

# Data Breach Crisis: Assessing the Threat Landscape and Implications for Bangladesh's Information Security



*“...recent news and surveys show us that 26 billion pieces of data have been leaked from many popular online services, including Telegram, LinkedIn, Dropbox, and X.”*

The stress of online life did not exist even a century ago. As the Internet era began in 1969, people gradually disappeared into virtual quicksand by entering online life. Now, in 2024, these are so complex that, facing these online problems, human life will be more complex daily. The apps and software are not only easing and prospering human life simultaneously; people are also bound to fix a certain time to maintain these sites from everyday life. Sometimes, they are posed with tremendous challenges to privacy. Since the total number of social media users is 5.04 billion, it shows us that 62.3 percent of the world's population uses social media, according to Kepois, surveyed in January 2024 (Kepois, 2024).[i] Everyone must enter their personal information to create a profile in any app. Every software and app contain various personal details of its users. Only X's (Twitter) website has 1.5 billion data; the Tencent, LinkedIn, Zynga, Adobe, and Canva platforms have 228 million. Because of the recent surge in Cyberattacks, these data are not risk-free unless data security is strengthened.

Unfortunately, recent news and surveys show us that 26 billion pieces of data have been leaked from many popular online services, including Telegram, LinkedIn, Dropbox, and X. It can threaten humankind badly. Scams and phishing email attacks can easily be launched using this information. Who owns the data is unknown, but technology analysts believe it was collected for sale. Who can do this occurrence? The head of Security Research and Cybernews, Mantas Sasnauskas, says, *“Impossible to say, my guess is one malicious actor, a data broker, Access broker or someone in academia with poor privacy understanding and research ethical approval board.”* (Cybernews, 2024). [ii] This leakage was named Mother of all

\* Graduate Student, Department of Applied Mathematics, Noakhali Science and Technology University, Bangladesh.

\*\* PhD Candidate, Department of History, Istanbul University, Türkiye.

\*\*\* Fellow, Teach For Bangladesh.

Breaches (MOAB) by its discoverer, considering its loss. It is known that MOAB short form was previously used by the Air Force Research Library of the United States of America in 2003 as the name of the most powerful non-nuclear weapon. The leaked information includes information from government agencies in the United States, Brazil, Germany, the Philippines, Turkey, and other countries. Personal information such as name, email address, phone number, residential address, gender, date of birth, and nationality is leaked from these sites. Work experience, educational information, and financial information, such as credit card and bank account numbers, are also included here. Considering the potential damage from this leak, we must be startled by its loss. This can harm citizens in various ways. Without any permission, leaked information can be used by an unauthorized person. Scams and Phishing attacks are becoming more alarming factors nowadays. Data leakage may compromise users' accounts, allowing thieves to steal information, launder money, or carry out other illegal actions. Social and Economic losses are also unavoidable threats to the modern world.

Consequently, if the government agency's information is disclosed, it could be detrimental to the public interest. We can't categorize as first world or third world here. We can't even categorize here as rich or middle class; every user of these sites seems to be under the threat of leakage. Data leaks are mostly caused by vulnerabilities in data protection and website infrastructure. In the context of Bangladesh, its people also aren't protected from data leaks. In Bangladesh, safeguarding personal information is a major concern. A data breach from the Bangladeshi government agencies happened on June 27, 2023, which led to the unapproved release and loss of approximately 50 million people's data (Sakib, 2023).[iii] The more alarming fact is that although Viktor Markopoulos, the finder of this leakage, Besides some other authorities related to the Bangladesh Government, also knocked on Bangladesh's Computer Incident Response Team (CIRT), he could not get an immediate response from it (Franceschi-Bicchierai, 2023).[iv] Among the total population of Bangladesh, 12 crores are voters. Everyone holds a National Identification Card (NID). Among these 12 crore NID holders, 5.5 crores have smart NID. The incident is that a Telegram channel disclosed that by entering the Date of birth and a total of 10 digits of smart NID instant, one can reach the name, parent name, phone number, address, and other details of this card holder. Since 174 institutions or organizations have access to the NID Server, one or some are surely liable for this breach, though it was controlled later (Tayeb, 2023).[v]

*“A data breach from the Bangladeshi government agencies happened on June 27, 2023, which led to the unapproved release and loss of approximately 50 million people's data.”*



If the causes of this leakage are examined, an Inadequate legal framework comes first. The data protection framework in Bangladesh must be improved to confront this problem. Untrained manpower is also liable for this occurrence. Sufficient training and skills are needed for data protection in Bangladeshi governmental and commercial entities. The quick response team also should be more active. The government should not share sensitive personal information with an organization that cannot guarantee online security, and integrity is not advisable. Unaware agencies should be punished. For example, in 2019, the Integrated Health Information System of Singapore was fined \$750,000 for the patient data theft incident (Tayeb, 2023).[vi]

Although the Bangladesh Government's cabinet approved the draft Data Protection Act in November 2023, The Act lacks the constraints and protections required for data security. There are many issues with Bangladesh's Data Protection Act. 'Confidential information' needs to be defined under the Data Protection Act. To reduce the likelihood of abuse of public authority, this definition must be defined in a way that aligns with the public interest. Considering the General Data Protection Regulation (GDPR), Bangladesh's data protection legislation must be updated and tightened. The terms "public interest" and "national security" should be precisely defined in data protection regulations. According to this act, if it is thought necessary for national security, the prevention or detection of an offense, any data may be gathered from a data subject. Transparency International Bangladesh suggested a monthly transparency report should be published regularly (Correspondent, 2023).[vii] Access Now and Tech Global believe that Attempting to obtain data without following the proper procedures runs the danger of infringing on the data subject's rights (Correspondent, 2023).[viii] They suggested that the requirement of data collection and access be made explicit, that the data gathering be proportionate to justifiable goals, and that it be subject to independent judicial monitoring.

The general populace also needs to be made aware of the significance of data protection. They need to take the required safety measures to safeguard their data. Because citizens' unawareness is also one of the factors behind this incident, individuals can take crucial steps to be risk-free from these data leaks to prevent such attacks. Regularly installing security updates is essential to removing hardware and software vulnerabilities. By periodically reviewing and updating Access controls, security will be stronger. Specialists suggest making secure passwords that should be 12 characters minimum, including symbols, numerals, and capital and lowercase letters. Requiring a password and an additional element, like a code or fingerprint, two-factor, or multi-factor authentication (2FA) can play a big role in this process by adding an extra layer of security.

Moreover, sharing confidential information on social media should be highly avoided by everyone. These steps can be taken to improve the overall cyber security infrastructure and protect people's personal information. Finally, online life must also be safe and secure for mental tranquility.

“...sharing confidential information on social media should be highly avoided by everyone. These steps can be taken to improve the overall cyber security infrastructure and protect people's personal information.”



## Endnotes

- [i] Kepois. (2024). *Global Social Media Statistics*. <https://datareportal.com/social-media-users>
- [ii] Cybernews. (2024, January). *Cybernews: Did we just discover the largest data leak ever?*. [Video]. [https://www.youtube.com/watch?v=2aRxnFL8Ml4&ab\\_channel=CyberNews](https://www.youtube.com/watch?v=2aRxnFL8Ml4&ab_channel=CyberNews)
- [iii] Sakib, N. S. (2023, July 10). Personal data of 50 million Bangladeshis leaked on government website: Government investigating after cybersecurity specialist discovers leak. *Anadolu Ajansı*. <https://www.aa.com.tr/en/asia-pacific/personal-data-of-50-million-bangladeshis-leaked-on-government-website/2940505>
- [iv] Franceschi-Bicchierai, L. (2023, July 7). Bangladesh government website leaks citizens' personal data. *TechCrunch*. <https://techcrunch.com/2023/07/10/bangladesh-government-takes-down-exposed-citizens-data/>
- [v] Tayeb, T. (2023, October 10). Smart Bangladesh, unsmart cybersecurity measures. *The Daily Star*. <https://www.thedailystar.net/opinion/views/closer-look/news/smart-bangladesh-unsmart-cybersecurity-measures-3439906>
- [vi] Tayeb, T. (2023, October 10). Smart Bangladesh, unsmart cybersecurity measures. *The Daily Star*. <https://www.thedailystar.net/opinion/views/closer-look/news/smart-bangladesh-unsmart-cybersecurity-measures-3439906>
- [vii] Staff Correspondent. (2023, November 28). Draft Data Protection Act: Cabinet okays it giving free rein to law enforcers. *The Daily Star*. <https://www.thedailystar.net/news/bangladesh/news/draft-data-protection-act-cabinet-okays-it-giving-free-rein-law-enforcers-3480656>

[viii] Staff Correspondent. (2023, November 28). Draft Data Protection Act: Cabinet okays it giving free rein to law enforcers. *The Daily Star*. <https://www.thedailystar.net/news/bangladesh/news/draft-data-protection-act-cabinet-okays-it-giving-free-rein-law-enforcers-3480656>

