International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 23s, 2025
https://www.theaspd.com/ijes.php

Cyber Crimes And Hackers: Impact On Environmental Data And Economy In Bangladesh

S. M. Mizan[1], Dr. Rajnish bishnoi[2]
[1]Research scholar, Faculty of Law, Guru Kashi University, sharifmizan73@gmail.com
[2]Assistant Professor, Faculty of Law, Guru Kashi University, rajnishbishnoi@gku.ac.in

Abstract: *The pace of the digitalization of Bangladesh has driven general economic growth, literally modernizing its financial services, and even making the public sector more efficient. But this jump into digital has also opened up serious vulnerabilities in cyber security. The amount and level of cybercrime, such as cyber hacking, phishing, ransom ware, and online financial fraud, is so great a volume that they no longer register as out- of-the-ordinary. These crimes have caused tremendous financial losses for victims, companies and the government, and have threatened our national security and compromised the integrity of our financial markets and investor confidence." This research finds out the features and impacts of cybercrimes and hackers activities in Bangladesh, expresses the challenges and suggests strategic policies and technological measures for checking the environmenta data and economic consequences of the situation in Bangladesh. The methodology used in this research is qualitative and based on secondary data.*

Keywords: *Cybercrime, Hacking, Economic Implication, Digital Security, Cyber security, Financial Fraud, Ransom ware, Phishing, SME Vulnerability, Digital Economy, Cyber Policy, Digital Bangladesh, Investor's Confidence, Cyber Threats.*

1. INTRODUCTION

Digitalization became the highest development priority of Bangladesh. From the introduction of the vision of "Digital Bangladesh" in 2009 and at this point of time the common acceptance of e-governance, internet banking, e-commerce and mobile financial services has brought Bangladesh to move a long way in relation with digital inclusion (Rahman, 2020). According to Digital Bangladesh (BTRC, 2023), internet has been used by 130 million peoples during the recent decades that turned Bangladesh into one of those countries having maximum digital penetration in South Asia.

And in so changing, as we've unlocked doors for innovation and economic growth, we've also made ourselves susceptible to the dark side of digitization – cybercrime. Public and private digital infrastructure is under attack by domestic and foreign criminals who have pounced on vulnerabilities. The cyber-attacks not only have financial implications, but also compromise personal privacy, and institutional trust and national security (Islam &Jahan, 2022).

While there have been a few legal or technical moves on this front, Bangladesh's cyber-readiness remains far below what is needed to face down increasingly advanced types of threats, such as systemic hacking attacks, ransom ware and data breach. There is a need for quantifying the nature and degree of economic damage of cybercrime in formulating appropriate policy and organizational level response.

2. Objectives

The objective of this study is to analyze the economic cost of cybercrimes and hackers activities in Bangladesh. Specific objectives include:

- To analyze the latest pattern and types of cybercrime in Bangladesh.
- To determine the economic losses (both direct and indirect) due to cyber-attacks.
- To assess the efficiency of the legal and institutional systems in confronting cyber threats.
- To make recommendations on how to improve the national cyber security and economic resilience.

3. METHODOLOGY

The loss due to cybercrime in Bangladesh will be evaluated in this paper and Qualitative research will be used for this task.

3.1 Data Collection

Some secondary data were collected from the statistical booklets that issued BGD e-GOV CIRT, Bangladesh Bank and from some specific academicians, research journals, related web sites, and blogs.

3.2 Data Analysis

We analyze the data qualitatively for an in-depth knowledge about cybercrimes, hackers and its effect in the economy of Bangladesh.

3.3 Limitations

This work is limited by the quality of incident data used, with small private organizations in particular tending to under-report attacks due to the potentially significant reputational costs of doing so. Additionally, stakeholders' interviews were somewhat limited in time and resources.

4. LITERATURE REVIEW

Cybercrime is a multicomponent and dynamic threat to economies and societies around the world. According to Anderson et al. (2019) the cost of cybercrime loss to be described as the fastest growing crime in the world and it values around $6 trillion per year and involves all forms of cybercrime. And like their brethren, whether pedophiles, scammers, carpet-bombing spammers or armed robbers, they're laughing all the way to the bank. 31 countries themselves fall victim to cybercrimes even the world's richest economy." a range of fresh techniques are used by crooks to target us according to reports biz/Harold, for them, bad actors are going where people are, and their data exports estimat450, 00 in 2010 to we guide them on the places we hang out, made from spam job and luing virus-riddled emails even bad guys the tech lobby call. Risks are even higher for developing countries like Bangladesh, where generations of cyber security are weak (OECD, 2021).

Islam and Jahan (2022) took an insight on the financial loss due to the cyber-crime incurred by the banks and other finance-based institutions in Bangladesh, National banks are incurring billions of BDT loss from unauthorized transaction and digital theft. Similarly, Ahmed and Karim (2022) expressed insufficient investment in cyber security activities to thwart digital threats of the majority of the banks in Bangladesh.

Amin (2021) explored the psychological and financial effects of end-user id theft and Internet scams, where females and younger people are discovered to be related to digital divide.

"The macroeconomic impacts of cyber threats and cyber security vulnerability," by Rahman & Uddin (2023) examined, on the other hand, the macroeconomic implications and associated the vulnerability of cyber security to a fall in foreign direct investment (FDI), with special concerns for tech and fintech industries.

Literature review also includes criticism of the Digital Security Act (DSA) 2018. Khan and Hossain (2022) contended that while the DSA 'was created in order to combat cybercrimes, the nebulous language of the DSA and the politically motivated usage of it have sometimes led to restriction of freedom of speech in cyberspace in the name of cyber security'.

Therefore the economic impact of cybercrimes in Bangladesh is multi-dimensional, from personal economic loss to reputation of national economy. But still on one hand there is space for evidences about to state how much this damage is getting bad estimated at the same time that on the other hand the measures are not stopping them, but keep maintaining them.

5. CYBERCRIME SITUATION IN BANGLADESH

"There has been a lot of rise of cybercrime in Bangladesh over the years. In 2022 the Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT) reported over 20,000

incidents, with phishing, ransom ware and hacking attacking bank, government and telecom systems being the most prominent.

The 2016 Bangladesh Bank heist (SWIFT attack) is perhaps the most infamous, where thieves attempted to take around USD 1 billion from the country's central bank by hacking SWIFT (Greenberg, 2017). In practice, just $81m was stolen, but the fact that the robbers could get their hands on $101m in total exposed the security of the banking system, and the confidence of its users, as full of gaping holes.

Reported Cybercrime Incidents in Bangladesh (2018–2023)

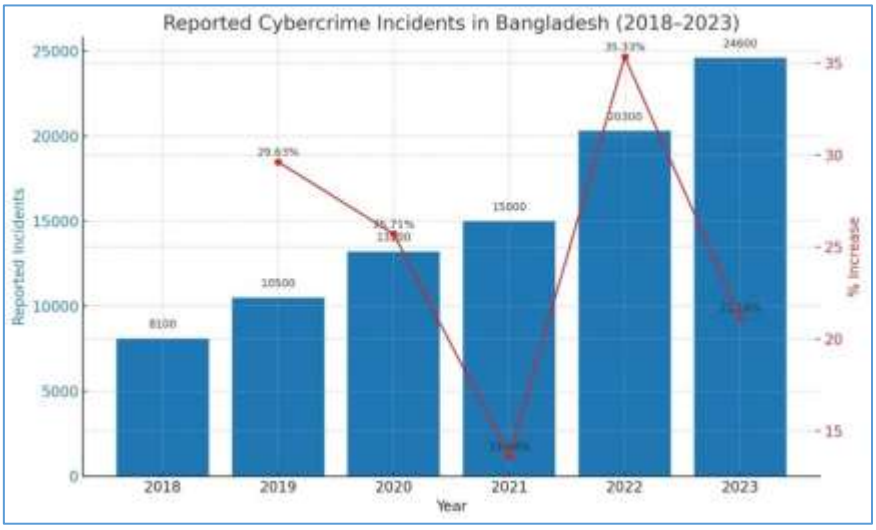
Here is the combined table showing the Reported Cybercrime Incidents in Bangladesh (2018–2023) along with the Year-on-Year Percentage Increase:

Year	Reported Incidents	% Increase from Previous Year
2019	10,500	29.63%
2020	13,200	25.71%
2021	15,000	13.64%
2022	20,300	35.33%
2023	24, 600	21.28%
Source: BGD e-GOV CIRT, 2023		

Here is a combined graph showing:

Blue bars: Number of reported cybercrime incidents in Bangladesh from 2018 to 2023.

Red line: Year-on-year percentage increase in reported incidents.



Source: BGD e-GOV CIRT, 2023

6. Environmental Data and Economic Impact of Cybercrime

6.1 Environmental data risk: Cybercrime poses significant risks to environmental data by enabling data theft and manipulation, where hackers can steal or alter climate, air quality, water quality, and soil data collected through IoT sensors, satellites, and GIS systems, leading to wrong policy decisions on pollution control, disaster management, or climate adaptation; for instance, if air quality data in Dhaka is hacked and made to appear "safe," the government may delay action, worsening health and environmental damage. Similarly, cyberattacks such as DDoS can disrupt real-time monitoring systems for flood levels, river pollution, or cyclone tracking, leaving environmental authorities blind

to immediate threats; for example, during cyclone season in Bangladesh, if the early warning system is hacked, millions of people and ecosystems remain vulnerable. Moreover, researchers rely on accurate long-term datasets like temperature, rainfall, and CO_2 levels, but cybercrime can erase or corrupt decades of such records, undermining scientific integrity and reducing the reliability of climate change studies, as seen when manipulated temperature records could weaken climate reports submitted to the IPCC. Cyberattacks also impose a financial burden on green projects—renewable energy, smart agriculture, and water management initiatives—by forcing higher spending on cybersecurity rather than sustainability measures. Finally, breaches in environmental data security erode public trust in governments and NGOs and discourage international partners from sharing crucial climate or environmental data with Bangladesh due to concerns about data insecurity, thereby weakening both local and global sustainability efforts.

6.2 Direct Financial Losses

Estimate of annual financial loss due to the cybercrime is estimated at BDT 500- 600 Crore (Ahmed & Karim, 2022). This refers to losses from banking frauds, e-commerce scams and online blackmail.

6.3 Losses to firms and SMEs

SMEs account for more than a quarter of the country's GDP and employ millions, but they are also the weakest link because they have less protection against cyber-attacks. There was business disturbance, data and reputation loss as the effect of cyber-attacks, and small companies were always bankrupted as a result of cyber-attacks (Chowdhury &Haque, 2021).

6.4 Decline of Investor's Confidence.

But the negligible cyber-security diminishes the attractiveness of Bangladesh for FDI. In particular, the investor d in the tech, digital finance, and outsourcing sectors perceive cyber security maturity as a requirement (Rahman & Uddin, 2023).

7. Common Cybercrime Techniques

Following are some of Hacking Techniques in Bangladesh.

Phishing: Fake emails or SMSs asking the user to input a sensitive piece of information.

Ransom ware: A type of malicious software that encrypts files and extracts payment for their release.

DDoS (Distributed Denial of Service): Deluges of traffic to take a website offline.

Social Engineering: Luring individuals into revealing their secret information.

SIM Swap Fraud: How to steal billions of mobile money in e-Governance times.

Even foreign hacking rings like Lazarus, have been tracked in their attacks on Bangladesh's financial infrastructure (Symantec, 2020).

8. Political and Legality Systems

Cyber offences are curbed under Digital security act, 2018. The Act does include provision for trials and fetching of digital evidence, but is criticized for being inherently ambiguous and lack of technical authenticity (Khan and Hossain, 2022). Besides, the courts under the Cyber Tribunal of Bangladesh has low conviction rate and pending cases as well.

BGD e-GOV CIRT The BGD e-GOV CIRT under the ICT Division is also responsible for monitoring and responding to the national cyber threats; however it is an under-resourced organization.

9. Recommendations

Cyber security Investment: Increasing national budget allocation for Cyber security infrastructure and man power.

- **Strengthen Cybersecurity Infrastructure:** Secure environmental databases and IoT monitoring systems with firewalls, encryption, and multi-factor authentication.
- **Regular Data Backup and Blockchain Use:** Maintain redundant backups and adopt blockchain for ensuring data integrity and preventing manipulation.

- **Capacity Building and Awareness:** Train staff in environmental agencies on cybersecurity best practices and conduct regular cyber drills.
- **Legal and Policy Frameworks:** Establish strong cyber laws and standards for environmental data security, aligned with international frameworks.
- **Backing Small Business Through Stronger Skills:** Sell SMEs cyber security tools and training at a cut-price.
- **Legal Measures:** Reform the Digital Security Act for ease of interpretation and fast track the judicial process.
- **Education:** Kick off campaigns about digital hygiene, password security and scams.
- **International Cooperation:** Collaborate with international organizations in information sharing and incidents response for cyber security.

10. CONCLUSION

Hackers and cybercrime are a major threat to Bangladesh economy. As the nation further digitizes, the cost of these cyber liabilities will only increase unless there is a shared responsibility that includes new regulation, tech investments, and a public educated in the nature of these attacks. He now must do (much) more to safeguard Bangladesh's digital economy.

REFERENCES

1. Ahmed, M., & Karim, R. (2022) Risk of Cyber Security in Bangladesh Banking Sector. Institute of Bank management Bangladesh.
2. Anderson, R.,Barton, C.,Bohme, R., Clayton, R., van Eeten, M. J. G.,Levi, M., & Savage, S. (2019). How much cybercrime costs? In The Economics of Information Security and Privacy (pp.).
3. BGD e-GOV CIRT. (2023). The report is called 'Rapport annuel Cyber Incident 2022'. https://www.cirt.gov.bd (accessed on 22 June 2025).
4. Chowdhury, S., and Haque, N. (2021). The cyber risk readiness of SMEs in the Bangladesh. Asian Journal of Business and Management, 9(2), 44-56.
5. Greenberg, A. (2017). The untold story of the epic disaster that some say was the Deadliest Wells Fargo Hack Ever. Wired. https://www.wired.com/story/bangladesh-bank-hack/ (accessed on 22 June 2025).
6. Islam, T., &Jahan, S. (2022). For the developing world: The economic impact of cybercrime for developing countries: A case of Bangladesh. Journal of Information Security, 13(1), 28–39.
7. Khan, M. & Hossain, T. (2022). The need for review of Bangladesh's Digital Security ActA critique. International Journal of Law and Cyber security, 3(1), 12–24.
8. OECD. (2021). Raise it up, then cut it down: National capacity building in cyber security for low-income countries. https://www.oecd.org (accessed on 22 June 2025).
9. Rahman A., Uddin F. (2023). IT Security and Investment Environment in Bangladesh. South Asian Economic Review, 15 (4), 102–115.
10. Symantec. (2020). The changing hyper-threat tactics of Lazarus group. https://www.symantec.com/blogs (accessed on 22 June 2025).