FROM CAMPUS TO COUNTRY: THE IMPACT OF CYBERSECURITY BREACHES ON UNIVERSITY STUDENTS AND NATIONAL SECURITY IN BANGLADESH

By

Afsana Islam Sristy (24412505030)
Department of International Relations
Faculty of Security & Strategic Studies
Bangladesh University of Professionals

Under the Supervision of
Abdul Hannan
Assistant Professor
Department of International Relations
Faculty of Security & Strategic Studies
Bangladesh University of Professionals

A thesis submitted for the degree of
Master of Social Science
May, 2025

Supervisor: Asst. Prof. Abdul Hannan

I, the undersigned, hereby declare that I have read this project paper and I have attended the thesis paper defense and evaluation meeting. Therefore, I certify that, to the best of my knowledge, this thesis paper is satisfactory in scope and quality as a thesis paper for the degree of Master's in Social Science, field of study: International Relations, Bangladesh University of Professionals.

THESIS PAPER REVIEW & EVALUATION COMMITTEE MEMBERS

(Chairman)

Signature _____

(Supervisor)

Signature _____

(Assessor)

Signature _____

ACKNOWLEDGEMENT

First and foremost, I would like to express my gratitude to Almighty Allah (Subhana WaTaala), the author of knowledge and wisdom, for blessing me with the ability, knowledge, capability, and opportunities to carry out this thesis and complete it. The author is grateful to her thesis supervisor, Asst Prof Abdul Hannan Sir, for his patient mentoring, passionate encouragement, and helpful critiques of this study work. The author would also like to express her gratitude to all the participants of the survey who gave their valuable time and knowledge for the betterment of mankind. Finally, the author wishes to thank her family members, especially her husband and friends, for their support and encouragement throughout the study.

ABSTRACT

The growing digitization of a country like Bangladesh puts it at risk of cybersecurity breaches targeting university students. Cybersecurity breaches targeting university students pose a significant threat to national security, particularly in a developing digitized country such as Bangladesh. If students are involved in research work, have access to the national databases, or are a part of plenty of other online platforms, they are bound to get exposed to cyber threats. These exposures can result in embezzling crucial national infrastructure, sensitive personal data, and extreme cases of intellectual property theft. This study investigates the relationship between cybersecurity threats directed towards varsity students and their implications on national security. The lack of awareness among the students about the risks they encounter is a major cybersecurity gap. This paper aims to underscore the information gap that students face when it comes to cybersecurity knowledge. Through the aid of various cyber laws applicable in Bangladesh, such as the ICT Act or Digital Security Act, this study maps out the available opportunities and advancement gaps. The conclusion reached indicates that even though government action and policies are attractive steps to combat cyber threats, more work is required to increase awareness and security measures within the institutions. Bangladesh needs to enhance its cybersecurity infrastructure to defend its citizens and critical systems. This comes with the growing need to protect personal security and national safety. As cyber threats evolve, the example of Bangladesh shows the necessity for implementing superior frameworks, alongside strengthening educational curricula on the subject and actively reinforcing legal structures about cybersecurity.

Key words: Cybersecurity, breaches, university students, national security, threat, Bangladesh.

Table of contents

List of tables:

List of figures:

List of abbreviations

AI: Artificial Intelligence

BTRC: Bangladesh Telecommunication Regulatory Commission

CIA: Confidentiality, Integrity, and Availability

DDoS: Distributed Denial of Service

ICT: Information and Communication Technology

ISP: Internet Service Provider

IoT: Internet of Things

MITM Man in the middle

R&D: Research and Development

V P N: Virtual Private Network

Wi-Fi: Wireless Fidelity

CHAPTER 1: INTRODUCTION

All sectors of society, including academic institutions, have been affected by the digitization of the world, which has caused a rapid increase in cybercrimes. Unlike more advanced nations, Bangladesh is still struggling with the digitalization of its infrastructure. Following the Smart Bangladesh initiative, cybersecurity has improved, but students attending universities and colleges remain particularly vulnerable to breaches (Alam, 2010). 'Cybercrime' is illegal activity conducted via computers and the internet. Data and identity theft are estimated to exceed intellectual property theft costs of one trillion dollars in 2008 (Hasan, 2015). Like in most countries, breaches of financial institutions in Bangladesh have seen an alarming increase over the years. Cybercriminals have adopted various new, more sophisticated methods, including the sending of threatening emails to high-profile individuals, embedding pornography onto mainstream websites, and even sending spam to foreign embassies (Arora, 2016). The rapid expansion of cyberspace has led to the increased availability of illegal ICT operations. The rapid development of new digital technologies comes with positive aspects; nevertheless, they create new vulnerabilities that cybercriminals can take advantage of. Cybercrime is a new area of concern, particularly with the rise in internet accessibility, targeting private data or destroying reputations through internet-enabled devices. Cybercrime is one of the main concerns of this century, alongside the growing availability of the internet, which amplifies threats to individual privacy, national defense, and world economic health (Vedantu, 2023; Tuli, 2021).

This research looks into a new yet understudied issue: the cybersecurity risks aimed at university students and their potential impacts on national security. A typical student possesses sensitive personally identifiable information, interacts with online government databases, and participates in national research programs. This demographic is at risk of various types of cyberattacks, including but not limited to data and ransom attacks, identity theft, and social engineering, with severe repercussions like loss of proprietary data, identity theft, disinformation, and even attacks on critical infrastructure. The main problem this research aims to resolve is the lack of awareness and preparedness among university students and the potential nationwide-level risks that are spawned once their digital security has been compromised. By analyzing actual case studies, current cybersecurity policies, and academic insights, this paper aims to highlight the imperative

of safeguarding students in the digital age, not only for their good but for the security of the nation as a whole.

1.1 Background of the study

1.1.1 Cybersecurity

In a world where over 61% of social and industrial interactions now occur online, maintaining high levels of security has become essential to promote seamless, efficient, and secure interactions (Arina, 2021). Some of the key factors that are put into ensuring strong security include data security, privacy, system reliability and availability, and cybersecurity itself. Cybersecurity is the primary defense system today against cyberattacks and cybercrimes, and it operates to safeguard interactions on social media and across industries.

Cybersecurity can be broadly defined as the protection of individuals, societies, organizations, systems, and technologies from abnormal or malevolent behavior. It is concerned with maintaining the Confidentiality, Integrity, and Availability (CIA) of computer resources—either belonging to a single organization or networked across organizations (Azmi, 2016). Technically, cybersecurity refers to the set of technologies, practices, and processes designed to protect networks, devices, data, and programs from attack, unauthorized use, or destruction. It is more popularly referred to by the synonymous term information technology (IT) security. Cybersecurity takes center stage in the modern digital era as nearly every aspect of life, whether social, economic, or political, depends on technology for stability and progress. Cyberattacks have devastating consequences, including financial losses, damage to reputation, disablement of critical services, and even loss of life in the event of sectors that handle critical infrastructure, like health and energy.

Cybercrime is also any action that is unauthorized and affects a system, network, or equipment. Two different types of cybercrime are: Crimes that use a system as a target, and crimes that a system unwillingly helps to create. Any organization's security begins with three principles: confidentiality, integrity, and availability. These three concepts are referred to as the security triangle, or CIA, and have been the standard for systems security since the very first computer systems (Palmieri et al., 2021). The principle of confidentiality dictates that sensitive data and

functionality must be accessible only to approved sources. Example: Military secrets (Confidentiality). The integrity principles state that sensitive data and functions can be modified, added or removed solely by authorized subjects and assets. Example: A person enters incorrect information into a database (Integrity). Availability Principles state that data, functions, and systems are available upon demand on agreed parameters based on service level (Availability) (Nguyen and Golman, 2021). Consequently, cybersecurity is applied across a wide range of fields, including small and medium enterprises, government, military, healthcare, academic institutions, energy, and transportation networks. Its key objectives are to protect personal data, secure critical infrastructures, and ensure confidentiality, integrity, and availability of sensitive information.

1.1.2 Cybersecurity and the education sector

Use of the cloud computing system in institutions of learning has helped the institutions of learning to improve the effectiveness and academic performance of learners. Institutions of learning are also in a position to manage their various operations through various cloud service models. Among them is the Infrastructure as a Service, which allows the institutions of learning to run their software on a virtual infrastructure (Verma and Dumka, 2020). One of the most common types of cloud services that universities can use is the Platform as a Service (PaaS), which allows them to develop and sustain applications with the use of various programming languages. This type of system can be very beneficial for information technology students. Another cloud service is in the form of Software as a Service, through which various applications can be used by educational institutions on a cloud platform (Magomedov et al., 2020).

One of the most prominent advantages of cloud computing is that it can provide various educational services, such as simulations and virtual laboratories. Through these, the students can improve their skills without the need to be physically present in the institution. The incorporation of this technology in higher learning institutions has also improved the productivity of the institutions (Yu and Liang, 2021). For communication, virtual learning tools like Zoom, GoToWebinar, and Cisco WebEx were the prime means of such communication. There are many other applications as well that are utilized in this field, including Microsoft Teams, Adobe Connect, and Livestorm.

According to a report released by Datanyze, the world's leading technography vendor, the three leading VCA tools in the year 2020 were Zoom, GoToWebinar, and Cisco Webex (Sengan et al., 2021). This was accomplished by analyzing various publications that were released in various digital libraries, such as ScienceDirect, Springerlink, and IEEE Xplore (Li et al., 2021). According to the report drawn up by ENISA, in 2020, the education sector was targeted by cyberespionage threat actors due to the interest in the results of COVID-19 research. In a different report, Kaspersky discovered that educational institutions were targeted more often due to the increasing number of remote learning courses (Zhao et al., 2021).

1.1.3 Evolution of Cybersecurity Breaches

Cybersecurity is comprised of the mechanisms that are designed to protect networks, systems, and information from physical damage, unauthorized access, theft, or loss. It ensures privacy, integrity, and availability of information whenever required. As digital networks have grown advanced and pervasive, the frequency and magnitude of cyberattacks have increased by leaps and bounds. Not only has the number of possible attackers grown, but the methods and tools available to them are more advanced, powerful, and damaging. Consequently, the cybersecurity landscape is evolving at a high speed, posing greater risks to individuals, organizations, and national security.

As the world becomes increasingly interconnected, technology has become an engine of social and economic progress. Information and communication technologies have revolutionized education, public administration, healthcare, and business sectors. However, this digital evolution has also introduced severe vulnerabilities. More than 382 new vulnerabilities have been detected since 2017, with attackers, more commonly known as hackers, moving to exploit these vulnerabilities faster than the cybersecurity community or software developers can patch them (Uddin, 2017). A rise in zero-day vulnerabilities has led to security breaches in major platforms operated by the likes of Google, Apple, and Microsoft. In the first six months of 2017 alone, these security vulnerabilities wreaked havoc, illustrating the imperative of proactive cybersecurity.

The evolution of cybersecurity incursions illustrates one clear trend: from simple cyber-related crimes to highly sophisticated forms of digital manipulation. With technology increasingly

embedded in all aspects of modern living, the potential consequences of cybersecurity failures are increasingly magnified. This underscores the imperative need for secure, robust cybersecurity systems, particularly in academic institutions, where incursions can potentially have ramifications larger than the individual, perhaps even threatening national security itself (Schneier & Bruce, 2011)

1.1.4 Types of cybersecurity attacks

There are many kinds of electronic attacks based on artistic style. A phishing attack is a method that likely relies on social engineering. The perpetrators prompt their victim to click on a link with malicious programs, hence infecting their device by sending messages whose subjects may become intriguing to a victim like that or by using the name of the victim, or malware (Koh, C., 2023). The moment the victim reads a message, the malicious person initiates the piracy process through emails, private messages, or even programs that have been downloaded on social media websites, which, since then, have become vulnerable to such attacks and threats.

Denial of service is claimed to be an insidious form of electronic attack. This attack begins with a computer program intended for the control of many computers and the development of robotic networks between them, which are known as botnets (Moisset, 2023). The hackers use these botnets to perform a denial of service attack. The offending networks bomb the victim computer system with different messages and requests, which in turn cause main services to be disrupted and halted, even though it was a website or even a person of a government e-service. A distributed denial of service attack is an attack that overwhelms the system resources, but it is executed by a tremendous number of host computers known as zombies that have been infected with malicious code by the attacker. The different forms of denial of service and distributed denial of service include Smurf attack, botnets, teardrop attack, and the ping-of-death attack. Man-in-the-middle attack is an attack whereby the hacker inserts himself or herself between the channel of communication between the sender and receiver. The attacks result in session hijacking, eavesdropping, or even modification of data being passed between the legitimate users.

Session hijacking is a type of MITM attack where hackers steal the session between the two trusted clients and the network server. In this attack, the machine that is going to be attacked will

change the IP address for the trusted client when the network server continues with the session; thus, the original users will continue believing that they are communicating with the right person (Sharma, 2022). IP spoofing, being a man-in-the-middle attack, is used by the attacker to cause any system to assume that it's exchanging information with a trusted and known one, thereby providing the attacker with the authority to access the system. The attacker then sends packets with their IP source address of a trusted and known host and not themselves to the destination host. Finally, the target host will be able to accept that packet and reply to it. A replay as an MITM attack occurs when the attacker attacks the communication channel and uses the old messages.

Day-Zero Gaps are the comparatively recent gaps in smartphones, computer applications, and operating systems that are yet to be discovered by security developers and researchers (Vesa, 2022). If any of the malicious individuals who pilfer information obtain them before the technicians can reach them, they will use such loopholes to seize all the remaining of application details with such controls. Backdoors are pre-existing loopholes but typically meant loopholes that the organizations or companies leave for themselves so that they can access the user's device directly to help solve some technical problems. For example, for purpose of helping collect information about the functioning of a mechanism or security agencies and organizations that install it. Whether or not the backdoors were installed as an administrative tool, they are generally an attack mechanism, and as a mechanism, it makes the governments and the malicious actors to have equal access to the encrypted data therefore a threat that needs to be concealed to avoid any unwanted exploitation (Alhayani, Abbas, Khutar & Mohammed, 2021). Backdoors tend to be difficult to detect, and the detection process tends to differ from the operating system of the computer. Oftentimes, the security software tends to have to collaborate with special abilities to enable protocol monitoring and therefore detect such vulnerabilities. In Supply Chain Attacks, hackers target less secure vendors for purposes of breaching their more secure partners—a technique witnessed in state-backed attacks. The Bangladesh Bank Heist of 2016 is a classic example, whereby hackers infiltrated the SWIFT system via supplier vulnerabilities (Finkle, 2016). In AI-Powered Cyber Attacks, Attackers use AI to automate, adapt, and personalize attacks, increasing their efficiency as well as rendering them hard to detect.

China's AI-driven drones and cyber units are nascent threats to Indian defense systems (Varinda, 2023). As more reliance is placed on cloud facilities, poorly configured access controls or lack of encryption can lead to astronomical data leakage. India's Aadhaar system leak in 2018 was caused by incorrect cloud security configurations, affecting over 1 billion citizens (Sharma, 2018). As of early 2019, expectations were high for a looming attack that was likely to jeopardize data integrity across the world despite the advances in cybersecurity technology and that was mulling new and innovative means like cyber hackers attacking cloud infrastructures, Internet of Things devices as well as service programming platforms. There is a need to regulate systems across the world in terms of data. This is necessary due to the continuous innovations by the hackers and malicious people. The hackers began using Ransomware as a strategy until it decreased at some point. It is therefore forecast that the malicious people will continue using this strategy with stated targets and ransom figures for money funds.

1.1.5 A Decade of Global Cyberattacks (2013–2023)

Cyberattacks have grown in scope, sophistication, and impact over the past decade due to technological evolution, global crises, and global tensions. Cyberattacks in developed and leading countries like the United States, China, the United Kingdom, etc. explain how common this issue is and how many threats underdeveloped countries like Bangladesh might face, if not taken into proper consideration regarding this.

2013–2015: Cloud computing and IoT drove attack surface expansion. Megadata breaches (Target, Adobe, Sony, Home Depot) and ransomware and APTs accelerated. Heartbleed and insider threats revealed vulnerabilities, especially within critical infrastructure (Elgan, 2024). Example: OPM Data Breach (USA) – Chinese government-employed hackers allegedly stole sensitive personnel data from the U.S. Office of Personnel Management, which included data on approximately 4 million current and former federal workers. This massive data breach was a significant counterintelligence risk, with attackers potentially using the personal information to identify, locate, or extort cleared American officials and contractors (Rushe, 2015).

2016–2017: Politically motivated cyberattacks accelerated during global political events like the U.S. election. Giant breaches (DNC, Yahoo) and DDoS attacks (Mirai botnet) occurred. The emergence of cryptocurrency supercharged ransomware (WannaCry, NotPetya) and

cryptojacking (Elgan, 2024). Case: Bangladesh Bank Heist (Bangladesh/USA) – The North Korean Lazarus Group compromised SWIFT banking systems and made off with $81 million from the Bangladesh central bank account at the New York Fed. Hackers used malware to generate fraudulent transfer orders; most requests were blocked, but $81 million was transferred to illicit accounts in the Philippines (Finkle, 2016). This state-sponsored bank heist uncovered vulnerabilities in the world financial messaging network. U.S. officials then described the operation as "state-sponsored," noting that nation-states could employ cyber capabilities for mass-scale financial exfiltration (Reuters Staff, 2017).

2018–2019: More stringent data protection regulation (GDPR) raised the stakes. Attacks became more focused, spear-phishing and IoT attacks on the rise. Healthcare and municipalities were significantly impacted (Marriott, Facebook-Cambridge Analytica, Capital One, Baltimore ransomware). Example: Operation "Cloud Hopper" (Global) – U.S. officials charged China's Ministry of State Security with a multi-year spy campaign (2014–2017) titled "Cloud Hopper." Taking advantage of trusted service links, Chinese cyber spies siphoned business secrets and government intelligence worldwide. This event revealed the national-security threat posed by supply-chain attacks: the attacker using third-party access to strike several key-sector targets undermines the integrity of global IT infrastructure (Stubbs et al., 2019).

2020–2021: The COVID-19 pandemic radically altered the cybersecurity landscape, overlaying remote-work exposures. Ransomware and phishing became even more aggressive, especially against healthcare and infrastructure. SolarWinds, Colonial Pipeline, and Log4j were some of the major breaches (Elgan, 2024). Example: Microsoft Exchange Server Hack ("Hafnium", Worldwide) – During spring 2021, Chinese state-sponsored HAFNIUM took advantage of four zero-day flaws in on-premises Microsoft Exchange servers. This incident, requiring global patching on the spot, signaled the danger posed by foreign actors to shared-use email infrastructure in governments and critical industries (Microsoft, 2021).

2022–2023: Geopolitics (e.g., Russia-Ukraine) fueled supply chain attacks. AI-enhanced threats began to reshape the landscape, enabling faster and more automated attacks. Notable incidents included MOVEit, Microsoft Exchange, and T-Mobile breaches (Elgan, 2024). Example: Microsoft Exchange Online Compromise (USA) – In mid-2023, Chinese state-sponsored hackers

(Storm-0558) spoofed authentication tokens to compromise the Microsoft cloud-hosted Exchange email service, breaking into tens of thousands of inboxes. U.S. government agencies, such as the State and Commerce Departments, acknowledged their networks were compromised and emails exfiltrated. The hack laid bare vulnerabilities in cloud identity services and triggered new U.S. efforts to fortify defenses for government and business cloud systems (Pearson et al., 2023).

During the decade, the most significant trends were the increasing sophistication of the attackers, the rise of nation-state attacks, and the rising use of AI and machine learning both in attacks and in protection. This shows how cybersecurity breaches can lead to national security threats in case of even more powerful states.

1.1.6 Cybersecurity policy:

Cyber has increased the productivity of society and spread information effectively over time. Whatever issue, application or field cyber is used in, production is always enhanced. Fast data transfer to the cyberspace lowers the overall system security mainly (Katrakazas et al., 2020). The system transitions into good and timely system hardware. The security condition vs. cyber performance need along the cyber-security policy is significant. The term "policy" is used in various cyber-security domains, and refers to information distribution rules and regulations, data preservation goals by non-governmental sectors, technology control running strategies by systems (Tam et al., 2021).

The cyber-security policy is adopted by the regulatory framework and is implemented formally alone to the affected portions of the regulator. Security policy components vary according to the range of the policy (Cheng et al., 2020). National cyber-security policy addresses all its citizens and possibly foreign businesspersons within its sphere, but corporate cyber-security addresses employees who have a valid contract or are employed and are meant to regulate their behavior toward the corporation (Alghamdi, 2021). The security policy is determined by the objectives of the regulatory authority in question. The national security objectives and the corporate security objectives are very different from each other. In the government, the way goals turn into policies and the way policies are embedded into law is not the same (Quigley et al., 2015).

The country's cyber policy is now part of the national security policy. Even if we consider a country's cyber-security policy as per the State Department policy or the economic policy, such types of policies and laws are not as sovereign as the constitution. In fact, policy is framed and shared in reports and lectures by discussion of some points and discussions. Policies are set to guide and define laws and rules. Cyber-security enforcement directives, rules and regulations may be issued without setting a cyber-security policy (Sakhnini et al., 2021).

Cyber-security policy may require that whenever the threat of disclosure of confidential information is high, information should not be provided directly without effectively scrutinizing the receiver's ability to provide information security (Arend et al., 2020). This policy removes the assessment of data risk from an executive who may want to cut expenses with outsourcing information flow to an office and hiring personnel outside of the office to perform information analysis. Such conditions become difficult and complicated with the fact that cyber-security controls have not evolved as much as accounting or human resource controls.

1.1.7 Cybersecurity Laws in Bangladesh:

In Bangladesh, the importance of cybersecurity has been receiving increasing significance in the past few years as Bangladesh has increasingly become integrated into global digital networks. The government has taken several legal measures to regulate cyber activities and fight cybercrimes to protect national security, businesses, and citizens against web-based threats.

- **The Information and Communication Technology (ICT) Act, 2006**

One of the most well-known legal instruments handling cybersecurity in Bangladesh is the Information and Communication Technology (ICT) Act of 2006. This Act was enacted to promote the use of ICT in Bangladesh and provide a legal framework for handling various cybercrimes. The ICT Act includes provisions on: Cybercrimes such as hacking, unauthorized access to computers, identity theft, and data breaches. The ICT Act has been amended numerous times to address emerging cyber threats, the most recent amendment being in 2018, which included provisions to enhance security and fight cybercrimes better (Karim, 2023).

- **Information Technology(Certifying Authorities) Rules, 2010**

This Rule provides instructions, guidance and information in respect of the matters on which the Controller of Certifying Authorities (CCA) will take action in its functioning and the activities of the Certifying Authorities (Rahman, 2023).

- **The Digital Security Act, 2018**

Such one of newer and broader legislations is the Digital Security Act (DSA) of 2018, enacted particularly to tighten the country's cybersecurity regime. The Act aims to: prevent cybercrimes such as data breaches, hacking, cyber espionage, and cyber terrorism, to provide protection to secure critical infrastructure, particularly within government and public sector agencies etc. (Karim, 2023).

- **Digital Security Rules 2020**

According to Section 60 of the Digital Security Act 2018 Government published the Digital Security Rules 2020 (Roy and Associates, 2021).

- **The Bangladesh Telecommunication Regulatory Commission (BTRC)**

Bangladesh Telecommunication Regulatory Commission (BTRC) plays the core part in the regulation of telecommunications and internet services in Bangladesh. BTRC ensures that ISPs abide by security protocols and cooperate in evading cybercrimes (Rahman, 2023). BTRC has been engaged in: Monitoring and regulating data transmission to prevent online crimes, directing ISPs to block unsafe websites or content posing threats to cybersecurity, etc.

- **The Cyber Crime Tribunal**

To respond to the growing menace of cybercrime, Bangladesh established the Cyber Crime Tribunal in 2013, a special court that is intended to handle cases of cybercrimes. The tribunal provides for the prosecution of cybercriminals and ensures that perpetrators of illegal activities on the internet are brought to justice. The legal institution ensures that justice is delivered speedily and increases the conviction rate in cases of cybercrime offenses.

- **International Cooperation and Standards**

In addition to internal legislation, Bangladesh also seeks to align its cybersecurity strategies with international standards and frameworks. It is a signatory to the Budapest Convention on Cybercrime, which provides international guidelines for harmonizing policies and laws in combating cybercrimes worldwide. It works with regional and international organizations to enhance its cybersecurity protection, share information, and create a safe digital platform.

1.2 Problem statement

In Bangladesh, as the government promotes initiatives like "Smart Bangladesh," cybersecurity for all citizens becomes increasingly important. Smart Bangladesh is about being inclusive—about the people, the citizens of Bangladesh. It is also about bridging the digital divide by innovating and scaling sustainable digital solutions that all citizens, regardless of their socio-economic background, and all businesses, regardless of their size, can benefit from. This approach aims to raise per capita income to $12,500 and reduce the poverty rate to zero. The economy would be characterised as cashless, circular, research- and innovation-oriented, and knowledge-based. The goal is to develop 50 unicorn startups (each worth $1 billion) by 2041(Palak, 2024). The dream of a Smart Bangladesh will be realised based on four core pillars: `Smart Citizen,' `Smart Economy, ' ' Smart Government,' and `Smart Society'. Digital Bangladesh has created a strong foundation for moving forward towards Smart Bangladesh. In the enriched Smart Bangladesh vision, Bangladesh is not only smart in terms of technology, but also smart in terms of the empowerment and well-being of its citizens, fostering a brighter future. However, the cybersecurity vulnerabilities of university students — a group highly engaged in national development through research, innovation, and internships within the public sector — have been largely neglected. Students often possess sensitive academic data, access government-related digital platforms, and engage with critical research fields, yet they remain key targets for cyberattacks due to insufficient cybersecurity awareness and safeguards.

The main objective is that student-targeting incidents can serve as doorways for more comprehensive attacks against national critical infrastructure, intellectual property theft, disinformation operations, financial fraud, and other national security risks. While students are becoming more digitally integrated with national systems, few holistic studies have examined how cybersecurity threats at the individual student level can escalate to national-level risks.

Closing this gap is crucial to safeguarding not only students' rights but also the integrity and security of Bangladesh's digital environment as a whole.

1.3 Rationale and significance

The increased dependence on web-based platforms in Bangladesh, fueled by plans like Smart Bangladesh from Digital Bangladesh, has made cybersecurity an urgent concern in every arena of society. While much emphasis is laid on safeguarding government institutions, enterprises, and banks, university students — a very networked, rapidly growing web-based population — are of supreme neglect. This disparity is dangerous as students are no longer passive consumers of technology; they are now active contributors to national research, innovation, infrastructure development, and economic growth. Choosing this theme is essential because cyber hacking among students can now longer be viewed as individualized or isolated cases. Students are most often involved in high-stakes government-funded research, sensitive research projects, and even internships with national institutions such as power grids, banks, telecommunication, and public service institutions. A student-level violation could be the entry point for larger-scale, more sophisticated cyberattacks on strategic national infrastructure, endangering national stability, economic security, and even international relations. Further, Bangladesh has seen a dramatic rise in cyber incidents over the last ten years, and digitally active young populations are among the prime targets. If this vulnerability is left unbridled, it can give rise to mass intellectual property theft, sabotage of vital services, brain drain, and even destabilization of public trust in government mechanisms.

This research matters because it highlights a relatively untested but highly sensitive area of national security: the cyber posture of students at universities. By listing the threats, vulnerabilities, and probable outcomes, this paper attempts to guide the development of particular awareness campaigns, stronger institution-level cyber policies, and national strategies with student populations as a critical priority area for cyber planning in mind. In essence, protecting the cybersecurity of university students is not so much an issue of personal privacy; it is a vital national security strategic initiative for Bangladesh's future in a super-connected world.

CHAPTER 2: LITERATURE REVIEW

The association between cybersecurity awareness among university students and national security threats has been of increasing scholarly interest, particularly in developing nations such as Bangladesh. The rising trend of cybercrime and increased digital dependence highlight the need for the challenge to be addressed from education as well as national security points of view.

Singer & Friedman (2012) provide an easy point of entry into the complexity of cybersecurity and cyberwarfare. Ten years ago, cyberspace was only a science fiction word that described the nascent network of computers linking a few university computer labs. Today, our whole contemporary existence, from communication to commerce to war, occurs almost entirely through the Internet. And the cybersecurity issues it generates bedevil literally everyone: politicians struggling with anything from cybercrime to internet freedom; generals protecting the nation from novel forms of attack, and planning new cyberwars; business executives protecting firms from previously unimaginable peril, and looking to make money out of them; lawyers and ethicists building new models of right and wrong. And yet, there is perhaps no issue that has grown so important, so quickly, and that touches so many, that remains so poorly understood. Addressed in a lively, accessible style, chock full of fascinating anecdotes and stories to make the point, the book is structured around cyberspace and its security's big question spaces: how it works, why it matters, and what can be done? Along the way, they take readers on a tour of the big (and entertaining) issues and characters of cybersecurity, from "Anonymous" hackers and the Stuxnet computer virus to China's and America's new cyberwar divisions.

Hirshman (2019) studied the geopolitics of cybersecurity and how trust deficits between countries increase vulnerabilities and rigorously analyzed how existing theories of international relations translate to the cyber world. In the view of Buchanan, there is a ready-made response to the question 'Why do countries hack into one another's most valuable computer networks? 'and that is 'to steal useful information or to attack.' But here there is not the full picture. This book employs often underappreciated leaked documents provided by Edward Snowden, true-case studies of cyber operations, and policymaker perspectives to show that penetrating other countries' networks has enormous defensive advantages too. Two states, neither of which is going to harm the other but neither of which is trusting the other, will generally find it in their

interest to intrude. This type of dilemma, in which the state's way of making itself secure threatens other people's security and has the ability to heighten tension, is the basis of international relations and is known as the 'security dilemma'. It shows not only that the security dilemma can be used in cyber operations, but that the particular character of the digital world is such that the effect is firmly ringing out;

Verma (2024) explained that the cybersecurity dilemma is both an inevitable component of modern statecraft and a way of making the vital elements of cyber operations understandable to all. It also discusses the evolving cyber threats with rapid digital transformation. While technology enhances efficiency, it also brings security threats such as data breaches, ransomware, and IoT vulnerabilities. He explained cyber attackers' opportunistic behavior, rising threat sophistication, and adoption of AI for cybersecurity, particularly threat detection and threat mitigation. Also, he addressed ethical concerns, regulatory settings, and global attempts to improve cybersecurity. Thus, this paper gives an in-depth overview of technological, ethical, and policy issues, offering insights to cybersecurity experts, policymakers, and researchers working within the digital space. The majority of developing countries, such as Bangladesh, lack constraints in information access, and it is not economically beneficial in the sense of inadequate proper infrastructure available and poor education. The barriers are overcome by the absence of a comprehensive infrastructure for information protection and training in cybersecurity. There is also a need for cooperation, partnership, and investment in security, which also generates a security standard culture to guarantee security problems. There also needs to be trust, just like in business or any operations, and trust can be attained when the professionals believe that the contract is protected. Therefore, business protection should be viewed as a strategic business partner, not as a cost facilitator. The National Council for Science and Technology (NCST) has been formed by the Government of Bangladesh to enhance cultural group living standards through the extension and implementation of science and technology development activities. The Executive Committee of NCST has also been formed to implement the policies formulated by the Council.

The most recent National Information and Communication Technology Policy (2002) has also provided ICT development with great potential to capture our share in the multi-billion-dollar software export sector, to formulate effective governance, to bring ICT-related policies together,

demarcation of resource mobilization to software development projects, to produce world-class ICT professionals.

Alqahtani (2022) has conducted an extensive survey that took into account the awareness of university students in cybersecurity in terms of password management, browser security, and social media behavior. The study used Cronbach's Alpha to find out the instrument's reliability and found greater overall internal consistency. It revealed that there is a straightforward correlation between personal cyber hygiene practices and institutional vulnerability. This study is a foundation for examining how seemingly personal-level cybersecurity negligence can translate into institutional and national risks.

Hasan, Sampa, and Mahmud (2023) similarly carried out a student cybersecurity awareness study via a guided survey at the Bangladesh University of Professionals (BUP). They observed telling gaps in awareness, especially for browser security and social media exploitation. Through these loopholes, educational institutions—and, indirectly, the country's databases—are vulnerable to cyberattacks, thus proving the thesis that student cybersecurity is a matter of national concern. At the higher policy level, Alam (2010) provided the initial insight on the evolving nature of cybercrime in Bangladesh, reporting on instances where hackers have attacked diplomatic platforms and public figures using malicious content and emails. The research illustrates how cybercrime has escalated from a cyber nuisance to matters of public and national security.

Arora (2016) further developed the point that ICT expansion is linked with both social benefits and novel crime opportunities, in affirming the need for systemic digital literacy and resiliency. Tuli (2021) emphasized that cybercrime is not merely a technological crisis but one with far-reaching implications for human rights, economic security, and national security. Similarly, Mohsin (2022) emphasized how the ubiquity of the internet has made the playground available to cybercriminals and has the tendency to make ordinary devices and networks, such as those used in universities, avenues for top-notch cyberattacks. Strategically, the Government of Bangladesh has aligned its national cybersecurity strategy with the five pillars of the International Telecommunication Union's (ITU) Global Cybersecurity Agenda. However, a critical analysis by Alam and others (2021) discovers that despite this alignment, the country remains woefully

behind the world in terms of preparedness. This gap between policy and practice, or more so within the education fraternity, subjects students and institutions to intrusions that echo through the national security spectrum.

Additionally, news platforms such as The Daily Star (2023) have also been alarmed at the lack of good cybersecurity training in Bangladeshi universities. In the absence of proper training, students cannot detect or respond to threats, hence becoming soft targets for cyberattacks.

In aggregate, these scholarly publications and survey studies suggest that universities are vulnerable but under-defended online environments. Personal information of students, if compromised, can be utilized for spying, economic sabotage, or disinformation operations—all of which are national security threats. Accordingly, higher education institution cybersecurity must be viewed not just an academic issue but a pillar of national security policy.

CHAPTER 3: RESEARCH GAP

Although there exists a growing body of research focused on the cybersecurity vulnerabilities of students as well as separate studies analyzing the impact of cybersecurity on national security, there remains a critical gap in the literature that interconnects these two domains. Prior studies have explored student-level cybersecurity awareness and practices, and other research has addressed how cyberattacks threaten national infrastructure and security. However, very few investigations have specifically examined how cybersecurity breaches targeting university students, such as data theft, identity theft, or phishing, can potentially escalate into broader national security threats. Most existing work has concentrated on cybercrimes affecting individuals, corporations, or state agencies, overlooking the academic sector's role as a soft but strategic target. This thesis seeks to bridge that gap by establishing how vulnerabilities in the digital behavior of university students in Bangladesh can pose significant risks to the country's national security. It highlights the overlooked yet crucial linkage between individual-level cyber hygiene and national-level cyber resilience, arguing that neglecting the cybersecurity preparedness of university students can expose critical weaknesses in Bangladesh's broader digital defense architecture.

3.1 Research questions:

3.1.1 Central research question:

How can cybersecurity breaches among university students in Bangladesh impact the nation's security?

3.1.2 Secondary research questions:

- What are the major cybersecurity threats among university students in Bangladesh?
- To what extent do students become victims of phishing, malware, or social engineering scams?
- How often do students enact recommended cybersecurity best practices (e.g., strong passwords, multi-factor authentication, secure browsing)?
- How are university students connected with the national critical infrastructure through academic and research activities?

- What are the potential effects of student-level cybersecurity breaches on national security?

3.2 Research objectives

3.2.1 General Objectives:

- To know how university students are connected with the national critical infrastructure through academic and research activities.
- To explain the potential effects of student-level cybersecurity breaches on national security.
- To explore the level of cybersecurity awareness among university students, including their familiarity with common threats, defense measures, and best practices.

3.2.2 Specific Objectives:

- To identify the cybersecurity threats most commonly faced by university students in Bangladesh.
- To assess the extent to which students are involved in research, internships, or computer systems connected to the national infrastructure.
- To highlight the urgent need for increased cybersecurity training for university students to protect them from growing cyber threats, since they are not very aware and engage in risky online activities.
- To evaluate the efficacy of current cybersecurity policies, programs, or initiatives being implemented in universities, or otherwise.
- To recommend effective strategies and policies to further enhance students' cybersecurity resilience.

CHAPTER 4: THEORETICAL FRAMEWORK

4.1 Realism

This study draws on the Theory of Realism, which is among the best-known paradigms in International Relations. Realism presumes that the international system is anarchic and does not have a central power to enforce order on states. Therefore, states must make survival, power, and security their paramount considerations at all costs. As per a realist perspective, any weakness—political, economic, military, or cyber—is felt to be an open threat to national sovereignty.

In terms of cybersecurity, Realism emphasizes that the internal threats of stability can significantly diminish a country's security functions in the global environment. The university students' cyber attacks are not single incidents of the theft of individual student data but potential national security threats. University students gain access to sensitive research information, engage in government-sponsored projects on their campuses, and utilize systems that are linked to national infrastructure. A successful penetration at the student level can hence unveil sensitive information that can be used by foreign competitors to weaken Bangladesh's strategic, technological, or economic position.

Realists hold that states must remain proactive to discover and close down such vulnerabilities. It therefore becomes a matter of national responsibility, not of privacy, to ensure cybersecurity in universities. Failure to safeguard the online operations of students at universities could lead to espionage, intellectual property theft, disinformation campaigns, and sensitive infrastructure compromise, all damaging the national security of Bangladesh.

In doing so, Realism provides a compelling theoretical lens with which to consider the seriousness of cybersecurity attacks on university students. Protecting this group is not solely about safeguarding individual data but about upholding the nation's broader security interests in the face of an increasingly networked and competitive world.

CHAPTER 5: METHODOLOGY

5.1 Research Design

A qualitative survey instrument was used to assess cybersecurity practice and knowledge among Bangladesh university students, mostly from the universities situated at the capital city of Dhaka. A survey was distributed through Google Forms with a purposive sampling technique to access technologically engaged students who actively (works six to seven hours a day in any electronic device) engages with technology in various aspects of their academic, personal, or professional life. This includes regular use of digital tools, platforms, or devices for learning, communication, collaboration, research, content creation, or problem-solving. Technologically active students often demonstrate a willingness to explore new technologies, adapt to emerging digital trends, and apply technological solutions to enhance their productivity, understanding, and connectivity in both educational and non-educational settings. This paper surveyed the technologically active students from departments like Engineering, Social Sciences, Business/Finance, and Health/Medical fields. These students are typically more exposed to digital environments, making them both more reliant on and more vulnerable to various cybersecurity threats. Their level of engagement with technology positions them as a critical demographic for assessing cybersecurity awareness, behaviors, and risk perception.

The 15-item survey had touched upon key subjects such as the security of passwords, protection of the browser, and awareness of national infrastructure vulnerabilities. Attitudes and self-perceived knowledge were assessed using a five-point Likert scale. There was also a multi-select feature so that the respondents can select as many of them as they wish. 170 responses from undergraduate and postgraduate students representing various universities were received and more in-depth information was gathered with the aid of semi-structured interviews.

5.2 Population and Sample

Population comprises students from various public university such as BUET, Dhaka University, Jahangirnagar University and Bangladesh University of Professionals, Medical college such as Manikganj Medical College and private university such as BRAC University, North South University, AIUB, IUB, MIST, East West University and UIU who are mostly undergraduates

and masters students in Dhaka city in Bangladesh and also some foreign students persuading their masters degree in Australia, United States, United Kingdom, Canada and New Zealand. In addition, 8 students with cgpa above 3.9 and 6 Lecturers from the department of Computer Science and Engineering (CSE) of BRAC University were selected for in-depth interviews to get a clearer picture on the subject.

A sample of 170 students was selected for the survey through the use of convenience sampling. Convenience sampling is a non-probability sampling technique in which participants are selected based on their accessibility, availability, and willingness to participate. Given the practical limitations of time, resources, and access, this method was deemed appropriate for reaching a sufficient number of respondents within the academic environment.

5.3 Data Collection Methods

Survey (Google Form): A set of questionnaires was developed using Google Forms. It included multiple-choice and Likert-scale questions to measure cybersecurity awareness, behavior, and attitude towards cyber threats. It was distributed to the respondents through different online platforms.

Interviews: Small-scale, semi-structured interviews with students and faculties were carried out in order to obtain more detailed views, experiences, and perceptions regarding cybersecurity threats and their link with national security.

5.4 Data Analysis Techniques

Answers to the survey questionnaires were analyzed dividing the responses into multiple patterns and sub-themes to identify the prevalence of the cybersecurity breaches faced by the university students and how they might affect the national security as a whole.

5.5 Ethical Considerations

Participants were informed about the research purpose before engaging. Voluntary participation was employed, and no personally identifiable information was collected. Confidentiality and anonymity were maintained at all levels of the study.

CHAPTER 6: FINDINGS AND ANALYSIS

6.1 Rising Cybercrime Trends in Bangladesh

There has been a fast technological advancement in Bangladesh, and this has led to increased access to digital devices, especially among youths. This has led to increased cases of hacking and other cybercrimes like unauthorized disclosure of personal information and propaganda over the internet. With better internet connectivity, there has been a steep increase in cybercrime in Bangladesh. By end-2023, over 131 million internet subscriptions were recorded nationwide making Bangladesh's online population one of the largest globally (31st anniversary issue-I, 2023). This connectivity boom has coincided with a surge in reported cyber offences. For example, the country's maiden Cyber Tribunal figures show that cases of cybercrime rose from just 3 in 2013 to 568 in 2017. A more recent report found that new or "neo" forms of cybercrime doubled in 2023 and now represent 11.85% of all reported crimes. Overall, new analysis indicates that social-media and account hacking is now the most common single cybercrime (some 21–22% of incidents) and financial frauds and data theft have also increased. Interestingly, 2020–2021 figures from a Cyber Crime Awareness Foundation survey show social and personal account break-ins rose from 15.35% of incidents in 2019 to 28.31% in 2020 (D. Islam, 2025). Conversely, traditional cyber crimes like fake news dissemination declined during this period, pointing to a shift towards personally directed crimes. Victim demographics are interesting: some 78–87% of victims of cybercrime are aged 18–30 years and a majority 59% of victims are female. In fact, one study found 61.3% of victims were university/college students and another 14.9% were school-going students (Barua et al., 2021). This suggests that higher education students are overproportionally targeted by cybercriminals.

There have been several cases in recent times that demonstrate the impact on students and educational institutions:

- **Phishing and Fraud Targeting Students:**

In early 2024, scammers posing as education officials defrauded more than 200 parents of 11th-grade students in Chattogram. Using stolen student data from scholarship applications, attackers phoned families and extorted money on the pretext of distributing government stipends.

At least four families lost a total of about Tk 103,000 in this scam (Chowdhury, 2024). This incident illustrates how personal data collected by educational boards can be used for financial cyber-fraud.

- **University Data Breaches:**

In April 2024 the United International University (UIU) reported that an individual ("Nooblesec") had leaked sensitive faculty professional and personal information on a hacking forum (Bangladesh Cyber Security Intelligence, 2024). The leaked data was reported to contain names, contact details, credentials and other personal records. Such breaches indicate how university databases can be hacked and how a single leak can compromise privacy and trust within the academic community.

- **Email Account Hacking:**

In October 2022, a self-styled "white-hat" group of hackers from BRAC University purported to hack the registrar's email account at North South University. The group sent an advertisement of NSU's new ranking but did so mainly to expose security flaws in the university systems. The same thing occurred at BRAC University itself, when students discovered hackers had infiltrated the BRACU registrar's email to distribute a political message (The Daily Star, 2022). While these intrusions were framed as awareness-raising, they point to real risk is that unauthorized system or email access at universities can both be a means of protest and an actual invasion of student/staff data.

- **Website Defacements:**

Hacktivist groups have also defaced institutional websites. In July 2024, for instance, a group called "The Resistance" defaced the official websites of the Bangladesh Police and the ruling party's student wing (Chhatra League). Their homepage images demanded an end to violence against students (Barua et al., 2021). While politically motivated, the attack shows that attackers can penetrate even high-level institutional networks, which is a concern for overall cybersecurity.

- **Other Incidents Reported:**

Lower-level scams, such as university admission scams or scholarship scams, frequently make the local news. Online harassment (such as dissemination of doctored images or threatening messages) of students has also occurred – reflecting nationwide trends for more online abuse and "revenge porn" cases (Barua et al., 2021).

While there are not many official statistics, experts note that even students of university age can unknowingly use vulnerable applications or click on phishing links, thus leading to account compromise and data loss.

6.2 Major cybersecurity threats in Bangladesh among university-going students

Bangladesh's sudden digital expansion has exponentially boosted the use of internet among students but also exposed them to fresh cyber threats. Cyber attacks, data breaches, and net crimes are now posing grim threats to the country's development (Das, 2025). University students are typically targeted as heavy users of the internet. Studies indicate Bangladeshi students in general have limited cybersecurity awareness, rendering them vulnerable to rising cyber threats through riskier online practices (Hasan et al., 2025). The following are the main threat categories referenced in national reports and recent studies:

1. **Phishing and Social Engineering**:

Deceptive ploys that manipulate users into revealing credentials (e.g., login passwords, bank OTPs) remain a significant concern. Bangladesh's e-Government CIRT ranks phishing (email fraud) and smishing (SMS fraud) as among Bangladesh's most critical cyber threats (Hasan et al., 2025). Criminals can also pose as officials or instructors to target students: for example, fraudsters had access to the names and class of the students and tricked guardians into providing ATM PINs and OTPs by claiming to process government allowance (Chowdhury, 2024). The ease of delivering credible bogus notifications via social media or email makes students a prime target for such social-engineering attacks.

2. **Malware (Viruses, Trojans, Ransomware):**

Malicious computer and mobile phone software is ubiquitous. Over 525,000 malware infections among Bangladesh telecom subscribers in a single quarter, including Android spyware and

trojans, were detected in a 2022 government threat report. Malware steals data or commandeers devices (Das, 2025). Ransomware (a form of Trojan that encrypts files in order to demand a ransom) is also prevalent globally. (Interestingly, industry analysis reveals Bangladesh users have one of the highest Trojan/ransomware infection rates in the world (Choudhury, 2022). The students may unknowingly download compromised apps or access malicious URLs, losing information or being extorted by such malware.

3. **Social Media Blackmail and Scam:**

Social media platforms are a hotbed of scams. Common tricks are copycat shopping websites (e.g., replicated Facebook stores) and "honeytrap" romance scams. For instance, Facebook/WhatsApp female impersonators who are thieves have conned young men into making intimate video calls and gone on to blackmail them by threatening to release the videos (Islam, 2025). The other reported crimes include cyberstalking and fake Instagram adverts that use victims' profile information for harassment or financial gain. University students, who use social media extensively, are frequently being targeted by these scams, which are founded on social networks and personal trust.

4. **Identity Abuse and Personal Information Theft:**

Personal information theft or leakage is a major issue. Reports suggest that identity theft and spoof-account fraud are two of the most common cyberattacks in Bangladesh (Rana & News, 2025). Fraudsters, for instance, utilized detailed student information from college stipend applications (class, name, etc.) to impersonate school authorities convincingly and cheat guardians. Alarmingly, large-scale data breaches have also affected the general public: a government database leak in 2023 exposed millions of Bangladeshi citizens' full names, phone numbers, e-mail addresses, and National ID numbers (Chowdhury, 2024). These data leaks pose risks to all Bangladeshi students to identity theft or targeted scams, as their own personal information (e-mail, NID, etc.) may be out in the open (Raywood, 2023).

6.3 Findings and analysis of the survey

This section shows the results of the survey conducted by taking some of the most prominent universities of Dhaka city in Bangladesh along with a detailed analysis on the responses of the respondents which shows a possibility of correlation between cybersecurity breaches of the varsity going students and national security.

6.3.1 Respondents' Academic Background

A majority of respondents were studying at the Master's level (57.4%), with undergraduates making up 34.3%. Fields of study represented included Engineering (30%), Social Sciences (22.4%), Business/Finance (15.3%), and Health/Medical fields (13.5%). The overrepresentation from Engineering and other technical fields is interesting, given that students from these disciplines are generally presumed to have more digital fluency. But as apparent in subsequent sections, technical affiliation alone does not readily imply higher cybersecurity competence. This necessitates specialist awareness programs outside of academic certification that focus on practical skill development and risk appreciation.

Table 1: Academic Background of Respondents

Category	**Response**	**Percentage**
Level of Study	Undergraduate	34.3%
	Masters	57.4%
Field of study	Social Science	22.4%
	Business/Finance	15.3%
	Health/Medical	13.5%

Source: Author’s own survey, 2025.

6.3.2 Familiarity with Cybersecurity:

Over 51.7% of respondents ranked their self-reported awareness of "cybersecurity" at the top (5), and 19.5% ranked it at 4. This indicates high self-reported awareness. Still, studies (Hasan et al., 2025; Azad et al., 2024) repeatedly find that self-reported awareness is more likely to be exaggerated. Students might overestimate what they know without being fully aware of technical threats. It supports the overall claim for this thesis: in spite of a relatively educated and confident student body, real-world cybersecurity practices are lacking.

Table 2: Familiarity with Cybersecurity

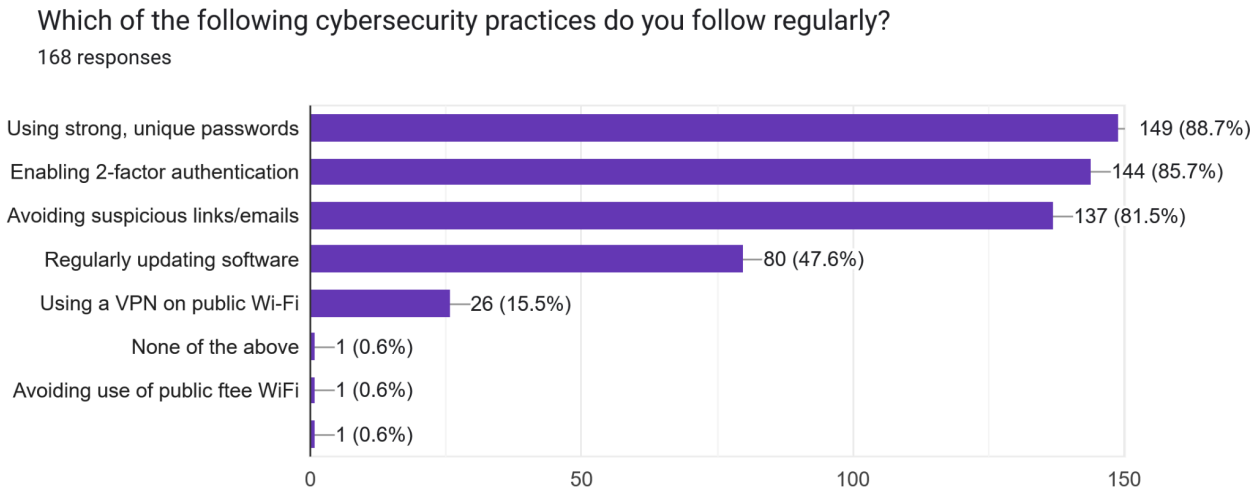
Familiarity Level	Description	Percentage (%)
3	Moderately Familar	16.6%
4	Familar	19.5%
5	Very Familar	51.7%

Source: Author's own survey, 2025.

6.3.3 Adoption of Cybersecurity Practices

Though 88.7% claimed to employ strong, unguessable passwords and 81.5% claimed to avoid suspicious links/emails, only 47.6% employed current software and only 15.5% employed VPNs while surfing the net through public Wi-Fi. This confirms a partial adoption of best practices. While students do enjoy basic hygiene, they lag in advanced protective behaviors. Literature reflects the same: students have a tendency to exhibit obvious, surface-level actions (e.g., spam avoidance), yet lack knowledge or intention to adopt more aggressive measures like encryption, 2FA, or VPN adoption (Hasan et al., 2025; Nigerian studies, 2022). This reflects a strong knowledge–action gap, aligning with this research.

Figure 1: Cybersecurity Practices by the students

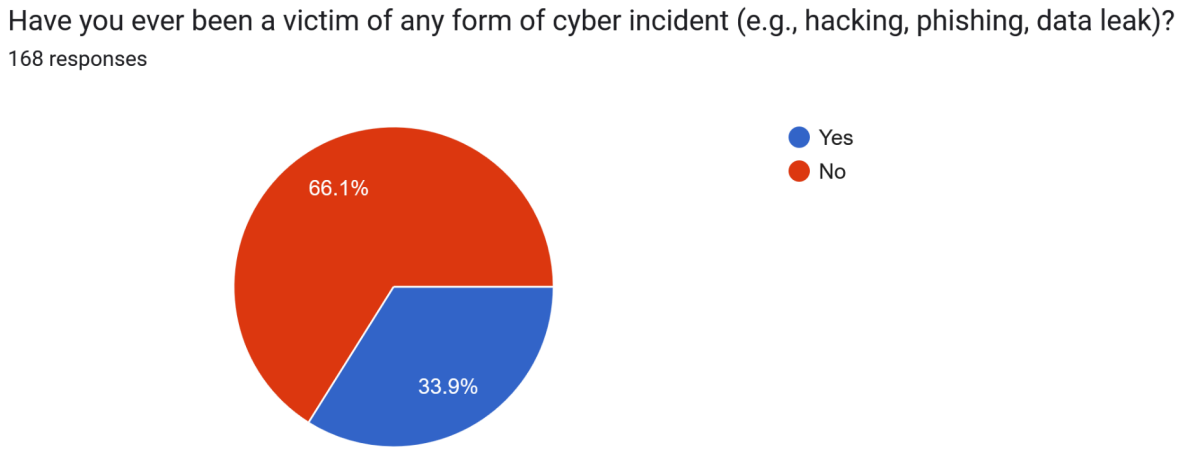


Source: Author's own survey, 2025.

6.3.4 Experience with Cyber Incidents

Approximately 33.9% of respondents reported experiencing a cyber incident, such as phishing, hacking, or data leakage. This is a substantial proportion and points to a growing exposure to online threats, even among an academically engaged population. The prevalence of such incidents reinforces the argument that increased awareness alone is insufficient to prevent breaches. Without proper training and institutional safeguards, students remain vulnerable despite having some level of familiarity with cybersecurity. These findings emphasize the urgency of integrating practical incident response training into academic curricula to mitigate the impact of inevitable cyber threats.

Figure 2: Students' experience with Cyber incidents

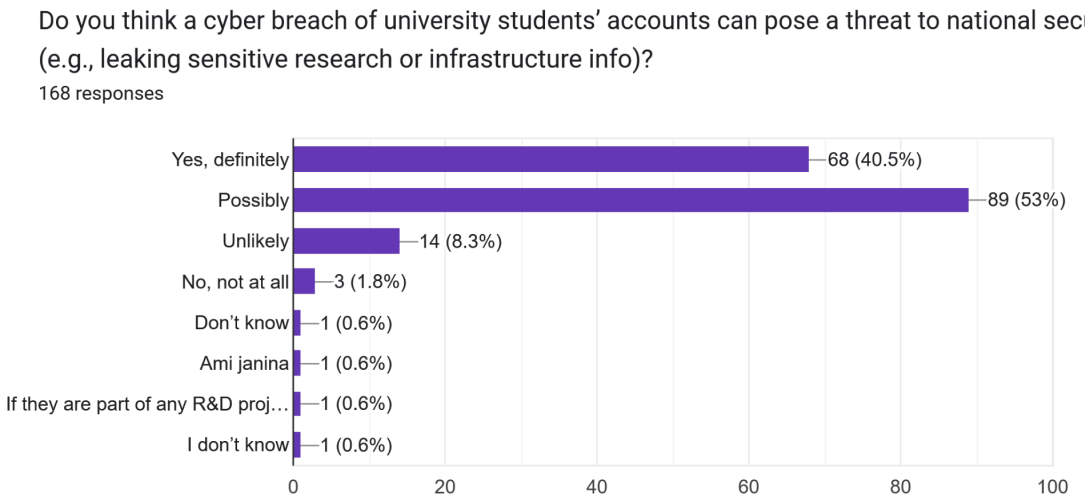


Source: Author's own survey, 2025.

6.3.5 Perceptions of National Security Risk

To the question of potential national security threat emanating from student account breaches, 40.5% responded "Yes" and 53% responded "Maybe," which translates to 93.5% of the respondents having admitted some degree of national exposure. Only 8.3% believed such threats were unlikely. Such is an attitude that resonates with contemporary cybersecurity discourses in which the university is regarded as an easy target for espionage, intellectual property theft, and infrastructure sabotage. The findings support the premise that students themselves recognize the strategic importance of protecting academic information, particularly in regions having emerging digital infrastructure. Given the tendency of academic research to intersect with government, defense, or critical infrastructure, this recognition calls for action by institutions in the way of policy and training.

Figure 3: Perceptions of National Security Risk

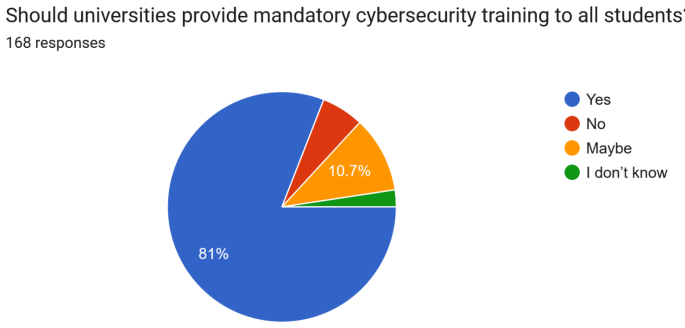


Source: Author's own survey, 2025.

6.3.6 Cybersecurity Training in Universities

An overwhelming majority (81%) supported mandatory cybersecurity training for students, with another 10.7% responding "Maybe." The consensus reflects widespread recognition of the necessity for formal intervention. The demand for formalized training signifies an engaged student population recognizing gaps in hands-on competence despite high levels of self-reported comfort. This aligns with best practice at the higher education level, where cybersecurity is being included in the definition of digital literacy awareness and readiness for response. Colleges that are slow to incorporate programs of this sort can risk not only student exposure but also reputational and operational harm from breach.

Figure 4: Cybersecurity Training in Universities

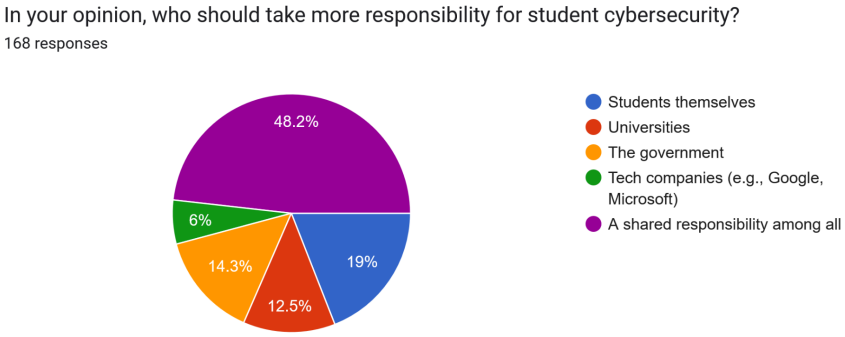


Source: Author's own survey, 2025.

6.3.7 Responsibility for Students' Cybersecurity

Nearly half of the participants (48%) believed that cybersecurity responsibility would be shared by all stakeholders—students, universities, governments, and tech companies. Only 19% blamed students directly, while 12.5% and 14.3% blamed universities and the government, respectively. This distribution reflects the growing need for shared responsibility, a principle gaining traction among worldwide cybersecurity governance. The shared responsibility model means that good cybersecurity culture cannot be developed independently, but requires institution infrastructure, state regulation, and coordination of technology providers for full protection of the students.

Figure 5: Responsibility for Student Cybersecurity

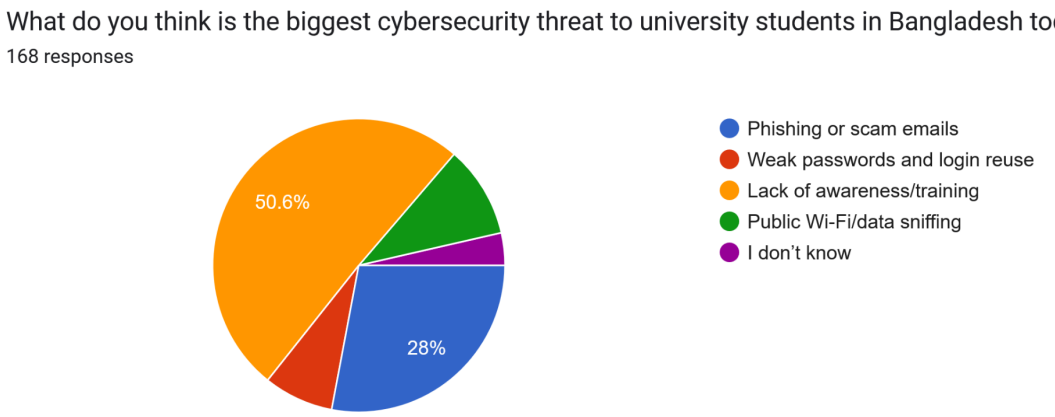


Source: Author's own survey, 2025.

6.3.8 Perceived Cybersecurity Threats to Students

The greatest single risk was lack of training or awareness (50.6%), followed by phishing or scam email (28%). This ranking reflects common acknowledgment of the fundamental role that education plays in cybersecurity resilience. It also corroborates wider national survey findings, where human fallibility and acts of negligence in numerous instances due to lack of proper training were responsible for most breaches. The facts strongly validate the argument that enhancing digital literacy and cybersecurity studies can mitigate a large percentage of the common threats to university students.

Figure 6: Perceived Cybersecurity Threats to Students



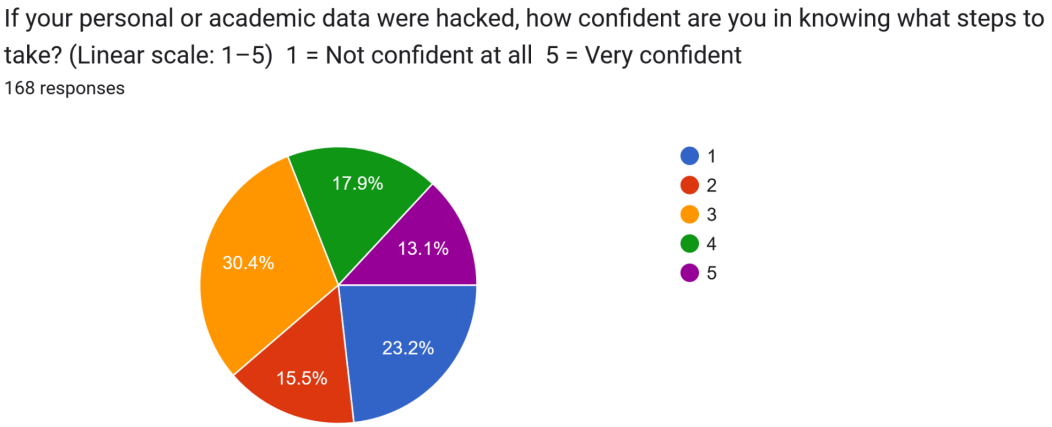
Source: Author's own survey, 2025.

6.3.9 Confidence of Students in Responding to Cybersecurity Breaches

Only 13.1% of students had their confidence in responding to data breaches at level 5 (highest) and 17.9% at level 4. The majority positioned themselves on a moderate level (3 at 30.4%) or low (1 at 23.2%). This is a significant weakness: students are aware of cybersecurity best practices but cannot respond when a breach is committed. The gap between action and awareness only increases the necessity for scenario training, exposure in workshops, and organizational

support mechanisms that prepare students to handle real-time incidents. Without practical preparedness, awareness is not sufficient to reduce cyber risk.

Figure 7: Confidence in Responding to Data Breaches



Source: Author's own survey, 2025.

6.3.10 Summary Analysis of Findings

The survey findings contained in sections 7.1 to 7.9 offer a picture of cybersecurity awareness, behavior, and attitude amongst students within Bangladeshi universities. A few broad trends emerge.

To begin with, the respondents' academic background comprises a technically minded, if heterogeneous, student cohort, with strong representation by Engineering and Master's courses. This profile appears to condition the high levels of self-declared familiarity with cybersecurity jargon and concepts (Sections 7.1–7.2). Yet, familiarity does not entirely mean full adoption of cybersecurity practices. Whereas basic measures like the use of strong passwords and shunning dubious links are prevalent, sophisticated ones like the use of VPN and frequent software updates are still in limited use (Section 7.3).

Second, a significant number of students have been victims of cyber incidents (Section 7.4), and the overwhelming majority value the fact that the hacking of student accounts could pose risks at the national level (Section 7.5). This valuation arises from greater sensitivity to the broader implications of cybersecurity, beyond one's privacy.

Most importantly, the results reveal an overwhelming level of agreement regarding the necessity of institutional intervention in cybersecurity education. The level of endorsement for compulsory cybersecurity training (Section 7.6) and the preference for co-responsibility (Section 7.7) underscore the perceived value of multi-stakeholder intervention. This includes schools and universities, government agencies, and private technology companies.

Also worth noting is the students' use of third-party websites such as Google Drive and ResearchGate (Section 7.8) as a sign that there is more control and education needed regarding secure data handling techniques. The sense of feeling poorly trained and under constant phishing attack coupled with low confidence in their ability to address data breaches (Section 7.9), highlight significant areas of practical inadequacy.

Overall, the results identify that while relatively high awareness of cybersecurity issues is present, there are glaring deficits in behavior, institutional preparedness, and response capacity. These results therefore highlight the basic premise of this study: increasing cybersecurity awareness and resilience among university students in Bangladesh requires efforts combining education, infrastructure, and policy-driven support mechanisms.

6.4 How university students can affect national security

University students often make use of government-funded systems, conduct important studies, or are part of national development programs. If personal information or study information by hackers, the nation may be targeted for damage. If a cybercriminal breaks into the university system and loots that information through the students who are doing significant projects under the Bangladesh government as an internship, they may sell it to foreign hackers or any foreign company may also steal the idea, patent it, and prevent Bangladesh from utilizing its own innovation. For instance:

1. **Public university research leak**

If one of the students from BUET is involved in a project involving national power grid systems and that got compromised, That data can be utilized to compromise the national power grid. This can also lead to power cuts throughout cities, damage the economy, and compromise national security. If A is a student at Dhaka University and a member of a research team working on water purification technology funded by the government for rural Bangladesh and someone hacks into the email account or university cloud account of the student and steals or leaks that research, any foreign firm may take the idea, patent it, and refuse Bangladesh use of its own innovation. This erodes economic independence and technological sovereignty.

2. **Psychological Profiling for Propaganda**

If Hackers target Jahangirnagar University students with social media attack, gather their political beliefs, interests, and personal information, they use this data to send forged news, gossip, or propaganda aiming to instill disunity and unrest among youth.This can destabilize student politics, spark protests, and impact national peace and security.

3. **Hacking Medical Students' Data**

BSMMU medical students use government hospital networks while undergoing training and if a student's computer is infected with malware, it will infect the hospital network.This can lead to Ransomware attacks on hospital networks and Medical records can be hacked, wreaking havoc in healthcare. It will undermine public trust in digital infrastructure.

4. **Job Application Scams**

If Final-year students of any university complete the online government job application form and Hackers create a fake job portal and gather their National ID, education details, phone numbers, this data can be utilized to create spurious citizens and commit fraud or even gain entry into the government systems with fake identities.

5. **Botnet Attacks Using Student Devices**

If Students download illegal games or software containing hidden malware and their laptops get included in a botnet (a pool of infected computers used to target sites). Such botnets can be used to attack government servers, knocking down public sites and can also interfere with elections or national portals.

6.5 Key Impacts of Enhancing Cybersecurity Awareness Among University Students

Improved Personal Data Protection: Students are more cautious in safeguarding their personal data, reducing the risk of identity theft and abuse.

Reduction in Cyber Threats: Awareness rose enhanced identification and avoidance of phishing attacks, malware, and other cyber threats, hence reducing successful cyberattacks.

Enhanced Academic Honesty: Learning about cybersecurity promotes integrity in online activities, avoiding plagiarism and upholding academic integrity.

Workforce Preparation: As professional students, well-trained cybersecurity-aware students are better equipped to address security concerns in their professional sphere, contributing to overall organizational security.

National Security Contribution: Educated students can act as a first line of defense against cyber attacks, making a huge contribution to the overall national cybersecurity infrastructure

6.6 Protecting cybersecurity from cyber criminals

Cyber-attackers typically have a master plan to help them to intrude into users' own and personal information and security. The best means to help parenting against such cyber-attacks is the implementation of simple and logical protection modes. Consistency and reliance on safeguard measures are crucial since an innocent click always leaves a small loophole to a lot of easy-to-accomplish damages to the systems. Paying attention to security now and applying basic measures makes everyone safer than cybercriminals. Simple safety habits that relate to internet security, which employ different and complicated passwords, updated software, have to be implemented.

1. **Technical methods:** These involve the creation of reverse tracking technologies that aid electronic attacks such that when applied, the sensors and the early warning systems that will quickly recognize attacks in their initial stages and thus help as an integral infrastructure to the creation of backup of for networks them. (Verma & Dumka, 2023).
2. **Cyber Alliance:** Expansion of the scope of the traditional alliance so that it includes the responsibility for the acquisition of cybersecurity following political agreement signing by some states.
3. **Development of cyber talent:** The nations must invest in the human element, i.e., the children who will help create intelligent technology. Secondly, the technology companies need to educate the children, encourage innovations and talents in the field of data privacy and information security, and then organize such competitions for the children. (Hart & Margheri, 2020).
4. **Awareness in the community:** The government ought to substitute the member awareness about the society in the programs dealing with the danger of their cyberspace and the different uses of technology which guide them on how to gain from the technologies that are available and evade their dangers and that is achieved through a partnership between the governance, the private sectors, and the society.
5. **Investment in cybersecurity insurance:** Most of the cybercriminals are instead inclined to attempt to devise sophisticated methods of violating the security lines of defense that have been built so that even the most vigilant companies of their security still keep on encountering the risks of getting attacked. According to 2017, a single data breach would cost up to $ 3.6 million, which can be translated to an equivalent value of $141 per record (Ricchi & Baggili, 2018). Decreasing cyber-attack losses is incurred from the data breaches and the cybersecurity expenditures to be incurred.
6. **Data backup and encryption:** Good self-defense against cybercrime is a strategy that needs two ingredients; prevention of access to private data or information and also making that information useless to the attacker who has access to that information. This is done through always encrypting company data (Singer, 2019).

CHAPTER 7: CONCLUDING REMARKS

7.1 Conclusions

This study examined cybersecurity awareness, practice, and perception in a heterogeneous sample of students from numerous universities, age groups, including a few international participants. Despite their differences, there was one thing in common: although the majority of students said they were aware of cybersecurity, there remains a gap between awareness and working readiness. The poll demonstrated that although students tend to use strong passwords and are cautious about clicking suspicious links, more advanced practices such as the use of VPN or software updates are not as common. Furthermore, a high percentage of students have been victims of cyber attacks, but only a small percentage are confident about how to counter such an attack. There is wide recognition of the national implications of academic cybersecurity breaches and strong support for mandatory cybersecurity education. The national security of Bangladesh might come under threat if the cybercriminals target those university students who are working in different research institutions as interns, as they are the common targets, bypassing whom, internal information can be achieved more easily. In addition, most view cybersecurity as the shared responsibility of students, universities, governments, and technology firms, demonstrating a mature understanding of the shared character of online security. Ultimately, this study corroborates the need for dedicated cybersecurity education, institutional support, and collaborative policy-making among the higher education community. With rising digital threats that are more sophisticated and extensive in scale, providing students with hands-on experience and institutional support will be paramount in shaping a safer and more resilient academic community.

7.2 Future work & limitations

This study provides us with useful knowledge about the cybersecurity awareness of university students, but certain limitations must be stated. Although participants were chosen from various universities, age groups, and even foreign backgrounds, the sample size was approximately 170. This small size may restrict the generalizability of the findings to the population of university students as a whole in Bangladesh or beyond. In addition, the study employed primarily a quantitative approach through a fixed survey. While this allowed for measurable comparisons

and the potential for trend analysis, it did not allow for the underlying motivations, attitudes, or surrounding circumstances that qualitative approaches such as interviews or focus groups might have revealed.

Future research can be enhanced by increasing the sample size and diversifying the respondent base, for example, by covering students from private and public universities across regions and disciplines. Incorporating qualitative methods would also provide richer data on behavioral, institutional, and social drivers of cybersecurity behavior. Although basic statistical analysis was conducted, more advanced analytical techniques such as structural equation modeling or logistic regression, can uncover more complex relationships between variables. This study can serve as a baseline benchmark for such additional empirical investigations.

Furthermore, future research must examine how legal, ethical, and institutional frameworks can be integrated into cybersecurity awareness initiatives. Because cyber threats typically transcend organizational and national boundaries, developing frameworks emphasizing international cooperation, incident reporting mandates, and institutional preparedness could be a valuable enhancement to national and educational cybersecurity policies.

7.3 Recommendations

In order to counter the advanced cyber attacks of the day, particularly for AI systems—organizations must adopt proactive, collaborative cybersecurity initiatives. These include dark web monitoring, threat feeds in real time, and safeguarding the entire AI pipeline from data to deployment using ethical control and secure, standardized frameworks (Alvarez et al., 2025). Bangladesh of today still has significant shortcomings in cybersecurity training, representation, and policy. Educationally, cybersecurity remains to be a separate undergraduate field, and postgraduate specializations are limited. School ICT training is primitive and fails to instill a sense of digital safety consciousness among youths—leaving adolescents particularly vulnerable on the web (Shahadat, 2025).

Bangladesh is also represented inadequately at international organizations shaping cybersecurity standards. The country largely imports foreign designs without incorporating Bangladeshi perspectives towards user privacy and online security. Lacking the availability of locally trained

cybersecurity specialists, reliance on foreign professionals continues. Developing a national research center for cybersecurity is necessary to reduce reliance and drive innovation. Priority should be accorded to academic collaborations, indigenous talent building, and participation in global forums. A strongly defined national cybersecurity policy with specific objectives, budgeting, and timelines is urgently required to address prevailing gaps and future challenges.

Based on the findings of this study, the following major recommendations can be drawn for enhancing the cybersecurity environment in Bangladesh, particularly among university students and the general national security framework. These recommendations would fill the lacuna of existing cybersecurity awareness, enhance legal enforcement, and get Bangladesh ready to counter the evolving threat landscape.

1. **Building Cybersecurity Education for University Students**

One of the identified gaps within this study is the lack of proper cybersecurity education among university students. In order to address this gap, it is recommended that universities integrate cybersecurity training programs into their curriculum. The training programs should focus on hands-on skills, such as the recognition of phishing attacks, shielding personal data, and attentiveness to potential threats associated with online locations. Universities also must adopt cybersecurity awareness programs to engage students and employees with active cybersecurity practices.

2. **Academic Institutions-Government Agencies Partnership**

For implementing a culture of cybersecurity, academic institutions must collaborate with government agencies like the Digital Security Agency (DSA). It can be in the form of developing joint resources, conducting joint workshops, and making sure that university systems align with national cybersecurity standards. Including students and faculty members in national cybersecurity initiatives will help Bangladesh develop a stronger digital ecosystem.

3. **Regular Cybersecurity Audits and Vulnerability Tests**

Schools and governmental bodies need to conduct periodic cybersecurity audits and vulnerability assessments on their digital systems. Colleges have significant research data and personal information, which would attract cybercriminals. Periodic audits will identify vulnerabilities in the existing infrastructure and refresh security practices according to changing threats. Further, universities need to implement disaster recovery plans to reduce the effect of cyber incidents.

4. **Enhanced Enforcement of the Digital Security Act (DSA)**

Although the Digital Security Act (DSA) is a robust legal instrument against cybercrimes, its enforcement and implementation must be prioritized further. Advanced equipment and professional training for law enforcement agencies must be offered to identify and prosecute cybercrimes in a professional way. Particular emphasis must be laid on freedom of speech matters and misuse of the DSA by politicians. The administration has to establish strict regulations in order to balance national security interests and individual freedoms so that the law is enforced fairly and openly.

5. **Public Awareness Campaigns on Cybersecurity Risks**

Besides training initiatives, national public campaigns should also be conducted to educate the general public on cybercrime threats and online safety best practices. The campaigns need to address global threats like phishing, identity theft, and ransomware, and emphasize the usage of strong passwords and updates of software on a regular basis. Grassroots awareness will enable the country to build a more society-conscious of cybersecurity.

6. **Investment in National Cybersecurity Infrastructure**

The government should consider investing in cybersecurity infrastructure, especially in sensitive areas like healthcare, energy, and telecommunications. It involves making organizations that handle sensitive data equipped with advanced cyber defense tools and security professionals. Further, national cybersecurity standards should be developed that can guide industries and institutions on how to lock down their digital assets.

7. **International Collaboration for Cybersecurity Threat Intelligence**

Cybersecurity is a global issue, and Bangladesh must actively participate in international cooperation to share intelligence on emerging threats and best practice. In its membership in the Budapest Convention on Cybercrime, Bangladesh must improve its collaboration with global bodies and regional neighbors to combat cross-border cybercrime. Information sharing, joint investigation, and joined-up response can all play significantly towards national security with growing sophisticated cyber threats.

REFERENCES

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, Challenges and Future Directions. *Cyber Security and Applications*, *2*(2), 100031. https://doi.org/10.1016/j.csa.2023.100031

Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," J. Cybersecurity, vol. 4, no. 1, p. tyy006, 2018

Alghamdi , M. I. (2019, June 12). *Effects of Knowledge of Cyber Security on Prevention of Attacks* . Journal of Basic and Applied Sciences.

Alhayani, B., Abbas, S. T., Khutar, D. Z., & Mohammed, H. J. (2021). WITHDRAWN: Best ways computation intelligent of face cyber attacks.

Alvarez, M., Caridi, C., & Chung, J. (2025). *IBM X-Force 2025 Threat Intelligence Index*. https://www.ibm.com/downloads/documents/us-en/1227cc9e83cb97ae

Alzubaidi, A. (2021). Cybercrime awareness among Saudi nationals: dataset. *Data in Brief*, *36*, 106965.

Arina, A. and Anatolie, A. (2021). Cyber Security Threat Analysis in Higher Education Institutions as a Resultof Distance Learning. International Journal of Scientific & Technology Research, 10(3),128-133.Bada, M. and Nurse, J.R.C. (2020). Chapter 4 - The Social and Psychological Impact of Cyberattacks, https://www.sciencedirect.com/science/article/pii/B9780128162033000046

Azmi, R., Tibben, W., & Win, K. T. (2016). Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy.

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., ... & Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, *22*, 3-13.

Bullock, J. A., Haddow, G. D., & Coppola, D. P. (2021). Cybersecurity and critical infrastructure protection. *Introduction to homeland security*, 425-497.

Catalano, C., Chezzi, A., Angelelli, M., & Tommasi, F. (2022). Deceiving AI-based malware detection through polymorphic attacks. *Computers in Industry*, *143*, 103751.

Elgan, M. (2024, July 9). *A decade of global cyberattacks: where they left us*. Ibm.com. https://www.ibm.com/think/insights/decade-global-cyberattacks-where-they-left-us

Ershadul Karim, M. (2023, April 3). *Bangladesh: The Cyber Security Act, 2023 | Refworld*. Refworld. https://www.refworld.org/legal/legislation/natlegbod/2023/en/148277

Finkle, J. (2016). *Exclusive: Bangladesh Bank Hackers Compromised SWIFT Software*. Reuters. https://www.reuters.com/article/world/exclusive-bangladesh-bank-hackers-compromised-swift-software-warning-issued-idUSKCN0XM0DW

Furnell, S., & Shah, J. N. (2020). Home working and cyber security–an outbreak of unpreparedness?. *Computer fraud & security*, *2020*(8), 6-12.

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. *Computer fraud & security*, *2020*(12), 6-12.

Godefrey, L. (14 C.E., March). *Shape or Deter? Managing Cyber-Espionage Threats to National Security Interests*. Studies in Intelligence Vol. 66, No. 1.

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. *IEEE Access*, *11*, 80218-80245.

Hart, S., Margheri, A., Paci, F. and Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. Computers & Security, 101827, https://doi.org/10.1016/j.cose.2020.101827

Hodges, A. (2025). *Countering nation-state cyber espionage: A CISO field guide*. ComputerWeekly.com. https://www.computerweekly.com/opinion/Countering-nation-state-cyber-espionage-A-CISO-field-guide

Hyginus, V., Eze, U., Ugwu, C. N., Ifeanyi Cornelius Ugwuanyi, & Kiu Publication Extension. (2023). *A Study of Cyber Security Threats, Challenges in Different Fields and its Prospective Solutions: A Review*. *9*(1), 13–24. https://www.researchgate.net/publication/367742804_A_Study_of_Cyber_Security_Threats_Challenges_in_Different_Fields_and_its_Prospective_Solutions_A_Review

Ibor, F.A. Oladeji, O.B. Okunoye, A survey of cyber security approaches for attack detection prediction and prevention, Int. J. Secur. Appl. 12 (2018) 15– 28

Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention*, *148*, 105837.https://www.jatit.org/volumes/Vol100No15/19Vol100No15.pdf

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. *Energy Reports*, *7*(7), 8176–8186. Sciencedirect. https://doi.org/10.1016/j.egyr.2021.08.126

Moisset, S. (2023, May 24). *How Security Analysts Can Use AI in Cybersecurity*. FreeCodeCamp.org. https://www.freecodecamp.org/news/how-to-use-artificial-intelligence-in-cybersecurity/

Narayanan, A. Ganesan, K. Joshi, T. Oates, A. Joshi, T. Finin, Early detection of cybersecurity threats using collaborative cognition, in: in 2018 IEEE 4th international conference on collaboration and internet computing (CIC), 2018, pp. 354–363.

Panimalar, G. Pai, S. Khan, Artificial intelligence techniques for cyber security, Int. Res. J. Eng. Technol. 5 (3) (2018) 122–124.

Patil, S. G., Zhang, T., Wang, X., & Gonzalez, J. E. (2023, May 24). *Gorilla: Large Language Model Connected with Massive APIs*. ArXiv.org. https://doi.org/10.48550/arXiv.2305.15334

Rahman, M. (2023, November 21). *Cyber Crime and Legal Fabric of Bangladesh - Law Firm in Bangladesh and Top Law Firm in Dhaka*. Law Firm in Bangladesh and Top Law Firm in Dhaka. https://lawfirm.com.bd/cyber-crime-and-legal-fabric-of-bangladesh/

Rawat, R., Mahor, V., Chirgaiya, S., & Garg, B. (2021). Artificial cyber espionage based protection of technological enabled automated cities infrastructure by dark web cyber offender. *Intelligence of Things: AI-IoT Based Critical-Applications and Innovations*, 167-188.

Ricci, J., Breitinger, F. and Baggili, I. (2018). Survey Results on Adults and Cybersecurity Education. Education and Information Technologies, 24(1), 231–249, https://doi.org/10.1007/s10639-018-9765-8.

Royandassociates. (2021, May 4). *Cyber Crimes and Cyber Laws in Bangladesh*. Roy & Associates. https://royandassociates.com.bd/cyber-crimes-and-cyber-laws-in-bangladesh/

Samuel-Okon, A. D., Olateju, O., Okon, S. U., Olaniyi, O. O., & Igwenagu, U. (2024). Formulating global policies and strategies for combating criminal use and abuse of artificial intelligence. *Available at SSRN 4873822*.

Schneier, B. (2011). Secrets and lies: digital security in a networked world. John Wiley & Sons, 2011. *Fraud with Danger: The Rise of Cyber Scams in Southeast Asia*. Fulcrum. https://fulcrum.sg/aseanfocus/fraud-with-danger-the-rise-of-cyber-scams-in-southeast-asia/

Shahadat, S. (2025, April 22). *Starlink in Bangladesh: A Digital Leap or Sovereignty Trade-Off?* Thediplomat.com; The Diplomat. https://thediplomat.com/2025/04/starlink-in-bangladesh-a-digital-leap-or-sovereignty-trade-off/

Sharma, V. (2022, November 1). *Most Extensive Cyber Security Challenges & Solutions in 2023*. Www.knowledgehut.com.https://www.knowledgehut.com/blog/security/cyber-security-challenges

Sharma, Y. (2018). *Aadhaar Data Leak: How One Mistake Exposed a Billion Identities*. The Quint. https://www.thequint.com/news/india/aadhaar-data-leak-uidai-cybersecurity-failur

Singar, A.V. and Akhilesh, K.B. (2019). Role of Cyber-Security in Higher Education. Smart Technologies, 249–264, https://doi.org/10.1007/978-981-13-7139-4_19

Syed, A. (2022). Cyber Security Threats to Educational Institutes: A Growing Concern for the New Era of Cybersecurity. International Journal of Data Science and Big Data Analytics, 2(2), 11-17. doi: 10.51483/IJDSBDA.2.2.2022.11-17.

"The National Cybersecurity Strategy of Bangladesh". Ministry of Posts, Telecommunications and Information Technology, 11 March 2014. www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf

Uddin, M. R. (2017). The National Cybersecurity Strategy of Bangladesh: A Critical Analysis. *International Journal of Data Science*, *21*(1-2), 155–174. https://www.researchgate.net/publication/348785720_The_National_Cybersecurity_Strategy_of_Bangladesh_A_Critical_Analysis

Venter, I.M., Blignaut, R.J., Renaud, K. and Venter, M.A (2019). Cyber Security Education Is as Essential as "the Three R's." Heliyon, 5(12), e02855, https://doi.org/10.1016/j.heliyon.2019.e02855.

Verma, R. (2024, January 23). *CYBERSECURITY CHALLENGES IN THE ERA OF DIGITAL TRANSFORMATION*. ResearchGate; unknown. https://www.researchgate.net/publication/377625512_CYBERSECURITY_CHALLENGES_IN_THE_ERA_OF_DIGITAL_TRANSFORMATION

Vesa, H. (2022). *Cyber Threats: Risks and Security Challenges Across Industries*. Pecb.com. https://pecb.com/article/cyber-threats-risks-and-security-challenges-across-industries

Verma, P. and Dumka, A. (2020). Perspectives of Blockchain in the Education Sector Pertaining to the Student's Records. Advances in Information Communication Technology and Computing, 135, 419–425, https://doi.org/10.1007/978-981-15-5421-6_42

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, £., Cetin, F. and Basim, H.N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 62 (1), 1–16, https://doi.org/10.1080/08874417.2020.1712269

Appendix

Questionnaire for survey

1. What is your level of study?
2. What is your field of study?
3. How familiar are you with the term "cybersecurity"?
4. Which of the following cybersecurity practices do you follow regularly?
5. Have you ever been a victim of any form of cyber incident (e.g., hacking, phishing, data leak)?
6. Do you use your university email or login to access government portals, research databases, or shared academic platforms?
7. Do you believe that poor cybersecurity practices by students could lead to risks for national security (e.g., through research data leaks or unauthorized access to sensitive platforms)?
8. Should universities provide mandatory cybersecurity training to all students?
9. In your opinion, who should take more responsibility for student cybersecurity?
10. Have you received any formal training (course, workshop, seminar) on cybersecurity?
11. Which platforms do you most frequently use for academic or research activities?
12. If your personal or academic data were hacked, how confident are you in knowing what steps to take?
13. Do you think the Bangladeshi government is doing enough to protect student data and academic digital infrastructure?
14. What do you think is the biggest cybersecurity threat to university students in Bangladesh today?
15. How often do you update the passwords for your academic or personal accounts?

Interview Transcript 1

Interviewee: Lecturer 1, Department of Computer Science and Engineering, BRAC University

Date: May 2025

Mode: In-person

Interviewer: Afsana Islam Sristy

Q1. How familiar do you think students are with cybersecurity as a concept?

Lecturer 1:

From my experience, students are generally familiar with the *term* "cybersecurity," especially those from technical disciplines. However, their practical understanding is often superficial. Many of them confuse general IT skills with cybersecurity literacy. For example, they might know about using antivirus software but lack deeper knowledge of how phishing attacks or data breaches occur.

Q2. Do you believe students in your university follow safe online practices (e.g., using strong passwords, avoiding suspicious links, etc.)?

Lecturer 1:

Basic practices like using strong passwords or avoiding unknown links are common among tech-savvy students. But I have seen many still use the same password across multiple platforms, and almost no one uses two-factor authentication. So, while awareness is present to some extent, consistent application is lacking.

Q3. Have you observed or heard of any cybersecurity incidents involving students (e.g., phishing, hacking, identity theft)?

Lecturer 1:

Yes, I've heard of students getting locked out of their email accounts due to phishing attempts. Some have lost access to academic documents or had sensitive information shared online. While not always severe, these incidents show how vulnerable students are.

Q4. How aware do you think students are of the connection between their cybersecurity breach and national security risks?

Lecturer 1:

Very few students consider the national implications of cybersecurity. They tend to think in terms of personal loss—grades, emails, social media. But university systems often connect with research databases or cloud platforms that store sensitive or strategic information. Students don't always realize they can be entry points for larger breaches.

Q5. Do you think formal cybersecurity training should be part of the academic curriculum?

Lecturer 1:

Absolutely. Not just for computer science students, but for everyone. Cybersecurity is now a core digital literacy skill. We should integrate short modules or mandatory workshops across departments.

Interview Transcript 2

Interviewee: Lecturer 2, Department of Electrical and Electronic Engineering, BRAC University

Date: May 2025

Mode: Virtual Interview (Zoom)

Interviewer: Afsana Islam Sristy

Q1. From your experience, how do you assess the general cybersecurity awareness among university students?

Lecturer 2:

It's mixed. Some students are well-informed, especially those involved in research or internships with tech firms, but many others are careless. They use public Wi-Fi without VPNs, don't update software regularly, and are unaware of how malware can be disguised in common files.

Q2. Do you think students understand the risks involved in using cloud platforms like Google Drive or ResearchGate for academic sharing?

Lecturer 2:

Not really. Most students use these platforms out of convenience, not security awareness. They often set sharing permissions to “anyone with the link” without understanding the risk. Academic data might not seem critical to them, but in the wrong hands, it can lead to IP theft or misuse.

Q3. Have any of your students ever reported falling victim to online scams or cyber incidents?

Lecturer 2:

Yes, a student once shared that their email was compromised after clicking on a fake university login portal. Another incident involved a shared thesis document being tampered with. These events are not isolated, but many go unreported due to embarrassment.

Q4. What role should universities play in protecting students from cyber threats?

Lecturer 2:

Universities need to take a more active role—implement better firewalls, offer cybersecurity training sessions, and perhaps appoint digital mentors in each department. Also, faculty and staff should receive similar training.

Q5. Do you believe students' lack of cybersecurity awareness could indirectly threaten national interests?

Lecturer 2:

Yes. Students are involved in sensitive research or collaborations with institutions connected to national infrastructure. If a student device is compromised, it could become a backdoor to broader systems. In that sense, their cybersecurity habits have national relevance.