Jurnal of Policy
Vol. 17, No. 1, June 2026 Page 1-16
P-ISSN 1979-0546

Jurnal of Policy

URL: *https://journal.uns.ac.id/policy*

Cybersecurity and Legal Models for Business Resilience: A Comparative Analysis of Singapore and Neighboring South Asian Nations

Tahira Attia Fariha[1*]; Mohammad Belayet Hossain[2]
[1]Fakultas Hukum, Universitas Sebelas Maret, Surakarta, Indonesia
[2]Faculty of Business, Curtin University, Sarawak, Malaysia
Email: tahira@student.uns.ac.id; belayet.hossain@curtin.edu.my

Keywords:
Business Resilience; Cybersecurity Laws; Legal Frameworks; Sustainable Development; South Asia

ABSTRACT

As digital transformation continues to reshape the global economy, legal frameworks become the essential drivers of corporate digital resilience. This paper presents a comparative legal analysis between Singapore's strong and proactive cybersecurity laws and the fragmanted legal systems of South Asian countries (Bangladesh, India, Maldives and Bhutan). This study finds that while Singapore focuses on prevention, cooperation and clear procedures for responding to cyber attacks, many South Asian countries rely on criminal liability after the cyber attacks have occurred. As a result of weak coordination between laws, shortage of skilled professionals in this field and absence of separate legal requirements for SMEs, the increase of cyber attacks increases across South Asia. Through a comparative socio-legal approach, this paper recommends establishing national SME Cyber Resilience Centers, improving regional cooperation through common SAARC cybersecurity standards, and adapting key features of Singapore's structured cybersecurity response model to strengthen cyber resilience across the region.

INTRODUCTION

The accelerated digital transformation of the twenty-first century has intricately linked global economic stability to digital infrastructure. Consequently, cybercrime, ransomware, and state-sponsored cyber operations now pose significant threats to national economies and business continuity (Klimburg, 2012; Maurer, 2018). The economic consequences are substantial: global cybercrime costs were estimated at USD 8 trillion in 2023 and are projected to reach USD 10.5 trillion annually by 2025 (Morgan, 2022). In emerging digital economies, particularly in South Asia, these threats are intensified by fragmented legal frameworks, limited institutional capacity, under-resourced enforcement agencies, and persistent digital skills shortages (Kshetri, 2019). As a result, effective cybersecurity legislation has become a critical component of business resilience and sustainable economic development. Research demonstrates that legal and regulatory frameworks significantly influence organizational cybersecurity investments by shaping liability, compliance obligations, and risk management practices (Böhme et al., 2017).

Among Asian jurisdictions, Singapore has emerged as a global benchmark for cybersecurity governance. Administered by the Cyber Security Agency of Singapore (CSA), the Cybersecurity Act 2018 established a comprehensive regulatory framework for critical information infrastructure (CII) protection, cybersecurity service provider licensing, and incident reporting. This framework is reinforced by the National Cybersecurity Strategy

2021, which seeks to create a secure and trusted digital environment that supports economic growth and innovation (CSA, 2021). Singapore's success is further attributed to its multi-stakeholder governance model, which promotes cooperation among government agencies, private enterprises, and academic institutions while supporting workforce development and business cybersecurity preparedness through initiatives such as SG Cyber Safe and the Cybersecurity Associates and Technologists (CSAT) programme (Ang et al., 2020).

In contrast, the cybersecurity legal landscapes of South Asian countries remain uneven and continue to face substantial regulatory and institutional challenges. India, despite possessing one of the world's largest digital economies, continues to confront difficulties relating to regulatory coordination, critical infrastructure protection, and implementation despite advances under the Information Technology Act and the Digital Personal Data Protection Act 2023 (Javed & Shah, 2021). Bangladesh has recently enacted the Cyber Security Act 2023 to replace the controversial Digital Security Act 2018, yet concerns remain regarding enforcement effectiveness and support for private-sector cybersecurity compliance (Islam, 2022). Similarly, Maldives and Bhutan have undertaken important legislative reforms but continue to face constraints arising from limited technical expertise, institutional capacity, and resource availability.

Against this backdrop, this study examines the widening gap between Singapore's advanced cybersecurity governance model and the developing legal frameworks of Bangladesh, India, Maldives, and Bhutan. The research seeks to answer three key questions: (1) how the cybersecurity legal frameworks of these jurisdictions compare in terms of structural design, regulatory scope, and enforcement capacity; (2) what legal gaps, regulatory shortcomings, and implementation challenges most significantly hinder business resilience, particularly for small and medium-sized enterprises (SMEs); and (3) what context-sensitive legal reforms and public–private partnership mechanisms, informed by Singapore's experience and international best practices, can strengthen cybersecurity governance in South Asia. To address these questions, the study undertakes a systematic comparative analysis of the selected jurisdictions against international standards, identifies key legal and institutional deficiencies affecting cyber resilience, and develops evidence-based recommendations for legal reform and institutional capacity building. By doing so, the research contributes to ongoing discussions on cybersecurity governance and offers practical pathways for strengthening business resilience and supporting a secure, sustainable digital economy in South Asia.

METHOD

This study uses a qualitative comparative legal research method to examine and compare cybersecurity laws and policies in Singapore, Bangladesh, India, Maldives, and Bhutan. The research focuses not only on the content of the laws but also on how they are applied in practice and how they contribute to business resilience against cyber threats. The methodology combines three approaches: legal analysis, case study analysis, and policy review. The legal analysis examines major cybersecurity, data protection, and digital governance laws in the selected countries. The case study analysis evaluates six significant cybersecurity incidents, including the Bangladesh Bank Cyber Heist, the WannaCry ransomware attack in India, the SingHealth data breach in Singapore, cybersecurity challenges in the Maldives' tourism sector, Bhutan's e-government initiatives, and cyber risks in Bangladesh's garment supply chain. The study relies on primary sources such as laws, regulations, government policies, and official guidelines, as well as secondary sources including academic articles, reports from international organizations, and industry publications. The comparison uses five core functions of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST, 2018). It is a voluntary framework issued by the United States' NIST first in 2014 and then used widely

internationally as a common language for managing cyber risk. Its five functions are: Identify (understanding assets and risks), Protect (safeguards and compliance duties), Detect (monitoring and reporting), Respond (incident response and investigation) and Recover (restoration and learning). The framework was chosen because it focuses on outcomes rather than the laws of a particular country. This makes it possible to compare countries with different levels of cybersecurity development using the same standard. Each legal framework and case study is therefore assessed according to these five functions to identify its main strengths and weaknesses. The study also considers international cybersecurity standards to support the analysis. Although every effort has been made to ensure accuracy, the research is limited by the rapid changes in cybersecurity laws, the availability of public information on enforcement practices, and challenges in interpreting some legal documents from different jurisdictions.

The six case studies were purposively selected using four criteria: (1) each country is represented by at least one case; (2) the cases cover important sectors such as finance, health, tourism, e-government, and manufacturing; (3) they show how legal strengths or gaps affect business resilience, including SMEs; and (4) reliable public evidence is available.

The cases include three specific incidents: Bangladesh Bank, WannaCry in India, and SingHealth in Singapore and three sector-level studies on recurring vulnerabilities in Maldives tourism, Bhutan e-government, and the Bangladesh garment sector. SingHealth is used as the benchmark for comparison. Each case is examined in four steps: (i) the legal and regulatory context; (ii) the impact on businesses; (iii) the legal strengths or gaps using the five NIST functions; and (iv) the relevant dimension in Table 1. Because the cases were purposively selected, the findings identify patterns and illustrate the effects of legal design rather than provide statistically representative results. This is recognised as a limitation.

Literature Review

The theoretical literature on cybersecurity governance has shifted from purely technical focuses toward a holistic integration of legal, institutional, and political-economic factors. Nye (2011) established a foundational framework for analyzing cybersecurity through power and interdependence, while Mueller (2010) situated national frameworks within broader digital infrastructure governance. Klimburg (2012) further defined "national cyber power" as a composite of technical, regulatory, and diplomatic capabilities, arguing that legal frameworks are constitutive components of state power. This shift has informed research by Deibert (2015) on norms and Maurer (2018) on the political economy of cyber operations.

Economic perspectives underscore the necessity of regulatory intervention; Böhme et al. (2017) demonstrated that imprecise liability regimes in South Asia under-incentivize security investment, creating market failures. Comparative studies, such as Gercke (2012), highlight significant divergence in legislative maturity linked to digital development, while Chander and Lê (2015) and Winn and Govern (2009) have documented structural weaknesses and compliance challenges across Asian jurisdictions, including imprecise offense definitions and inadequate evidence provisions.

Regionally, scholarship is polarized between surveillance-heavy legislative models and proactive governance. Islam (2022) identified tensions in Bangladesh's Digital Security Act 2018 regarding constitutional rights, while Javed and Shah (2021) noted common failures in incident response frameworks across India and Pakistan. Conversely, Greenleaf (2019) characterized Singapore's approach as a "middle ground" balancing commercial utility with privacy, a model complemented by the CSA's centralized coordination (Ang et al., 2020).

Resilience; distinct from mere security has emerged as a central concern. The World Economic Forum (2022) defines it as the capacity to anticipate, withstand, and

recover from disruption. Linkov and Kott (2019) emphasize that effective legal frameworks must address both "robustness" (withstanding attack) and "resilience" (adaptation and recovery), noting that many existing laws focus disproportionately on punitive prevention. Bada and Nurse (2019) highlight that complex regulations often create a "compliance burden" that leads SMEs to defer security investment, inadvertently increasing systemic risk.

The debate on data protection further reveals a tension between digital trust and innovation. Schwartz and Solove (2014) argue that strong laws are prerequisites for digital trust, yet Chiriță (2018) warns that overly prescriptive regimes can dampen innovation. Recent analyses of India's Digital Personal Data Protection Act 2023 reflect this struggle, balancing global market integration with government data exceptions and cross-border restrictions (Bhatia and Jhunjhunwala, 2023).

Finally, while international best practices provided by the ITU (2018) and norms from the UNGGE/OEWG (UN, 2021) offer benchmarks, their application remains fraught. Standards like ISO/IEC 27001 and the NIST Cybersecurity Framework (NIST, 2018) are increasingly referenced, but Kshetri (2019) cautions that adopting these without local adaptation creates implementation gaps in resource-constrained jurisdictions. This is relevant to the study in two ways. First, the NIST Cybersecurity Framework is used as an analytical lens, not a model to copy because it may be difficult to apply unchanged in low-resource settings (Kshetri, 2019). Second, Singapore's model is examined critically rather than simply recommended for adoption.

Despite these contributions, the literature remains siloed. Research frequently treats "cybersecurity law" as a monolithic deterrent rather than a dynamic driver of corporate governance. There is a critical lacuna in linking doctrinal legal findings to a functional analysis of business resilience across diverse economic maturity levels. This paper addresses this gap in three parts. First, existing studies focus on cybersecurity law as doctrine and deterrence (Gercke, 2012; Islam, 2022) but rarely examine its effects on businesses. This study therefore combines legal analysis with business-focused case studies. Second, SME research highlights compliance burdens (Bada & Nurse, 2019; Chiriță, 2018) but rarely connects them to comparative legal analysis; this study addresses this through SME-related cases. Third, comparative studies often examine jurisdictions with similar levels of development (Gercke, 2012; Winn & Govern, 2009), whereas this study compares jurisdictions at different levels of maturity using functional comparative law (Michaels, 2006; Zweigert & Kötz, 1998). The five NIST functions provide the common framework, with Singapore as the benchmark because of its advanced cybersecurity system (Greenleaf, 2019; Ang et al., 2020).

Results and Discussion

Comparative Analysis of Cybersecurity Legal Frameworks

The cybersecurity legal frameworks of Singapore, Bangladesh, India, Maldives, and Bhutan demonstrate varying levels of legal maturity, institutional capacity, and regulatory effectiveness. Among the jurisdictions examined, Singapore possesses the most comprehensive and advanced cybersecurity governance regime, while the South Asian countries continue to face significant challenges in institutional coordination, critical infrastructure protection, incident reporting, data governance, and support for private-sector cybersecurity resilience.

Singapore's Cybersecurity Act 2018 is widely regarded as a model cybersecurity statute due to its centralized governance structure and risk-based regulatory approach. The Cyber Security Agency (CSA) serves as the single authoritative body responsible for cybersecurity governance, enabling clear accountability, effective policy implementation, and strong coordination among government agencies, critical infrastructure operators, and private-sector stakeholders (Ang et al., 2020). The Act focuses heavily on the

protection of Critical Information Infrastructure (CII), covering eleven designated sectors, including government, healthcare, banking, energy, and transportation. CII owners are subject to extensive legal obligations, including compliance with codes of practice, regular audits and risk assessments, mandatory incident reporting, and participation in national cybersecurity exercises (CSA, 2018). Singapore also regulates cybersecurity service providers through a licensing regime for penetration testing and managed security operations centre services, thereby addressing third-party cybersecurity risks. Enforcement mechanisms are robust, combining criminal sanctions, administrative penalties, and civil enforcement powers.

In contrast, Bangladesh's Cyber Security Act 2023 (CSA 2023) represents an important legislative step but remains relatively underdeveloped in comparison to Singapore's framework. Enacted following criticism of the Digital Security Act 2018, the legislation criminalizes unauthorized access, data theft, manipulation of information systems, and cyberterrorism while establishing the Digital Security Agency (DSA) as the principal regulatory authority. However, cybersecurity governance in Bangladesh remains institutionally fragmented, with responsibilities shared among the DSA, the Bangladesh Telecommunication Regulatory Commission, Bangladesh Bank, and law enforcement agencies. This fragmentation creates coordination challenges and regulatory overlap. Although the Act introduces the concept of critical information infrastructure, it lacks detailed designation criteria, sector-specific obligations, and systematic review mechanisms necessary for effective implementation. Furthermore, the Act provides limited guidance on minimum cybersecurity standards, supply-chain security, cloud computing protection, and incident response planning for businesses, particularly small and medium-sized enterprises (SMEs).

India possesses the most complex cybersecurity framework among the South Asian jurisdictions. The Information Technology Act 2000 (amended in 2008) remains the foundational legislation governing cybercrime, electronic transactions, and information security. Section 43A imposes liability on organizations that fail to implement reasonable security practices, while Section 70B establishes the Computer Emergency Response Team-India (CERT-In), a central component of India's cyber incident response architecture. The enactment of the Digital Personal Data Protection Act 2023 (DPDPA) significantly strengthened India's data governance framework by introducing obligations relating to purpose limitation, data minimization, storage limitation, and security safeguards. The Act also created the Data Protection Board of India to oversee compliance. Nevertheless, concerns remain regarding broad government exemptions, restrictions on cross-border data transfers, and regulatory uncertainty arising from extensive delegated legislative powers. Institutionally, India's cybersecurity governance structure involves multiple entities, including CERT-In, the Ministry of Electronics and Information Technology, the National Critical Information Infrastructure Protection Centre (NCIIPC), sector-specific regulators, and the Data Protection Board, resulting in a complex and sometimes overlapping regulatory environment (Javed & Shah, 2021).

The Maldives and Bhutan have made important legislative advances but continue to face capacity-related constraints. The Maldives' Computer Crimes Act 2015 primarily focuses on criminalizing unauthorized access and data interference rather than establishing a comprehensive cybersecurity governance framework. While the Communications Authority of Maldives has issued sector-specific cybersecurity guidelines for banking and tourism, these remain non-binding and therefore have limited practical impact. Similarly, the Maldives National University Cybersecurity Framework (2021) contributes to capacity building but is constrained by a shortage of qualified cybersecurity professionals.

Bhutan's Cybersecurity Act 2023 represents a more recent effort to establish a modern cybersecurity governance framework. The Act created the Bhutan Computer

Incident Response Team (BtCIRT) as the national authority for cyber incident coordination and introduced reporting obligations for designated critical infrastructure operators. Notably, Bhutan places considerable emphasis on international cooperation, recognizing the transnational nature of cyber threats. However, private-sector cybersecurity obligations remain limited, and the effectiveness of BtCIRT is constrained by shortages in technical expertise and institutional resources.

A key area of divergence among the jurisdictions concerns critical information infrastructure protection. Singapore's CII regime is the most sophisticated, employing a risk-based designation process supported by legally enforceable obligations, regular audits, and meaningful penalties. India's NCIIPC oversees protection of critical infrastructure across six designated sectors, but its enforcement authority over non-government operators is comparatively limited. Bangladesh, Bhutan, and the Maldives have introduced initial CII-related provisions but lack the detailed regulatory mechanisms and enforcement capacity necessary to operationalize effective protection.

Cyber incident reporting frameworks reveal similar disparities. Singapore maintains one of the most comprehensive systems globally, requiring reporting of serious CII incidents within as little as two hours (CSA, 2018). India has strengthened incident reporting through CERT-In's 2022 Directions, which mandate reporting within six hours of discovering specified cyber incidents, although these requirements have been criticized for imposing substantial compliance burdens on organizations (Bhatia & Jhunjhunwala, 2023). Bangladesh's reporting provisions remain vague, lacking clear reporting thresholds and timelines. The Maldives and Bhutan operate basic reporting mechanisms through their national incident response teams but have not yet developed comprehensive frameworks for private-sector engagement.

Data protection regulation further highlights the gap between Singapore and the South Asian jurisdictions. Singapore's Personal Data Protection Act (PDPA), particularly following its 2021 amendments, incorporates mandatory breach notification requirements, stronger enforcement powers, and higher financial penalties, bringing it closer to international standards such as the GDPR (Greenleaf, 2019; PDPC, 2021). India's DPDPA 2023 similarly represents a significant advancement, although implementation remains ongoing. By contrast, Bangladesh, Bhutan, and the Maldives lack comprehensive personal data protection legislation, leaving substantial gaps in privacy protection and data governance (Schwartz & Solove, 2014).

Finally, support for SMEs remains a major differentiating factor. Singapore has implemented several targeted initiatives, including the Chief Information Security Officer-as-a-Service (CISOaaS) scheme, the Data Protection Essentials Programme, and the Cybersecurity Essentials Mark certification, all designed to provide affordable cybersecurity assistance to smaller businesses (CSA, 2021). Comparable initiatives are largely absent in Bangladesh, India, Bhutan, and the Maldives, where SMEs often face disproportionate compliance burdens due to limited technical expertise and financial resources (Bada & Nurse, 2019). Consequently, while Singapore presents a mature and integrated cybersecurity governance model, the South Asian jurisdictions continue to face significant challenges in strengthening institutional capacity, regulatory coherence, data protection, and business cyber resilience.

In conclusion, while South Asian nations have accelerated legislative progress, a persistent "resilience gap" remains between their emerging regimes and Singapore’s mature, centralized ecosystem. Singapore successfully transforms cybersecurity into a strategic economic asset through proactive, risk-prioritized oversight and tiered SME support, whereas South Asian frameworks often suffer from institutional fragmentation, vague compliance mandates, and a disproportionate burden on smaller businesses. Ultimately, the functional efficacy of these legal regimes depends less on the passage of statutes and more on sustained investment in technical human capital, public-private

collaboration, and simplified pathways for business compliance, all of which are essential to cultivate the digital trust required for sustainable economic growth.

Table 1: Comparative Assessment of Cybersecurity Legal Frameworks

Dimension	**Singapore**	**Bangladesh**	**India**	**Maldives**	**Bhutan**
Regulatory Architecture	Centralised; CSA as sole authority	Fragmented; DSA, BTRC, BB	Fragmented; CERT-In, NCIIPC, MeitY, TRAI	Limited; CAM as focal point	Emerging; BtCIRT established
CII Protection Scope	11 designated sectors; systematic	Introduced but vague; no designation process	6 sectors via NCIIPC; limited private-sector reach	Nascent; no formal designation	Introduced; designation criteria absent
Incident Reporting	Mandatory; 2-hr window for CII	Vague; no mandatory timeframe	Mandatory; 6-hr window (CERT-In 2022)	Voluntary; no statutory obligation	Basic; limited private sector scope
Data Protection Law	PDPA 2012 (amended 2021); mature	No standalone law; scattered provisions	DPDPA 2023; implementing rules pending	Electronic Transactions Act only	No standalone law
SME Support Programs	CISOaaS; Cyber Essentials Mark; subsidies	None dedicated	Limited; no national SME cyber program	None	None
Licensing of Cyber Services	Yes; two licensable service classes	No	No	No	No
Enforcement Sanctions	Fines up to SGD 250,000; imprisonment	Fines and imprisonment; limited enforcement	Fines under IT Act; moderate enforcement	Minimal; limited enforcement capacity	Minimal; limited enforcement capacity
Public-Private Partnership	Structured; SG Cyber Safe, ISAC	Absent; informal arrangements only	Nascent; sector-level only	Absent	Absent
International Cooperation	Bilateral agreements; ASEAN framework	Limited bilateral treaties	Bilateral agreements; UNGGE participation	CAM regional engagement	Explicitly provided in 2023 Act
Digital Literacy Programs	Comprehensive; national campaigns	Limited; ad hoc initiatives	Growing; DigiLocker, PMGDISHA	Tourism sector focus only	Integrated into e-government

Dimension	Singapore	Bangladesh	India	Maldives	Bhutan
					plan
Cloud Security Provisions	Yes; covered under codes of practice	Absent	Partial; CERT-In directions apply	Absent	Absent
Overall Maturity Rating	Strong	Developing	Moderate	Nascent	Nascent

Table 1 synthesizes the comparative assessment and provides an explicit mapping between each regulatory gap and its supporting case study evidence. The 'Key Case Evidence' row identifies the specific case study that most directly illustrates each country's performance on the assessed dimensions. This table should be read in conjunction with the Case Study (CS) analysis: Bangladesh's 'Developing' ratings across CII protection, incident reporting, and SME support are given empirical substance by CS1 (Bangladesh Bank Cyber Heist) and CS6 (Garment Industry Supply Chain), which demonstrate the concrete business harms flowing from these regulatory gaps. India's 'Moderate' ratings on incident reporting and enforcement are grounded in CS2 (WannaCry, Indian SMEs), showing the limitations of the existing framework in protecting small businesses from preventable attacks. Singapore's 'Strong' rating across all dimensions is validated by CS3 (SingHealth Data Breach), which demonstrates the framework's capacity to produce structured accountability and systemic improvement following a major incident. For Maldives and Bhutan, the 'Nascent' ratings are evidenced by CS4 (Maldives Tourism) and CS5 (Bhutan E-Government) respectively, which show digital economic activity proceeding at scale in the absence of the legal protections that the table identifies as absent.

Case Study Analysis

The Bangladesh Bank Cyber Heist (2016)

In February 2016, hackers subsequently attributed by US investigators to the North Korean Lazarus Group compromised the SWIFT messaging credentials of Bangladesh Bank and fraudulently transferred approximately USD 81 million from its Federal Reserve Bank of New York account to accounts in the Philippines and Sri Lanka (Maurer, 2018). The attack remains one of the largest and most consequential financial cyber heists in history.

At the time of the attack, Bangladesh's cybersecurity legal framework was rudimentary. The ICT Act 2006 contained provisions relating to unauthorized computer access, but it lacked specific mandatory security standards for financial institutions, mandatory incident reporting obligations, and a coordinated national incident response architecture capable of mounting a rapid response to a sophisticated state-sponsored attack. The discovery of the breach was delayed by several days, and the full extent of the loss was only established through the involvement of international partners including the US Federal Bureau of Investigation. The direct financial loss of USD 81 million represented approximately 6% of Bangladesh's foreign exchange reserves at the time (Maurer, 2018). Beyond the immediate financial loss, the breach caused lasting reputational damage to

Bangladesh's financial sector, raised serious questions about the safety of international correspondent banking relationships, and triggered a prolonged and costly international legal dispute over the recovery of the stolen funds. The case starkly illustrates the consequences of the absence of mandatory minimum cybersecurity standards for critical financial infrastructure.

The Bangladesh Bank case study demonstrates three critical legal deficiencies: the absence of minimum security standards for critical financial infrastructure; the lack of a structured incident reporting and response framework capable of enabling a rapid coordinated national response; and the inadequacy of the existing criminal justice framework for investigating and prosecuting sophisticated, state-sponsored cybercrime. These deficiencies have not been fully remedied by the CSA 2023, which does not contain sector-specific security standards for the financial sector.

WannaCry Ransomware Attack - Impact on Indian SMEs (2017)

The WannaCry ransomware attack of May 2017 exploited a vulnerability in Microsoft Windows operating systems, infecting an estimated 300,000 computers across 150 countries within hours of its initial deployment. India was one of the most severely affected countries, with estimates suggesting that over 100 organizations were significantly impacted, with SMEs in manufacturing, logistics, and retail sectors bearing the heaviest burden (Javed, M., & Shah, S. 2021).

India's IT Act 2000, as amended, contained provisions requiring corporate bodies to implement 'reasonable security practices and procedures,' but the absence of specific, operational minimum security standards and the absence of any legal requirement to maintain current software patching meant that many affected SMEs had no clear legal obligation to implement the basic security measures that would have prevented infection. CERT-In issued an alert about the vulnerability exploited by WannaCry some weeks before the attack, but the non-mandatory nature of CERT-In's communications to the private sector significantly limited uptake (Government of India, 2008). The attack caused severe operational disruptions to affected Indian SMEs, with estimated costs including system recovery expenses, lost productivity, and, in some cases, permanent loss of unrecoverable data. For businesses in just-in-time manufacturing supply chains, even short operational disruptions caused cascading losses throughout the supply chain. The absence of business interruption insurance coverage for cyber incidents among the majority of affected SMEs meant that the full cost of recovery fell directly on the businesses themselves.

WannaCry exposed three systemic legal and regulatory deficiencies: the inadequacy of the 'reasonable security practices' standard in the IT Act as a driver of concrete security investment by SMEs; the absence of mandatory information sharing mechanisms that could have ensured timely dissemination of CERT-In's pre-attack vulnerability alerts to small businesses; and the lack of a coordinated legal framework for business continuity planning that could have reduced the operational impact of the attack. The CERT-In Directions of 2022 have addressed some of these gaps, but significant deficiencies remain, particularly in relation to SME-specific guidance (Bhatia & Jhunjhunwala, 2023).

Singapore's Response to the SingHealth Data Breach (2018)

In June and July 2018, attackers subsequently linked by government investigators to a state-sponsored advanced persistent threat actor accessed the database of Singapore's largest public healthcare group, SingHealth, and exfiltrated the personal data and outpatient medication records of approximately 1.5 million patients, including Prime Minister Lee Hsien Loong (CSA, 2021). The breach was detected by IHiS, the public health sector IT agency, and reported to the CSA and Ministry of Health in accordance with mandatory incident reporting obligations.

The legal and regulatory response to the SingHealth breach illustrates the operational effectiveness of Singapore's mature cybersecurity legal framework. Following the mandatory incident report, the CSA conducted a comprehensive investigation under its statutory investigation powers. The Personal Data Protection Commission (PDPC) conducted a parallel investigation under the PDPA and, in January 2019, issued findings and directions that imposed financial penalties of SGD 750,000 on IHiS and SGD 250,000 on SingHealth for failures to implement adequate security arrangements (PDPC, 2021).

The SingHealth case study provides a benchmark of how a mature legal and institutional framework enables a rapid, structured, and proportionate response to a major cybersecurity incident. The legally mandated response process resulted in: comprehensive public disclosure to affected patients; a thorough independent review (the COI Report) that identified both technical and governance failures; meaningful accountability through financial sanctions on the responsible organizations; and a comprehensive set of systemic improvements to the governance of health sector cybersecurity, including enhanced security requirements for all public health sector entities.

The SingHealth case demonstrates that the value of a robust cybersecurity legal framework lies not only in deterrence but in its structuring function: by providing clear legal authority, mandatory reporting obligations, and defined investigative and remediation processes, the framework enabled a coordinated, multi-agency response that produced both accountability and systemic improvement. This structuring function is absent from the cybersecurity legal frameworks of the South Asian nations under study.

The SingHealth model cannot be directly copied in Bangladesh and Bhutan because they have fewer institutional and technical resources. However, its basic structure like clear legal authority, mandatory reporting, defined investigation and proportionate accountability can be adapted.

A phased approach is recommended: (1) begin with high-risk sectors, such as finance and garments in Bangladesh and e-government in Bhutan; (2) require simple, time-bound reporting to one designated body, with clear agency roles; (3) use standardised post-incident reviews and proportionate penalties, with guidance and corrective measures for SMEs; (4) strengthen capacity through public-private partnerships, donor support, and cooperation with advanced CERTs; and (5) review and expand the system as capacity grows.

Bhutan could benefit from shared or regional response services, while Bangladesh could use sector-specific rules and SME support. These are proposed adaptations and should be tested against each country's resources and administrative capacity.

Maldives Tourism Sector Cyber Vulnerabilities (2019–2022)

Tourism contributes approximately 25–30% of GDP and over 60% of foreign exchange earnings to the Maldivian economy, with the sector highly digitally integrated through online booking platforms, property management systems, payment processing infrastructure, and guest-facing digital services. The COVID-19 pandemic period (2019–2022) accelerated digital transformation in the sector, with resorts and hotels adopting contactless check-in, digital concierge services, and automated revenue management systems, significantly expanding their digital attack surfaces.

Multiple cybersecurity incidents affecting Maldivian tourism businesses during this period including ransomware attacks on resort property management systems, phishing campaigns targeting hotel finance departments, and data breaches affecting guest personal and payment data occurred in a legal context in which the Computer Crimes Act 2015 provided only basic criminal offense provisions, with no specific sector security standards, mandatory incident reporting obligations, or legal framework for business continuity planning.

The absence of a sector-specific cybersecurity regulatory framework for tourism has had several adverse consequences for business resilience: affected businesses have faced significant financial losses from ransomware payments and system recovery costs; breaches of guest personal and payment data have created legal liability exposure under the laws of guests' home countries, particularly GDPR for European visitors; and the absence of mandatory incident reporting has prevented the development of a national picture of cyber risk in the sector that could inform proportionate regulatory intervention (Kshetri, 2019).

The Maldives tourism case study highlights the particular vulnerability of small island developing states whose economies are concentrated in a single digitally dependent sector. The absence of sector-specific cybersecurity standards, mandatory incident reporting, and legal frameworks for business continuity planning creates systemic risks not only for individual businesses but for the broader national economy.

Bhutan's E-Government Initiative and Cyber Risks (2020–2023)

Bhutan's ambitious e-government development program, accelerated during the COVID-19 pandemic, has digitized a broad range of government services including tax administration, business registration, land records management, and social welfare delivery. This digital transformation has significantly expanded the government's digital attack surface while simultaneously creating dependencies on digital infrastructure that create new risks for business operations and continuity.

Bhutan's Cybersecurity Act 2023 was enacted in part to provide a legal foundation for the secure development of e-government services. However, the Act's implementing regulations including the sector-specific security standards and mandatory incident reporting frameworks remain under development. In the absence of these implementing measures, e-government systems have been deployed without clear mandatory security requirements, creating vulnerabilities that have been exploited in several documented incidents (Government of Bhutan, 2023).

The cybersecurity vulnerabilities of e-government systems create direct risks for businesses that have integrated their operations with government digital services. Disruption to tax administration systems, business registration portals, or customs management systems can have immediate operational impacts on businesses, while breaches of government-held business data can expose confidential commercial information.

The Bhutan case study illustrates the risks of digital government transformation that outpaces the development of the legal and institutional frameworks necessary to secure it. The existence of a modern cybersecurity statute provides an essential foundation, but without implementing regulations, institutional capacity, and the integration of security-by-design requirements into e-government procurement, the Act's provisions remain aspirational.

Bangladesh Garment Industry Supply Chain Cyber Risks (2021–2023)

Bangladesh's ready-made garment (RMG) sector is the world's second-largest apparel exporter, accounting for approximately 84% of Bangladesh's total export earnings and employing over 4 million workers. The sector is increasingly digitally integrated, with factory management systems, inventory platforms, and enterprise resource planning systems connected to the procurement systems of international brands and retailers through complex supply chain digital interfaces.

Multiple cybersecurity incidents affecting Bangladeshi garment manufacturers during 2021–2023 including ransomware attacks on factory management systems, business email compromise fraud targeting procurement departments, and unauthorized access to production schedule and pricing data occurred in a legal context offering no

specific cybersecurity standards for the sector, no mandatory incident reporting obligations for non-financial sector businesses, and no legal framework for the security of supply chain digital interfaces (Islam, 2022).

The cybersecurity vulnerabilities of RMG sector businesses have had several adverse consequences for business resilience: operational disruptions caused by ransomware attacks have resulted in missed production deadlines with significant financial penalties; business email compromise fraud has caused direct financial losses estimated in millions of dollars across the sector; and unauthorized access to production pricing data has compromised the commercial position of affected manufacturers in sourcing negotiations with international buyers.

The Bangladesh garment industry case study illustrates the systemic implications of the SME cybersecurity compliance gap for global supply chains. International brands and retailers are increasingly imposing cybersecurity requirements on their supply chain partners as a condition of procurement, reflecting both their own regulatory obligations and the recognition that supply chain cyber vulnerabilities represent a systemic risk to their own operations (WEF, 2022). In the absence of a national legal framework that drives minimum cybersecurity standards across the RMG sector, Bangladeshi manufacturers face the risk of losing market access as international buyers impose their own supply chain security requirements.

Key Findings

1. Singapore as a Mature Proactive Model: Singapore's cybersecurity legal framework stands as a mature, proactive model that treats business resilience and economic competitiveness not merely cybercrime deterrence as its central purpose. Its combination of comprehensive CII protection, structured service licensing, robust incident reporting, coherent institutional architecture, and dedicated SME support programs creates a regulatory environment in which businesses can invest in cybersecurity with clarity and confidence (Ang et al., 2020; CSA, 2021). The SingHealth data breach case study validates this in practice: the legally mandated response produced public disclosure, meaningful organizational accountability, and systemic governance improvements an outcome unachievable under any of the South Asian frameworks examined.

2. Fragmentation and Reactive Orientation in South Asian Frameworks: The South Asian frameworks share a predominantly reactive orientation, prioritizing post-incident criminal punishment over the proactive building of cyber resilience through compliance obligations, capacity building, and public-private partnership (Kshetri, 2019). The Bangladesh Bank cyber heist case study renders this consequential: the absence of mandatory security standards for financial institutions, a structured incident reporting framework, and adequate law enforcement capacity meant the breach's full extent was uncovered only through international intervention, with legal mechanisms wholly inadequate to the scale of harm.

3. The SME Cybersecurity Compliance Gap: All four South Asian jurisdictions consistently lack adequate legal and institutional provisions to support SME cybersecurity compliance (Bada & Nurse, 2019). The WannaCry case study is illustrative: Indian SMEs suffered disproportionate disruption precisely because the regulatory framework offered no accessible minimum security standards, affordable technical assistance, or proportionate liability guidance. The Bangladesh garment industry case study extends this finding to a systemic level - SME cyber weaknesses ripple outward into global supply chains, threatening Bangladesh's market access and international trade reputation.

4. Data Protection Law Gaps and Their Business Implications: The absence of comprehensive personal data protection legislation in Bangladesh, Maldives, and Bhutan generates significant legal uncertainty with compounding business consequences: liability exposure under foreign data protection regimes, barriers to participation in data-transfer-

dependent digital markets, and erosion of the consumer trust on which e-commerce depends (Schwartz & Solove, 2014).

5. Institutional Capacity as the Critical Binding Constraint: Across all four South Asian jurisdictions, inadequate institutional capacity emerges as the single most critical constraint on the real-world effectiveness of cybersecurity legal frameworks (Klimburg, 2012). A modern statute is necessary but not sufficient: without adequately funded, technically capable regulatory and enforcement bodies, legal obligations remain aspirational. The Maldives and Bhutan case studies are particularly instructive both countries' recent legislative advances have produced frameworks that substantially exceed their current institutional capacity to implement.

Recommendations

Based on the findings of this research, the following evidence-based recommendations are advanced by jurisdiction.

Recommendations for Bangladesh

1. **Enact a Standalone Personal Data Protection Act** aligned with international standards, establishing an independent supervisory authority, mandatory breach notification obligations, and workable cross-border data transfer provisions — a foundational prerequisite for Bangladesh's meaningful participation in global digital value chains.
2. **Supplement the Cyber Security Act 2023 with Detailed Implementing Regulations** specifying minimum cybersecurity standards by sector and firm size, mandatory incident reporting timeframes and procedures, and structured public-private information sharing mechanisms to transform the Act's legislative ambitions into operational obligations.
3. **Establish a National Cyber Resilience Centre for SMEs** modeled on Singapore's CyberSG initiative, providing subsidized cybersecurity advisory, training, and certification services through a public-private funding model that makes compliance achievable for businesses with limited technical and financial resources.
4. **Develop Sector-Specific Cybersecurity Frameworks for Financial Services and the RMG Industry**, building on existing Bangladesh Bank cybersecurity guidelines and directly addressing the supply chain security requirements increasingly imposed on garment exporters by international buyers as a condition of procurement.

Recommendations for India

5. **Accelerate Issuance of Implementing Rules under the Digital Personal Data Protection Act 2023**, with particular urgency on workable cross-border data transfer standards, to resolve the regulatory uncertainty currently constraining business compliance planning and India's integration into global data markets.
6. **Strengthen NCIIPC's Statutory Powers, Dedicated Funding, and Enforcement Mandate** to engage with and enforce compliance by private sector critical information infrastructure operators, addressing the current gap between NCIIPC's formal mandate and its practical regulatory reach over non-government CII.
7. **Rationalize the CERT-In 2022 Incident Reporting Directions** by introducing proportionality provisions that calibrate reporting obligations to the severity and scope of incidents, reducing the disproportionate compliance burden on smaller entities while maintaining the national situational awareness value of the reporting system.
8. **Establish a National SME Cybersecurity Program** through the Ministry of Electronics and Information Technology, delivering accessible self-assessment tools, government-subsidized certifications, and sector-specific guidance that makes meaningful cybersecurity compliance achievable for small and medium-sized enterprises.

Recommendations for Maldives

9. **Enact a Comprehensive Standalone Cybersecurity Act** establishing a full framework for CII protection, mandatory incident reporting, and regulatory oversight of cybersecurity service providers moving decisively beyond the crime-focused Computer Crimes Act 2015, which lacks the institutional architecture and compliance framework necessary for systemic cyber resilience.
10. **Develop Sector-Specific Cybersecurity Standards for the Tourism Industry** in close consultation with operators, given the sector's overwhelming contribution to GDP and foreign exchange earnings and its acute and growing digital exposure across booking platforms, payment systems, and guest-facing digital services.
11. **Pursue Regional Cybersecurity Cooperation Arrangements** through the SAARC framework or bilateral agreements with Singapore, securing access to shared technical resources, threat intelligence, and capacity building support that Maldives' small state resources alone cannot sustainably provide.

Recommendations for Bhutan

12. **Develop Implementing Regulations for the Cybersecurity Act 2023 as an Immediate Priority**, informed by neighboring countries' regulatory experiences and supported by international technical assistance, to translate the Act's sound legislative framework into specific, enforceable obligations with clear compliance pathways for regulated entities.
13. **Invest Substantially in BtCIRT Institutional Capacity —** including technical staffing, specialist training, and operational infrastructure — through structured partnerships with more advanced CERT organizations and international development partners, to bring BtCIRT's practical capabilities in line with its statutory mandate.
14. **Integrate Security-by-Design Requirements into All Components of the E-Government Development Program**, embedding mandatory cybersecurity standards into procurement processes and development specifications before new digital government systems are deployed, rather than attempting to retrofit security into systems already in operation.

Regional Recommendations

15. **Develop a SAARC Regional Cybersecurity Cooperation Framework** encompassing structured mechanisms for cyber threat intelligence sharing, coordinated cross-border incident response, harmonization of national legal frameworks to facilitate mutual legal assistance in cybercrime cases, and dedicated capacity building support for the region's less developed member states.
16. **Establish a Formal South Asia–Singapore Cyber Partnership** inviting Singapore to serve as a structured technical and policy partner in South Asian cybersecurity capacity development, building on existing bilateral cooperation arrangements into a multilateral regional engagement model that leverages Singapore's proven governance expertise.
17. **Develop Regional Minimum Cybersecurity Standards for SMEs**, produced collaboratively by the region's development banks and business associations, calibrated to the resource constraints and risk profiles of smaller businesses in emerging digital economies, and designed to provide a practical, achievable, and independently verifiable compliance benchmark.

CONCLUSION

This study highlights significant disparities in the maturity and effectiveness of cybersecurity legal frameworks across Singapore, Bangladesh, India, the Maldives, and Bhutan. The analysis demonstrates that governance weaknesses can lead to substantial

financial losses, operational disruptions, and diminished trust in digital systems. However, recent legislative developments including the 2023 cybersecurity and data protection acts in Bangladesh, India, and Bhutan indicate a growing commitment to strengthening regional cyber governance. Rather than adopting Singapore's model in its entirety, South Asian jurisdictions can adapt core principles such as risk-based critical infrastructure protection, clear incident reporting, and targeted SME support to their specific legal and economic contexts. As digital economies become increasingly interconnected, vulnerabilities in one jurisdiction create risks that transcend borders, threatening regional stability. Therefore, sustained legal reform, effective enforcement, and institutional capacity building remain essential for fostering a secure, resilient, and trustworthy digital ecosystem across South Asia.

REFERENCES

Javed, M., & Shah, S. (2021). Comparative Analysis of Cybersecurity Laws in South Asia. International Journal of Law and Information Technology, 29(3), 215-240.

Ang, J., Lim, D., & Teo, S. (2020). Singapore's cybersecurity governance architecture: Institutional design and emerging challenges. Asian Journal of Public Administration, 42(1), 112-135.

Bada, M., & Nurse, J. R. C. (2019). The social and psychological impact of cyberattacks on SMEs. Computers in Human Behavior, 87, 281-289.

Bhatia, R., & Jhunjhunwala, A. (2023). India's Digital Personal Data Protection Act 2023: A critical analysis. Journal of Information Policy, 13(1), 1-35.

Böhme, R., Schwartz, G., & Chuang, J. (2017). Modeling cyber-insurance: Towards a unifying framework. Proceedings of the 2017 Workshop on the Economics of Information Security (WEIS).

Chiriță, A. D. (2018). Data Protection and Small and Medium-sized Enterprises. European Law Review, 43(4), 540-562.

Chander, A., & Lê, U. P. (2015). Data nationalism. Emory Law Journal, 64(3), 677-739.

Cyber Security Agency of Singapore (CSA). (2018). Cybersecurity Act 2018 (No. 9 of 2018). Government of Singapore.

Cyber Security Agency of Singapore (CSA). (2021). Singapore's National Cybersecurity Strategy 2021. Government of Singapore.

Deibert, R. J. (2015). The geopolitics of cyberspace after Snowden. Current History, 114(768), 9-15.

Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. International Telecommunication Union (ITU).

Government of Bangladesh. (2023). Cyber Security Act 2023. Bangladesh Gazette.

Government of Bhutan. (2023). Cybersecurity Act of Bhutan 2023. Royal Government of Bhutan.

Government of India. (2000). Information Technology Act, 2000 (No. 21 of 2000). Ministry of Law and Justice.

Government of India. (2008). Information Technology (Amendment) Act, 2008. Ministry of Law and Justice.

Government of India. (2023). Digital Personal Data Protection Act, 2023 (No. 22 of 2023). Ministry of Law and Justice.

Government of Maldives. (2015). Computer Crimes Act (Law No. 17/2015). Republic of Maldives.

Greenleaf, G. (2019). Asian data privacy laws: Trade and human rights perspectives. Oxford University Press.

International Telecommunication Union (ITU). (2018). Guide to developing a national cybersecurity strategy: Strategic engagement in cybersecurity. ITU Publications.

Islam, M. R. (2022). Digital Security Act 2018 of Bangladesh: An analysis from constitutional law perspective. Bangladesh Journal of Law, 19(1), 23-56.
Klimburg, A. (Ed.). (2012). National cyber security framework manual. NATO Cooperative Cyber Defence Centre of Excellence.
Kshetri, N. (2019). Cybersecurity and development. Oxford Development Studies, 47(1), 1-14.
Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In A. Kott & I. Linkov (Eds.), Cyber resilience of systems and networks (pp. 1-25). Springer.
Maurer, T. (2018). Cyber mercenaries: The state, hackers, and power. Cambridge University Press.
Michaels, R. (2006). The functional method of comparative law. In M. Reimann & R. Zimmermann (Eds.), The Oxford handbook of comparative law (pp. 339-382). Oxford University Press.
World Economic Forum. (2023). Global Cybersecurity Outlook 2023. World Economic Forum.
Mueller, M. (2010). Networks and states: The global politics of internet governance. MIT Press.
National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity, Version 1.1. NIST.
Nye, J. S. (2011). Nuclear lessons for cyber security? Strategic Studies Quarterly, 5(4), 18-38.
Personal Data Protection Commission (PDPC), Singapore. (2021). Personal Data Protection (Amendment) Act 2020 and advisory guidelines. PDPC.
Schwartz, P. M., & Solove, D. J. (2014). Reconciling personal information in the United States and European Union. California Law Review, 102(4), 877-916.
United Nations (UN). (2021). Report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security. A/75/816. UN General Assembly.
Van Hoecke, M. (2015). Methodology of comparative legal research. Law and Method, December 2015.
Winn, J. K., & Govern, K. H. (2009). Cybercrime in Asia: Trends and challenges. In Cybercrime and society (2nd ed., pp. 150-178). SAGE Publications.
World Economic Forum (WEF). (2022). Global cybersecurity outlook 2022. World Economic Forum.
Zweigert, K., & Kötz, H. (1998). An introduction to comparative law (3rd ed., T. Weir, Trans.). Oxford University Press.