TECHGLOBAL INSTITUTE

Breached and Unanswered:

A Cartography of Bangladesh's Data Breach Epidemic 2023-2026

Apon Das, Mir Rownak, Kalim Ahmed, Shahnewaj Patwari, Fowzia Afroz, Shahzeb Mahmood

EXECUTIVE SUMMARY

Between January 2023 and May 2026, at least 68 data breach incidents affecting both government institutions and the private sector appear to have occurred in Bangladesh. Drawing from cybersecurity advisories, dark-web monitoring services, threat-intelligence feeds, and mainstream newspapers, our findings revealed that of these data breaches, 36 involved government organisations and 32 involved private ones. The data exposed across these incidents includes, but is not limited to, national identity numbers, biometric records, passport details, and other personally identifiable information.

A second finding runs throughout almost every incident in the dataset: the failure of institutions to recognise warning signs of a data breach — i.e., institutional blindness. Almost all documented cases involved breaches identified by external security researchers, news outlets, or dark-web monitoring services rather than by the affected organisations themselves; the two rare exceptions were the Bangladesh Election Commission's detection of leaks within its own verification ecosystem and one police investigation into an alleged breach. Where a response can be traced at all, it is far more often silence or denial than an acknowledgment, and a published post-mortem or forensic analysis is rare to the point of near-absence. The pattern points to a widespread lack of round-the-clock security operations and proactive threat hunting: most organisations in the dataset did not have systemic organisational controls to know they had been breached. These organisations also do not run bug bounty programs that reward the good actors who tend to surface these vulnerabilities and report them via the institutions' official channels.

Data breaches in Bangladesh have escalated into a critical national security crisis, yet the systemic response from the government and key stakeholders remains largely inadequate. The consequences of these incidents extend far beyond individual privacy violations, affecting state security, public trust in digital services, and the integrity of critical institutions. Despite the growing frequency and severity of breaches, Bangladesh still lacks robust accountability mechanisms, mandatory breach notification requirements, and effective institutional responses to protect citizens' data and hold organisations accountable. This report addresses these systemic vulnerabilities by highlighting the immediate risks, identifying critical gaps in the existing policy and legal frameworks, and proposing actionable pathways toward institutional accountability.

BACKGROUND

Two decades ago, the average Bangladeshi citizen's life revolved around papers: paying one's utility bills, accessing government subsidies and welfare, making financial transactions, or checking one's bank balance. Working with paper documentation also meant navigating bureaucratic burdens and processes in person, coordinating schedules, completing forms, and working around for working hours and public holidays. This was a significantly time-consuming process for what should otherwise be a straightforward task. Then, the introduction of the national identity (NID) and, in subsequent years, the initiation of *Digital Bangladesh* and later *Smart Bangladesh*, significantly changed the nature of how day-to-day civic engagements were typically carried out. Within a decade, the NID evolved from a paper-based laminated card to a machine-readable biometric identification card supported by the World Bank via its IDEA project, to the smart NID with an embedded microchip reportedly storing impressions of all ten fingers, iris scans, 32 unique citizen data types, and 25 security features.

The NID became the central document Bangladeshis needed to access all the aforementioned essential services. Evidently, this administrative mandate applied to a massive civic base. By late 2024, the Bangladesh Election Commission had prepared roughly 81 million smart NID cards against a total electorate of nearly 122 million registered voters. Crucially, holding an identity record did not automatically mean a citizen was online. Instead, this institutional centralisation ran parallel to a separate, massive expansion in the country's consumer connectivity. By the end of 2025, a distinct digital population of roughly 83 million people — about half the country — had come online, a footprint supported by around 186 million mobile connections. While at the same time, mobile banking transitioned from a novelty to an economic backbone, accumulating more than 200 million registered mobile-financial-service accounts, of which 89.38 million are active. Together, these overlapping digitisation efforts pulled millions of people who had never had a bank account into the formal economy, carried services into places they had never reached, and made daily life easier.

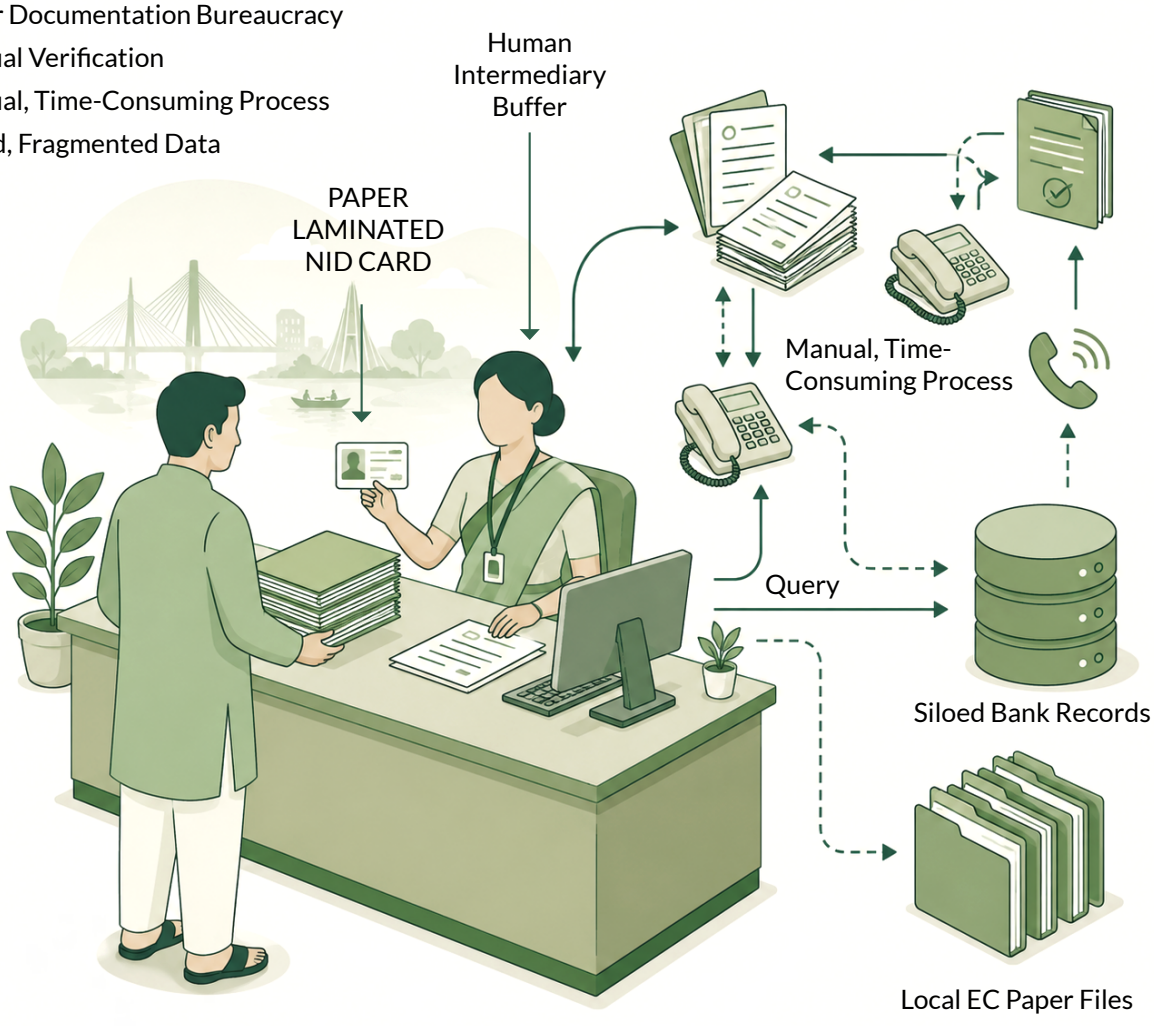
While this digitalisation offers greater convenience to the lives of millions, it has created a fundamental shift in what an identity document does. The paper NID was simply about establishing identity, while the smart NID is about access that permeates every walk of life – directly or indirectly. Access in a digital ecosystem means each interaction (for instance, a tap to check a balance or to pay a bill) is a request passed through an application programming interface (API), a small act of permission that lets a system reach into data tied to you. That data was the precondition for issuing the card in the first place: your name, your parents' names, your date of birth, your fingerprints, and over two dozen other data points in total.

Moreover, this kind of intermediated access regime is not new and it existed even in the paper era, just with a human layer wrapped around it. When a citizen walked into a bank to inquire about a deposit, the clerk did not hold that data personally; instead, the clerk queried

a system that already had programmatic, API-level access to it, and the query was simply mediated by a human interface. Consequently, what digitisation changed was the removal of that human layer, so the request now runs directly between citizen and system rather than through an intermediary. Over a decade, that accumulation gave Bangladesh an enormous, concentrated store of its citizens' data, and each new service built atop it has extended a further layer of access to government institutions, private bodies, and others. Meanwhile, the safeguards that should accompany such concentration — robust security practice, data-protection law, and institutional oversight — have consistently been, and continue to be, deferred.

THEN (PAPER-BASED) (circa 2004)

- Establish Identity Only
- Paper Documentation Bureaucracy
- Manual Verification
- Manual, Time-Consuming Process
- Siloed, Fragmented Data



Generated with ChatGPT

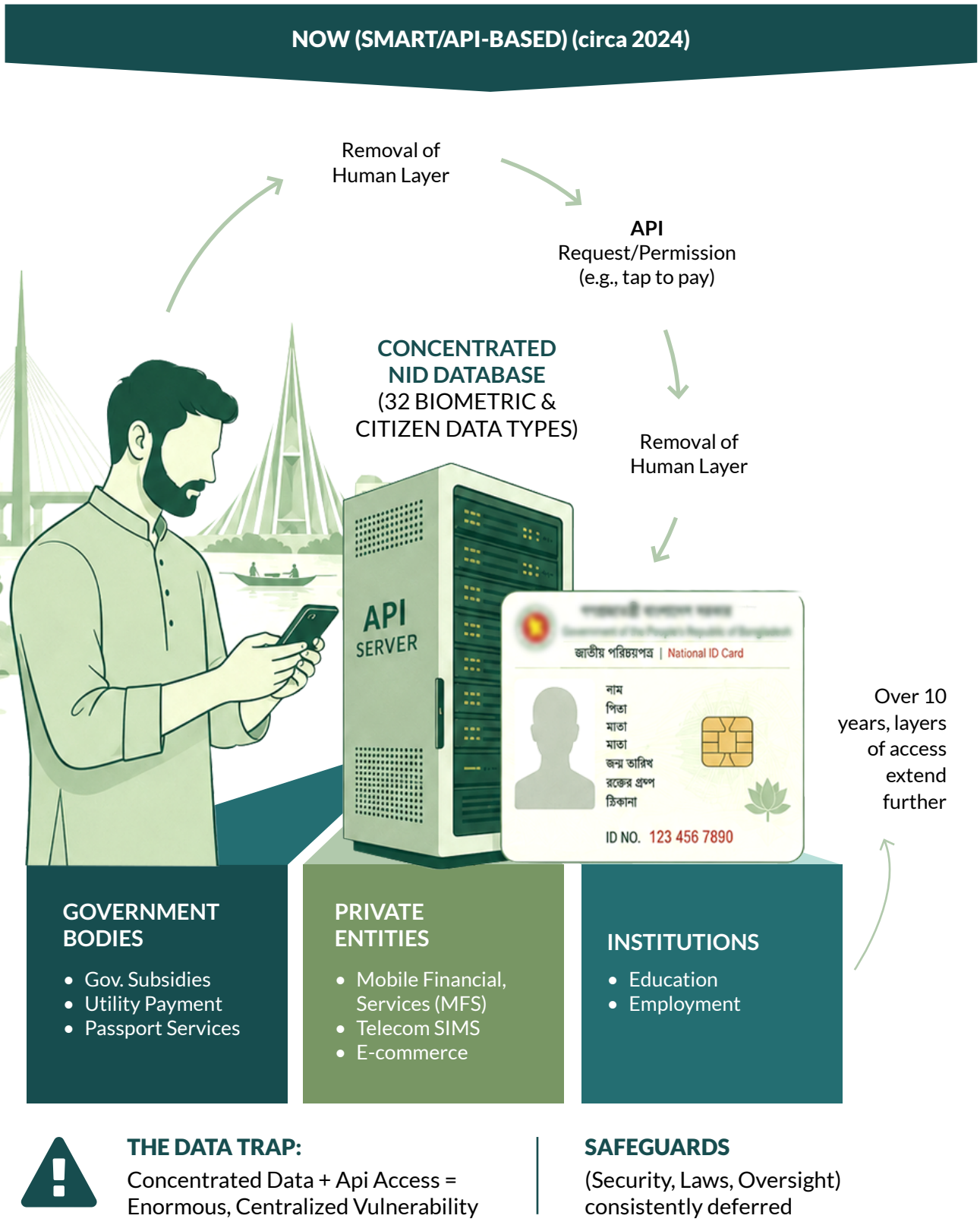


Figure 1: An illustration of the transformation of Bangladesh's NID ecosystem from a paper-based verification model (circa 2004) to the contemporary smart NID and API-based architecture (circa 2024).

Generated with ChatGPT

WHAT CONSTITUTES A DATA BREACH?

A data breach, in plain terms, is when information about you ends up somewhere it was not meant to go. The "how" aspect of it varies. A hacker group may break into a system and take the data; or an organisation simply leaves a digital door open, allowing the data to remain exposed or spill out by accident. The method and motive differ. What stays constant is the outcome: people's information ends up outside the bounds it was meant to stay within, often in hands of people who were never authorised to access it.

According to the *Personal Data Protection Act, 2026,* a personal data breach means a breach of security of personal data resulting in unauthorised access to or unlawful transfer, disclosure, alteration, or loss of or intrusion into any personal data processed under this statute, or in the absence of the necessary equipment for proper processing and storage. Similar definitions exist in regulations elsewhere around the world, including the so-called gold standard for global data protection, the *EU General Data Protection Regulation.*

We found that in most cases the information at stake is what is known as personally identifiable information (PII). This can be characterised as any fact or information, or combination of facts and information, that can be traced back to a specific person, such as a name, a phone number, a national identity number, an address, or biometric data such as fingerprints and iris scans. The list is illustrative, not exhaustive.

What makes a PII leak consequential is that not all of it can be taken back. A leaked password is a lock you can change, but a leaked fingerprint is not. If your payment PIN is exposed, you reset it and move on. But your biometrics, the patterns in your fingertips, the structure of your iris, are yours for life. Once exposed, they cannot be revoked or reconfigured.

As this collection of data began mapping onto nearly every domain of Bangladeshi life, a trade-off was set in motion the moment the paper NID became the stepping stone toward Digital Bangladesh. Once a single identity links every essential interaction, the convenience it delivers also carries visibility whereby the state can see, in one place, what each citizen does. The same concentration of data also creates opportunities for private actors, whether through commercial profiling, data exploitation, or unauthorised access, to gain detailed insight into individuals' lives. A concentration of data is therefore not only a criminal's prize but also an instrument of surveillance and control.

In cybersecurity terms, those who exploit such data are called threat actors. Although the term typically refers to external adversaries, the same concentrated data are also, in most cases, lawfully possessed by the state. An enhanced surveillance capability does not need bad intentions to cause harm because once a single identifier maps individual identity to activity, it lowers the cost of finding a person, monitoring dissent, and applying pressure at scale.

THE COUNT AND SPLIT

The numbers best state the material reality of the problem. Tech Global Institute (TGI) compiled a dossier of 68 documented breach incidents affecting Bangladeshi organisations between 2023 and 2026. These were drawn from four categories of sources: localised threat intelligence from Bangladesh Cyber Security Intelligence (BCSI); international dark-web and ransomware monitors (e.g., Ransomware.live, Ransomlook.io, and RedPacket Security); threat-alert aggregators (e.g., Daily Dark Web on X); and national dailies including *The Daily Star*, *Prothom Alo*, and *The Business Standard*. Details of the methodology are available in the Appendix.

The headline finding is the near-even split between public and private targets: 36 government organisations and 32 private ones over the 41-month window. However, these incidents represent only those that could be identified and corroborated through TGI's source matrix and methodology. Additional breaches may have escaped detection, remained confined to private disclosures, or gone entirely unreported. As such, this dataset should be understood as a documented baseline rather than an exhaustive census of breach activity, offering a conservative view of the broader cyber risk landscape rather than a complete accounting of it.

Attribution follows the data controller: each incident is logged against the institution whose data was exposed, even where the leakage occurred through a partner organisation's authorised access or an insider rather than through a compromise of the institution's own systems. Several incidents linked to the Bangladesh Election Commission are of precisely this kind — citizens' NID data leaking through verification channels operated by private and public entities — and are counted against the country's electoral agency as custodian of the national identity database. The government-private distinction should be read with that convention in mind: it describes where the exposed data lived, not necessarily where the security failure occurred.

Year	Government Organisation	Private Organisation	Total
2023	6	1	7
2024	9	18	27
2025	8	6	14
2026	13	7	20
Total	**36**	**32**	**68**

Table 1: Documented data breach incidents by year and sector.

For each incident, TGI logged the data exposed, the vector (where known), who discovered the breach, whether the organisations acknowledged it, whether any post-mortem followed, and the verification status of the claim.

DIVERSITY OF AFFECTED ORGANISATIONS AND THE UNDERLYING RISKS

Upon mapping the distribution of the reported data breach incidents, it is evident that the affected organisations span a broad cross-section of Bangladesh's institutional landscape, cutting across government and non-government agencies and multiple sectors. With the exception of 2024, data breach incidents were more frequent in the public sector than in the private sector every year for the covered period.

Count of Type of Breached Organization

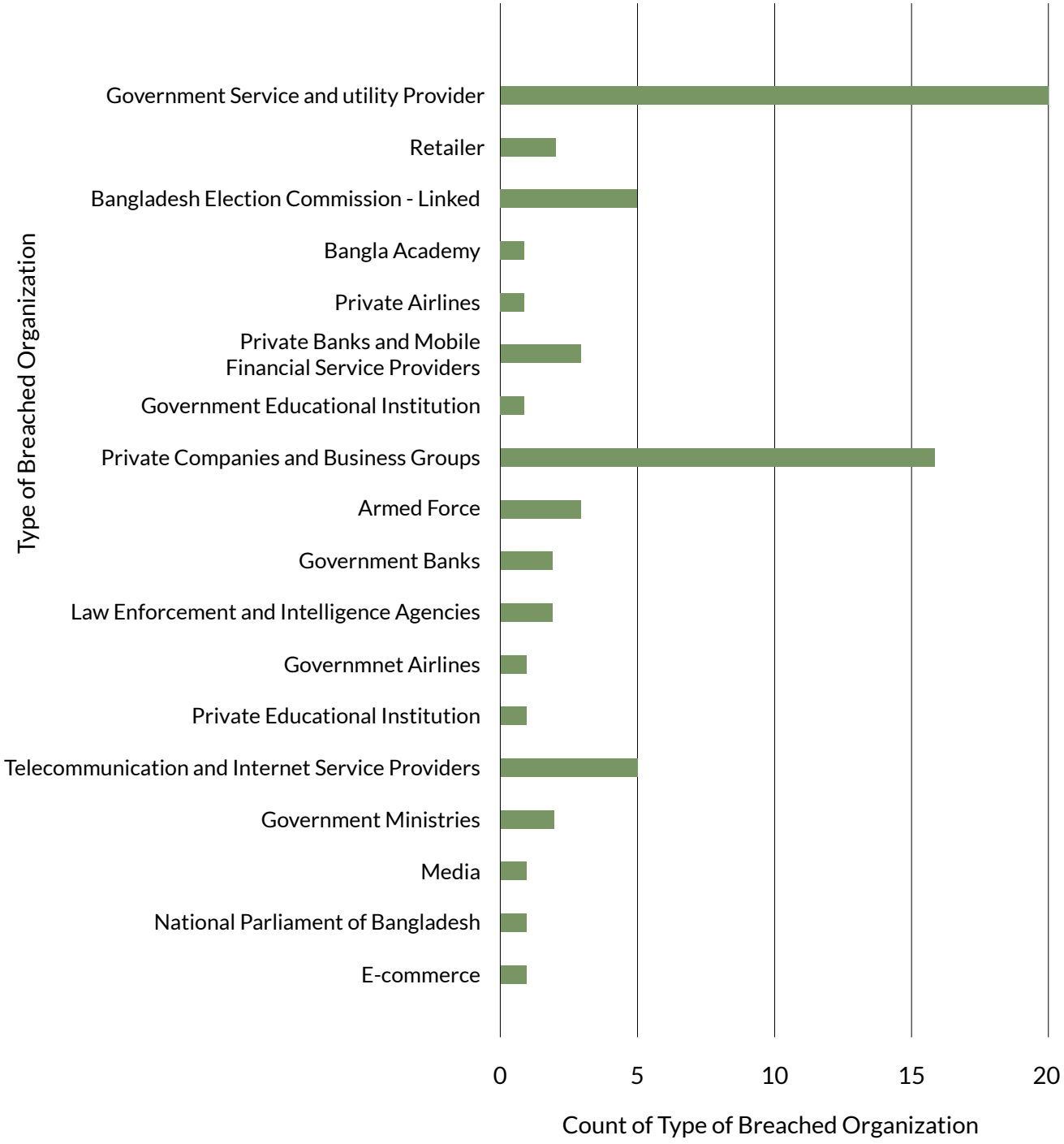


Figure 2: Approximate distribution of data breaches by organisation type.

A closer look at the affected entities shows that the overwhelming majority are formally structured organisations — government ministries, regulatory bodies, financial institutions, registered private enterprises, and other entities that maintain large-scale databases containing extensive personal information on citizens — rather than informal or unregistered entities. While indicative, this pattern should not be interpreted as suggesting that organisational scale alone determines exposure. Rather, it reflects one of several factors that shape cybersecurity risk in an increasingly digitalised economy, where the growing volume and value of data held by public and private institutions, together with extensive digital infrastructure, interconnected systems, and large repositories of PII, make certain organisations particularly attractive targets. At times, the incentive lies not merely in the volume of data, but in its economic or strategic value. For example, institutions connected to overseas employment and inward remittances may hold information on individuals with predictable income flows, making such datasets especially valuable to cybercriminals.

Of particular concern is the presence of highly sensitive state agencies within the breach list, most notably the National Telecommunication Monitoring Centre (NTMC). The NTMC is known to intercept phone calls, emails, and social media communications, to collect and retain communication data, to filter and block online content, and to support broader national security and public order objectives through communication intelligence. It reportedly operates a platform through which nearly 500 officials from 42 public organisations are authorised to access citizens' data for verification and investigative purposes. According to reports, the NTMC system was exploited using the credentials of two law enforcement officers to collect and sell via encrypted messaging services confidential information, including NID information and mobile call data records (CDR), for financial gain. An incident of unauthorised access and data exfiltration and breach involving an agency of this nature is categorically different from a breach at a retailer or news portal as the data it handles is not merely personal or financial, but intercepted communications and surveillance records that, if exposed or misused, could compromise the privacy and safety of individuals being monitored, reveal intelligence methods, or be exploited by malicious actors for blackmail, targeted harassment, or further unauthorised surveillance.

Another notable case is the alleged breach of the database of the Ministry of Expatriates' Welfare and Overseas Employment, a government ministry that collects and handles records of millions of Bangladeshi migrant workers. The compromised data reportedly included passport records, NID information, electronic tax identification number (eTIN) details, and financial and banking documents along with transaction records. This category of data is exceptionally sensitive, as it combines identity verification, tax, and financial information in a single dataset — information that could be exploited for multiple malicious purposes, including voter manipulation, blackmail, identity-based scams, and financial fraud targeting one of the country's most economically significant demographics.

Similarly, the appearance of armed forces agencies, ministries, and the Bangladesh

Election Commission among the breached entities raises the stakes considerably. These institutions are custodians of information tied directly to national security, governance integrity, and the democratic process. A breach at the Bangladesh Election Commission warrants particular attention: it is the most recurrent institution in the dataset, linked to at least five incidents — the exposure of NID-linked voter data on Telegram in October 2023, the leakage of citizens' NID data through five partner organisations' verification access in February 2025 and two others in May 2025, the insider syndicate uncovered by the Criminal Investigation Department (CID) in January 2026, and the exposure of roughly 14,000 journalists' accreditation records through a flaw in an electoral agency-run portal days later. Two features of this record require elaboration. First, in none of these cases has an external intrusion into the agency's central NID database been publicly established; the agency has maintained that its core systems were not hacked, and nothing in our dataset contradicts that. Second, and precisely because of that, the recurring failure mode is the ecosystem built around the database — authorised third-party verification channels, several of them operated by private institutions, and insiders holding valid credentials. Data leaked through an authorised channel is no less exposed than data exfiltrated from the Bangladesh Election Commission, but the remedy differs: it turns less on firewalls and more on access governance, contractual controls, continuous monitoring, and sanctions.

Unlike breaches in the commercial sector, where the primary harm is typically financial or reputational, breaches in this category carry the potential to escalate into incidents with national security implications or to directly infringe on citizens' fundamental rights.

A TIMELINE OF DATA BREACHES, CIRCA 2023 - 2026

When the 68 incidents of data breaches are thoroughly collated chronologically with an incident log carrying several data points, it shows a clear escalation over time in terms of both frequency and severity. The earliest incidents were largely ransomware campaigns and isolated database exposures. Over time, however, the threat landscape broadened into large-scale leaks of citizen data and attacks on critical infrastructure, government agencies, financial institutions, telecommunication providers, and major private firms.

As the incidents accumulate, a second pattern is observed, which points towards institutional negligence and lack of preparation.

Date	Organisation	Exposed Data Type	Discovered Through	Verification
Jul 2023	Office of the Registrar General, Bangladesh Birth & Death Registration. (Government)	Names, NID, phone, email - about 50 million citizens	External researcher; reported by TechCrunch	Verified
Oct 2023	Smart NID voter data, via authorised third-party access. (Government / Private)	NID numbers, photographs, parents' names, phone, address	Surfaced through a public Telegram channel.	Verified
Nov 2023	National Telecommunication Monitoring Centre. (Government)	Names, NID numbers, phone records, passport & bank details, fingerprint images	External security researcher (via WIRED), NTMC denied	Verified
Jun 2024	myLocker, government-backed document-storage platform under the Digital Bangladesh programme. (Private)	Names, email, phone, NID, dates of birth - about 2.5M users	Listed for sale on a dark-web forum	Verified
Nov 2024	bKash, mobile financial service. (Private)	10M+ user records claimed, as well as service & telecommunication metadata	Claim posted on a dark-web forum	Unverified claim

Date	Organisation	Exposed Data Type	Discovered Through	Verification
Dec 2024	Bangladesh Police. (Government)	Records of 100,000+ officers, government system login credentials, as well as at least 50 types of case related information retained in Crime Data Management System	Newspaper investigation (Prothom Alo)	Verified
Jul 2025	Bangladesh Road Transport Authority (BRTA). (Government)	NID, passport, parents' names, addresses - about 1M+ claimed	Listed for sale on a dark-web forum	Unverified claim
Dec 2025	Shwapno, supermarket chain. (Private)	Names, phone numbers, purchase history - about 4M customers	Data surfaced on social media, reported by major news outlets	Verified
Apr 2026	Ministry of Expatriates' Welfare & Overseas Employment. (Government)	Passport, NID, eTIN, financial & banking records (claimed)	Offered for sale on a dark-web forum, covered by Brinztech	Unverified claim
May 2026	Bureau of Manpower, Employment & Training (BMET). (Government)	Passport, NID, addresses, registration records, pre-departure orientation enrollment information, and emergency contacts	Advertised on a darkweb forum	Unverified claim

Table 2: A non-exhaustive list of major data breach incidents, covering both verified and unverified cases. A complete table listing all documented incidents can be found in the Appendix.

The following is a closer dissection of these findings, year by year

2023: 2023 saw an escalation in ransomware attacks that expanded to strategically important institutions, including state-owned Biman Bangladesh Airlines and Bangladesh Krishi Bank. In the latter case, the ransomware group reportedly exfiltrated more than 170 GB of sensitive information, including financial and employee records, indicating the growing sophistication of extortion-driven cybercrime targeting Bangladesh.

A major turning point occurred in 2023 with the exposure of citizen data on an unprecedented scale. In November, a database reportedly linked to the NTMC exposed highly sensitive information belonging to millions of citizens, including names, addresses, NID numbers, passport information, banking details, phone records, vehicle registrations, and even biometric data. Following a report by the Wired, the NTMC reportedly issued a formal denial, refuting claims of any data leaks originating from its systems.

Months earlier, in July, another publicly accessible government database maintained by the Office of the Registrar General, Birth and Death Registration reportedly exposed information relating to more than 50 million citizens, including names, phone numbers, email addresses, and NID numbers. Although investigations suggested that the exposure resulted from insecurely configured online systems rather than a conventional intrusion, the authorities have admitted its failure to determine the extent of the breach. These incidents represented some of the largest known data leaks in Bangladesh's history and highlighted systemic weaknesses in public-sector data governance and security practices.

The year 2023 also witnessed the widely discussed and debated Smart NID data leak. Personal information associated with the national identity system became accessible through a Telegram bot and channel, enabling unauthorised users to retrieve voter information, photographs, addresses, and family details upon prompting the bot. Although authorities stated that the Bangladesh Election Commission's central database had not been directly compromised, the incident indicates vulnerabilities in third-party access mechanisms and demonstrates how data-sharing ecosystems can become a significant source of privacy risks.

2024: Throughout 2024, the diversity of sectors affected by data breaches increased substantially. Educational institutions, telecommunications companies, internet service providers, non-governmental organisations, e-commerce platforms, and government agencies all appeared among breached organisations. For instance, faculty information from United International University was reportedly leaked on underground forums, while Aamra Networks suffered a compromise involving Citrix infrastructure and internal credentials. A database containing sensitive information belonging to 5,991 employee users, alongside 10,000 employee entries from TranscomBD, was advertised for sale on cybercrime forums. Similar incidents affected organisations such as Volunteer for Bangladesh, Bangladesh-China Youth Student Association, Tappware, myLocker, and Travela.xyz, StylehoodBD, and Foodi, exposing personal information including names, contact details, account credentials, customer records, and transaction-related data.

Critical infrastructure organisations also became prominent targets during 2024. More than 110,856 customer records belonging to Dhaka Electric Supply Company (DESCO) were reportedly leaked, exposing customer identifiers, contact details, and addresses. Moreover, the Road Transport and Highways Division experienced a database compromise affecting training and administrative records, while Titas Gas allegedly had root-level access to its firewall infrastructure sold on underground markets. These incidents raised concerns that cyberattacks were increasingly targeting organisations responsible for essential public services. At the same time, ransomware campaigns reportedly affected institutions such as the Bangladesh Police, Agrani Bank, Popular Life Insurance, Globe Pharmaceuticals, and educational institutions, indicating that public and private entities in Bangladesh continue to attract financially motivated threat actors.

By late 2024, breaches increasingly involved highly valuable datasets. A threat actor claimed to have compromised and obtained data associated with over 10 million bKash users, while another incident allegedly exposed applicant information from recruitment platform of Unilever, including names, addresses, phone numbers, and user accounts. These cases illustrated how both consumer-facing services and human-resource platforms had become significant repositories of sensitive information vulnerable to compromise.

2025: The pattern intensified further in 2025, when government agencies emerged as particularly attractive targets, with alleged breaches affecting the Ministry of Road Transport and Bridges and the Bangladesh Road Transport Authority; the latter listing alone reportedly involved over one million records containing NID numbers, passport information, contact details, and residential addresses.

Even more concerning was a July 2025 forum listing offering approximately 4.1 million birth and death registration records, including detailed civil registration data and extensive PII. This listing should not be conflated with the July 2023 exposure of the same registry: the available evidence does not establish whether it reflects a fresh compromise or the repackaging and resale of data already exposed in 2023. Either reading is troubling — a new breach would indicate that the registry's security posture had not materially improved two years after its first exposure, while a resale would demonstrate that citizens' civil-registration data, once leaked, continues to circulate and retain market value indefinitely.

The most consequential 2025 development, however, sat inside the NID ecosystem itself. In February, the Bangladesh Election Commission confirmed that five partner organisations — the Directorate General of Health Services, UCB Fintech's Upay, the Chattogram Port Authority, the Department of Women Affairs, and the Ministry of Finance's iBAS++ — had likely leaked citizens' NID data to third parties through their verification access, and issued show-cause notices. In May, the electoral agency suspended the verification access of two other organisations, Ansar-VDP and BRAC Bank, on the same grounds. Evidence does not indicate that the episode involved an intrusion into the agency's own database; both involved the authorised data-sharing channels built on top of it — a reminder that every organisation granted verification access effectively extends the perimeter of the national identity system.

The private sector also remained vulnerable during 2025. Evaly, a non-operational online

marketplace, reportedly suffered a breach affecting more than 783,611 users, exposing customer and merchant information, including names, phone numbers, addresses, and order records. Link3 Technologies, one of the country's largest internet service providers, allegedly experienced a compromise affecting approximately 189,000 customers and employees, exposing subscription details, account credentials, contact information, and addresses. Another significant case involved FR Express, where source code, configuration files, operational systems, and infrastructure details were reportedly leaked, illustrating a shift from simple data theft toward the exposure of sensitive technical assets.

2026: The trend continued into 2026, with numerous alleged breaches targeting government agencies and critical information systems. Until May 2026, these included alleged compromises involving the Ministry of Expatriates' Welfare and Overseas Employment, the Bureau of Manpower Employment and Training, the Directorate General of Drug Administration, the Bangladesh Agricultural Development Corporation, and Bangladesh Water Development Board. Several incidents reportedly exposed internal databases, source code repositories, administrative credentials, migrant worker records, and critical operational information. Particularly concerning were allegations involving the Bangladesh Armed Forces and its military infrastructure, where threat actors claimed access to sensitive network and operational data. Although many of these claims remain unverified, they indicate a growing interest among threat actors in targeting strategic government systems.

Earlier in the year, in January 2026, also produced the starkest demonstration yet of the insider problem. An investigation by the CID uncovered a syndicate operating through an office assistant and an outsourced data-entry operator at the Bangladesh Election Commission, using nationwide-access credentials to access and sell more than 365,000 citizens' NID records within a single month; two men were arrested. No intrusion was required — the credentials were valid, and the access was, on paper, authorised. Weeks later, a flaw in the electoral agency's newly mandated online accreditation portal exposed the personal data of roughly 14,000 journalists who had applied to cover the 2026 national elections — names, NID numbers, phone numbers, photographs, signatures, and complete application documents; the portal was taken offline after the exposure was reported, but the authority issued no statement on whether the data had been copied or disseminated.

What the timeline shows

Over nearly four years, the picture displays a persistent pattern of large-scale data exposures across both the public and private sectors. What follows the breach is the most telling of all — relative silence and inaction. More often than not, the affected institutions have failed to find the breach, not acknowledging it once others did, and never accounting for how it happened. What recurs across these years is a trend of concealment: breaches brushed over, denied, or left to fade, while the same failures insecure databases, loose access controls, leaky third-party arrangements, compromised credentials go unaddressed or are secretly patched because they are never openly named. Most importantly, the progression of incidents shows that Bangladesh's digital transformation has been accompanied by an expanding attack surface, making robust cybersecurity governance, stronger regulatory oversight, and improved institutional security practices increasingly urgent.

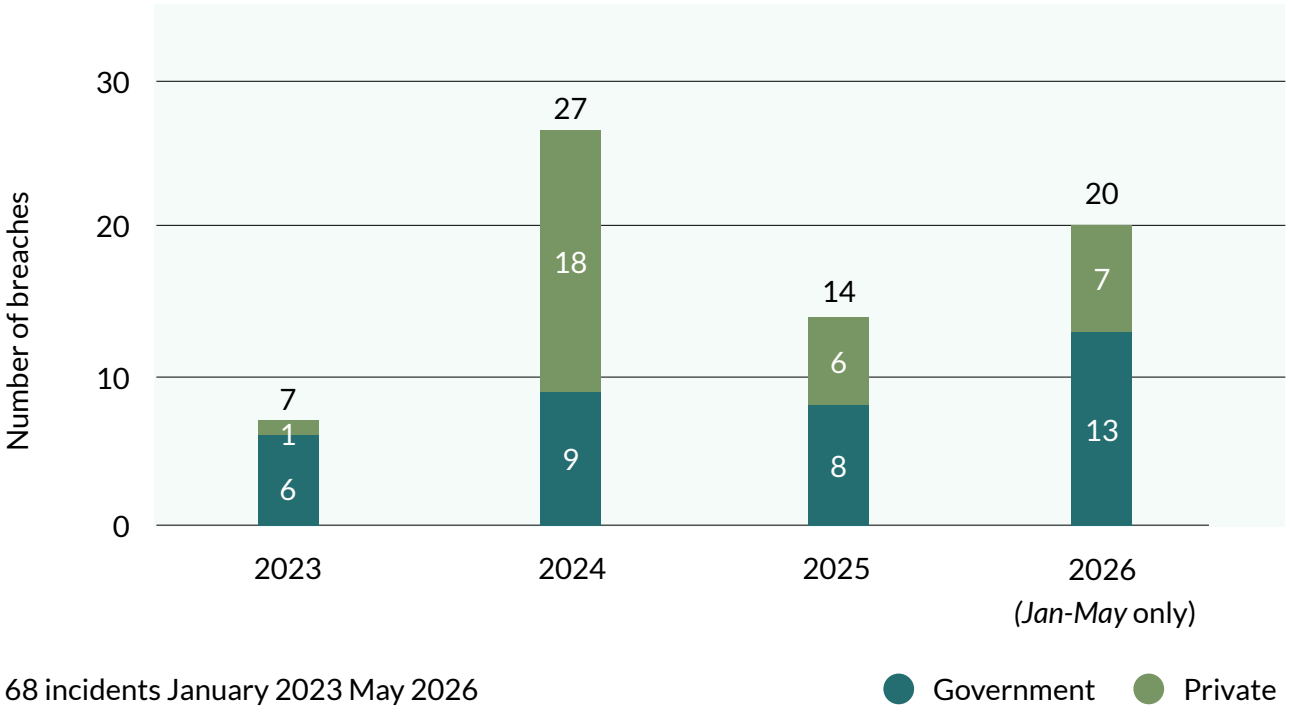


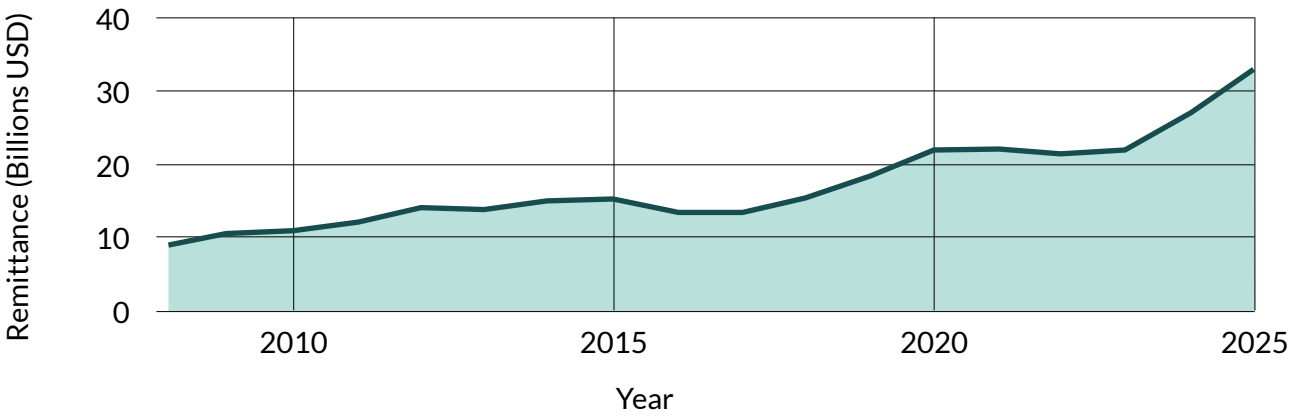
Figure 3: Documented data breach incidents in Bangladesh by sector between January 2023 and May 2026.

Additionally, aggregated totals tend to flatten the picture. A count of incidents tells you how often breaches happened, but it cannot tell you that the same target was hit deliberately, more than once. Several institutions in the dataset were targeted, or claimed as targets, on separate occasions: the Bangladesh Election Commission's NID ecosystem (five incidents, discussed above — through partner channels, insiders, and a flawed portal rather than any established intrusion into the central database), the country's road-transport agencies (one verified breach followed by two unverified sale listings), the armed forces (three separate leak-site claims, none independently verified and one made by an actor known to recycle false claims), and, most tellingly for what follows, the country's migrant-worker data systems.

In April and May 2026, databases linked to the Ministry of Expatriates' Welfare & Overseas Employment, its overseas-worker platforms, and the manpower and training bureau were advertised on criminal forums three separate times within roughly six weeks, together involving claims of well over a million migrant-worker records, passport details included. Bangladesh's labour migration is one of the load-bearing pillars of the country's economy. Remittances sent home by overseas workers surpassed thirty billion dollars in the 2024-25 financial year, a national record, and now equal roughly 6.57 percent of gross domestic product, which finances close to half of the country's import bill. More importantly, the attacker(s) are seemingly aware that this is not a one-time flow but a recurring one. Remittances proved

resilient through the COVID-19 pandemic and rebounded within months of the political upheaval of 2024, because the underlying behaviour of a worker abroad sending money to family at home repeats month after month and year after year. In fact, the latest data show that remittance inflows reached US$ 3.42 billion in May 2026, more than 15% higher year-on-year than the US$ 2.96 billion recorded in May 2025. A breached passport number or overseas contact detail is valuable every time the next remittance is due, as it can be leveraged repeatedly for phishing, identity fraud, account takeover attempts, and other scams timed to intercept or exploit recurring financial transactions. Evidently, remittances are predictable and repeated, and that rhythm turns the workers behind them into predictable, repeated marks.

Yearly Remittance Inflows to Bangladesh



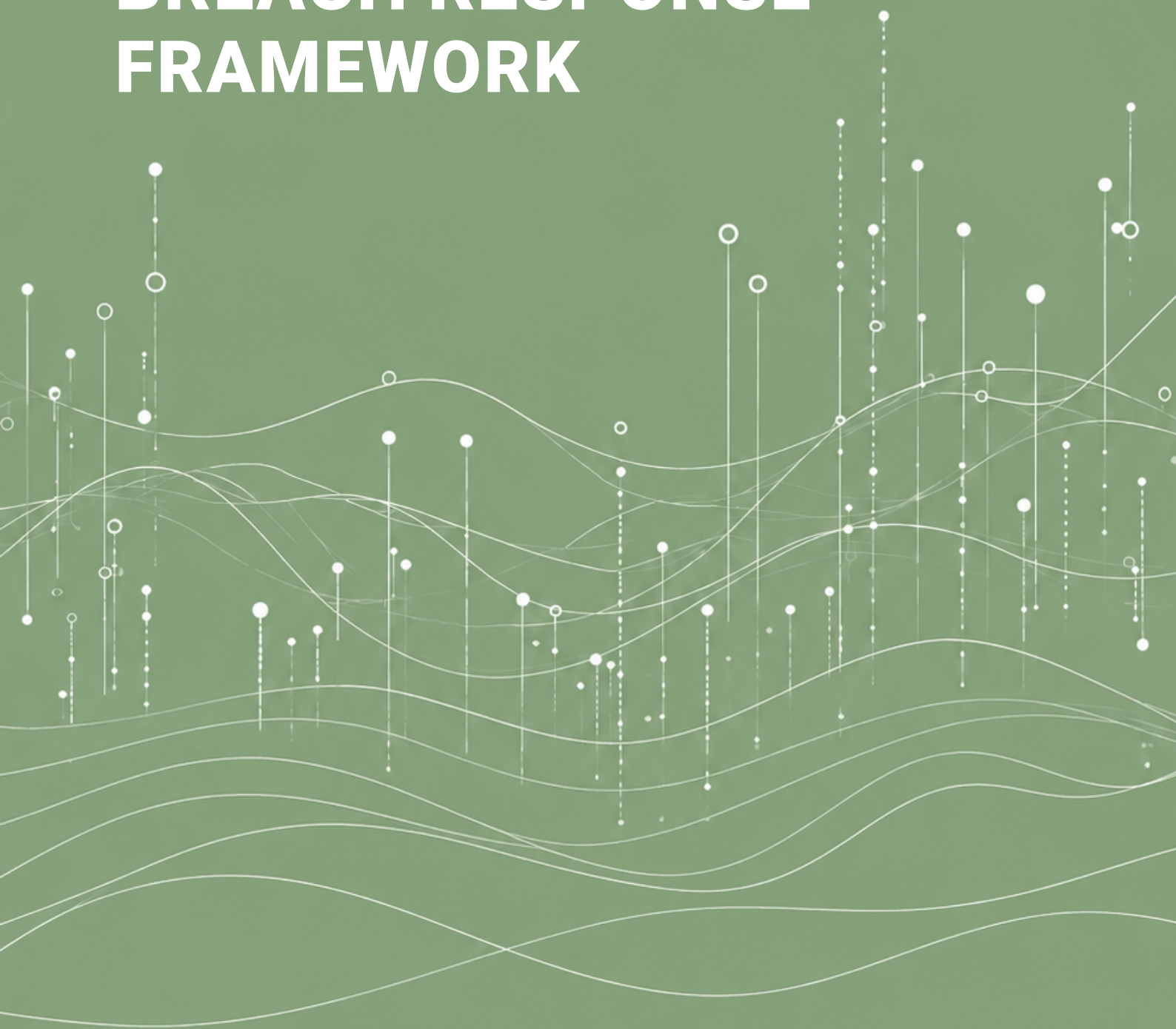
Source: Bureau of Manpower Employment & Training

Figure 4: Annual remittance inflows from migrant workers to Bangladesh between 2008 and 2025, rising from approximately US$ 9 billion in 2008 to more than US$ 32 billion in 2025.

Crucially, the population exposed is among the most vulnerable to follow-on fraud: migrant workers and their families, who already navigate multiple middle players and associates, are exactly the people a scammer armed with a leaked passport number and other PII can most easily deceive. It is equally concerning in democratic context, as malicious actors can exploit the personal credentials of citizens living abroad to engineer proxy voting, manipulate postal ballots, or execute targeted voter suppression. Given the large number of overseas Bangladeshis, such breaches pose significant risks to the integrity and credibility of national elections.

The bigger takeaway that the timeline and the aggregates tells one is that the data being exposed has grown more permanent and more central to civic life over time, even as the institutions holding it have shown, through repeated breaches, that they are not learning from each hit.

LEGAL ANALYSIS: THE ACCOUNTABILITY DEFICIT IN BANGLADESH'S DATA BREACH RESPONSE FRAMEWORK



Between January 2023 and May 2026, Bangladesh recorded at least 68 reported data breach incidents across public and private institutions, with incidents recurring at an elevated tempo in every year since 2024.. A review of available sources on these 68 incidents identifies limited instances in which legal actions were meaningfully pursued against a breached entity or a responsible party. This absence of enforcement is significant not simply because Bangladesh lacks adequate statutory framework governing data protection, but because the frameworks that exist have not yet produced an operative accountability mechanism capable of translating statutory rights and obligations into enforceable outcomes.

At present, Bangladesh's data governance architecture comprises both sector-specific instruments and a newer, more comprehensive suite of laws enacted in recent months. For instance, the *National Identity Registration Act, 2023* treats NID information as confidential and criminalises unauthorised access to and disclosure of such information. It also simultaneously preserves formal pathways for third-party access, although those conditions remain vague and insufficiently defined in practice. While there have been reports of investigations and arrests in connection with the alleged unlawful access to and sale of NID information from within the Bangladesh Election Commission, the cases involved operational and support personnel, not senior officers. It also remains unclear whether the accused were ultimately prosecuted under the statute, and whether the incidents prompted broader institution-wide reforms to strengthen governance and oversight. Similarly, although the Bangladesh Election Commission has, on several occasions, suspended or terminated NID verification access for third-party organisations following alleged data irregularities, there is little publicly available information on whether the individuals responsible were subject to legal or disciplinary sanctions beyond the suspension or termination of their organisations' access.

Within the banking sector, the *Bank Companies Act, 1991*, for instance, restricts the cross-border transfer of banking information while mandating confidentiality in information management. Similarly, the *Bangladesh Telecommunication Act, 2001* criminalises the unauthorised disclosure, by telecommunications operators and associated individuals, of information transmitted over telecommunication networks, while prohibiting regulatory officials from unlawfully disclosing information obtained in the course of their duties. Yet, despite repeated incidents involving unauthorised disclosures and data breaches across both sectors, these statutory frameworks are structured around isolated and narrowly framed provisions that focus on confidentiality and the penalisation of unauthorised disclosure, rather than forming part of a coherent and integrated regulatory scheme; they provide comparatively little by way of comprehensive data breach governance, such as mandatory breach notification, clear institutional responsibilities following a breach, regulatory oversight, or meaningful avenues of accountability and redress for affected individuals. Equally significant is the apparent absence of publicly reported, precedent-setting judicial or administrative decisions in which these provisions have been used to establish institutional accountability or provide effective

remedies to individuals affected by large-scale data breaches or unauthorised disclosures.

Previously, under the now-repealed *Digital Security Act, 2018*, it was a criminal offence to collect, sell, possess, supply, or use another person's PII without lawful authority. Yet, during the law's five-year operation between 2018 and 2023, despite more than 7,000 cases reportedly being filed under it, there appear to have been no publicly reported prosecutions invoking this provision in relation to data breach incidents. More broadly, while the repealed statute and its three successor enactments — including the currently operative *Cyber Protection Act, 2026* — have all contained offences relating to hacking or unauthorised access to computer systems, there likewise appear to have been no publicly reported prosecutions in which those provisions were invoked in connection with major data breach incidents arising from hacking or unauthorised access over nearly eight years of Bangladesh's cybercrime legislation.

A more comprehensive data accountability framework, the *Personal Data Protection Act, 2026*, emerged only recently and, for the first time, defined and introduced a statutory data breach notification obligation. However, the obligation is narrowly framed: notification is required only where a breach is likely to cause "significant damage" to the data subject, while the form, content, and timeframe for notification are deferred to future regulations. This creates uncertainty for data fiduciaries as to when the notification duty is triggered and how it is to be operationalised. Moreover, the provision mandates notification to the Personal Data Protection Authority, but does not expressly require timely notification to affected data subjects, thereby limiting its immediate utility as a mechanism for enabling individuals to mitigate the consequences of a breach.

Zooming out, despite recognising data-subject rights and requiring data fiduciaries and processors to implement appropriate technical and organisational safeguards, the statute's data breach framework falls short of ensuring meaningful accountability in several respects that remain central to any serious legal diagnosis.

First, its implementation is subject to delayed commencement, leaving key elements of the enforcement and institutional framework in abeyance even after enactment. As a result, failures to comply with the breach notification obligation during the transitional period may not attract regulatory scrutiny or statutory penalties, nor can incidents occurring during that period be sanctioned retrospectively once the law becomes fully operational.

Second, the enforcement model remains predominantly regulator-centred rather than victim-centred: the statute does not establish an independent civil cause of action for data breach through which affected individuals may seek relief before the ordinary courts without first engaging the regulatory authority, nor does it clarify how the compensation mechanism, prescribed without defined parameters, could be operationalised in practice. Additionally, the scale of available administrative penalties may not fully correspond to the scale of harm: maximum fines ranging between BDT 2.5 million and 5 million may be insufficient for large-scale data controllers processing population-level personal and sensitive data.

Third, the *National Data Management Act, 2026 establishes* an expansive interoperability

and centralised data-governance framework through mandatory database integration, a national data exchange infrastructure, and executive authority over certain categories of information, while also empowering the regulator to require compulsory storage of such databases within national data centers. Without robust accountability mechanisms, these provisions increase the surface area of exposure in the event of a data breach.

Fourth, and most importantly, the statute contains broad exemptions permitting the processing of personal data on grounds including national security, defence, public order, public interest, and the prevention, detection, investigation, or prosecution of offences, in addition to various governmental functions. While such exemptions are not uncommon in comparative data protection legislation, their breadth, coupled with the absence of robust oversight mechanisms, raises legitimate concerns in Bangladesh's institutional context. Even if these exemptions do not extend to data breaches, if violations by public officials are treated primarily as internal departmental misconduct rather than as matters attracting independent regulatory liability, compensation, personal accountability, and public disclosure, deterrence may be substantially weaker than in the private sector. Given that public bodies are among the country's largest collectors and processors of personal data, and account for the largest share of documented breach incidents in this report, the framework leaves unresolved the question of how meaningful accountability will be secured in a high-risk digital ecosystem where the entity responsible for a breach is itself a public authority operating within or adjacent to these exemptions.

Viewed collectively, the laws assessed leave an accountability vacuum. Statutory obligations exist, and remedial provisions are drafted, but the questions of who bears responsibility for a breach, through which forum liability is to be established, and under what timeline enforcement is to occur, remain legally unsettled. Until the transitional provisions are activated, the interlocking relationship between administrative, civil, and criminal remedies is clarified, the interpretation of the exemptions is settled, and the independence of the enforcing authority from public-sector fiduciaries is institutionally secured, Bangladesh's data protection regime is likely to remain, as the pattern across the 68 documented incidents — the overwhelming majority of them never publicly investigated, remediated, or even acknowledged — suggests, a framework of formal rights without a corresponding structure of practical enforcement.

RECOMMENDATIONS

Amend the data-law framework before scaling integration. Bangladesh government should revise its current data, cybersecurity, telecommunication, and national identity laws so that further digital integration proceeds only within a framework that is clearly rights-respecting and secure. At a minimum, the legal architecture should guarantee strict purpose limitation, data minimisation, necessity and proportionality tests for high-risk data exchange, data retention limitation, clear thresholds for access to identity-linked data, mandatory notification to both regulators and affected individuals after serious breaches, enforceable rights to correction and remedy, and genuinely independent oversight and redressal mechanism.

Make operational security and disclosure legally mandatory. Bangladesh government should make pre-deployment standard operating procedures a legal requirement for all high-risk identity, telecommunication, and data-exchange systems. This should entail independent security testing, impact assessments, API governance, vendor storage restrictions, least-privilege access, logging and retention controls, time-bound user notification, and post-incident reporting.

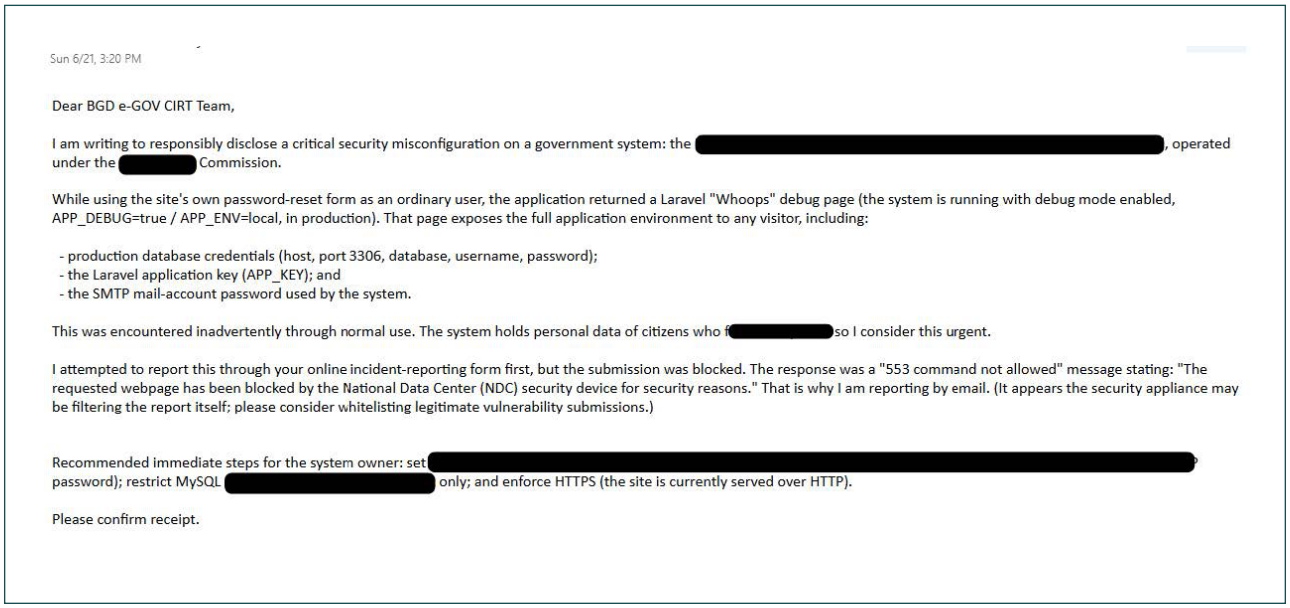
Make government systems secure before they launch, not after they leak. Adopt a secure-by-design baseline for public digital services: no system handling NID, biometric or registry data, or other PII can go live without independent penetration testing (in other words, hiring a *friendly burglar to break in and show you how*), as well as an access-control review and a signed risk acceptance. Several documented incidents in 2026 occurred shortly after the affected systems became operational, suggesting that stronger pre-deployment baseline security assurance could have reduced the risk of compromise. At the same time, because the technical root causes of most breaches are never publicly disclosed, it is difficult to assess whether the baseline can be expected to prevent most incidents. These security requirements should also be embedded in government procurement, so that the outside vendors and contractors who build these systems are held to the same standard, including basic secure-development practices such as never storing passwords, encryption keys, or other credentials within application source code.

Re-architect the identity core for a world where breaches are inevitable. Treat the most sensitive national registries on Zero Trust principles — the security philosophy of treating a network like a high-security building where every internal door requires your badge to be checked, rather than a castle with a single gate and unrestricted movement once inside. Put differently, identity, authentication, and permission should be verified at every checkpoint, every time, no matter how a user or device initially gained access.. What this means in practice is separating the NID and biometric databases from public-facing websites; giving each employee access only to the information necessary for their role; requiring a second authentication factor (such as a code generated on a mobile phone, so that a stolen password alone cannot be used to gain access) for every administrative account; and maintaining comprehensive audit logs so that suspicious activity can be detected quickly. These measures should be complemented by offline, regularly tested backups, reducing the leverage of the "we copied your files too" element of double-extortion attacks.

Build the capacity a fast-digitising country needs. Establish a national detection capability, a security operations centre, and threat hunting and dark-web monitoring as a corestate capability so the country stops outsourcing breach discovery to private monitors and volunteers by default. Extend cybersecurity training beyond banking into utilities, health, and local government, and create shared security services for the small institutions that cannot staff their own security operations. Pair every digital-service rollout with plain public education: how to recognise an impersonation call that quotes your real order history and what to do about a SIM-swap attempt. The citizen is the last line of defence precisely because the data has already leaked.

UNEVEN FUTURE REQUIRES STRONGER FUNDAMENTALS

In June 2026, while compiling this report, TGI's research team conducted a routine assessment of a public-facing government portal. During a standard test of the portal's password recovery feature, the backend server crashed. Because the application had been left running in debug mode, the error response exposed the portal's entire internal configuration file directly in the browser. What appeared on our screen was a comprehensive snapshot of the internal architecture: plain-text administrative passwords to the master database, the cryptographic keys used to validate all active user sessions, and the login credentials for the government's official email system. Anyone in possession of the exposed credentials could potentially authenticate as a legitimate user from within the trusted environment, leaving the system unable to distinguish between an authorised user and an attacker using the compromised credentials. The findings were reported to the Bangladesh Computer Emergency Response Team (BGD e-GOV CIRT) the same day. Their official response did not dispute anything we had documented; in fact, it acknowledged identifying further gaps in the system.



Sun 6/21, 3:20 PM

Dear BGD e-GOV CIRT Team,

I am writing to responsibly disclose a critical security misconfiguration on a government system: the [redacted], operated under the [redacted] Commission.

While using the site's own password-reset form as an ordinary user, the application returned a Laravel "Whoops" debug page (the system is running with debug mode enabled, APP_DEBUG=true / APP_ENV=local, in production). That page exposes the full application environment to any visitor, including:

- production database credentials (host, port 3306, database, username, password);
- the Laravel application key (APP_KEY); and
- the SMTP mail-account password used by the system.

This was encountered inadvertently through normal use. The system holds personal data of citizens who f[redacted] so I consider this urgent.

I attempted to report this through your online incident-reporting form first, but the submission was blocked. The response was a "553 command not allowed" message stating: "The requested webpage has been blocked by the National Data Center (NDC) security device for security reasons." That is why I am reporting by email. (It appears the security appliance may be filtering the report itself; please consider whitelisting legitimate vulnerability submissions.)

Recommended immediate steps for the system owner: set [redacted] password); restrict MySQL [redacted] only; and enforce HTTPS (the site is currently served over HTTP).

Please confirm receipt.

Figure 5A: TGI's same-day disclosure email to BGD e-GOV CIRT on June 21, 2026, reporting the exposed configuration file and credentials. Sections identifying the affected portal and the exposed credentials have been redacted for security reasons, as the underlying issues had not been confirmed as fully remediated at the time of writing this report.

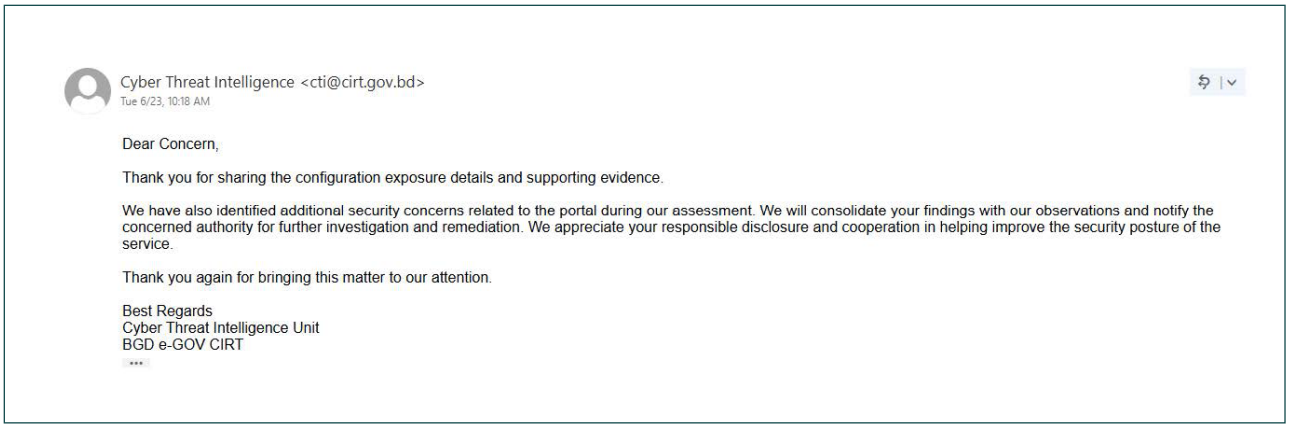


Figure 5B: BGD e-GOV CIRT's response on June 23, 2026 acknowledging TGI's disclosure and noting that its own review had identified additional gaps in the system.

Bangladesh is undergoing an ambitious digital transformation, and the political and institutional momentum behind this expansion is evident in its rapid adoption across both the public and private sectors. Yet the foundational disciplines that underpin secure digital infrastructure — routine security audits, configuration management, identity governance, and continuous assurance — have not matured at a commensurate pace. Our assessment is that the country's most immediate cybersecurity risks receive neither the policy priority nor the public attention they warrant. Instead, the discourse is often drawn toward more politically salient and technologically fashionable issues, such as artificial intelligence, online content regulation, and foreign influence operations, while the less visible but far more consequential investments required to reduce systemic risk remain persistently neglected. The exposures documented in this report are therefore attributable not principally to exceptionally capable adversaries, but to an institutional culture of complacency reflected in preventable failures of governance, security engineering, and operational discipline. In such an environment, sophisticated adversaries need not overcome robust defences; they need only exploit weaknesses that should never have remained exposed.

APPENDIX

Methodology

This report utilises a descriptive, exploratory mixed-methods design to investigate the landscape of data breaches in Bangladesh between January 2023 and May 2026. By combining quantitative content analysis with qualitative thematic analysis, we map the frequency, distribution, and systemic patterns of data breach incidents across both public and private sectors.

The primary dataset was compiled from 68 documented incidents. We aggregated information from four distinct categories of sources to understand the threat environment:

Localised threat intelligence: Advisories from the Bangladesh Cyber Security Intelligence (BCSI).

International dark-web monitoring: Data from platforms such as Ransomware.live, Ransomlook.io, and RedPacket Security.

Threat-alert aggregators: Information sourced from active threat-intelligence channels, including *Daily Dark Web*.

Mainstream media reporting: Coverage from national dailies, specifically *The Daily Star*, *Prothom Alo*, and *The Business Standard*.

For each recorded incident, we systematically logged eight data points: date; organisation and sector; type of data exposed (as claimed); attack vector (where known); discovery mechanism; whether the organisation acknowledged the incident; whether any post-mortem was published; and the verification status of the claim.

To complement our quantitative findings, we conducted a qualitative policy and legal analysis to contextualise the regulatory environment governing these breaches. This involved a systematic review of Bangladesh's sectoral and general data and identity laws, including the *National Identity Registration Act, 2023*, as well as those governing cybersecurity, banking, and telecommunication sectors. We also reviewed the *Personal Data Protection Act, 2026* and the *National Data Management Act, 2026*. By tracing the historical progression, we aimed to evaluate the "sequencing gap" between the rapid deployment of digital public infrastructure and the delayed development of rights-protective privacy legislation. This analysis specifically examined, at a high level, how vague provisions, wide executive discretion, and fragmented enforcement mechanisms, rather than a total absence of law, contributed to the systemic vulnerabilities and institutional silence observed in our incident dataset.

It is important to note three limitations regarding this dataset. First, it reflects only reported and discoverable breaches; the true frequency of incidents is almost certainly higher. Second, because we rely on a mixture of official advisories, news reports, and third-party threat-intelligence claims, the volume figures cited are often based on the claims of the threat actors themselves, which may be exaggerated for extortion purposes. We have categorised these findings with confidence tiers distinguishing between verified incidents, reported but unconfirmed events, and unverified dark-web claims to ensure transparency regarding the evidentiary strength of each case. Third, incident

narratives are summarised for this report, and where specific data samples are discussed, they are treated in aggregate to maintain the privacy of the victims. Every incident in the table is hyperlinked to at least one source. The sole exception applies where the only available link points directly to leaked data, an active sale listing, or a threat-actor channel: publishing such a link would further amplify the exposure of victims' information. These entries are marked with an asterisk (*) and the link is withheld.

Incident Table

All 68 documented incidents (January 2023 – May 2026)

Verification. Where a field cannot be established from the available evidence it is marked plainly ("Not disclosed", "None published", "No public acknowledgment found").

Verification key.

Verified = confirmed by a national authority (BCSI or CIRT), the breached organisation's own acknowledgment, or substantive mainstream reporting.

Reported, unconfirmed = a credible outlet noted the claim but it was not officially confirmed or we could not independently verify.

Unverified claim = exists only as a leak-site or dark-web-forum listing, not independently confirmed and we could not independently verify.

Of the 68: 32 Verified · 5 Reported, unconfirmed · 31 Unverified claims. "Exposed" figures originating from criminal or leak sources are claims, not confirmed counts.

Date	Organisation & Sector	Data Exposed (claimed)	Vector	Discovered by	Acknowledged?	Post-mortem?	Verification
18 Mar 2023	Biman Bangladesh Airlines (Government) - aviation	Email server; about 100GB threatened including Passenger and employee passport & flight data	Email-server compromise (malware / "zero-day")	Internal detection, widely reported	Yes - confirmed ransomware (press release 23 Mar 2023)	Probe begun; none published	Verified - major outlets; organisation confirmed forming a probe into the attack
9 Jun 2023	Advanced Chemical Industries (Private) - pharmaceutical, conglomerate	Corporate data offered as torrent dump	Not disclosed (ransomware)	Leak site (RedPacketSecurity / Akira)	No	None published	Unverified claim - leak-site listing only
6 Jul 2023	Bangladesh Krishi Bank (Government) - state-owned bank	Claimed >170GB, including financial records & employee information	Not disclosed	Leak site + reporting	No - bank did not respond	None published	Verified - widely reported, including by *The Daily Star*

Date	Organisation & Sector	Data Exposed (claimed)	Vector	Discovered by	Acknowledged?	Post-mortem?	Verification
8 Jul 2023	Office of the Registrar General, Bangladesh Birth Death Registration. (Government) - civil registry	~50M+ citizens, including names, phone numbers, email, NID	Insecurely configured public database (not an intrusion)	Security researcher, reported by *TechCrunch*; and notified CIRT	Yes - CIRT acknowledged, site *reportedly* taken down and issue investigated	Investigation launched; no public post-mortem	Verified - TechCrunch verified samples; CIRT acknowledged
4 Oct 2023	Unspecified organisation with access to Smart NID and voter data (Government/ Private) - national identity registry	Voter data via Telegram bot names, photos, parents' names, phone, address (NID-keyed)	Abuse of authorised third-party access (not a central database hack)	Surfaced via Telegram; reported by *The Daily Star*	Partial - Bangladesh Election Commission confirmed that central database was not hacked; suspended partner access; investigated	None published	Verified - *The Daily Star*; Bangladesh Election Commission responded
8 Nov 2023	National Telecommunication Monitoring Centre - NTMC (Government) - state intelligence agency	Names, address, NID, phone records, passport, bank information, blood group, parents' names, call durations, vehicle reg, fingerprint images, amongst others	Exposed / open database	Security researcher; reported by *WIRED*	No - NTMC reportedly denied	None published	Verified - *WIRED*; NTMC reportedly denied
1 Dec 2023	Bangladesh Parliament (Government) - legislature	Claimed web-server access ($1,000)	Not disclosed (server-access sale)	Dark-web forum (Daily Dark Web X)	No	None published	Unverified claim - forum listing only
19 Jan 2024	TranscomBD (Private) - conglomerate	~16,000 employee records, ~6,000 login credentials, and admin-panel access	Not disclosed (forum sale)	BCSI advisory	No	None published	Verified - BCSI advisory
7 Feb 2024	Aamra Networks (Private) telecommunication and internet service provider	Citrix credentials, network-monitoring & customer-management access	Stolen Citrix credentials	BCSI advisory	No	None published	Verified - BCSI advisory
26 Feb 2024	United International University (Private) - tertiary education provider	Faculty names, contact details, academic credentials	Not disclosed (forum post by "Nooblesec")	BCSI advisory	No	None published	Verified - BCSI advisory

Date	Organisation & Sector	Data Exposed (claimed)	Vector	Discovered by	Acknowledged?	Post-mortem?	Verification
28 Feb 2024	Bangladesh Police (Government) - law enforcement	Claimed ~13GB internal infrastructure files	Not disclosed	Leak site (Ransomware.live / Mogilevich)	No	None published	Unverified claim - Mogilevich later admitted to being a fraud / hoax operation
29 Feb 2024	Bangladesh-China Youth Student Association (Private) - non-profit organisation	Student database (PII)	Unclear / not disclosed	BCSI advisory	No	None published	Verified - BCSI advisory
21 Mar 2024	RabbitBD (Private) - e-commerce	Unspecified	Not disclosed	Leak site (Ransomware.live / KillSec)	No	None published	Unverified claim - leak-site listing only
23 Apr 2024	Tappware (Private) - government contractor	~2.3M rows (34GB) - names, addresses, phone	Not disclosed (forum leak)	BCSI advisory	No	None published	Verified - BCSI advisory
6 May 2024	Volunteer for Bangladesh (Private) - youth platform	Full .sql database + sample files (users' PII)	Not disclosed (database exposure)	BCSI advisory	No	None published	Verified - BCSI advisory
17 May 2024	Agrani Bank (Government) state-owned bank	Unspecified	Not disclosed	Leak site (Ransomware.live KillSec)	No	None published	Reported, unconfirmed - leak-site claim; not confirmed
20 May 2024	Bangabandhu-Grandmaster.com (Government) - government website	~94,000 users - name, phone, email, FB ID, photo, occupation, institution, DOB, address, password (SQL file)	Not disclosed (DB dump)	BCSI advisory	No	None published	Verified - BCSI advisory
30 May 2024	Amber IT (Private) - telecommunication and internet service provider	Admin and ticketing credentials; claimed 1.5M SMS records with user credentials	Malware on a staff computer + tunnelling	BCSI advisory (re-investigation)	No - initially denied by the organisation, BCSI re-investigation confirmed	None published	Verified - BCSI advisory
7 Jun 2024	myLocker (Private) - government-backed platform for documents	~2.5M users, including names, emails, phone, NID, DOB	Not disclosed (forum sale, $150)	BCSI advisory	No	None published	Verified - BCSI advisory
9 Jun 2024	Travela.xyz (Private) - marketplace	226 hosts, including name, phone, email, birthdate, bKash MSISDN, amongst others	Not disclosed (forum leak)	BCSI advisory	No	None published	Verified - BCSI advisory

Date	Organisation & Sector	Data Exposed (claimed)	Vector	Discovered by	Acknowl-edged?	Post-mortem?	Verification
28 Jun 2024	StylehoodBD (Private) - e-commerce	~5,800 customer invoices, including names, phone, delivery address, order and transaction data	Not disclosed	BCSI advisory	No	None published	Verified - BCSI advisory
30 Jul 2024	Road Transport & Highways Division (Government) - government ministry	Database of road and training including training records, and employee and trainee PII	SQL database compromise (actor "frog")	BCSI advisory	No	BCSI analysing; none published	Verified - BCSI advisory
12 Aug 2024	Grameenphone (Private) - tele-communication	Claimed network-monitoring dashboard access + internal data	Not disclosed	Dark-web forum ("Indian Cyber Force" claim)	No	None published	Unverified claim - political / hacktivist claim, no evidence
11 Sep 2024	Dhaka Electric Supply Company. - DESCO (Government) - electricity utility company	110,856 customers - customer numbers, names, identity information, email, address, mobile	Not disclosed	BCSI advisory	No	None published	Verified - BCSI advisory
16 Sep 2024	Globe Pharmaceuticals (Private) - pharmaceutical	Unspecified	Not disclosed (ValenciaLeaks RaaS)	BCSI threat-intel platform	No	None published	Verified - BCSI advisory
26 Sep 2024	Foodi (Private) - food delivery	~249,588 entries - names, mobile, email, delivery addresses	Not disclosed (forum sale, $100)	BCSI advisory	No	None published	Verified - BCSI advisory
4 Oct 2024	Bangabandhu (Tarakanda) Govt College (Government) - education provider	Student records, including academic data and course information. Student names, exam dates, subject names, grade levels, student IDs, and marks/scores	Not disclosed (ransomware)	Leak site (KillSec)	No	None published	Verified - BCSI advisory
13 Oct 2024	Confidence Group (Private) - conglomerate	~350GB threatened (unspecified)	Not disclosed (RansomHub RaaS)	BCSI advisory	No	None published	Verified - BCSI advisory, RansomHub claim

Date	Organisation & Sector	Data Exposed (claimed)	Vector	Discovered by	Acknowl-edged?	Post-mortem?	Verification
25 Oct 2024	Unilever (Private) - FMCG	~4.1M job applicants, including names, address, postal code, phone number, country; 28,856 accounts compromised	Not disclosed (Telegram sale, $100)	BCSI advisory	No	None published	Verified - BCSI advisory
1 Nov 2024	Titas Gas (Government) - gas utility company	Root firewall access (control of critical infrastructure)	Sold root firewall access (initial vector undisclosed)	BCSI advisory	No - Titas claimed systems secure	None published	Verified - BCSI verified the breach
14 Nov 2024	Popular Life Insurance (Private) - insurance provider	Claimed ~36GB files + SQL databases, including company and client data	Not disclosed (ransomware)	BCSI advisory	No	None published	Verified - BCSI advisory, The Daily Star reporting
24 Nov 2024	bKash (Private) - mobile financial service	Claimed 10M+ records, including conversation identity, service keys, receiver details, tele-communica-tion metadata (4.99GB CSV)	Not disclosed	Dark-web forum (Daily Dark Web / X)	No public response found	None published	Unverified claim - not corroborated in major coverage
29 Nov 2024	Public Works Department - PWD (Government) - government department	Government information, including employee records (limited details)	Not disclosed	Dark-web forum (Daily Dark Web / X)	No	None published	Unverified claim - forum listing only
7 Dec 2024	Bangladesh Police (Government) - law enforcement	100,000+ officers' data, 4,717 admin-panel credentials, ~700,000 login records,and access to Crime Data Management System	Credential leak (sold on forums / Telegram)	*Prothom Alo* investigation	No	None published	Verified - *Prothom Alo* investigation
21 Jan 2025	Bangladesh Navy (Government) - military	Alleged personnel and sailor data (unspecified)	Not disclosed (ransomware)	Leak site (ransomware.live / FunkSec)	No	None published	Unverified claim - leak-site listing only
21 Jan 2025	The City Bank (Private) - bank	Unspecified	Not disclosed	Leak site (Ransomware.live / FunkSec)	No	None published	Reported, unconfirmed - leak-site claim

Date	Organisation & Sector	Data Exposed (claimed)	Vector	Discovered by	Acknowl-edged?	Post-mortem?	Verification
27 Jan 2025 (Est.)	Bangla Academy (Government) - cultural institution	Fellowship applicants, including name, email, phone, application details	Accidental self-publication (process failure)	Surfaced via fraud reports, organisation's own notice	Yes - Bangla Academy issued a public warning	None published	Verified - organisation's own notice
10 Feb 2025	Bangladesh Election Commission – NID verification ecosystem: DGHS, UCB Fintech (Upay), Chattogram Port Authority, Department of Women Affairs, iBAS++ (Government / Private) - national identity registry	Citizens' NID data leaked to third parties through five partner organisations' verification access	Misuse of authorised third-party verification access	Bangladesh Election Commission's own monitoring; reported by major media outlets	Yes – Bangladesh Election Commission reportedly confirmed and issued show-cause notices	None published	Verified – Bangladesh Election Commission reportedly confirmed; *The Daily Star*
3 Apr 2025	Bangladesh Armed Forces (Government) - military	Unspecified (leak-site listing)	Not disclosed	Leak site (Ransomware.live / Babuk2)	No	None published	Reported, unconfirmed - actor (Babuk2) is a known claim-recycler; likely false
6 May 2025	Bangladesh Election Commission – NID verification via Ansar-VDP and BRAC Bank (Government / Private) - national identity registry	Citizens' NID data leaked through the verification access of two partner institutions	Misuse of authorised third-party verification access	Bangladesh Election Commission's own monitoring	Yes – Bangladesh Election Commission suspended both institutions' verification access	None published	Verified – EC confirmed; multiple outlets
23 May 2025	Evaly (Private) - e-commerce	~783,611 users, including names, email, phone, order details, merchant information, shipping address ($500)	Not disclosed (site defacement noted)	Dark-web forum (dailydarkweb.net)	No	None published	Reported, unconfirmed - sale listing included sample data and the company's website was reportedly defaced; not independently confirmed and no company response
27 May 2025	Road Transport & Highway Division - e-services (Government) - government ministry	SQL snippets, employee training records, user information, database backups, including information on audit, asset, vehicle, and project	Not disclosed	Dark-web forum (Daily Dark Web / X)	No	None published	Unverified claim - forum listing only

Date	Organisation & Sector	Data Exposed (claimed)	Vector	Discovered by	Acknowledged?	Post-mortem?	Verification
5 Jul 2025	BD Group (Private) - conglomerate	Unspecified (RaaS double-extortion claim)	Not disclosed	Leak site (Ransomware.live / Arcus media)	No	None published	Unverified claim - leak-site listing only
30 Jul 2025	Office of the Registrar General, Birth & Death Registration (Government) civil registry	~4.1M citizens, including names, NID, DOB, address, father's name, phone, life-status, registration identity information	Not disclosed	Forum listing	No	None published	Reported, unconfirmed
31 Jul 2025	Bangladesh Road Transport Authority - BRTA (Gov) - registry	1,008,506 records - usernames, NID, DOB, parents' names, passport, contact, email, address ($1,200)	Not disclosed (sample provided)	Dark-web forum (Daily Dark Web / X)	No	None published	Unverified claim - forum listing only
17 Sep 2025	Link3 Technologies (Private) - internet service provider	~189,000 users, including subscription information, phone, email, usernames, subscription passwords, addresses, SMTP logs ($400)	Not disclosed	Dark-web forum (Daily Dark Web / X)	No	None published	Unverified claim - forum listing only
28 Nov 2025	FR Express (Private) - internet service provider	Billing and management source code (ABillS), database files, SMTP / MySQL configuration, and payment-gateway files	Not disclosed (source-code and infrastructure exposure)	Dark-web forum (Daily Dark Web / X)	No	None published	Unverified claim - forum listing only
25 Dec 2025	Shwapno (Private) - retail outlet	Claimed ~4M customers, including names, phone, purchase histories	Not disclosed (ransom demanded)	Data circulated on social media; reported by *The Daily Star*	Partial - company did not confirm extent	None published	Verified - *The Daily Star* reporting
6 Jan 2026	Aarong (Private) - retail outlet	~3.5M records, including names, email, phone, date of birth, gender, address, and account metadata	Not disclosed	Dark-web forum (Daily Dark Web / X)	No	None published	Unverified claim - forum listing only

Date	Organisation & Sector	Data Exposed (claimed)	Vector	Discovered by	Acknowl-edged?	Post-mortem?	Verification
7 Jan 2026	BD Morning (Private) - news portal	User IDs, usernames, encrypted passwords, emails, names, activation keys	Not disclosed (DB dump)	Dark-web forum (Daily Dark Web / X)	No	None published	Unverified claim - forum listing only
15 Jan 2026	Bangladesh Election Commission – NID database, insider access (Government) - national identity registry	365,608 citizens' NID records accessed and sold within one month; 112,150 within a single week; nationwide-access credentials misused	Insider misuse of privileged credentials (EC office assistant and an outsourced data-entry operator; syndicate per CID)	CID Cyber Police Centre investigation; public briefing, 15 Jan 2026	Yes – CID disclosed publicly; two arrested	None published	Verified – *The Business Standard; The Daily Star*
31 Jan 2026	Bangladesh Election Commission (Government) - election body	~14,000 journalists - names, phone, NID, photos, signatures, full application docs	IDOR / broken access control (URL manipulation)	Reported by *The Daily Star*	Partial - portal taken offline; no statement on copying	None published	Verified - The Daily Star reporting
11 Mar 2026	Steadfast Courier (Private) - logistics service provider	Full DB ($2,000) - names, phone, delivery addresses, tracking IDs	Not disclosed	Dark-web forum (Daily Dark Web / X)	No	None published	Unverified claim - forum listing only
3 Apr 2026	Jamalpur Upazila Administration Portal Government) - local government	~50,000+ citizens, including names (in Bengali), NID, birth registration number numbers, beneficiary identity information, enrollment, serials	Not disclosed	Dark-web forum (Daily Dark Web / xrcat)	No	None published	Unverified claim - forum listing only
8 Apr 2026	AusBD Bazaar (Private) - e-commerce	~500,000 records, including customer names, addresses, emails, employee information	Not disclosed	Dark-web forum (Daily Dark Web / VIP)	No	None published	Unverified claim - forum listing only
9 Apr 2026	Ministry of Power, Energy & Mineral Resources - Fuel Pass (Government) - government ministry	Alleged NID, vehicle registration information, mobile, driving licence, fuel-purchase records	Not disclosed	Social-media posts (X); Daily Dark Web	No	None published	Unverified claim - download link inactive; unconfirmed

Date	Organisation & Sector	Data Exposed (claimed)	Vector	Discovered by	Acknowl-edged?	Post-mortem?	Verification
13 Apr 2026	Bangladesh Water Development Board - Hydrological Information Management System Government) - flood warning system	Access to river, rainfall, flood-alert data, and dam and irrigation status ($100)	Not disclosed	Dark-web forum (Daily Dark Web / X)	No	None published	Unverified claim - forum listing only
20 Apr 2026	Local Government Engineering Department - Geographic Information System (Government) - government portal	User records, government emails, information on officials and medical professionals (alleged ZIP dump)	Possible content management system / backend access	Dark-web forum (Daily Dark Web / weykofa)	No	None published	Unverified claim - forum listing only
22 Apr 2026	Ministry of Expatriates' Welfare & Overseas Employment (Government) - government ministry	Alleged passport records, NID, eTIN, financial and banking information, transactions	Not disclosed	Threat-actor sale post (Daily Dark Web/X)	No	None published	Unverified claim - description states authenticity not verified
27 Apr 2026 (Est.)	NovoAir (Private) - aviation	Internal documents (unspecified)	Not disclosed (ransomware leak claim)	Leak site (SOCRadar / APT73)	No	None published	Unverified claim - leak-site listing; small sample
27 Apr 2026 (Est.)	Bank Asia (Private) - bank	Unspecified (ransomware leak claim)	Not disclosed	Leak site (SOCRadar / APT73)	No	None published	Unverified claim - leak-site listing; actor is a LockBit-imitator
30 Apr 2026	RentalHomeBD (Private) - property rental service provider	1,648 property records, 1,200+ user accounts - names, email, phone, IDs, admin creds/ tokens	CORS misconfig, no-MFA admin panel, user enumeration, privilege escalation (claimed)	Dark-web forum (Daily Dark Web / X)	No	None published	Unverified claim - forum listing only
8 May 2026 (Est.)	Rural Development & Co-operatives Division - RDCD (Government) - government division	Alleged personal data, human resource records, roles, project information, authentication files, system metadata	Not disclosed	Dark-web forum (Daily Dark Web / X)	No	None published	Unverified claim - forum listing only

Date	Organisation & Sector	Data Exposed (claimed)	Vector	Discovered by	Acknowl-edged?	Post-mortem?	Verification
11 May 2026	Bangladesh Agricultural Development Corporation - BADC (Government) - statutory corporation	Private re-positories, in-cluding source code, database credentials, payment-gate-way configura-tions, internal documents, and admin access	Exposed Git repositories / secrets in code	Dark-web forum (Daily Dark Web / X)	No	None published	Unverified claim - forum listing only
11 May 2026	Directorate General of Drug Administration - DGDA Government) - regulatory agency	Alleged database, including regulatory / admin records	Not disclosed	Dark-web forum (Daily Dark Web / X)	No	None published	Unverified claim - forum listing only
25 May 2026	Bureau of Manpower, Employment & Training - BMET (Government) - government agency	732,000+ worker records, including names, passport, date of birth, mobile, email, address, job and training records, identity information, biometric status	Not disclosed (alleged AP I /contractor weakness)	Dark-web forum (Daily Dark Web / X)	No	None published	Unverified claim - forum listing only
29 May 2026	Probashi Portal - Ministry of Expatriates' Welfare & Overseas Employment Government) - migrant platform	482,000 migrant-worker records, including names, passport, NID, mobile, email, date of birth, address, emergency contacts, enrollment	Not disclosed	Dark-web forum (Daily Dark Web)	No	None published	Unverified claim - forum listing only
31 May 2026	Bangladesh Army - Qadirabad Cantonment (Government) - military	Network information, including 500+ devices, routing, MAC addresses, 50+ internal networks, 100+ subscriber connections	Exposed MikroTik rout-er + SNMP misconfigura-tion	Dark-web forum (Daily Dark Web / X)	No	None published	Unverified claim - military claim, unverified

www.techglobalinstitute.com