

Chapter 14

The Economics of Cyber Resilience: Shifting from Technical Firewalls to Institutional Risk Management in India

Ayushi Gupta, B. Com, University of Delhi, M. Com Allahabad University

Abstract

Cybersecurity has been historically viewed as a technical problem in India—i.e., firewalls, malware scanners, intrusion detection systems, etc., were thought of as the primary means of defending against cyber threats³³⁰. However, due to the rapid growth of the digital economy (driven by Aadhaar, UPI, Fintech, digitisation and all of the other records of the artificial digital economy), there has come about a need for a shift in perspective regarding Cyber Resiliency. As such, this chapter argues that cyber resiliency should not only be considered a technology-based product but as an economic and institutional necessity³³¹.

This chapter discusses how cyber risk is viewed as an external systemic risk, i.e., a breach at one entity can create cascading impact on multiple entities across financial markets, supply chains, and critical infrastructures³³². The chapter contrasts the extremely high costs for organizations due to data breaches (i.e., downtime, brand damage, regulator penalties, etc.) with comparatively lower investments made by parties to defend against such breaches (i.e., as cyber insurance, redundancy systems, and institutional governance frameworks)³³³. Finally, the chapter discusses specific Cyber Resiliency challenges faced within the Indian economy (e.g., limited resources available to deal with cybersecurity risks, the fact that breaches are frequently unreported, the limited number of skilled cybersecurity professionals available) while highlighting the necessity of developing and incorporating Cyber Resiliency processes and planning into future economic and policy-making initiatives³³⁴.

As the foundation of resilience, Institutional risk management includes board-level accountability, mandatory disclosure norms, and recovery planning. The chapter evaluates regulatory frameworks such as SEBI's Cyber Security and Cyber Resilience Framework (CSCRF)³³⁵, the Reserve Bank of India's (RBI) Banking Guidelines on Cyber Security³³⁶, and the Crisis Management Protocols developed by CERT-In³³⁷. These frameworks are also compared with global models, including the European Union's NIS2 Directive³³⁸ and the NIST Cyber Security Framework developed by the United States government³³⁹.

³³⁰ Palo Alto Networks, *The History of Firewalls* (2024).

³³¹ World Bank, *Cybersecurity as a Systemic Risk to Financial Stability* (2022).

³³² *ibid*

³³³ Ponemon Institute, *Cost of a Data Breach Report 2023* (IBM Security, 2023).

³³⁴ *ibid*

³³⁵ Securities and Exchange Board of India (SEBI), *Cyber Security and Cyber Resilience Framework for Stock Exchanges, Depositories and Clearing Corporations* (2024).

³³⁶ Reserve Bank of India, *Master Directions on Information Technology Governance, Risk, Controls and Assurance Practices* (2023).

³³⁷ Indian Computer Emergency Response Team (CERT-In), *Cyber Crisis Management Plan* (Government of India, 2022).

³³⁸ Directive (EU) 2022/2555 (NIS2 Directive).

³³⁹ National Institute of Standards and Technology (NIST), *Cybersecurity Framework 2.0* (US Department of Commerce, 2024).

The chapter is clear that resilience is not just about eliminating risk; it is about providing the ability to continue, adapt, and maintain trust in India's digital economy. Ultimately, the chapter argues that India must integrate cyber resilience into its governance and financial systems to ensure a future that is digitally enabled. Cybersecurity will be considered an institutional and economic challenge—as opposed to strictly a technical challenge. In doing so, India protects its digital transformation and creates an opportunity to become a global leader in resilient digital governance.

Keywords: *Cyber Resiliency, SEBI's Cyber Security, NIST Cyber Security Framework*

Introduction

In the digital age of India, now cyber resilience has become the most critical concept. It defined as the ability of institution to anticipate, recover from anticipated loss caused by cyber threats. Unlike traditional cybersecurity, which focus on providing protection through technical safeguards such as firewalls, antivirus software, hacks detention system and encryptions, cyber resilience recognizes that cyber-attacks may be occur in any institution in the future. It shifts the focus from solely defending against the cyber-attacks to ensuring continuity of the institutional operation, minimizing the economic losses and help institutional to adapt to an evolving threat ecosystem. In this way, resilience is not limited to technical protection, but it is about institutional capacity, accountability and systematic preparedness to address the anticipated cyber threats³⁴⁰.

The difference between cyber security and cyber resilience is important. Cyber security primarily defensive in nature, aiming to block the unauthorized access and prevent the breaches through technical measures or we can say that traditional method. In contrast, cyber resilience is anticipatory and adaptive in nature, and it believes that no system or method can provide 100% security. Cyber resilience focusing on recovery speed, accountability and ability to absorb cyber shocks without affecting institutional continuity. This shift is very important in the modern digital age where critical infrastructure is digitally and well connected with financial system, supply chain, health care and national security. Therefore, a single cyber-attack can harm not only just one system but multiple interconnected system, leading to serious economic and operational loss³⁴¹.

From an economic point of view, cyber-attacks is not solely a technical problem, but systemic shocks that affect entire economy system. They disturb market, destabilize supply chain, break customer confidence, and impose heavy financial losses on both institution and government sector³⁴².

For Example, cyber-attacks can paralyze hospitals operations, while breaches in financial institutions can decrease the confidence of investors and trigger capital outflow. The economic sees cyber-attacks as an external sock that ripples across the economy, recuring institutional way to mitigate the impact. Cyber resilience is not a luxury but a necessity for safeguarding economic stability and national security for both institutions and the government³⁴³.

³⁴⁰ NIST (n 11)

³⁴¹ World Bank (n 4).

³⁴² OECD, *Digital Security Risk Management for Economic and Social Prosperity* (2015).

³⁴³ World Bank (n4).

As we observe, India is rapidly advancing towards becoming a 'Digital India'; consequently, we have become digitally dependent for a vast array of tasks. The most significant threat arising from this is the risk to our data privacy. We must recognize the gravity of the risk involved in storing all our personal information across numerous applications. This data security challenge cannot be resolved solely through technical measures—such as firewalls and antivirus software as many antivirus programs lack the necessary robustness to effectively shield users from hackers. In fact, many such programs merely create the illusion of providing protection. Furthermore, this is no longer merely a technical issue; it has evolved into a social issue where software alone is insufficient³⁴⁴.

companies are setting aside funds meant for spotting threats before they strike. Not waiting until things go live matters just as much as how money gets spent later. Funds once saved for emergencies now shift toward early warnings and smarter defenses shaped during design phases³⁴⁵.

Right now, India stands deep into a shift toward digital life - fueled fast by tools like Aadhaar, UPI, along with wider access to stock trading. Thanks to these steps, more people can reach banking services while systems run smoother, pushing India ahead on the world tech scene. Yet just beyond that progress comes rising danger: fake messages pretending to be real, tricks played online, money costs growing sharper every month³⁴⁶.

India is getting better at dealing with cyber threats. The Reserve Bank of India has made rules for banks to follow when it comes to cybersecurity. These rules say that banks should think about the risks they face and have plans in place to deal with problems³⁴⁷. The Securities and Exchange Board of India is also working to make the financial markets safer.

The government of India is doing things like making a National Cybersecurity Policy and CERT-In is giving out guidelines to help organizations get ready.

- Even with all these things happening many organizations in India are still relying too much on things like firewalls to keep them safe. They are not paying attention to other important things like making sure they have good leaders and plans to manage risks. Indian organizations need to work to make sure they are safe, from cyber threats. The Reserve Bank of India and the Securities and Exchange Board of India are doing their part. Organizations need to do more to make themselves safe³⁴⁸.

The Traditional Firewall Approach

The way we think about cybersecurity has been about using technical defences like firewalls, antivirus software and intrusion detection systems. These tools started in the 20th century when the main worry was people getting into networks without permission and bad code getting into systems. Firewalls help control traffic between networks we trust and ones we don't. Antivirus programs scan files and application to detect and remove malware from working and Intrusion detection systems watch network activity for suspicious patterns³⁴⁹.

³⁴⁴ Ponemon Institute (n 5).

³⁴⁵ OECD (n 14).

³⁴⁶ National Payments Corporation of India (NPCI), *UPI Annual Report* (2023).

³⁴⁷ RBI (n 8)

³⁴⁸ SEBI (n 7), RBI (n 8)

³⁴⁹ Palo Alto Networks (n2)

This technical defence model assumes that threats come from outside and can be stopped with traditional approaches. The digital world has changed a lot. The rise of cloud computing, mobile devices and connected supply chains the lines around networks are blurry. This has made technical safeguards less effective and exposed institutions to new risks³⁵⁰.

Limitations of the Technical Defence Paradigm

- Insider threats are a problem because they can easily get around the security measures that are in place to protect the organization. This is because people like employees and contractors already have access to the system. They can use this access to do things like leak important information or hurt the computer systems. Firewalls are not very good at stopping these kinds of threats because they cannot tell the difference between what's normal and what is not³⁵¹.

For example, phishing and social engineering attacks are very good at tricking people into doing things that can hurt the organization. These attacks focus on people not on the technology. If someone gets a phishing email that looks real, they might give away their login information. Download something bad. This means that the attackers can get around the security systems that're in place like firewalls and antivirus software. This shows that cybersecurity is not about having the right technology it is also about how people behave³⁵².

- Another problem is supplying chain attacks. These happen when organizations trust outside vendors and service providers much. Many organizations use software and hardware from companies, and they think it is safe. Sometimes attackers can compromise these suppliers and put bad code into their products. When the organization uses these products, they are putting themselves at risk without knowing it. The problem is that these threats come from people the organization trusts so the usual security tools, like firewalls often cannot detect them. Insider threats and supply chain attacks and phishing are all problems that organizations need to worry about³⁵³.

➤ Case Example

2017, computers everywhere began locking up without warning. Because of a hidden flaw in Microsoft Windows, malicious code slipped through like smoke under a door. Instead of stopping it, firewalls stood idle while files vanished behind digital locks. Hospitals in the UK could not access patient records, trains halted, operations got delayed. Over 150 countries watched helplessly as machines froze one after another. Antivirus tools already installed made little difference when faced with something this fast. What looked secure yesterday failed completely by noon. Speed turned weakness into chaos before anyone could react.³⁵⁴ Still firewalls matter but relying completely on it not enough. Antivirus software or traditional approaches not able to detect system hidden danger alone. People make

³⁵⁰ Palo Alto Networks (n2)

³⁵¹ Ajay Biyani, 'Why Insider Threats Are Cybersecurity's Next Big Challenge' *Hindustan Times* (25 September 2024).

³⁵² Cybersecurity and Infrastructure Security Agency (CISA), *Avoiding Social Engineering and Phishing Attacks* (2021).

³⁵³ CrowdStrike, 'What Is a Supply Chain Attack?' (2023).

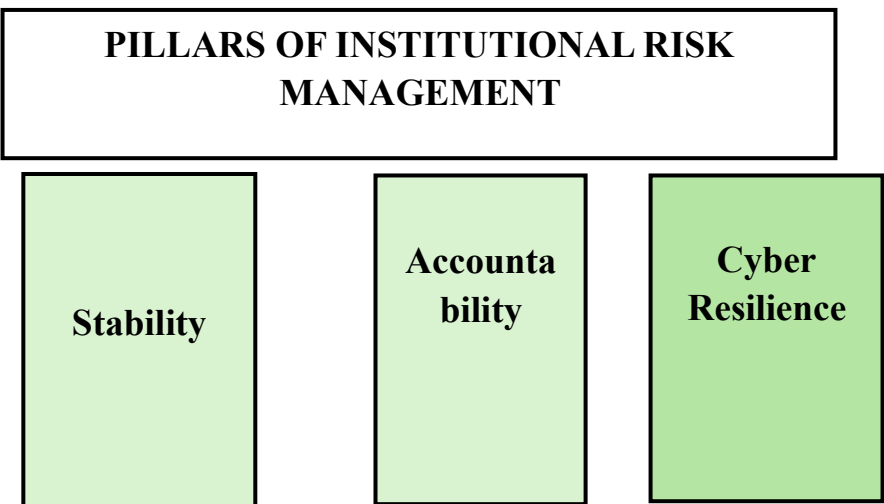
³⁵⁴ Cloudflare, 'What Was the WannaCry Ransomware Attack?' (2017).

mistakes. System gets compromised through suppliers too. WannaCry already showed how fast chaos spreads. all interconnected system gets blocked and not working. Strength comes not from blocking everything but staying upright after a hit. It can be done through proper planning, taking right decision, teaching and training team member on related problem. This builds real resistance³⁵⁵.

Institutional Risk Management: A Paradigm Shift

Institutional risk management in the cyber sphere refer to top level management approach that focus on operational stability, accountability and systematic resilience instead of relying on technical approaches. Traditional approaches mainly focus on preventing attacks through firewall, antivirus security and encryption method. But institutional risk management assume that no system or method can provide 100% security³⁵⁶. Instead on focusing on technical method, this approach gives importance on institution stability through accept it that no system provides overall security, recover the losses and adapt it without compromising with their core functions. It recognises that cyber threats are not just a technical issue anymore, but it becomes systematic challenge. This risk has capacity to destabilise the financial market, digital payment system and critical interrelated infrastructure³⁵⁷.

Institution risk management integrated with three most important pillars: -



Stability = continuity of operations, Accountability = board-level responsibility, Cyber Resilience = recovery and adaptation)

Board-Level Accountability

³⁵⁵ OECD (n 14).

³⁵⁶ ational Institute of Standards and Technology (NIST), *Risk Management Framework for Information Systems and Organizations* (2018).

³⁵⁷ World Economic Forum, *Global Risks Report 2024* (2024).

It's not just tech teams handling cyber resilience anymore. Directors now face growing pressure to manage digital threats through their duty to protect company interests. Setting long-term goals comes before funding decisions when preparing for destabilisation. Making cybersecurity part of broader risk systems becomes essential under this approach. Indian authorities like SEBI and RBI require top-level supervision, reflecting the shift of accountability to higher levels³⁵⁸.

Risk Audits and Disclosure Standards

Start with clear checks on possible threats - those happen repeatedly - to keep institutions strong. When systems get reviewed, weak spots show up in how IT works, daily operations run, even in decision-making chains. Because of these reviews, people involved - like those who invest or oversee rules - learn what digital dangers exist. Openness like this doesn't just sit well - it earns confidence slowly over time. It also moves in step with standards seen elsewhere, including Europe's updated network safety rulebook. That framework pushes countries to demand full, timely reports when issues arise³⁵⁹.

Planning for Incident Response and Recovery

Most of the time, strong systems survive because they know how to react when problems hit. Such blueprints lay out steps to spot trouble, limit damage, share details, then rebuild. What stands out is their focus on keeping things running - money flowing, hospitals working, power grids stable - even mid-cyberattack. A quiet force behind India's shield, CERT-In guides countrywide reactions³⁶⁰. At the same time, industry watchdogs require individual bodies to shape tailored bounce-back methods³⁶¹. This method resembles the way, how companies top level management predict risks to protect future spending, keeping functions steady when uncertainty occur in the organisation.

India's Regulatory Frameworks

India set new rules for institution cyber resilience through regulatory framework that focuses on stability of operational function, accountability by top level management and resilience by taking appropriate mandatory framework.

SEBI's Cyber Security and Cyber Resilience Framework (CSCRF):

Now securities and Exchange Board of India make legal law that requires stock exchange, depositories and market intermediaries to adopt cyber resilience framework. These include well defined governance

³⁵⁸ SEBI (n 7), RBI (n 8)

³⁵⁹ NIS2 Directive (n 10)

³⁶⁰ CERT (n 9)

³⁶¹ Gartner, *Incident Response Planning Best Practices* (2023).

and accountability structure, incident reporting and mandatory periodic auditing. This framework focuses on stabilized functioning of financial market, monitoring that cyber shocks can negatively affect investor confidence and systematic liquidity³⁶².

RBI's Guidelines for Banks

Reserve bank of India always makes rules and laws regarding the smooth functioning of banking system by making legal and strict laws. RBI holds main function regarding the stability of banks and services. RBI requires banks to implement board approved cyber security policies, conduct regular risk assessment, making incident response system. Updated guidelines to insure stabilize banking system and digital payment services it also helps to hold customer trust on Indian banking system³⁶³.

CERT-In's Crisis Management Plans:

The main strategic framework of this plan is to prepare management for respond to and recover from cyber shocks and phishing attacks. The main aim of this plan is to minimize damage to critical infrastructure. Its key components involve identifying potential cyber crises and provide specific actions to stakeholders, focusing on that losses are minimised, and recovery is carried out effectively and efficiently³⁶⁴.

In this sense, these frameworks can be regarded as a paradigm shift, since cyber resilience should be considered a matter of governance rather than just a technical problem³⁶⁵.

The approach to managing risk on an institutional level represents a significant pivot of cyber-resilience in the country. India is incorporating governance, continuity and systemic resilience into its regulatory frameworks, moving beyond technical safeguards to being institutionally prepared by organisations having appropriate levels of accountability at the board level, performing risk audits and developing recovery plans that provide continuity for the organisation when experiencing a cyber event. Through the implementation of regulatory initiatives (SEBI, RBI and CERT-In), India is adopting best practices on a global level which will enable organisations to accept responsibility to adapt to, and recover from, cyber shocks while providing continuity of service³⁶⁶.

As the digital economy in India continues to grow, institutional risk management will become increasingly important order to provide security for the financial markets, payment systems and critical infrastructure. Collectively, this shift is indicative of a greater understanding that resilience against cyber threats and vulnerabilities is a challenge beyond technical, but that cyber resilience is an economic and institutional necessity³⁶⁷.

³⁶² SEBI (n 7)

³⁶³ RBI (n 8)

³⁶⁴ CERT (n 9)

³⁶⁵ OECD (n 14).

³⁶⁶ SEBI (n 7), RBI (n 8), CERT (n 9), NIS2 Directive (n 10).

³⁶⁷ International Monetary Fund (IMF), *Cyber Risk and Financial Stability* (2021).

The Economics of Cyber Resilience

Cyber risk is both a technical challenge and an economic externality because incidents involving one firm produce consequences that can affect other firms—such as suppliers, customers, financial institutions, and even infrastructure on a national scale. For example, a ransomware attack targeting one hospital may disrupt care across multiple hospitals in the same region, while a payment gateway breach could undermine consumer trust and confidence in the entire digital ecosystem. Because of this interdependence, cyber resilience is an overall economic issue rather than one that only affects individual organizations³⁶⁸.

Cyber Risk as an Economic Externality

As defined by economists, externalities represent costs or benefits incurred by individuals or parties (third parties) that did not participate directly in the transaction. Cyber incidents can be perfectly described as externalities because of how they expose many other companies to the risk of being harmed by someone else's attack due to their interconnectedness. Companies in the same supply chain expose all other companies within their supply chain to exposure from an attack if one of the companies in the supply chain has been attacked. Likewise, if one of the banks has an intrusion or is compromised it will diminish the public's trust and confidence in all other banks in the banking industry. In India, where UPI, Aadhaar and several fintech platforms connect hundreds of millions of users to the digital economy through their interconnectedness, this externality effect is compounded, thus it is important to view cyber resilience as a public good and invest accordingly through regulations and coordination³⁶⁹.

Cost-Benefit Analysis of Resilience

Organizations typically compare the costs of investing in resilience to those that may result from a potential breach. Resilience investments include cyber insurance premiums, redundant backup systems, audit activity, and employee training. While these may seem burdensome to micro, small, and medium-sized enterprises (MSMEs); the costs associated with economic losses due to breaches—such as downtime, reputational damage, regulatory fines and customer attrition—far exceed these amounts³⁷⁰.

For example, downtime resulting from a digital payment system outage can effectively bring retail transactions to a halt across the country. A single day's outage of the UPI system could mean billions of rupees in lost commerce. Therefore, from a cost versus benefit viewpoint, spending on resilience is not a 'nice to have'; it's a 'must have'. The challenge is quantifying those risks so that SMBs have incentive to invest in them before a breach occurs (rather than reactively)³⁷¹.

³⁶⁸ IMF (n 39)

³⁶⁹ World Bank, *Cybersecurity as a Systemic Risk to Financial Stability* (2022).

³⁷⁰ Ponemon Institute (n 5).

³⁷¹ NPCI (n 18)

Cyber Insurance as a Financial Instrument

Cyber insurance is becoming a popular way to manage your financial risk throughout the world. In India, however, we are facing challenges related to its adoption as an insurance solution.

- **Actuarial Data:** Insurers in India have difficulty in pricing their cyber insurance policies because of insufficient historical data on cyber incidents³⁷².
- **Affordability:** Small to medium-sized businesses (MSMEs) typically operate on very narrow margins, making it cost-prohibitive for them to purchase cyber insurance premiums³⁷³.
- **Awareness Gap:** Many businesses still look at cyber-risk as a technology issue instead of a financial issue in their risk management strategy³⁷⁴.

Bringing together these facts, implementing a way to facilitate rural economic resilience using cyber insurance has the potential to become a very valuable financial tool for organizations. In addition to spreading the financial risk to different organizations in a region, cyber insurance creates a financial buffer to recover from catastrophic losses, while also providing incentives to organizations for implementing risk mitigation practices. Policymakers can promote the adoption of cyber insurance products through subsidies, tax incentives or regulatory mandates for all organizations, but especially for organizations operating in critical industry sectors such as banking and healthcare³⁷⁵.

Economic Resilience Tools

Apart from insurance there are different ways of employing Economic Resilience Mechanisms listed below that will enhance a company's ability to withstand attack and recover from disaster.

Public-Private Partnership: To reduce the asymmetry of information, organizations need to share Cyber Risk Threat intelligence. Examples include the Government of India's Cyber Emergency Response Team, (CERT-In)³⁷⁶; Additional cooperation with Industry Associations by Gov't can provide additional preparedness.

Investment in Redundancy: Organizations should invest in backups, Disaster Recovery sites and cloud-based continuity of operations failover facilities. Although initially expensive, they will result in fewer losses when a company experiences an attack³⁷⁷.

Regulatory Frameworks: The SEBI and the Reserve Bank of India (RBI) are embedding Cyber Resilience in their Rules and Regulations. Section 8020 et al to make it a requirement of doing business, or as a required component of doing business to be compliant as an organization, as opposed to optional³⁷⁸.

³⁷² Insurance Regulatory and Development Authority of India (IRDAI), *Report on Cyber Insurance in India* (2022).

³⁷³ IRDAI (n 44)

³⁷⁴ IRDAI (n 44)

³⁷⁵ OECD, *Insurance and Risk Management for Cyber Resilience* (2021).

³⁷⁶ CERT (n 9)

³⁷⁷ Gartner (n 33)

³⁷⁸ SEBI (n 7), RBI (n 8)

Case Study: UPI's Resilience Planning

This is the case study of a financial system that is functioning well and providing a reliable service for millions of people every day. It is a vital component of India's digital payment system (Unified Payments Interface - UPI) and processes billions of transactions each month. A failure of the UPI payment system would have serious and numerous negative implications throughout India's economy³⁷⁹.

To prevent system failures, the UPI has taken extensive measures to ensure that:

- Its operational systems are designed with redundancy and backup systems that support uninterrupted operation.
- Real-time system monitoring and management to detect any anomalies or problems before they become critical.
- Developing and implementing incident response procedures that will allow the UPI to quickly restore service in the event of a security breach or incident.

The successful implementation of these resilience investment plans has helped UPI maintain consumer trust in its service and allowed UPI to remain an active participant in the growth of India's digital economy despite increasing threats from cybercrime. As demonstrated by the UPI case study, investing in resilience benefits individual organizations; it benefits the entire economy³⁸⁰.

1. India-Specific Challenges

India's progress towards improving its Cyber Resilience has been faced with certain unique challenges due to the Country's Economic Structure, Regulatory Framework, and Organizational Culture. Although there has been significant progress made in Digital Transformation, vulnerabilities still prevent the successful implementation of Resilience Strategies³⁸¹.

Micro Small and Medium Enterprises (MSME's) do not have the funds available for Resilience: MSME's are the Heart and Soul of the Indian Economy (30% of GDP, with millions of Employees), however, MSME's are operating on Tight Margins and Having Limited Budgets. As such, investing in Cyber Resilience (Insurance, Audits, Security Devices, etc.) is viewed as a Luxury, rather than a Necessity. Most MSME's are using Old Technology, Have Limited Full Time IT Personnel, and are Very Dependent on Third Party Service Providers; several of these factors contribute to the Issue of Supply Chain Risk. The Affordability Gap in Cyber Insurance compounds this issue leaving MSME's Vulnerable to the Financial Impacts associated with Breaches. The issue creates a Systemic Risk given the Deep Integration of MSME's into Larger Supply Chains since one Breach will create multiple impacts across Industries³⁸².

³⁷⁹ NPCI (n 18)

³⁸⁰ NPCI (n 18)

³⁸¹ Ministry of Electronics and Information Technology (MeitY), *National Cyber Security Strategy Draft* (2021).

³⁸² Federation of Indian Chambers of Commerce and Industry (FICCI), *Cybersecurity Challenges for MSMEs in India* (2022).

2. Underreporting of Breaches Weakens Collective Defence

There is a long-standing problem of organizations failing to report cyber incidents due to fear of damaging their reputation, incurring regulatory scrutiny, or losing customer trust. This lack of a reporting culture hinders the sharing of threat intelligence, which contributes to the overall lack of effective collective defence mechanisms. Additionally, without reporting of breaches, regulators and policymakers cannot access the data necessary to assess systemic vulnerabilities or create effective interventions. Lastly, without a culture of strong disclosure, corporations are unable to learn from one another's experiences, resulting in a cycle of unpreparedness. As exemplified by global frameworks such as the EU's NIS2 Directive, this highlights the need for India to strengthen enforcement pertaining to mandatory reporting of incident breaches³⁸³.

3. Shortage of Skilled Cybersecurity Professionals

Cybersecurity Professional Shortage India has a remarkably large talent gap in cybersecurity. While the country has a significant pool of IT graduates, it has very few specializing in areas such as threat intelligence, incident response, and resilience planning. Most qualified cybersecurity professionals are further concentrated in metropolitan areas, causing those working in small cities or rural enterprises to be left without ample support. There is significant market demand for qualified cybersecurity professionals, which continues to greatly exceed supply; therefore, many micro-, small-, and medium-sized enterprises (MSMEs) and others are faced with increasing challenges when trying to hire highly qualified staff. The gap in the regulatory frameworks has left government agencies and regulators unaffected by the potential implications of this continuing problem and, therefore, limits their ability to monitor compliance and have effective responses in the event of a crisis. To bridge this gap, significant investment in specialised training programs, industry-academia partnerships and economic incentives to attract and retain talent within the country will be required³⁸⁴.

4. Policy Enforcement Gaps Despite Strong Frameworks

Despite the existence of strong policy frameworks, there remain numerous gaps between the design of regulatory frameworks and their enforcement. This is true for many of India's regulatory bodies, including the Reserve Bank of India (RBI)'s Cybersecurity Guidelines for Banks, the Securities and Exchange Board of India (SEBI)'s Cyber Security and Cyber Resilience Framework (CSCRF) and CERT-In's Crisis Management Protocols. Specifically, the lack of adequate resources and penalties for non-compliance create an environment where regulatory authorities cannot fully audit and assess compliance. Consequently, many companies view compliance as a "checkbox" exercise rather than incorporating resilience into their operational culture, and the lack of consistent enforcement of existing laws perpetuates an ineffective regulatory framework³⁸⁵.

³⁸³ NIS2 Directive (n 10)

³⁸⁴ NASSCOM, *Cybersecurity Talent Report India* (2023).

³⁸⁵ SEBI (n 7), RBI (n 8), CERT (n 9).

5. Cultural Challenge: Cyber Risk as an IT Issue, not a Business Continuity Issue

The issue of cyber risk being perceived as an IT issue rather than a business continuity issue is likely the most significant obstacle facing organisations in India. Many Indian companies still perceive cyber risk solely as an IT-related issue, and therefore, the responsibility for managing that risk lies exclusively with their IT departments, instead of being viewed as a strategic issue that requires oversight from the board. The limited perspective encourages lack of investment into resilience preparation as well as ignoring continuity strategies. Building cyber resilience requires adopting an integrated viewpoint across governance, risk management and operational continuity but organizational inertia frequently inhibits organizations from undertaking the necessary change. Until organizations develop a true understanding of the notion that cyber risk falls within the umbrella of business continuity risk; they are always going to be reactive to cyber resilience rather than proactive³⁸⁶.

Policy Recommendations

India's fast-paced digital development is why Internet Safety is one of the highest priorities on the National to-do list. SEBI's CSCRF has improved Security for Financial Services but there are many other Industries like Manufacturing, Health, Energy, and Transport where Cyber Crime is just as much of a threat as it is in the Financial Industry³⁸⁷.

Here are some Policy ideas to increase Cyber Resilience in India:

1.Expanding SEBI's CSCRF Principles Beyond Finance

SEBI has very Strong Corporate Governance Processes for Financial Services (CSCRF) however, Security Processes in other industries could benefit from Corporate Governance Processes like CSCRF so that management will be accountable for ensuring that they have completed a Risk Assessments for their Organization and created a Security Resilience Plan for their Business. By normalizing Security Processes for all Industries, the Government will create very Good Security Practices for All of our Nation's Businesses and make it much easier for the Government Agencies involved to Develop and Execute a National Response to Cyber Crime³⁸⁸.

2.Incentivizing Cyber Insurance Adoption

Cyber Insurance currently does not exist in a way that organizations find affordable. Therefore, we recommend to government officials to create incentives such as Tax Benefits for Cyber Insurance, Premium Subsidies for Qualified and Registered MSMEs, and Startup a Financial Risk Pool where Private Insurance Companies Pool Risks from Public and Private Sector Organizations into one combined Financial Risk Pool. Organizations can reduce the financial damage caused by cyber-attacks by implementing cyber insurance as part of their overall financial risk management while enabling the

³⁸⁶ PwC India, *Cyber Risk as Business Continuity Risk* (2022).

³⁸⁷ MeitY (n 29).

³⁸⁸ SEBI (n 7).

insurer to create systemic resilience via the data collected and the industry standards that are created. This will also lead to greater transparency since insured organizations will typically be more willing to report incidents, they experience to meet the policy requirements³⁸⁹.

3. Building MSME Capacity Through Subsidies and Shared Platforms

MSME Capacity Building Through Subsidy and Shared Platforms Micro, small, and medium enterprises (MSMEs) are the foundation of India's economy yet remain constrained in their ability to build resilient organizations. By providing government-funded subsidies for basic cybersecurity tools, shared resilience platforms (e.g., cloud-based backup and monitoring), and additional training programs, this gap can be closed. A framework based on a collective resilience model that allows MSMEs to pool resources (e.g., intelligence sharing) to protect themselves from threats and build redundancy would have a positive impact on reducing costs and increasing systemic protection through economies of scale. The approach will be like other cooperative models created in agriculture and finance but adapted for the digital economy³⁹⁰.

4. Mandating Breach Disclosure to Strengthen Systemic Awareness

Creating Systemic Awareness Through Mandated Breach Disclosures The underreporting of breaches is one of the most significant weaknesses in India's cyber ecosystem. The implementation of mandatory breach disclosures and legal protections against potential reputational harm will create greater systemic awareness and allow for a quicker and more efficient response collectively. Disclosures from companies should be differentially tiered: minor incidents reported to the regulator; major breaches reported publicly to strike a balance between openness and practicality. Being collectively accountable through building sustained collaboration will create an environment where being resilient as opposed to being at a competitive disadvantage is just as important to everyone as it is for those who actively work on their own transformation efforts³⁹¹.

5. Fostering Public-Private Partnerships for Intelligence Sharing

Fostering Public-Private Partnerships for Joint Intelligence Sharing The pace of change in cyber threats far exceeds the speed of regulatory change. Thus, sharing intelligence between the public and the private sector is necessary. A public-private partnership (PPP) provides a forum to establish an institutionalized form of collaboration among government, industry associations, and private firms. There will be collaborative platforms established for sharing real-time threat intelligence, coordinating responses to incidents, and providing joint training and exercise opportunities. This will also allow the development of public-private partnerships with universities and research entities so that India can develop the homegrown skills to model cyber risks and the technology solutions required for enhancing resilience³⁹².

³⁸⁹ OECD (n 47)

³⁹⁰ Confederation of Indian Industry (CII), Building Cybersecurity Capacity for MSMEs in India (2022).

³⁹¹ NIS2 Directive (n 10)

³⁹² WEF (n 29).

6. Integrating Cyber Resilience into National Economic Planning

Integrating Cyber Resilience into National Economic Risks Cycles India must embed cybersecurity within its overall monetary policy. Just as physical risk has been incorporated into infrastructure policy, so too must cyber risk be factored into the digital infrastructure public policy. In addition to allocating a line item for growth resilience in national economic policy, all national macroeconomic forecasts must embed cyber risk in making estimates of GDP; and resilience must be treated as public good. As a result, India's digital growth will match up with systemic health and innovation will not be compromised by the risk of being vulnerable³⁹³.

Conclusion

The evolution of India's digital economy has proven that relying solely on traditional technical firewalls and perimeter defences is insufficient to address the systemic and interconnected risks facing the current threat landscape. While technical security controls (firewalls, antivirus software, and intrusion prevention systems) are still critical to protecting our systems, they are no longer adequate to address the increasing prevalence of cyber threats and the way in which they are intertwined with one another. There needs to be a transition towards using institutional risk management (as opposed to solely technical security) to build resilience into governance, policy, and finance³⁹⁴. This approach recognizes that cyber threats are not only technical disruptions but can also result in economic losses that will destabilize markets, supply chains, and critical infrastructure. Cyber resilience will be a fundamental component of India's digital economy. The costs associated with cyber incidents (financial losses, lost productivity, reputational harm, and regulatory penalties) far exceed the investments required to develop public's confidence and to continue to allow for the ongoing adoption of India's digital economy, particularly considering the rapid digitization that has occurred (Aadhaar, UPI, and fintech growth)³⁹⁵. By treating cyber risk as an externality to the economy, India is acknowledging that the vulnerability of one organization can have a cascading effect across multiple sectors and lead to systemic fragility throughout the economy. As such, resilience will be a shared responsibility that will require coordinated efforts among regulators, industries, and businesses³⁹⁶.systems that can remain resilient over time³⁹⁷. Resilient systems are essential to maintain the

It is critical to note that there is no perfect way to completely reduce risk - resilience is rooted in ensuring some degree of continuity, rapid recovery and adaptability. The objective of resilience is to ensure that vital functions – such as financial transactions, delivery of healthcare services, provision of energy, and protection or performance of government functions – can continue to operate, notwithstanding their potential disruption because of an event³⁹⁸. The fundamental purpose of building resilience is to shift the mode of cyber risk management from being reactive to pro-active.

³⁹³ IMF (n 39).

³⁹⁴ National Institute of Standards and Technology (NIST), *Cybersecurity Framework 2.0 Draft* (2023).

³⁹⁵ NPCI (n 18)

³⁹⁶ IMF (n 39), NPCI (n 18)

³⁹⁷ IBM Security, *Cost of a Data Breach Report* (2023).

³⁹⁸ OECD (n 14).

Organizations need to develop the processes and capabilities to anticipate, absorb and recover from external shocks while maintaining their long-term viability³⁹⁹.

To enable the future growth of the digital economy in India, it will be essential to build resilience into India's institutional fabric. This will entail developing systems that embed resilience into governance structures and regulatory and financial instruments, such as board-level accountability, cyber insurance, etc⁴⁰⁰. At the same time, it will be necessary to help the micro, small and medium enterprises (MSMEs), which constitute the mainstay of the Indian economy, through the provision of subsidies, shared resilience platforms and training for them to build up their resource capacity⁴⁰¹. Furthermore, India will need to develop stronger standards for breach disclosure and promote intelligence-sharing and public-private partnerships, as well as work towards achieving alignment with other international standards of resilience. By institutionalizing resilience⁴⁰², India will protect its digital transformation, as well as position itself as a global leader in the development of economic security standards for the digital age⁴⁰³.

To build India's digital future, we need to focus on solidifying the fundamentals of continuous service delivery, rather than creating large barriers to entry. The country must prioritize cyber resiliency at a national economic level, which includes embedding it throughout government, policy and financial systems. By making resilience the foundation of India's digital initiative, we can turn weaknesses into strength, providing an ever-larger, more flexible, and globally competitive digital economy that can withstand changing cyber threats⁴⁰⁴.

³⁹⁹ Gartner (n 33)

⁴⁰⁰ SEBI (n 7), IRDAI (n 44).

⁴⁰¹ FICCI (n 54), CII (n 62).

⁴⁰² NIS2 Directive (n 10), WEF (n 29).

⁴⁰³ World Bank, *Cybersecurity as a Public Good* (2022).

⁴⁰⁴ IMF (n 39).