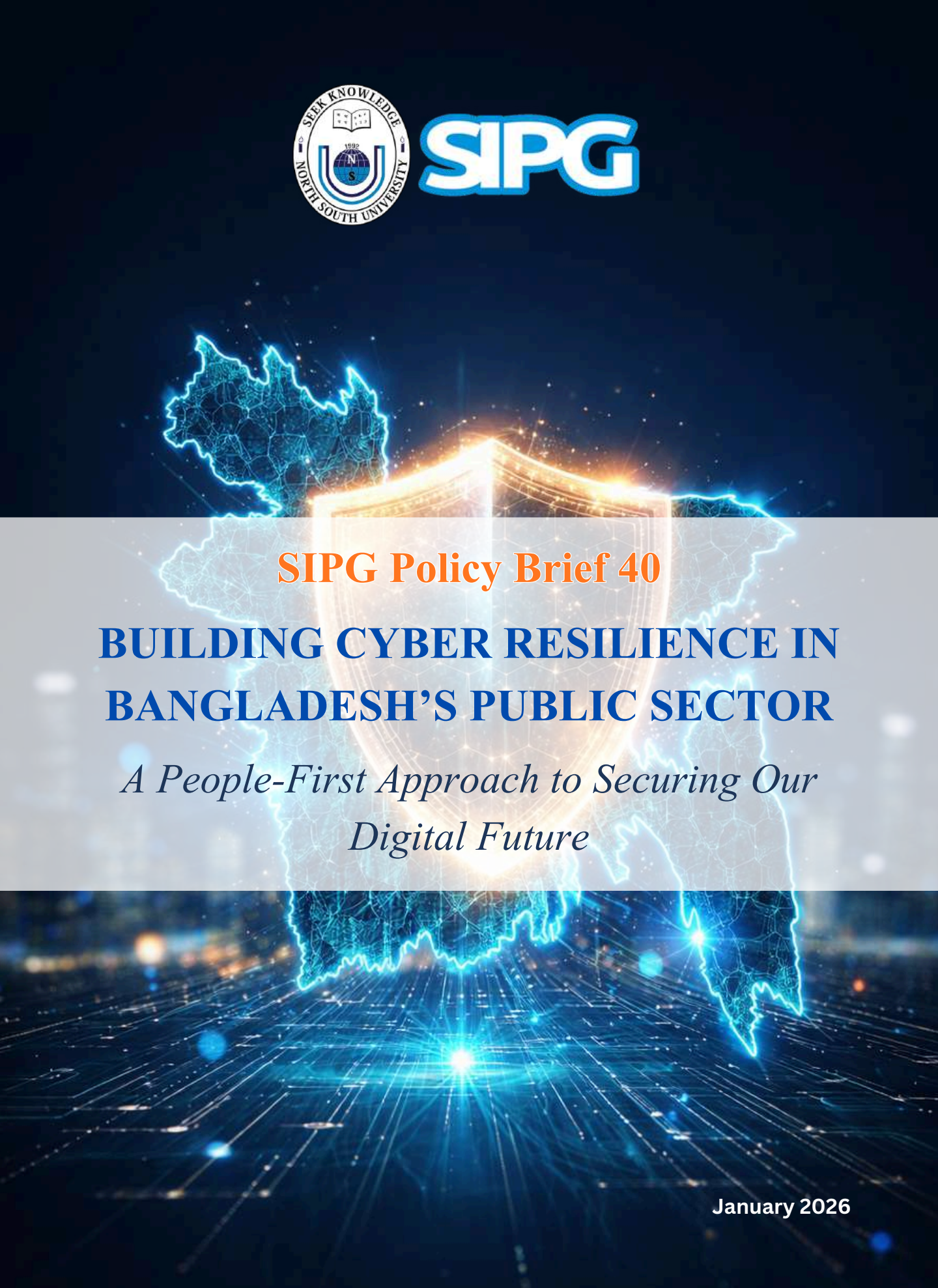

SIPG Policy Brief 40

BUILDING CYBER RESILIENCE IN BANGLADESH'S PUBLIC SECTOR

A People-First Approach to Securing Our Digital Future

January 2026

Why This Matters: The Stakes Are Real

Bangladesh is living through a digital revolution. Services that once demanded paper files, stamps, and long hours in government offices are now accessible online. Citizens can apply for birth certificates, check land records, file taxes, or access healthcare databases with far greater speed and transparency than before. For millions, this has reduced burdens, saved time, and built confidence in public services. But this same transformation has opened the door to new risks that grow more serious each year. Cyberattacks are no longer isolated incidents; they are frequent, sophisticated, and damaging. In 2023 alone, a single breach exposed the personal data of more than 50 million citizens, including sensitive National ID details. Ransomware attacks have crippled ministries and even airlines, leaving essential services offline for days. Hacktivist groups have disrupted government websites, undermining public confidence in the state's ability to protect its digital systems. If citizens begin to doubt the safety of these platforms, they will withdraw from them, undermining the entire Smart Bangladesh vision. At its core, cybersecurity is not just a technical matter, it is about protecting trust, safeguarding national security, and ensuring that government can continue to serve people reliably in the digital age.

The Problem: What's Failing and Why It's Urgent

Despite important progress, serious weaknesses persist:

Outdated Infrastructure
Many ministries still use computers and servers that are too old to update. These "legacy systems" are well-known to hackers, who can easily exploit their vulnerabilities.

Shortage of Skilled People
In most government offices, cybersecurity expertise is either missing or extremely limited. Roles like threat analysts, forensic investigators, and incident responders are rarely present. This leaves massive blind spots.

No Unified Response Plan
When breaches happen, confusion spreads on who takes the lead—the ministry, the Bangladesh Computer Council (BCC), or the National Committee on Security Affairs (NCSA)? Without clear lines of responsibility, response is delayed, recovery takes too long, and sometimes the attack isn't even detected until much later.

Fragmented Governance
Cybersecurity is spread across the BCC, NCSA, and Bangladesh Telecommunication Regulatory Commission (BTRC). But coordination is weak. It's like three fire departments responding to the same fire without speaking to each other.

Weak Vendor Oversight
Much of government's software and hardware comes from outside vendors. But there are no strong vetting processes to ensure that these tools are safe, updated, and free from hidden risks.

Cybersecurity as an Afterthought
Many leaders still think cybersecurity is a responsibility of the IT department, rather than a governance issue. Until this mindset changes, systems will remain fragile.

Inadequate Funding
Budgets rarely include cybersecurity as a priority. Rural or smaller offices often have no funds at all, leaving them fully exposed.

Smarter Threats Are Already Here
Cybercriminals are moving ahead with AI tools, deepfakes, and ransomware-as-a-service. Yet our defenses are still designed for yesterday's problems.

The current picture of Bangladesh's cybersecurity is mixed, showing both progress and vulnerability. On one hand, Bangladesh has made notable strides, climbing 25 places in the International Telecommunication Union's (ITU) Global Cybersecurity Index in 2020, now ranked 53rd worldwide and 11th in the Asia-Pacific region. This reflects real progress in updating laws, improving technical capacity, and building cooperation. On the other hand, the country remains far behind global leaders such as the United States, the United Kingdom, Estonia, South Korea, and Singapore, where cybersecurity is embedded deeply into governance and national strategy.

Table 2: Current Cybersecurity Weaknesses and Expert Assessment in Bangladesh

Issue	**Key Detail**	**Expert Insight**
Outdated Infrastructure	Easy to exploit legacy systems for hackers.	Experts warn they are a "ticking time bomb."
Skills Shortage	Few trained analysts or responders in government.	Major blind spots; far behind global leaders.
No Unified Response	Confusion between ministries, BCC, and NCSA.	active Computer Emergency Response Team (CIRT), but weak overall coordination.
Fragmented Governance	Oversight split across BCC, NCSA, BTRC.	Lack of communication like fire departments.
Vendor Risks	Rarely vetted external software/hardware.	Hidden vulnerabilities enter government systems.
Mindset Problem	Seen as IT issue, not governance.	Laws exist, but mindset undermines resilience.
Low Funding	Budgets rarely prioritize cybersecurity.	Despite ITU progress (53rd globally), resources remain thin.
Smarter Threats	Criminals use AI, deepfakes, ransomware.	Threats evolving faster than defenses.

Within Bangladesh, the BGD e-Gov CIRT has handled incidents and shown the value of having a response body, yet its overall capacity remains limited and coordination across agencies is still weak. Local experts we spoke to underscored a common warning: "legacy systems are a ticking time bomb," pointing to the old and vulnerable infrastructure that many ministries continue to rely on. The conclusion is clear: Progress is real, but the resilience of Bangladesh's cyber defenses remains fragile.

What's Being Done—and Why It's Not Enough

The government has laid some foundations:

- Policies and Laws: The Cybersecurity Policy (2014), the Digital Security Act (2018), and the later Cyber Security Act (2023) were important signals of intent.
- Institutions: Bodies like the BCC, NCSA, and BGD e-Gov CIRT exist to provide oversight and response.
- Capacity Building: Some professional associations (like, Information Systems Audit and Control Association (ISACA)) run trainings.

But these efforts are fragmented and reactive. Policies are outdated, agencies overlap, training is not systematic, and funding is not proportional to the risks. The system exists on paper, but it is not yet effective in practice.

The Framework to Address the Risk Cycle

The Hybrid Adaptive Cybersecurity Framework, developed by the South Asian Institute of Policy and Governance (SIPG), is not just another checklist. It is a comprehensive, multi-layered defense model tailored to Bangladesh's realities: underfunded offices, outdated infrastructure, shortage of skilled staff, and fragmented governance. At the same time, it borrows from best global practices like National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 27001, and Zero Trust, ensuring that our systems are aligned with international standards.

What makes this framework different is its flexibility and adaptability. Instead of assuming every ministry can adopt advanced cybersecurity tools overnight, it introduces phased implementation, where agencies start with basic protections, then gradually move toward advanced AI-driven security. This ensures inclusivity where even rural or resource-strapped offices can participate.

Table 3: Current Cybersecurity Efforts and Their Limitations

What's Being Done	Why It's Not Enough
Policies & Laws (2014, 2018, 2023)	Outdated and reactive
Institutions (BCC, NCSA, CIRT)	Overlap, weak coordination
Capacity building (ISACA trainings)	Not systematic, limited reach
Funding & resources	Not proportional to risks

Ten Actionable Steps Toward Cyber Resilience

1. **One Clear Cyber Authority**
   Right now, responsibility is scattered between BCC, NCSA, and BTRC. This creates confusion and delays. A single National Cybersecurity Authority under the Prime Minister's Office would provide unified leadership, coordinate incident responses across ministries, and act as the central command hub in times of crisis.

2. **One National Framework**
   Ministries today use different and sometimes no security standards. A phased Hybrid Cybersecurity Framework would unify everyone under one system, combining international benchmarks (like NIST, ISO, Zero Trust) with local realities. For example, Phase 1 could focus on patching and strong passwords, Phase 2 on real-time monitoring, and Phase 3 on advanced threat intelligence.

3. **Cyber Risk Dashboard**
   Currently, breaches often go unnoticed for days. A National Cyber Risk Registry, updated in real time, would allow ministries to see threats as they emerge, much like a "digital health check-up" for government systems. This ensures small breaches are spotted before they become national crises.

4. **Train Everyone**
   The biggest vulnerability is human error whether a clerk clicking a phishing link or an officer reusing weak passwords. Training cannot be limited to IT staff. Clerks, data-entry operators, police officers, judges, and senior officials all need continuous, role-specific training. Regional training hubs, simulation exercises, and e-learning modules would help build a cyber-aware workforce nationwide.

5. **Secure Procurement**
   Too often, vulnerable software and hardware enter government systems through vendors. Every procurement contract should include mandatory cybersecurity vetting asking: Is this system updated regularly? Is it free from backdoors? Does the vendor comply with international security standards?

6. **Nationwide Awareness Campaign**
   Awareness is low, especially outside Dhaka. A national campaign using posters in government offices, radio programs, short videos in schools, and village-level workshops can make cybersecurity understandable for everyone. Just as Bangladesh once raised awareness about sanitation and disaster preparedness, it must now do so for digital safety.

7. **Dedicated Cybersecurity Budgets**
   At present, cybersecurity is often treated as a side expense, if funded at all. Every ministry should have a separate cybersecurity budget line. For smaller or rural offices, a national Cybersecurity Fund should provide resources. Critically, these funds should be tied to performance indicators: fewer breaches, faster recovery times, and stronger compliance.

8. **Public-Private Collaboration**
   Banks, telecoms, and IT companies already fight cyberattacks every day. Government should not fight alone. A Cyber Threat Sharing Network would allow public and private sectors to exchange intelligence, tools, and solutions in real time just as financial institutions already share data to stop money laundering.

9. **Update Laws & Build Forensics Capacity**
   Existing laws like the Digital Security Act are outdated and sometimes misused. Bangladesh needs modern legislation that clearly defines cybercrimes, protects personal data, and strengthens digital rights. Alongside laws, forensic labs and trained investigators are essential so that attacks don't just get patched; they are properly investigated and punished.

10. **Integrate Security from Day One**
    Too often, cybersecurity is added as an afterthought to digital projects. This must change. Every new digital initiative, whether an e-health portal, land registry, or tax filing system, must integrate cybersecurity during planning, just like budgets or legal reviews. This will reduce costly fixes later.

Table 4: Proposed Framework for Strengthening Cybersecurity

Step	Core Idea	Why It Matters
1. One Clear Authority	Single National Cybersecurity Authority under PMO	Unified leadership, faster crisis response
2. One Framework	Phased Hybrid Framework (NIST, ISO, Zero Trust + local reality)	Consistent standards across ministries
3. Cyber Risk Dashboard	Real-time National Cyber Risk Registry	Detect small breaches early
4. Train Everyone	Continuous, role-specific training for all staff	Reduces human error, builds awareness
5. Secure Procurement	Mandatory vendor vetting	Blocks weak/unsafe systems from entry
6. Awareness Campaign	Nationwide education (schools, radio, workshops)	Builds digital safety culture
7. Cyber Budgets	Dedicated funding + national fund for small offices	Ensures sustained, measurable investment
8. Public-Private Collaboration	Cyber Threat Sharing Network	Leverages banks/telecom expertise
9. Update Laws & Forensics	Modern cyber laws + forensic labs	Clear accountability, stronger justice
10. Security by Design	Build cybersecurity into all new projects	Prevents costly afterthought fixes

The Bottom Line: Trust Is Digital Sovereignty

Cybersecurity is not optional. It is the foundation of Smart Bangladesh. Without strong defenses, digital services collapse, citizens lose confidence, and development goals stall.

Bangladesh now stands at a crossroads:

- Act now to secure digital trust and resilience, or
- Face the danger of systemic digital chaos tomorrow.

With political will, sustainable funding, and a people-first approach, Bangladesh can build a future that is not only digital and smart, but also safe, resilient, and trusted.

Acknowledgement

We acknowledge the copy-editing service from the NSU-Office of Research

This Policy Brief is Prepared by

Professor M A Rashid, PhD
Senior Research Fellow
South Asian Institute of Policy and Governance (SIPG), North South University

South Asian Institute of Policy and Governance (SIPG)
North South University, Dhaka, Bangladesh
Phone: +8802-55668200 Ext. 2164
E-mail: sipg@northsouth.edu
Website: www.sipg.northsouth.edu