyber threats have become a major national security concern, prompting countries to implement security rules for critical infrastructure operators as part of their efforts to be resilient to cyber threats (Broeders, 2021; Lilli, 2021). There are different models for protecting critical infrastructure, ranging from relying on the market to government ownership. While it might seem obvious to have strong government oversight for cyber resilience in critical infrastructures, the effectiveness of governance and achieving sustainable business excellence are closely connected. To achieve comprehensive corporate sustainability, it depends on macroeconomic policies and regulations that either help or hinder the translation of strong governance into overall excellence. In a supportive policy environment, stakeholders can enhance cyber risk management through collaboration between public and private entities. This implementation ensures secure infrastructure, rules for handling breaches, and adherence to technical cybersecurity standards (Kure et al., 2022; Malatji et al., 2022). The ongoing discourse about digital surveillance primarily revolves around the authorities' ability to access encrypted data. Mainly, it focuses on potential regulatory intervention in stakeholders' affairs and the protection of civil rights within the context of security measures. Regular audits of IT assets with frameworks such as NIST's cybersecurity provides risk management support. These frameworks assist in resource allocation based on the prevalent risk situation. In response to the mounted threats, regulatory authorities have strengthened the current regulatory framework (Alexander and Panguluri, 2017; Malatji et al., 2022). It results in a framework that is more robust, albeit complex. The emphasis on disclosing breaches and enforcing cybersecurity standards underscores the industry's need for resilience. According to recent literature, specific policy approaches become imperative to enhance governance efficiency.

These policies foster sustainable excellence through secure digital capabilities. A notable aspect is the consideration given to smaller or less complex firms and organizations, with regulatory adjustments aimed at reducing the operational burdens for these entities. Policymakers normally contend with the challenge of balancing financial stability while maintaining a competitive domestic environment. In this way, the policy landscape provides crucial resources, such as data repositories, threat indicators, and response toolkits, which can enable the government to leverage collective knowledge for enhanced defense and strategic formulation in cyber resilience. Basically, governance relies on external policy platforms to comprehend the significance of potential risks and approaches to mitigate them. Also, the cybersecurity landscape shares similarities with antitrust issues, as it involves preventive detrimental behavior (Broeders, 2021; Liu et al., 2022). In order to implement the regulations that facilitate official data sharing between the government and businesses it is necessary to support organizational learning. It allows the government to find a balance between digital hazards and benefits. Diverse perspectives exist regarding the necessity of precise regulations for cyber risk. Some researchers argue that current laws which cover technological and operational risks are sufficient. On the other side a few researchers advocate for a specialized regulatory framework (Michalec et al., 2022a; Rajapathirana and Hui, 2018; Saeed et al., 2023b). However, cybersecurity from a regulatory standpoint not only provides a richer analytical framework but also expands the range of possible responses. Furthermore, adopting solutions from other regulatory contexts offers a broader menu of policy choices. While effective policies promote governance competencies, sometimes the implementation may lead to internal conflicts. Hence, harmony in policy settings is essential to avoid disputes that could undermine governance effectiveness and overall performance. Ekelund and Iskoujina (2019) stated that the optimal level of cyber intrusions is not zero and cybersecurity expenditures should not be infinite. Therefore, an economic perspective emphasizes achieving an efficiently manageable level of cyber-attacks rather than the impossible goal of preventing all attacks.

Hence, the study hypothesizes.

H11. Macroeconomic cyber policies and regulations positively moderate the relationship between governance efficacy and sustainable business excellence, that is existence of impactful policies significantly strengthens the association between governance efficacy and sustainable excellence.

The above discussions lead to developing a theoretical framework conceptually which is provided in Fig. 1.

The above figure elucidates that cybersecurity resilience, entailing its three components - cyber security compliance, risk management, and incident response effectiveness – is likely to influence innovation capabilities which eventually influence sustainable business excellence of the firms mediated through governance efficacy. Besides, cyber security resilience influences both sustainable business excellence and governance efficacy. The figure also shows that macro-economic policies and regulations could moderate the relationship between governance efficacy and sustainable business excellence.

4. Research methodology

4.1. Sample and data collection

The empirical study utilized a survey of IT firms to analyse cybersecurity resilience in the context of research and development. Investigating cybersecurity resilience in the IT Sector is significant for several reasons. Firstly, specialized IT firms in cybersecurity possess the expertise to deal with cybersecurity challenges, rendering them well-placed to offer insights into practical aspects of cybersecurity resilience. Secondly, these firms play a direct role in providing services that contribute to the cybersecurity and overall operational resilience of organizations, making their perspectives invaluable for understanding the connection between cybersecurity resilience and sustainable business excellence (Felício et al., 2022; Haseeb et al., 2019; Wiertz et al., 2004). Lastly, IT firms involved in cybersecurity are likely well-versed in the regulatory environment, facilitating a nuanced exploration of the moderating effect of macroeconomic policies and regulations. The sample was drawn from the total population of listed IT companies. According to information sourced from the Money control for BSE (Bombay Stock Exchange) database, India's IT sector comprises a total of 197 companies (data accessed on Nov 07, 2023), with a majority being SMEs having an annual average market cap of 199 billion INR. A subset of 129 companies with a market cap exceeding 10 million INR was selected. Be it mentioned here that India has been preferred to collect data for this study for many reasons. Some of the authors of this study are based out of India. They have some closed link with the practitioners of Indian IT firms. Besides, India is considered as one of the fastest growing emerging economies and a part of BRICS countries. An online questionnaire, self-administered, was sent to these companies, reaching out to 496 respondents. The sample size surpassed the minimum threshold required for the employed technique (Partial Least Squares modeling, PLS) in this research, ensuring acceptable levels of statistical power (Reinartz et al., 2009). The data collection commenced with the initial questionnaire, gathering information on cybersecurity resilience, innovation ability, sustainable business excellence, and control variables. The first mailing resulted in 372 complete questionnaires. After a four-week interval, the same 129 firms were approached with a second questionnaire to collect information about governance efficacy, and macroeconomic policies and regulations. Following the exclusion of incomplete responses, 359 appropriately completed questionnaires, yielding an overall response rate of 72.37%–34% were answered by the company's senior managers, 48% by IT managers, and the remaining by other company managers. Here, non-response bias test has been performed following the procedure recommended by Armstrong and Overton (1977). For this, independent *t*-test has been performed analysing the responses of first and last 100 respondents. No marked deviation of results was noted in these two cases. It confirms that non-response bias could not pose a major threat in this study. It is worth mentioning that 142 responses were not considered for two reasons: some of the respondents (47) were found to have kept the response sheet completely vacant and the remaining respondents (95) put tick mark in more than one option against each question.

4.2. Measures

Maintaining cybersecurity compliance is crucial for protecting sensitive data and building stakeholder confidence. Shaheen and Zolait (2023) standardized scale assess adherence to security protocols, measuring commitment through the implementation of cybersecurity standards. This includes allocating resources, executing incident management policies, and establishing clear governance. The framework ensures consistent log monitoring, reflecting a dedication to effective cybersecurity practices.

Effective cybersecurity risk management involves continuous processes to identify, assess, and address system vulnerabilities. Marsch (2018), in their Global Cyber Risk Perception Survey, proposes a quantitative evaluation, emphasizing organizational capabilities in threat detection and response. Their questionnaire assesses the prioritization of cybersecurity in the overall risk management strategy, gauges confidence in managing cyber-attacks, and examines roles and responsibilities between the IT department and the board. Furthermore, it explores the existence of a well-developed plan for promptly addressing cybersecurity incidents. The corresponding descriptive statistics are provided in Table 1.

Efficient incident response, vital for prompt detection and recovery from security breaches, relies on key metrics such as reaction timeliness, detection accuracy, and restoration completeness. Catota et al. (2018) provides a set of 5 scale items for rigorous evaluation. The questionnaire

Table 1
Descriptive statistics.

	Mean	STDEV	CYBSEC	CRM	MPR	GE	INC	IRE	SBE	OrgAge
CYBSEC	3.61	0.82								
CRM	3.80	0.72	0.09							
MPR	3.67	0.80	0.133*	0.09						
GE	3.82	0.74	0.206**	0.04	0.393**					
INC	3.80	0.68	0.202**	0.114*	0.325**	0.282**				
IRE	3.86	0.68	0.166**	0.03	0.247**	0.263**	0.334**			
SBE	3.65	0.82	0.274**	0.151**	0.394**	0.307**	0.200**	0.229**		
OrgAge	1.77	0.70	−0.04	−0.07	−0.01	−0.02	−0.05	0.02	0.02	
OrgSize	2.34	0.77	−0.04	0.00	0.06	0.05	0.04	0.06	0.06	−0.151**

Note: Significance of Correlations: (*p < 0.050), (**p < 0.010) (Authors' calculation).

assesses the use of alerts for timely threat detection, the efficiency of incident handling processes, and the organization's ability to swiftly respond to cybersecurity incidents. It also explores information sharing for enhanced cybersecurity awareness, the regularity of vulnerability analysis, and the use of effective malware analysis techniques.

Staying ahead of cybersecurity threats involves building innovation capability and enhancing practices. Metrics for gauging capability include proficiency in producing, assimilating, and executing new methods. Calantone et al. (2002) offers five items for measurement. The questionnaire assesses the frequency of experimenting with new ideas, the perceived creativity in methods, and the ability to pioneer new products and services.

Effective governance is essential to ensure that cybersecurity is in line with business objectives. The governance construct was evaluated using a set of five scale items from Kim et al. (2013). The questionnaire analyzes the organizations and their IT service providers' distribution of resources, shared knowledge of objectives, and comprehensive assessment of governance efficiency. Also, all the constructs evaluated the extent to which IT service providers prioritize cybersecurity in their decision-making and their readiness to provide governance support.

Sustainable business excellence is the integration of economic, social, and environmental factors into security measures to ensure the continued progress of a firm. The questionnaire evaluated the active incorporation of responsibility, with a focus on achieving sustainable business excellence (Felício et al., 2022; Haseeb et al., 2019; Wiertz et al., 2004). It consists of five questions from Haseeb et al. (2019). This examines the level at which sustainable practices are essential to the company plan and evaluates their compatibility with long-term sustainability, with the ability to achieve excellence in their environmental and social impact.

It is essential, yet difficult to adjust cybersecurity measures to continuously evolve regulatory settings. The evaluation centers on the organizational capacity to adapt and comply with standardized metrics as outlined by Khan et al. (2021). The questionnaire evaluates the effective execution of the National Policy on Information Technology, and the implications for any breaches of the policy to guarantee adherence. Furthermore, it explores the implementation of technical awareness training and the promotion of a culture that values IT literacy.

4.3. Statistical method

Common method variance refers to the variance of variables resulting from biases in using a single survey instrument to collect data from respondents on independent and dependent variables (Tehseen et al., 2017). These biases arise from respondents potentially answering questions in a positive way to favor attractive correlations, rather than being realistic (Jakobsen and Jensen, 2015). To address this, tests are essential to observe and eliminate such biases, known as common method variance. Tehseen et al. (2017) emphasize the need for a statistical approach, particularly in PLS-SEM. Kock (2023) argues that common method bias exists when the variance inflation factor (VIF) exceeds 3.0. However, in this study, the maximum inner VIFs in model 1 and model 2 are 1.007 and 1.037, respectively, indicating the absence of common method bias (CMB) and multicollinearity. To confirm that this study is not impacted by CMB, Harman's single factor test (SFT) has been conducted. The results show the first factor came out to be 26.21% of the variance which is less than the recommended highest valued of 50% (Podsakoff et al., 2003). Since, researchers criticized that Harman's SFT is not a conclusive proof for testing CMB as opined by Ketokivi and Schroeder (2004), marker corelation ratio test has duly been performed (Lindell and Whitney, 2001). Both these statistical tests did not provide any evidence of having CMB. Hence, it should be construed that CMB could not affect the data. In this context, the Cronbach's alpha, Composite Reliability (CR), and Average Variance Extracted (AVEs) of the constructs have been computed and is shown in Table 2. The estimated values of Cronbach's alpha (α), composite reliability (CR), and average variance extracted (AVE) were found to be within the specific range (Chin, 2010; Hair et al., 2017).

The researchers employed structural equation modeling (SEM), specifically PLS-SEM with Smart-PLS software (Matthews et al., 2016), to test predicted hypotheses. PLS-SEM is suitable for complex models, allowing constructs measured with both single and multiple items, as in the current study. Additionally, PLS-SEM is widely used in IT field studies (Alharbi and Sohaib, 2021; Dash and Paul, 2021; Henseler et al., 2016). Besides, the PLS-SEM approach does not require any sample restriction (Willaby et al., 2015). The PLS-SEM approach also does not require the data to be normally distributed which is considered to be the essential condition for CB-SEM approach (Rigdon et al., 2017). The study followed a two-step procedure, assessing the measurement model and then the structural model, based on a statistically significant sample size and advanced statistical techniques to ensure result validity and reliability (Hair et al., 2010).

4.4. Results

The study investigates the relationships among cybersecurity (CYBSEC), Cybersecurity Risk Management (CRM), Incident Response Effectiveness (IRE), Innovation Capability (INC), Governance Efficacy (GE), Sustainable Business Excellence (SBE), and the moderating effect of Macroeconomic Policies and Regulations (MPR) on the relationship between GE and SBE. The descriptive statistics show a favorable

Table 2
Scale validity.

Variables	Cronbach's alpha	Composite reliability	Average variance extracted (AVE)
CRM	0.814	0.976	0.614
CYBSEC	0.843	0.887	0.608
GE	0.848	0.875	0.621
INC	0.843	0.845	0.614
IRE	0.837	0.880	0.599
MPR	0.847	0.878	0.617
SBE	0.873	0.876	0.664

perception about all variables (See Table 1). The reliability analysis (Cronbach's alpha) indicates strong internal consistency for all constructs. Composite reliability and average variance extracted (AVE) values exceed recommended thresholds, confirmed convergent validity (Table 2). For examining the discriminant validity of the construct, Heterotrate Monotrate (HTMT) test has been conducted. The results confirm discriminant validity of the constructs, and the results are shown in Table 3. From Tables 3 and it appears that all the HTMT vales did not exceed the highest threshold value of 0.85 (Henseler et al., 2015).

Results reveal a positive and significant impact of cybersecurity compliance (CYBSEC→INC: β = 0.134, p = 0.006) and incident response effectiveness (IRE→INC: β = 0.336, p = 0.000) on innovation capability. However, the influence of cybersecurity risk management on innovation capability (CRM→INC: β = 0.098, p = 0.081) is positive but not statistically significant. These findings imply that organizations with robust cybersecurity compliance and effective incident response mechanisms tend to exhibit higher innovation capabilities. Cybersecurity compliance (CYBSEC→GE: β = 0.158, p = 0.002), incident response effectiveness (IRE→GE: β = 0.200, p = 0.001), and innovation capability (INC→GE: β = 0.190, p = 0.001) positively and significantly contribute to governance efficacy. Surprisingly, cybersecurity risk management (CRM→GE: β = 0.010, p = 0.912) does not exhibit a significant influence on governance efficacy (See Table 4). These results emphasize the pivotal role of cybersecurity compliance, incident response, and innovation in bolstering governance efficacy within organizations.

All three cybersecurity components—compliance (CYBSEC→SBE: β = 0.177, p = 0.000), risk management (CRM→SBE: β = 0.119, p = 0.013), and incident response effectiveness (IRE→SBE: β = 0.086, p = 0.111)—positively impact sustainable business excellence. Additionally, governance efficacy (GE → SBE: β = 0.149, p = 0.009) and the moderating effect of Macroeconomic Policies and Regulations (MPR x GE → SBE: β = 0.119, p = 0.016) exhibit positive and significant relationships with sustainable business excellence. These results underscore the interconnectedness of cybersecurity practices, governance, and external regulatory environments in shaping sustainable business outcomes.

The study confirms the mediating role of governance efficacy in enhancing the relationship between innovation capability and sustainable business excellence. Moreover, Macroeconomic Policies and Regulations (MPR) act as a significant moderator, strengthening the positive association between governance efficacy and sustainable excellence. This highlights the importance of regulatory frameworks in augmenting the impact of governance on long-term business sustainability.

5. Discussion on the findings

The research introduced a new integrated framework to improve understandings of business excellence and cybersecurity resilience associations. The developed framework provided governance-technical insights for industry experts, academics, policymakers and firm managers. Firstly, based on resource-based view, organizations can achieve continued competitive benefit through the strategic use of unique and valuable resources. The study examines empirically from a management view to fill the gap in cybersecurity literature. Park et al. (2017) as well as Xu and Mahenthiran (2021) argued firms need both IT and organizational tools to address and control cybersecurity risks. In this study, cybersecurity resilience is a critical factor that contributes positively to innovation capability. Out of the components of cybersecurity resilience, the significant and positive relationship between cybersecurity compliance and innovation capability aligns with Resource-Based Theory principles. Organizations who invest in robust cybersecurity practices not only safeguard digital assets but also encourage an environment good for creative thinking and technological progress.

The secure foundation from compliance allows employees to focus on innovation rather than be worried about security. Secondly, incident response effectiveness provides feedback to security routines when the team sees what technical and procedural aspects worked well and which did not and need fixing. Hence, the security team is responsible not just for management of the technical response after an incident but also to provide input for improvement in the incident response process. Therefore, it can be stated that resource-based view also stresses the importance of effective resource management. Unlike above two, the non-significant relationship between cybersecurity risk management and governance efficacy highlights a nuanced aspect of resource allocation. It suggests while risk management is crucial for assets protection, its direct influence on governance efficacy might depend on other factors. For example, allocation of resources for risk management can be more directly tied to maintenance assets than determining governance structures. This finding prompts organizations to critically assess how they distribute resources across cybersecurity areas. With reference to the literature review results (Choucri et al., 2014; Lees et al., 2018), based on the characterization of cybersecurity in industrial contexts, cyber risk management and incident response recovery are considered the main industrial components involved in cybersecurity resilience.

Setting aside externalities, there are evidence that firms invest in cybersecurity activities at a level below what would be optimal. There are few firms that had a major cybersecurity breach recently (e.g. Amazon, Facebook, and Google, are constantly subject to cyber threats) shows a significant step for the firms to increase their cybersecurity investments. Even though, government assumed business firms are underinvesting in cybersecurity activities. However, effective cybersecurity practices are valuable organizational resources that contribute to long-term sustainability. Organizations that view cybersecurity not just as a compliance requirement but a strategic resource are better positioned to achieve sustainable business excellence. The results emphasize cybersecurity is not just a defensive strategy but an integral part of the organizational resource portfolio which can shape business into long-

Table 3
Discriminant validity (HTMT) – Matrix.

Variables	CRM	CYBSEC	GE	INC	IRE	MPR	SBE
CRM							
CYBSEC	0.114						
GE	0.076	0.244					
INC	0.135	0.238	0.339				
IRE	0.087	0.201	0.315	0.410			
MPR	0.136	0.179	0.466	0.384	0.296		
SBE	0.179	0.319	0.361	0.231	0.281	0.460	
MPR × GE	0.094	0.079	0.176	0.044	0.084	0.122	0.094

Table 4
PLS-SEM assessment.

Paths	β-values	P-values
CRM → GE	0.006	0.912
CRM → INC	0.095	0.081
CRM → SBE	0.117	0.013
CYBSEC → GE	0.155	0.002
CYBSEC → INC	0.132	0.006
CYBSEC → SBE	0.176	0.000
GE → SBE	0.150	0.009
INC → GE	0.188	0.001
IRE → GE	0.199	0.001
IRE → INC	0.333	0.000
IRE → SBE	0.086	0.111
MPR → SBE	0.296	0.000
MPR × GE → SBE	0.118	0.016
Var	R-square	R-square adjusted
GE	0.152	0.142
INC	0.162	0.155
SBE	0.279	0.266
Model Fit	Saturated model	Estimated model
SRMR	0.057	0.073
Chi-square	1058.562	1099.950
NFI	0.812	0.804

term sustainable outcomes. On the other side, several national governments have adopted laws aimed at penalties and punishments for specific cyber-attacks or exploitation. For example, India has adopted laws for various criminal conducts such as improper intrusion and deliberate damage of computer systems. China also adopted similar rules governed by China's Cyberspace Administration. They decided if a firm violated the country's network security law, data security law, and personal information protection law, strict action would be taken. On a broader note, if companies make profit from personal information, it means they have extra responsibility to protect and secure that data. A successful cyber-attack can cause major damage to a business. It can affect the bottom line, business standing, and consumer trust. The impact of a security breach can be divided into three categories: financial, reputational, and regulations.

If we look at the third aspect, regulations, we could relate it to institutional theory. Institutional theory states organizations are influenced by the broader institutional environment. In this study, the moderating effect of Macroeconomic Policies and Regulations (MPR) on the relationship between governance efficacy and sustainable business excellence aligns with this view. MPR serves as an institutional force that shapes organizational behaviour. The positive and significant interaction suggests adherence to external regulations strengthens the impact of governance efficacy on sustainable business excellence. Organizations who operate within a regulatory framework are more likely to align governance with societal expectations and reinforce commitment to sustainable practices.

Overall, our research findings align with the sustainable business excellence of cybersecurity resilience. Our results suggested firms' innovation ability has a positive effect on business excellence. Institutional Theory also views governance structures as institutional mechanisms organizations adopt to conform to pressures. The positive relationships between cybersecurity practices, innovation capability, and governance efficacy highlight the institutional role of cybersecurity. Governance efficacy serves as a mechanism through which organizations respond to demands for secure and responsible practices. The results underscore cybersecurity is not only a technical necessity but an institutional imperative which each organization must embed in governance. A study by Tosun (2021) examined the stock market impact of cybersecurity breaches on publicly traded US firms. Their study shows some breaches have a significant negative effect, but there has been a general downward shift in the impact breaches have on firms. Furthermore, the mediating role of governance efficacy in enhancing the innovation capability and sustainable business excellence relationship aligns with both Resource-Based Theory and Institutional Theory. From a resource perspective, governance efficacy acts as a mechanism through which innovation capability, facilitated by cybersecurity practices, translates into sustained excellence. Institutionally, the mediation reflects the embeddedness of governance in translating innovation into tangible, sustainable outcomes. It reinforces that innovation needs effective governance to meaningfully contribute to long-term achievement.

6. Implications of the study

In today's digital world, the ever-growing complexity of cybersecurity issues has led CEOs and boards to prioritize digital protection as a top priority. The need to protect digital assets is closely associated with the duty of trust as illustrated by a 2021 Deloitte survey which found that 85% of CEOs consider cybersecurity to be a significant fiduciary obligation (Deloitte, 2021). This emphasizes the increased importance of digital assets in the corporate world. Executives and managers must navigate the complex challenge to discover a middle ground between financial factors, regulatory adherence, and other consequences. Cybersecurity has become recognized as a competitive edge, goes beyond a simple focus on compliance. The implementation of strong practices such as subsequent regulations, risk management, and an integrated response system to incidents is essential to offer an adequate foundation for organizational activities (Ahmad et al., 2020; Mishra, 2023). This perspective views cybersecurity as more than just a reactive control mechanism, but also as a proactive facilitator of innovation and excellence. Essential to this fundamental change in perception is the development of an organizational culture that effortlessly integrates innovation with security. Effective decision-making, based on data, is crucial for ensuring comprehensive protection and utilizing digital prospects in today's interconnected world. Organizations must respond promptly and efficiently to the unpredictable and more sophisticated cyber threats that exist in today's dynamic landscape. The present study has uniquely advocated that without ensuring better cybersecurity measures, it is very different for the organizations to protect their VRIN related data helpful to navigate businesses with their partners who form part of their business ecosystems. Besides, different cybersecurity measures help in superior use of organizational VRIN related data for different innovation purposes such as inventing new products, modernizing processes, and developing new business models. This study has also suggested that cybersecurity measures become more important and critical when any dramatic changes happen abruptly since in such time organizations need cybersecurity resilience to address such dramatic situations.

Malicious entities and cybercriminals utilize a range of methods, such as malware, phishing, ransomware, and social engineering, to take advantage of vulnerabilities and security flaws (Choucri et al., 2014; Kure et al., 2022; Timofeyev and Dremova, 2022). In order to effectively respond to the ever-changing nature of these threats, organizations must not only facilitate innovation but also seamlessly incorporate security measures into their processes. The key aspect of this integration involves the execution of training initiatives that cultivate a deep-seated awareness of cybersecurity accountability among staff members which highlights the harmonious coexistence of innovation and security. The study highlights the necessity for businesses to assess their strategies for the allocation of resources, especially when confronted with limitations such as restricted finances and a shortage of trained individuals. These constraints present obstacles that prevent strong security measures. To achieve an effective equilibrium in investments in compliance, risk management, and incident response, one must possess a deep comprehension of the specific requirements and goals of the firm. Managers are advised to strengthen governance frameworks that are in line with cybersecurity practices while acknowledging the important role of governance efficacy. This entails emphasizing and assigning specific duties and obligations to ensure strong supervision and monitoring and regularly evaluating policies. Although several companies involve third-party providers, Eisenbach et al. (2022) emphasized that these associations can bring forth possible challenges. Threats to suppliers might compromise organizational systems and data that require due diligence and the implementation of robust processes when interacting with third parties. Mainly, management bears the primary responsibility for the acquisition and effectiveness of security systems, while IT teams with expertise are responsible for their implementation, monitoring, and maintenance.

An established governance structure arises as the means of transforming the advantages of innovation and cybersecurity into long-lasting economic superiority. MPR is recognized as a beneficial factor that enhances the effectiveness of governance and promotes long-term excellence. It is crucial for managers to actively comply with and embrace external regulations. This not only safeguards against legal concerns but also improves governance effectiveness, which in turn promotes sustainability. Boards are recommended to designate a person who will comprehend security requirements and conditions, deliver updates, and handle significant concerns. Regularly monitoring legislative changes enables flexibility and conformity with expectations. Managers are expected to promote innovation that is in line with sustainable objectives, recognizing the complex links between innovation, governance, and excellence. This entails incorporating sustainability

into the process of innovation and ensuring that governance frameworks guide innovative initiatives. In order to keep up with the ever-changing digital environment, it is essential to constantly adjust and modify cybersecurity methods. Managers should implement procedures for continuous evaluation of processes, governance, and resilience through audits, assessments, and scenario planning. It is considered crucial to provide thorough training that covers practices, policies, and adherence in order to develop a cybersecurity attitude. In this sense, governance refers to the required organizational modifications and enhancements to established procedures (Hartmann and Carmenate, 2021; Selimoglu and Saldi, 2023). The fundamental principles of corporate governance, including fair treatment of shareholders, transparency, accountability of the board, adherence to legal requirements, and oversight of regulations, continue to be relevant. It is crucial for managers to ensure that staff fully understand their roles in security and innovation. They should also encourage collaboration both within and outside the organization to gain valuable insights and enhance their overall posture. Additionally, managers must focus on building and regularly updating reaction plans, including protocols, teams, and exercises. This study focuses on cybersecurity, but it also suggests the possibility of future research investigating the impact of disclosures on investment decisions.

7. Conclusion

The contemporary business landscape has embraced the concept of cybersecurity resilience, permeating both technological and governance domains. While developed markets have integrated this paradigm shift, emerging markets are taking their initial steps in this direction. This research has explored the intricate relationships involving cybersecurity resilience, innovation capabilities, governance effectiveness, and sustainable business excellence. The findings of the study are relevant for innovation ecosystems as they suggest that cybersecurity, and more specifically cybersecurity resilience, positively influences the innovation capabilities of organizations belonging to an innovation ecosystem and that innovation capabilities in their turn influence positively sustainable business excellence. More generally, we find that without proper cybersecurity measures, organizations part of innovation ecosystems cannot effectively protect their data and information systems that possess VRIN characteristics (Barney, 1991) that are critical to innovate new products, processes, and business models.

Second, this research further reveals the mediating role of governance effectiveness in enhancing the connection between innovation capabilities and sustainable excellence. These results underscore the importance of cybersecurity resilience in a digital world where the protection of data and information systems is at the heart of any business activity and especially of business activities involving more than just one organization.

Third, this study suggests that cybersecurity is not merely a technical requirement but a strategic and institutional imperative for organizations and organizational ecosystems to achieve sustainable business excellence.

Last, this work highlights that as cyber threats have become a major security concern for organizations, also regulators should articulate appropriate security policies and regulations as a part of their endeavours to shape a secure business environment.

8. Limitations of this study and direction for future research

This study is not without limitations. First, the study results principally rely on data which are cross sectional. Scholars could undertake a longitudinal study in the future to control for potential endogeneity issues. Second, the present study results are based on the inputs of the respondents who are based in India. This creates external validity issues. Future researchers are suggested to consider responses of respondents scattered across the globe. This would assure more generalizability of the study. Third, this study did not analyse a rival model which could help to compare the proposed theoretical model with the rival model to analyse whether the proposed theoretical model is of superior quality compared to the rival model. This should be considered as another limitation of this study and future researchers are suggested to nurture this issue. Last, the explanatory power of the model could have been improved by consideration of other constructs and other boundary conditions. Future researchers should investigate this issue.

CRediT authorship contribution statement

Kuldeep Singh: Writing – review & editing, Writing – original draft, Visualization, Validation, Resources, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Sheshadri Chatterjee:** Writing – review & editing, Writing – original draft, Visualization, Validation, Resources, Methodology, Investigation, Formal analysis, Data curation. **Marcello Mariani:** Writing – review & editing. **Samuel Fosso Wamba:** Writing – review & editing.

Data availability

The data that has been used is confidential.

References

Ahmad, A., Desouza, K.C., Maynard, S.B., Naseer, H., Baskerville, R.L., 2020. How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology 71 (8), 939–953.

Alexander, R.D., Panguluri, S., 2017. Cybersecurity terminology and frameworks. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level 19–47. https://doi.org/10.1007/978-3-319-32824-9_2.

Alharbi, A., Sohaib, O., 2021. Technology readiness and cryptocurrency adoption: PLS-SEM and deep learning neural network analysis. IEEE Access 9, 21388–21394.

Al-Sartawi, A.M.M., Razzaque, A., 2020. Cyber Security, IT governance, and performance: a review of the current literature. Implementing Computational Intelligence Techniques for Security Systems Design, pp. 275–288. https://doi.org/10.4018/978-1-7998-2418-3.ch014.

Armstrong, J.S., Overton, T.S., 1977. Estimating nonresponse bias in mail surveys. J. Mark. Res. 14 (3), 396–402.

Audretsch, D.B., Belitski, M., Guerrero, M., 2022. The dynamic contribution of innovation ecosystems to schumpeterian firms: a multi-level analysis. J. Bus. Res. 144, 975–986.

Barney, J., 1991. Firm resources and sustained competitive advantage. Journal of management 17 (1), 99–120.

Borchert, O., 2008. Resource-based theory: creating and sustaining competitive advantage. J. Market. Manag. 24 (9–10), 1–17.

Bredt, S., 2019. Artificial Intelligence (AI) in the financial sector—potential and public strategies. Frontiers in Artificial Intelligence 2, 16–20. https://doi.org/10.3389/frai.2019.00016.

Broeders, D., 2021. Private active cyber defense and (international) cyber security - pushing the line? Journal of Cybersecurity 7 (1), 1–10.

Calantone, R.J., Cavusgil, S.T., Zhao, Y., 2002. Learning orientation, firm innovation capability, and firm performance. Ind. Mark. Manag. 31 (6), 515–524.

Catota, F.E., Morgan, M.G., Sicker, D.C., 2018. Cybersecurity incident response capabilities in the Ecuadorian financial sector. Journal of Cybersecurity 4 (1), 1–12.

Cavelty, M.D., Wenger, A., 2022. Cyber security politics: socio-technological transformations and political fragmentation. In: Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation. https://doi.org/10.4324/9781003110224.

Cavusoglu, H., Cavusoglu, H., Son, J.Y., Benbasat, I., 2015. Institutional pressures in security management: direct and indirect influences on organizational investment in information security control resources. Inf. Manag. 52 (4), 385–400.

Chatterjee, S., Chaudhuri, R., Mariani, M., Wamba, S.F., 2023. The consequences of innovation failure: an innovation capabilities and dynamic capabilities perspective. Technovation 128, 102858.

Chatterjee, S., Chaudhuri, R., Vrontis, D., Thrassou, A., 2021. The influence of online customer reviews on customers' purchase intentions: a cross-cultural study from India and the UK. Int. J. Organ. Anal. 30 (6), 1595–1623.

Chatterjee, S., Khorana, S., Kizgin, H., 2022. Harnessing the potential of artificial intelligence to foster citizens' satisfaction: an empirical study on India. Gov. Inf. Q. 39 (4), 101621.

Chaudhuri, R., Chatterjee, S., Vrontis, D., 2022b. Antecedents of privacy concerns and online information disclosure: moderating role of government regulation. EuroMed J. Bus. 18 (3), 467–486.

Chaudhuri, R., Chatterjee, S., Vrontis, D., Vicentini, F., 2022a. Effects of human capital on entrepreneurial ecosystems in the emerging economy: the mediating role of digital knowledge and innovative capability from India perspective. J. Intellect. Cap. 24 (1), 283–305.

Chin, W.W., 2010. How to write up and report PLS analyses. In: Wynne, W. (Ed.), Chin Handbook of Partial Least Squares, pp. 655–690.
Choo, K.K.R., Gai, K., Chiaraviglio, L., Yang, Q., 2021. A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. Comput. Secur. 102, 102136.
Choucri, N., Madnick, S., Ferwerda, J., 2014. Institutions for cyber security: international responses and global imperatives. Inf. Technol. Dev. 20 (2), 96–121.
Connor, T., 2002. The resource-based view of strategy and its value to practising managers. Strateg. Change 11 (6), 307–316.
Cosenz, F., Noto, G., Cavallo, A., 2023. Understanding the microfoundations of entrepreneurial ecosystems: toward a value-based method and theory. IEEE Trans. Eng. Manag. 71, 7298–7310.
Cram, W.A., D'Arcy, J., 2023. 'What a waste of time': an examination of cybersecurity legitimacy. Inf. Syst. J. 33 (6), 1396–1422.
Dalal, R.S., Howard, D.J., Bennett, R.J., Posey, C., Zaccaro, S.J., Brummel, B.J., 2022. Organizational science and cybersecurity: abundant opportunities for research at the interface. J. Bus. Psychol. 37 (1), 1–29.
D'Ambra, J., Akter, S., Mariani, M., 2022. Digital transformation of higher education in Australia: Understanding affordance dynamics in E-Textbook engagement and use. Journal of Business Research 149, 283–295.
Dash, G., Paul, J., 2021. CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting. Technol. Forecast. Soc. Change 173, 121092.
Dehghani, M., Niknam, T., GhasemiGarpachi, M., Alhelou, H.H., Pourbehzadi, M., Javidi, G., Sheybani, E., 2023. Public policies for cyber security of sustainable dominated renewable smart grids. IET Gener., Transm. Distrib. 17 (18), 4057–4071.
Deloitte, 2021. Future of cyber survey. Deloitte cyber | empowering your people for the future. Available at: https://www2.deloitte.com/in/en/pages/risk/articles/future-of-cyber.html . (Accessed 12 January 2023).
Demetris, V., Chatterjee, S., Chaudhuri, R., 2022. Examining the impact of adoption of emerging technology and supply chain resilience on firm performance: moderating role of absorptive capacity and leadership support. IEEE Trans. Eng. Manag. https://doi.org/10.1109/TEM.2021.3134188 (in press).
DiMaggio, P.J., Powell, W.W., 1983. The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. Am. Sociol. Rev. 48 (2), 147–160.
Dube, D.P., Mohanty, R.P., 2021. The application of cyber security capability maturity model to identify the impact of internal efficiency factors on the external effectiveness of cyber security. Int. J. Bus. Inf. Syst. 38 (3), 367–392.
Dupont, B., 2019. The cyber-resilience of financial institutions: significance and applicability. Journal of cybersecurity 5 (1), 1–12.
Economist, 2017. The world's most valuable resource is no longer oil, but data. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. (Accessed 30 October 2020).
Eisenbach, T.M., Kovner, A., Lee, M.J., 2022. Cyber risk and the us financial system: a pre-mortem analysis. J. Financ. Econ. 145 (3), 1–15.
Ekelund, S., Iskoujina, Z., 2019. Cybersecurity economics–balancing operational security spending. Inf. Technol. People 32 (5), 1318–1342.
Elia, S., Giuffrida, M., Mariani, M.M., Bresciani, S., 2021. Resources and digital export: an RBV perspective on the role of digital technologies and capabilities in cross-border e-commerce. J. Bus. Res. 132, 158–169.
Felício, J.A., Rodrigues, R., Patino-Alonso, C., Felício, T., 2022. Allostasis and organizational excellence. J. Bus. Res. 140, 107–114.
Galati, A., Chaudhuri, R., Sakka, G., Grandhi, B., Siachou, E., Vrontis, D., 2021. Adoption of social media marketing for sustainable business growth of SMEs in emerging economies: the moderating role of leadership support. Sustainability 13 (21), 12134.
Garcia-Perez, A., Cegarra-Navarro, J.G., Sallos, M.P., Martinez-Caro, E., Chinnaswamy, A., 2023. Resilience in healthcare systems: cyber security and digital transformation. Technovation 121, 102583.
Giovando, G., Chatterjee, S., Chaudhuri, R., Vrontis, D., 2023. Digital workplace and organization performance: moderating role of digital leadership capability. Journal of Innovation & Knowledge 8 (1), 100334.
Granstrand, O., Holgersson, M., 2020. Innovation ecosystems: a conceptual review and a new definition. Technovation 90, 102098.
Grant, R.M., 1991. The resource-based theory of competitive advantage: implications for strategy formulation. Calif. Manag. Rev. 33 (3), 114–135.
Gutiérrez Ponce, H., Chamizo González, J., Al-Mohareb, M., 2023. Sustainable finance in cybersecurity investment for future profitability under uncertainty. Journal of Sustainable Finance & Investment 13 (1), 614–633.
Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E., 2010. Multivariate data analysis. Vector. https://doi.org/10.1016/j.ijpharm.2011.02.019.
Hair, J.F., Hollingsworth, C.L., Randolph, A.B., Chong, A.Y.L., 2017. An updated and expanded assessment of PLS-SEM in information systems research. Ind. Manag. Data Syst. 117 (3), 442–458.
Hartmann, C.C., Carmenate, J., 2021. Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: implications for practice, policy, and research. Current issues in auditing 15 (2), A9–A23.
Haseeb, M., Hussain, H.I., Ślusarczyk, B., Jermsittiparsert, K., 2019. Industry 4.0: a solution towards technology challenges of sustainable business performance. Soc. Sci. 8 (5), 154–162.
Henseler, J., Hubona, G., Ray, P.A., 2016. Using PLS path modeling in new technology research: updated guidelines. Ind. Manag. Data Syst. 116 (1), 2–20.
Henseler, J., Ringle, C.M., Sarstedt, M., 2015. A new criterion for assessing discriminant validity in variance-based structural equation modelling. J. Acad. Market. Sci. 43, 115–135.
Hodapp, D., Hanelt, A., 2022. Interoperability in the era of digital innovation: an information systems research agenda. J. Inf. Technol. 37 (4), 407–427.
Hoskisson, R.E., Gambeta, E., Green, C.D., Li, T.X., 2018. Is my firm-specific investment protected? Overcoming the stakeholder investment dilemma in the resource-based view. Acad. Manag. Rev. 43 (2), 284–306.
Hsu, C., Lee, J.N., Straub, D.W., 2012. Institutional influences on information systems security innovations. Inf. Syst. Res. 23 (3-part-2), 918–939.
Jakobsen, M., Jensen, R., 2015. Common method bias in public management studies. Int. Public Manag. J. 18 (1), 3–30.
Jarjoui, S., Murimi, R., 2021. A framework for enterprise cybersecurity risk management. In: Advances in Cybersecurity Management. Cham: Springer International Publishing, UK, pp. 139–161.
Jossen, S., 2017. The world's most valuable resource is no longer oil, but data. The Economist 423, 5–8.
Ketokivi, M.A., Schroeder, R.G., 2004. Perceptual measures of performance: fact or fiction? J. Oper. Manag. 22 (3), 247–264.
Khan, S.A.R., Ponce, P., Thomas, G., Yu, Z., Al-Ahmadi, M.S., Tanveer, M., 2021. Digital technologies, circular economy practices and environmental policies in the era of COVID-19. Sustainability 13 (22), 12790.
Kim, Y.J., Lee, J.M., Koo, C., Nam, K., 2013. The role of governance effectiveness in explaining IT outsourcing performance. Int. J. Inf. Manag. 33 (5), 850–860.
Kock, N., 2023. Contributing to the success of PLS in SEM: an action research perspective. Commun. Assoc. Inf. Syst. 52 (1), 730–734.
Kosutic, D., Pigni, F., 2022. Cybersecurity: investing for competitive outcomes. J. Bus. Strat. 43 (1), 28–36.
Kriaa, S., Bouissou, M., Laarouchi, Y., 2019. A new safety and security risk analysis framework for industrial control systems. Proc. Inst. Mech. Eng. O J. Risk Reliab. 233 (2), 151–174.
Kure, H.I., Islam, S., Mouratidis, H., 2022. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Comput. Appl. 34 (18), 15241–15271.
Lattanzio, G., Ma, Y., 2023. Cybersecurity risk and corporate innovation. J. Corp. Finance 82, 102445.
Lee, I., 2021. Cybersecurity: risk management framework and investment cost analysis. Bus. Horiz. 64 (5), 659–671.
Lees, M.J., Crawford, M., Jansen, C., 2018. Towards industrial cybersecurity resilience of multinational corporations. IFAC-PapersOnLine 51 (30), 756–761.
Li, Y., Liu, Q., 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Rep. 7, 8176–8186.
Lilli, E., 2021. Redefining deterrence in cyberspace: private sector contribution to national strategies of cyber deterrence. Contemp. Secur. Policy 42 (2), 163–188.
Lindell, M.K., Whitney, D.J., 2001. Accounting for common method variance in cross-sectional research designs. J. Appl. Psychol. 86 (1), 114–121.
Liu, X., Ahmad, S.F., Anser, M.K., Ke, J., Irshad, M., Ul-Haq, J., Abbas, S., 2022. Cyber security threats: a never-ending challenge for e-commerce. Front. Psychol. 13, 927398.
Lockett, A., Thompson, S., Morgenstern, U., 2009. The development of the resource-based view of the firm: a critical appraisal. Int. J. Manag. Rev. 11 (1), 9–28.
Malatji, M., Marnewick, A.L., Von Solms, S., 2022. Cybersecurity capabilities for critical infrastructure resilience. Information & Computer Security 30 (2), 255–279.
Mariani, M., 2018. The Role of Policy Makers and Regulators in Coopetition. Routledge companion to coopetition strategies, pp. 105–116.
Mariani, M.M., Machado, I., Magrelli, V., Dwivedi, Y.K., 2023. Artificial intelligence in innovation research: a systematic review, conceptual framework, and future research directions. Technovation 122, 102623.
Mariani, M., Borghi, M., 2019. Industry 4.0: a bibliometric review of its managerial intellectual structure and potential evolution in the service industries. Technol. Forecast. Soc. Change 149, 119752.
Marsch, 2018. By the Numbers: Global Cyber Risk Perception Survey. Available at: https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Marsh%20Microsoft%20Global%20Cyber%20Risk%20Perception%20Survey%20February%202018.pdf. (Accessed 12 March 2024).
Matthews, L.M., Sarstedt, M., Hair, J.F., Ringle, C.M., 2016. Identifying and treating unobserved heterogeneity with FIMIX-PLS: Part II–A case study. Eur. Bus. Rev. 28 (2), 208–224.
Melaku, H.M., 2023. A dynamic and adaptive cybersecurity governance framework. Journal of Cybersecurity and Privacy 3 (3), 327–350.
Meszaros, J., Buchalcevova, A., 2017. Introducing OSSF: a framework for online service cybersecurity risk management. Comput. Secur. 65, 300–313.
Mhlanga, D., 2020. Industry 4.0 in finance: the impact of artificial intelligence (ai) on digital financial inclusion. Int. J. Financ. Stud. 8 (3), 45–56.
Michalec, O., Milyaeva, S., Rashid, A., 2022a. Reconfiguring governance: how cyber security regulations are reconfiguring water governance. Regulation & Governance 16 (4), 1325–1342.
Michalec, O., Milyaeva, S., Rashid, A., 2022b. When the future meets the past: can safety and cyber security coexist in modern critical infrastructures? Big Data & Society 9 (1), 20539517221108369.
Mishra, A., Alzoubi, Y.I., Gill, A.Q., Anwar, M.J., 2022. Cybersecurity enterprises policies: a comparative study. Sensors 22 (2), 538–553.
Mishra, S., 2023. Exploring the impact of ai-based cyber security financial sector management. Appl. Sci. 13 (10), 5875.
Naseer, A., Naseer, H., Ahmad, A., Maynard, S.B., Siddiqui, A.M., 2021. Real-time analytics, incident response process agility and enterprise cybersecurity performance: a contingent resource-based analysis. Int. J. Inf. Manag. 59, 102334.
Obitade, P.O., 2019. Big data analytics: a link between knowledge management capabilities and superior cyber protection. J. Big Data 6 (1), 71.

Ording, L.G., Gao, S., Chen, W., 2022. The influence of inputs in the information security policy development: an institutional perspective. Transforming Gov. People, Process Policy 16 (4), 418–435.
Park, J., Lee, J.N., Lee, O.K.D., Koo, Y., 2017. Alignment between internal and external IT governance and its effects on distinctive firm performance: an extended resource-based view. IEEE Trans. Eng. Manag. 64 (3), 351–364.
Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y., Podsakoff, N.P., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. J. Appl. Psychol. 88 (5), 879–893.
Rajapathirana, R.J., Hui, Y., 2018. Relationship between innovation capability, innovation type, and firm performance. Journal of Innovation & Knowledge 3 (1), 44–55.
Ranjan, C., Chatterjee, S., Vrontis, D., 2022. AI and digitalization in relationship management: impact of adopting AI-embedded CRM system. J. Bus. Res. 150, 437–450.
Ranjan, C., Chatterjee, S., Vrontis, D., 2021. Usage intention of social robots for domestic purpose: from security, privacy, and legal perspectives. Inf. Syst. Front. https://doi.org/10.1007/s10796-021-10197-7 (in press).
Ranjan, C., Chatterjee, S., Kraus, S., Vrontis, D., 2023. Assessing the AI-CRM technology capability for sustaining family businesses in times of crisis: the moderating role of strategic intent. J. Fam. Bus. Manag. 13 (1), 46–67.
Reinartz, W., Haenlein, M., Henseler, J., 2009. An empirical comparison of the efficacy of covariance-based and variance-based SEM. Int. J. Res. Market. 26 (4), 332–344.
Renaud, K., Von Solms, B., Von Solms, R., 2019. How does intellectual capital align with cyber security? J. Intellect. Cap. 20 (5), 621–641.
Rigdon, E.E., Sarstedt, M., Ringle, C.M., 2017. On comparing results from CB-SEM and PLS-SEM: Five perspectives and five recommendations. Marketing ZFP 39 (3), 4–16.
Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E., Alabbad, D.A., 2023a. Digital transformation and cybersecurity challenges for businesses resilience: issues and recommendations. Sensors 23 (15), 6666.
Saeed, S., Suayyid, S.A., Al-Ghamdi, M.S., Al-Muhaisen, H., Almuhaideb, A.M., 2023b. A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. Sensors 23 (16), 7273.
Safitra, M.F., Lubis, M., Fakhrurroja, H., 2023. Counterattacking cyber threats: a framework for the future of cybersecurity. Sustainability 15 (18), 13369.
Sahu, A.K., Sahu, A.K., Sahu, N.K., 2020. A review on the research growth of industry 4.0: IIoT business architectures benchmarking. International Journal of Business Analytics 7 (1), 77–97.
Salimath, M.S., Philip, J., 2020. Cyber management and value creation: an organisational learning-based approach. Knowl. Manag. Res. Pract. 18 (4), 474–487.
Schmitz-Berndt, S., 2023. Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. Journal of Cybersecurity 9 (1), 1–17.
Selimoglu, S.K., Saldi, M.H., 2023. Blockchain technology for internal audit in cyber security governance of banking sector in Turkey: a swot analysis. In: Contemporary Studies of Risks in Emerging Technology, Part B. Emerald Publishing, (UK) Limited, pp. 23–55.
Shaheen, K., Zolait, A.H., 2023. The impacts of the cyber-trust program on the cybersecurity maturity of government entities in the Kingdom of Bahrain. Information & Computer Security 31 (5), 529–544.
Sheshadri, C., 2019. Influence of IoT policy on quality of life: from government and citizens' perspectives. Int. J. Electron. Govern. Res. 15 (2), 19–38.
Sheshadri, C., 2021. Dark side of online social games (OSG) using Facebook platform: effect of age, gender, and identity as moderators. Inf. Technol. People 34 (7), 1800–1818.
Sheshadri, C., Chaudhuri, R., Vrontis, D., Jabeen, F., 2022. Digital transformation of organization using AI-CRM: from microfoundational perspective with leadership support. J. Bus. Res. 153, 46–58.
Siachou, E., Sakka, G., Chatterjee, S., Chaudhuri, R., Ghosh, A., 2022. Societal effects of social media in organizations: reflective points deriving from a systematic literature review and a bibliometric meta-analysis. Eur. Manag. J. 40 (2), 151–162.
Singh, H.P., Alshammari, T.S., 2020. An institutional theory perspective on developing a cyber security legal framework: a case of Saudi arabia. Beijing Law Rev. 11 (3), 637–650.
Slapničar, S., Vuko, T., Čular, M., Drašček, M., 2022. Effectiveness of cybersecurity audit. Int. J. Account. Inf. Syst. 44, 100548.
Smaili, N., Radu, C., Khalili, A., 2023. Board effectiveness and cybersecurity disclosure. J. Manag. Govern. 27 (4), 1049–1071.
Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., Zema, T., 2021. Cybersecurity and sustainable development. Procedia Comput. Sci. 192, 20–28.
Sun, L., Zhang, H., Fang, C., 2021. Data security governance in the era of big data: status, challenges, and prospects. Data Science and Management 2, 41–44.
Taherdoost, H., 2022. Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. Electronics 11 (14), 2181.
Teece, D.J., Pisano, G., Shuen, A., 1997. Dynamic capabilities and strategic management. Strategic management journal 18 (7), 509–533.
Tehseen, S., Ramayah, T., Sajilan, S., 2017. Testing and controlling for common method variance: a review of available methods. Journal of management sciences 4 (2), 142–168.
Timofeyev, Y., Dremova, O., 2022. Insurers' responses to cybercrime: evidence from Russia. International Journal of Law, Crime and Justice 68, 100520.
Tosun, O.K., 2021. Cyber-attacks and stock market activity. Int. Rev. Financ. Anal. 76, 101795.
van Rijmenam, M., Logue, D., 2021. Revising the 'science of the organisation': theorising AI agency and actorhood. Innovation 23 (1), 127–144.
Viardot, E., Brem, A., Nylund, P.A., 2023. Post-pandemic implications for crisis innovation: a technological innovation view. Technol. Forecast. Soc. Change 194, 122680.
Vittori, D., Natalicchio, A., Panniello, U., Messeni Petruzzelli, A., Cupertino, F., 2022. Business Model Innovation between the embryonic and growth stages of industry lifecycle. Technovation 117, 102592.
Von Solms, R., Van Niekerk, J., 2013. From information security to cyber security. Comput. Secur. 38, 97–102.
Vrontis, D., Chaudhuri, R., Chatterjee, S., 2022. Adoption of digital technologies by SMEs for sustainability and value creation: moderating role of entrepreneurial orientation. Sustainability 14 (13), 7949.
Wang, W.H., Espinosa, V.I., Peña-Ramos, J.A., 2021. Private property rights, dynamic efficiency and economic development: an Austrian reply to neo-Marxist scholars Nieto and Mateo on cyber-communism and market process. Economies 9 (4), 165.
Weishäupl, E., Yasasin, E., Schryen, G., 2018. Information security investments: an exploratory multiple case study on decision-making, evaluation and learning. Comput. Secur. 77, 807–823.
Wiertz, C., De Ruyter, K., Keen, C., Streukens, S., 2004. Cooperating for service excellence in multichannel service systems: an empirical assessment. J. Bus. Res. 57 (4), 424–436.
Willaby, H.W., Costa, D.S., Burns, B.D., MacCann, C., Roberts, R.D., 2015. Testing complex models with small sample sizes: a historical overview and empirical demonstration of what partial least squares (PLS) can offer differential psychology. Pers. Indiv. Differ. 84, 73–78.
Wójcik, P., 2015. Exploring links between dynamic capabilities perspective and resource-based view: a literature overview. Int. J. Manag. Econ. 45 (1), 83–107.
Xu, H., Mahenthiran, S., 2021. Users' perception of cybersecurity, trust and cloud computing providers' performance. Information & Computer Security 29 (5), 816–835.

Kuldeep Singh, PhD, is an assistant professor at the Faculty of Management Studies, Gati Shakti Vishwavidyalaya, Vadodara, India. His research area is Financial Management and Corporate Social Responsibility (CSR). He obtained his Doctorate in Finance from the Indian Institute of Information Technology, Allahabad, India, in 2022. In recognition of his scholarly work, he was honoured with the Best Paper Award at the 6th Management Doctoral Colloquium, IIT Kharagpur in 2020. Dr Singh has also contributed to the academic community by publishing several research papers in renowned journals and publishers. Furthermore, he has presented his research findings at esteemed international conferences such as IEEE and the Academy of Management (AOM).

Sheshadri Chatterjee, PhD, is a post-doctoral research scholar at Indian Institute of Technology Kharagpur, India. He has completed PhD from Indian Institute of Technology Delhi, India. He is having work experience in different multinational organizations such as Microsoft Corporation, Hewlett Packard Company, IBM and so on. Sheshadri has published research articles in several reputed journals such as Government Information Quarterly, Information Technology & People, Journal of Digital Policy, Regulation and Governance and so on. Sheshadri is also a certified project management professional, PMP from Project Management Institute (PMI), USA and completed PRINCE2, OGC, UK and ITIL v3 UK.

Marcello Mariani, PhD, is a Professor of Management at the University of Reading (UK) and University of Bologna (Italy), member of the Henley Center for Entrepreneurship, the Academy of Management and the European Institute for Advanced Studies in Management. His current research interests include the drivers and consequences of the adoption of digital technologies (e.g., big data and analytics, Artificial Intelligence, robots, AVR, IoT) by firms and consumers, as well as a wide range of topics and issues in the strategic management, innovation management, entrepreneurship, and marketing fields. He has authored more than 200 publications also in leading journals such as the *Academy of Management Journal*, *Harvard Business Review, MIT Sloan Management Review, Industrial and Corporate Change, Journal of Business Research, Long Range Planning, Technovation,* and more.

Samuel Fosso Wamba, PhD, is Associate Dean for Research at TBS Education, France, and a Distinguished Visiting Professor at The University of Johannesburg, South Africa. He earned his Ph.D. in industrial engineering at the Polytechnic School of Montreal, Canada. His current research focuses on the business value of information technology, blockchain, artificial intelligence for business, business analytics, and big data. He is among the 2% of the most influential scholars globally based on the Mendeley database that includes 100,000 top scientists for 2020, 2021 and 2022. He ranks in Clarivate Analytics' Highly Cited Researchers List, which consists of the top 1% of the "world's most impactful scientific researchers," for 2020, 2021 and 2022, and in CDO Magazine's Leading Academic Data Leaders 2021. ORCID: 0000-0002-1073–058X