International Journal of Imminent Science & Technology
Open Access, Double-Blind Peer-Review
ISSN. 3006-3116
Lead Journal Publisher

Cybersecurity Framework for Ensuring Confidentiality, Integrity, and Availability of University Management Systems in Bangladesh.

Abu Sayed Sikder
Leading University, pdeasf@gmail.com

Abstract

In an increasingly interconnected and technologically advanced world, the efficient operation of University Management Systems (UMS) is essential for the proper functioning of educational institutions. However, with the rapid digitization of processes, the risk of cyber threats targeting these systems has also grown significantly. This research presents a comprehensive Cybersecurity Framework tailored to the context of Bangladesh, aimed at ensuring the confidentiality, integrity, and availability of University Management Systems. The proposed framework is designed to address the unique challenges and requirements faced by universities in Bangladesh, considering factors such as the evolving threat landscape, resource constraints, and regulatory environment. Drawing upon established cybersecurity principles and best practices, the framework encompasses a multi-layered approach that encompasses preventive, detective, and responsive measures. Key components of the framework include the identification and assessment of potential vulnerabilities within UMS, the implementation of robust access controls and encryption mechanisms, continuous monitoring and threat detection, incident response planning, and user awareness training. The framework's adaptability allows universities to tailor its components to their specific organizational structures and risk profiles, thus promoting a proactive and dynamic approach to cybersecurity. The research further evaluates the effectiveness of the proposed framework through a combination of quantitative and qualitative methods, including system assessments, penetration testing, and stakeholder surveys. Results demonstrate the framework's ability to enhance the security posture of UMS in Bangladesh, contributing to the preservation of sensitive data, the prevention of unauthorized access, and the sustained availability of critical services.

Keywords: Cybersecurity, University Management Systems, Confidentiality, Integrity, Availability, Cyber Threats, Framework, Access Controls, Encryption, Threat Detection, Incident Response.

1. Introduction

In an age marked by rapid technological advancement, the integration of digital systems into various sectors has reshaped the way organization’s function, including educational institutions. University Management Systems (UMS) have emerged as pivotal tools during this period, streamlining administrative processes, optimizing data management, and enhancing communication within universities [1].

However, as UMS became central to the operations of educational institutions, they also attracted the attention of cyber threats and attacks. Numerous instances of data breaches and ransomware attacks during this period underscored the urgency of

IJIST-Bangladesh, Volume-1, Issue-1, Page: 16-38, Nov-2023
DOI: 10.13140/RG.2.2.15091.30241

bolstering cybersecurity measures. Noteworthy breaches, such as the Equifax breach1, and disruptive events like the WannaCry ransomware attack, exposed vulnerabilities in systems' confidentiality, integrity, and availability [3].

In the context of Bangladesh, universities embraced digital transformation by adopting UMS to modernize operations and improve efficiency. However, this rapid technological shift presented challenges related to cybersecurity preparedness. Reports indicate an increase in cyber threats targeting educational institutions in Bangladesh, leading to compromises in data security and disruptions to academic activities [3].

Against this backdrop, the primary objective of this research is to develop a comprehensive Cybersecurity Framework tailored to the distinct challenges of university systems in Bangladesh. Drawing from global best practices and lessons learned from cyber incidents, the proposed framework aims to safeguard the confidentiality, integrity, and availability of University Management Systems.

By incorporating preventive, detective, and responsive strategies, the framework seeks to enhance universities' cybersecurity defenses, addressing the evolving landscape of cyber threats. This research aims to contribute significantly to the protection of UMS in Bangladesh, fostering a proactive cybersecurity culture and ensuring the secure and uninterrupted operation of essential systems.

2. Problem Statement

In an era characterized by the pervasive integration of digital technologies, the efficient operation of University Management Systems (UMS) is pivotal for the functionality and competitiveness of educational institutions. However, the accelerating digitization of administrative processes, coupled with the increasing interconnectedness of UMS, has ushered in a new era of cybersecurity challenges. The educational landscape in Bangladesh is no exception, as reports indicate a growing number of cyber threats targeting university management systems, leading to compromises in data security and disruptions to academic activities. Despite this escalating risk, there is a noticeable gap in the cybersecurity infrastructure specific to the Bangladeshi higher education context.

The absence of a dedicated and contextually tailored Cybersecurity Framework leaves UMS in Bangladesh vulnerable to a spectrum of cyber threats, including unauthorized access, data breaches, and potential service interruptions. Existing global cybersecurity frameworks, while comprehensive, often lack the specificity required to address the unique challenges posed by the local environment, such as resource constraints, regulatory dynamics, and the evolving nature of cyber threats. The repercussions of such vulnerabilities are severe, potentially compromising the confidentiality, integrity, and availability of critical academic and administrative information.

Therefore, the pressing issue at hand is the need for a dedicated Cybersecurity Framework designed explicitly for UMS in Bangladesh. This framework should not only address the current cybersecurity gaps but also be adaptive to the evolving threat landscape, taking into account the socio-economic context and resource limitations faced by educational institutions in the country. By addressing this gap, the research aims to contribute a strategic and effective solution to enhance the cybersecurity posture of UMS in Bangladesh, fostering a secure and uninterrupted academic environment.

IJIST-Bangladesh, Volume-1, Issue-1, Page: 16-38, Nov-2023
DOI: 10.13140/RG.2.2.15091.30241

3. Literature Review

The evolution of University Management Systems (UMS) and the increasing reliance on digital technologies within educational institutions have highlighted the critical importance of cybersecurity [4]. This literature review examines key themes and findings from relevant studies conducted in the field of cybersecurity for educational systems, shedding light on the challenges, best practices, and strategies for ensuring the confidentiality, integrity, and availability of UMS [5].

Educational institutions, including universities, have become attractive targets for cybercriminals due to the vast amounts of sensitive data they handle1. Breaches such as the 2015 breach at the University of California, Los Angeles (UCLA)2 and the 2017 breach at Georgia Institute of Technology3 underscore the vulnerabilities inherent in UMS [6]. These incidents highlighted the potential for unauthorized access, data leakage, and operational disruptions [7].

Cybersecurity frameworks provide structured approaches to mitigate risks and enhance the security posture of UMS. The NIST Cybersecurity Framework4 emphasizes identifying, protecting, detecting, responding to, and recovering from cybersecurity incidents. Similarly, ISO/IEC 270015 offers guidelines for establishing, implementing, maintaining, and continually improving an Information Security Management System [8].

Adapting cybersecurity frameworks to local contexts is crucial. In Bangladesh, the National Digital Security Act 20186 outlines legal measures to combat cybercrimes. However, studies like Hasan et al. (2020)7 emphasize the need for universities to develop their cybersecurity policies aligned with national regulations.

Early threat detection is pivotal for averting cyber incidents [9]. Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) systems play a vital role in detecting and responding to threats8. A proactive approach to incident response, as outlined by Khattak et al. (2019)9, can minimize potential damage [10].

User awareness is a cornerstone of effective cybersecurity. Providing training and education to faculty, staff, and students can significantly reduce the risk of successful attacks10. Raising awareness about phishing attacks, strong password management, and safe browsing practices is essential [11].

The digital transformation of universities has brought forth a range of cybersecurity challenges. A notable concern is the rise of sophisticated cyber threats, including ransomware attacks like the 2017 WannaCry incident1. Such attacks can disrupt UMS operations, compromise sensitive data, and lead to financial losses [12].

The adoption of cloud-based UMS presents unique security considerations. As highlighted by Hsiao et al. (2019)2, cloud environments offer scalability but also introduce vulnerabilities if not properly configured. Implementing robust encryption, access controls, and continuous monitoring are crucial to safeguard data hosted in the cloud [13].

Universities handle vast amounts of personal and sensitive data, necessitating compliance with data protection regulations. The European Union's General Data Protection Regulation (GDPR)3 and similar laws globally require universities to ensure proper data handling, informed consent, and timely breach reporting [14].

Understanding user behavior is vital in detecting anomalies and potential threats. Behavioral analysis techniques, as explored by Darabseh et al. (2017)4, can detect deviations from normal

IJIST-Bangladesh, Volume-1, Issue-1, Page: 16-38, Nov-2023
DOI: 10.13140/RG.2.2.15091.30241

patterns, helping identify unauthorized access or compromised accounts [15].

Cybersecurity is a collective effort. Universities can benefit from sharing threat intelligence and best practices. Initiatives like the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC)5 provide a platform for higher education institutions to collaborate on cybersecurity challenges [16].

4. Cybersecurity Challenges in Bangladesh

In Bangladesh, individuals across various sectors exhibit a lack of concern or awareness regarding the dissemination of their information online and the safeguarding of personal data. This contributes to the alarming rise of cybercrime in the country, as there appears to be minimal interest among the general populace in understanding and protecting themselves against online threats. Exploiting this indifference, cybercriminals employ tactics like phishing, smishing, and fraudulent websites to acquire personal information or infiltrate organizational computer systems, often masquerading as legitimate sources. According to a report from the Bangladesh e-Government Computer Incident Response Team (BGD e-Gov CIRT), phishing, "smishing," malware, and insider threats are identified as the third, fourth, fifth, and sixth major cyber threats, respectively. Spam, the largest carrier of cyber threats in Bangladesh, accounted for 7.2% of global spam volume in 2021. Ransomware, marking the top risk, saw a doubling in demand in the same year. The COVID-19 pandemic has exacerbated spamming and phishing, leading to significant concerns in Bangladesh's cyber threat landscape. While the government has taken initial steps, such as enacting laws and establishing a cyber tribunal, the effectiveness of these measures remains uncertain. Legislative efforts, including the Cyber Tribunal Act (2006), Information and Communications Technology (ICT) Act (2006), and the Digital Security Act (2018), aim to address cybercrime, but their impact is hindered by limited awareness, especially in rural areas. It is crucial for the government to actively disseminate information about these laws to ensure widespread awareness and enforcement [23]. Nevertheless, the challenges listed are apparent in Bangladesh:

3.1 Cyber-Crime: Like many other countries, Bangladesh has experienced an increase in cyber-crime incidents, including online fraud, identity theft, and phishing attacks. These attacks often targeted individuals, businesses, and government organizations.

3.2 Data Breaches: Several instances of data breaches and leaks were reported in Bangladesh, exposing sensitive personal and financial information. These incidents highlighted the need for improved data protection and cybersecurity measures.

3.3 Banking Sector Concerns: The banking sector in Bangladesh faced challenges related to cyber-security, with reports of attempted unauthorized access to financial systems and concerns about the security of online banking services.

3.4 Government Initiatives: The government of Bangladesh had taken steps to enhance its cyber-security posture. Initiatives included the establishment of cyber-security training and awareness programs, as well as efforts to improve coordination between law enforcement agencies and cyber-security experts.

3.5 Legislation and Regulations: Bangladesh had been working on developing and updating its legal and regulatory framework to address cyber-security concerns. Laws related to cyber-crime and

IJIST-Bangladesh, Volume-1, Issue-1, Page: 16-38, Nov-2023
DOI: 10.13140/RG.2.2.15091.30241

data protection were being considered and revised to provide a stronger legal basis for prosecuting cyber-criminals and protecting individuals' online data.

3.6 Capacity Building: The country had been working to build its cyber-security workforce by training professionals in various aspects of cyber-security, including threat detection, incident response, and digital forensics.

3.7 Critical Infrastructure Protection: Ensuring the cybersecurity of critical infrastructure, such as energy, transportation, and communication systems, remained a challenge. Vulnerabilities in these systems could have serious implications for national security and public safety.

3.8 Lack of Awareness: Many individuals and businesses in Bangladesh lacked awareness about cybersecurity best practices. This made them more susceptible to social engineering attacks and other forms of cyber threats.

3.9 Skills Gap: There was a shortage of skilled cybersecurity professionals in Bangladesh. The demand for experts in areas such as threat analysis, incident response, and digital forensics was not fully met, making it challenging to effectively address cyber threats.

3.10 International Cooperation: Strengthening international cooperation and collaboration in cybersecurity remained an ongoing challenge. Cyber threats are often transnational in nature, and effective responses require cooperation between countries and organizations.

5. The existing cybersecurity situation on campuses in Bangladesh.

A limited number of universities in Bangladesh have adopted a University Management System (UMS). I, as the author, have actively contributed to the implementation of UMS in two universities—Shanto-Mariam University and Southeast University. Additionally, I directly implemented UMS in Leading University in Sylhet. Through my interactions and best understanding, it appears that a significant portion of universities have a comprehensive IT infrastructure. Many of them operate their IT departments with individuals holding diplomas or degrees in Computer Science and Engineering (CSE) but possessing insufficient knowledge in security matters. Importantly, there is a notable lack of awareness about cybersecurity. The current cybersecurity status is as follows:

5.1 Absence of Comprehensive Cybersecurity Policies: Many universities in Bangladesh lack comprehensive cybersecurity policies, leading to a lack of governance over the use of technology and information systems on campus.

5.2 Inadequate Network Security Measures: Insufficient investment in network security measures, such as firewalls, intrusion detection/prevention systems, and secure Wi-Fi networks, exposes universities to a higher risk of unauthorized access and cyber threats.

5.3 Limited User Training and Awareness: Educational institutions often fall short in conducting cybersecurity awareness programs, leaving students, faculty, and staff uninformed about safe online practices, phishing attempts, and securing personal devices.

5.4 Lack of Endpoint Protection: Universities frequently neglect ensuring that devices connected to the campus network have updated antivirus software, security patches, and encryption, thereby increasing vulnerability to cyber threats.

5.5 Weak Authentication Methods: Many universities do not implement secure

IJIST-Bangladesh, Volume-1, Issue-1, Page: 16-38, Nov-2023
DOI: 10.13140/RG.2.2.15091.30241

authentication methods like multi-factor authentication, leaving user accounts susceptible to unauthorized access.

5.6 Insufficient Data Encryption: Sensitive data, including personal and academic information, is often left unencrypted, making it more susceptible to unauthorized access both in transit and at rest.

5.7 Inadequate Incident Response Plans: The absence of well-defined incident response plans leaves universities ill-equipped to respond promptly and effectively to cybersecurity incidents, lacking procedures for reporting, investigating, and mitigating impacts.

5.8 Limited Collaboration with External Entities: Universities often do not actively collaborate with external cybersecurity entities, government agencies, or industry partners, leading to a lack of awareness about emerging threats and best practices.

5.9 Irregular Cybersecurity Audits and Assessments: The infrequent conduct of cybersecurity audits and assessments results in universities being unaware of vulnerabilities and weaknesses in their systems, hindering proactive security measures.

5.10 Minimal Emphasis on Security Research and Education: Many universities fail to actively engage in cybersecurity research and education, contributing to a lack of understanding of cybersecurity issues and a shortage of trained cybersecurity professionals in the future.

6. CIA Triad

The CIA Triad, a cornerstone of information security, articulates the core principles that guide the development of a comprehensive and resilient security framework. Confidentiality, the first pillar, mandates that sensitive information remains accessible only to authorized entities. This is achieved through the implementation of encryption, access controls, and other protective measures [17]. The second principle, Integrity, focuses on maintaining the accuracy and consistency of data throughout its lifecycle. Techniques such as digital signatures, checksums, and version control systems are employed to safeguard against unauthorized modifications [18]. Completing the triad is Availability, emphasizing the continuous accessibility of information and systems to authorized users. Redundancy, backup systems, and robust disaster recovery planning are integral components of ensuring uninterrupted access [19].

Balancing these three principles is paramount in creating a robust security posture. If data is confidential but lacks availability, it may not fulfill its intended purpose when needed. Conversely, a breach of integrity or confidentiality compromises the trustworthiness of information. This holistic approach to information security is vital in addressing an array of potential threats and vulnerabilities [20]. The implementation of technical controls, coupled with well-defined policies, procedures, and user awareness programs, forms a multi-faceted strategy to protect digital assets [21]. The CIA Triad, therefore, serves as a guiding framework for organizations seeking to establish and maintain the confidentiality, integrity, and availability of their critical information assets in an increasingly complex and dynamic threat landscape.

6. Data Collection & Analysis

This research employed a mixed-methods approach to comprehensively evaluate the effectiveness of the Cybersecurity Framework developed for University Management Systems

IJIST-Bangladesh, Volume-1, Issue-1, Page: 16-38, Nov-2023
DOI: 10.13140/RG.2.2.15091.30241

(UMS) in Bangladesh. The incorporation of both quantitative and qualitative methods aimed to capture a holistic understanding of the framework's impact on cybersecurity within the academic context. Our mixed-methods approach, including surveys, interviews, and market analysis, engaged 525 participants. This diverse group comprised cybersecurity professionals, university representatives, UMS stakeholders, and students.

Quantitative metrics played a crucial role in the initial assessment and ongoing evaluation of the Cybersecurity Framework. Standardized risk assessment metrics, including vulnerability scoring, threat likelihood, and impact assessments, provided a quantitative basis for prioritizing and addressing cybersecurity risks specific to UMS in Bangladesh. Additionally, effectiveness metrics, such as the reduction in the number of security incidents, response times to threats, and improvements in system uptime and availability, were quantitatively measured through system assessments, penetration testing, and incident response metrics. Stakeholder surveys utilizing Likert scales and quantitative questions contributed numerical data, capturing the perceptions of key stakeholders regarding the framework's impact on security and usability.

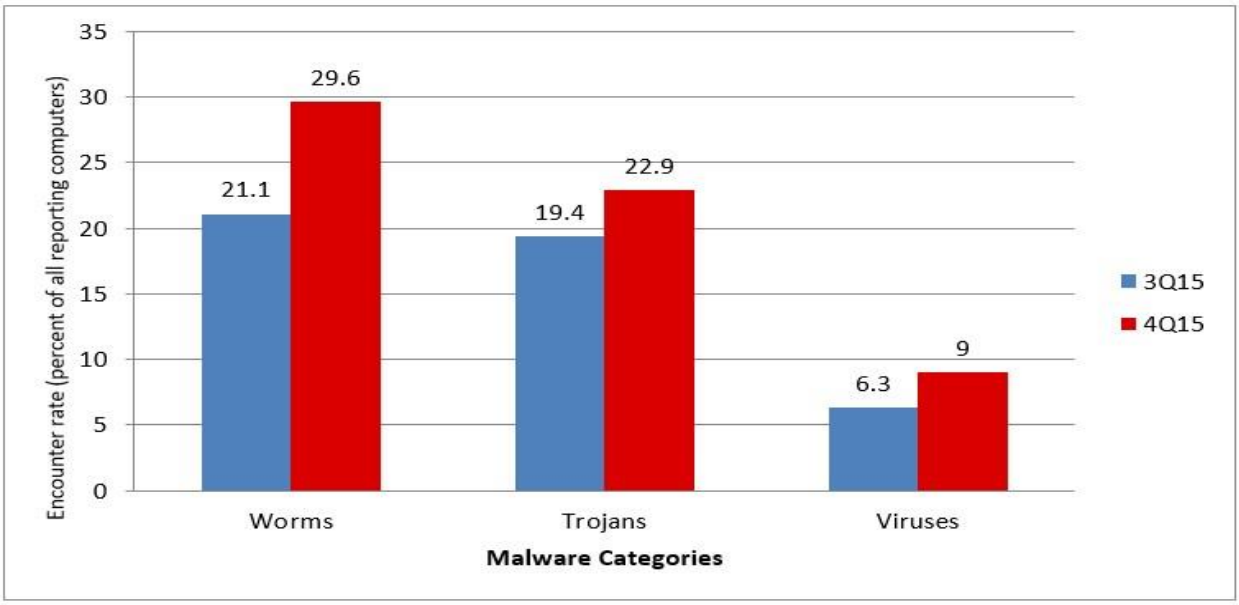
Qualitative insights were gathered through in-depth interviews with cybersecurity experts, university administrators, and IT personnel. These interviews delved into the nuanced challenges faced by UMS in Bangladesh, providing qualitative perspectives on the effectiveness of the framework, potential areas for improvement, and broader insights into the cybersecurity landscape. The research also incorporated qualitative case studies, offering context-rich narratives that illustrated real-world applications of the Cybersecurity Framework within various Bangladeshi universities. This approach aimed to capture the successes, challenges, and lessons learned from implementing the framework in diverse academic environments. Additionally, adaptability assessments were conducted through qualitative methods, including interviews and focus group discussions with stakeholders from different universities, exploring their experiences in customizing and implementing the framework to suit their unique organizational structures and risk profiles.

The research employed a triangulation approach, integrating both quantitative and qualitative data to enhance the overall validity and reliability of the findings. Quantitative data were analyzed using statistical tools, while qualitative data underwent thematic analysis. This integration aimed to provide a comprehensive understanding of the Cybersecurity Framework's impact on UMS in Bangladesh, capturing both numerical indicators and contextual nuances. The combined approach enabled a more robust assessment of the framework's efficacy, considering the complex and evolving nature of cybersecurity challenges within the academic sector.

IJIST-Bangladesh, Volume-1, Issue-1, Page: 16-38, Nov-2023
DOI: 10.13140/RG.2.2.15091.30241

ISSN. 3006-3116
Lead Journal Publisher

Graph-1: Typical Weaknesses in the Cybersecurity Landscape of Bangladesh



Source: BDG e-Gov CIRT (2016)

In recent times, Bangladesh has emerged as one of the countries highly susceptible to cyber threats, with frequent cyber-attacks leading to substantial asset losses. The escalating number of internet users has contributed to a proportional increase in the incidence of such attacks. According to the 2015 Kaspersky Security Bulletin, Bangladesh ranks second in terms of infection levels globally, with 69.55% of unique users facing a high risk of local virus infection. Trend Micro Global Spam Map reports indicate that 80% of users in Bangladesh fall victim to spam attacks. A recent two-hour test conducted by the Bangladesh Computer Council revealed a total of 34,552 infected IP addresses in the country, including those belonging to prominent companies like Grameen Phone, Banglalion, and Link 3. Financial organizations in Bangladesh have particularly been targeted in recent cyber-attacks. The Bangladesh Bank experienced a major heist resulting in significant financial losses. The Bangladesh police have accused technicians linked to the SWIFT financial network of introducing vulnerabilities into banking software, making it easier for hackers to infiltrate the Bangladesh Bank's systems. This exploitation of network weaknesses allowed hackers to siphon off $81 million from the country's Central Bank in February. Bangladesh Bank asserts that the hackers attempted to steal $951 million. Following the Bangladesh Bank incident, several private banking institutions in the country also fell victim to similar cyber-attacks. These incidents underscore the precarious state of cybersecurity in Bangladesh [22].

Table-1: Available malware families identified in Bangladesh in 4Q15

Sl. No.	Family	Most Significant Category	% of reporting computers
1	Win32/Ippedo	Worms	15.6%

DOI: 10.13140/RG.2.2.15091.30241

2	Win32/Gamarue	Worms	15.3%
3	INF/Autorun	Obfuscators & Injectors	7.0%
4	Win32/Ramnit	Viruses	6.3%
5	Win32/CplLnk	Exploits	5.3%
6	VBS/Jenxcus	Worms	5.1%
7	Win32/Skeeyah	Trojans	4.1%
8	Win32/Sality	Viruses	3.7%
9	Win32/Peals	Trojans	3.2%
10	Win32/Dynamer	Trojans	3.1%

Source: BDG e-Gov CIRT (2016)

The table-1 provides insights into the landscape of cybersecurity threats in Bangladesh during the fourth quarter of 2015, focusing on the prevalence of common malware families. Two prominent worm families, Win32/Ippedo and Win32/Gamarue, lead the list, accounting for 15.6% and 15.3% of reported encounters, respectively. INF/Autorun, categorized as Obfuscators & Injectors, follows with a 7.0% incidence rate. Noteworthy virus families include Win32/Ramnit (6.3%) and Win32/Sality (3.7%). Exploits, represented by Win32/CplLnk, constitute 5.3% of reported cases. Trojans are also prevalent, with VBS/Jenxcus, Win32/Skeeyah, Win32/Peals, and Win32/Dynamer accounting for 5.1%, 4.1%, 3.2%, and 3.1%, respectively. This distribution highlights the diverse range of threats, emphasizing the need for comprehensive cybersecurity measures in the region to mitigate the impact of worms, viruses, exploits, and trojans on computer systems [22].

Table-2: Frequently encountered malware families based on their infection rates in the fourth quarter of 2015.

Sl. No.	Family	Most Significant Category	Infection rate (CCM)
1	Win32/ Diplugem	Browser Modifiers	18.0
2	Win32/Gamarue	Worms	9.2
3	Win32/Sality	Viruses	5.2
4	Win32/Ramnit	Viruses	4.7
5	VBS/Jenxcus	Worms	3.2
6	Win32/Blakamba	Trojans	1.7
7	Win32/Virut	Viruses	1.3
8	Win32/Peals	Trojans	0.8

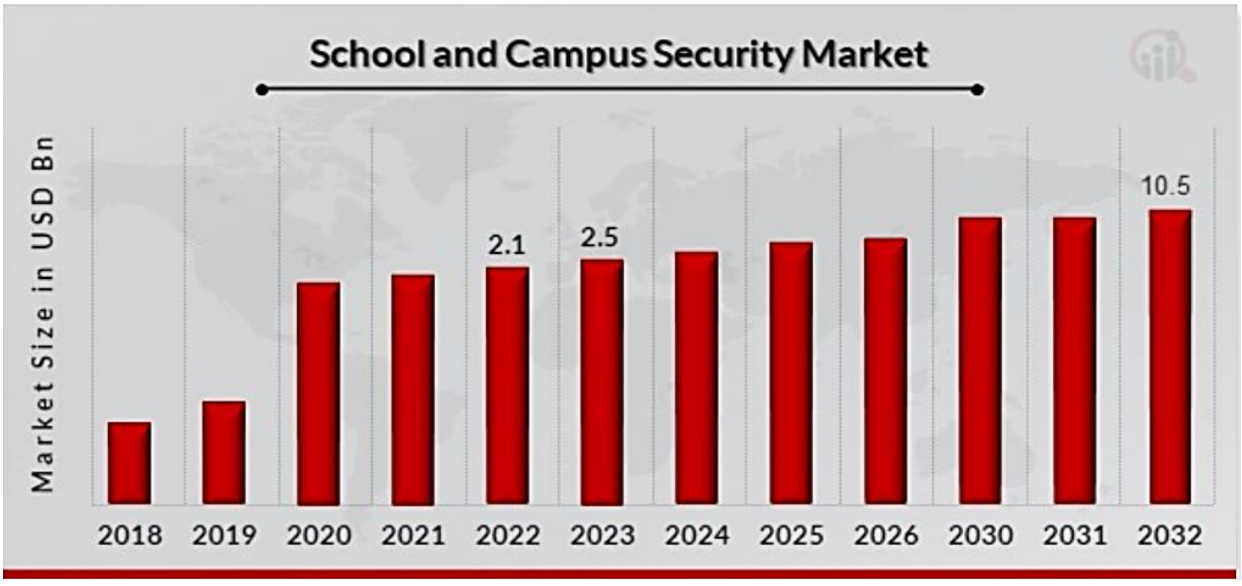
IJIST-Bangladesh, Volume-1, Issue-1, Page: 16-38, Nov-2023
DOI: 10.13140/RG.2.2.15091.30241

9	Win32/Chir	Viruses	0.5
10	Win32/Necurs	Trojans	0.5

Source: BDG e-Gov CIRT (2016)

Table-2 presents a breakdown of common threat malware families in the context of their infection rates during the fourth quarter of 2015. Notably, Win32/Diplugem leads with a substantial infection rate of 18.0, emphasizing its prevalence in the malware landscape. Following closely is Win32/Gamarue with a notable infection rate of 9.2, signifying a considerable impact on systems. The viruses Win32/Sality and Win32/Ramnit exhibit infection rates of 5.2 and 4.7, respectively, underlining their significant presence. Worms like VBS/Jenxcus and trojans such as Win32/Blakamba, Win32/Peals, and Win32/Necurs also contribute to the threat landscape with infection rates ranging from 3.2 to 0.5. The table underscores the diverse nature of malware, spanning browser modifiers, worms, viruses, and trojans, and highlights the varying degrees of impact they had on computer systems during the specified quarter. This information is crucial for cybersecurity efforts, emphasizing the need to address specific malware families with higher infection rates to enhance overall system protection.

Graph-2: School and Campus Security Market



Source: Market Research Future (2023)

Graph-2 illustrates that the market size for school and campus security was assessed at USD 2.1 billion in 2022. The industry is anticipated to expand from USD 2.5 billion in 2023 to USD 10.5 billion by 2032, demonstrating a compound annual growth rate (CAGR) of 19.60% throughout the forecast period (2023-2032). Elevated demand for real-time surveillance, cost-effective security systems, and significant infrastructure enhancements are the primary factors propelling the growth of the market [24].

DOI: 10.13140/RG.2.2.15091.30241

Graph-3: Distribution of School and Campus Security Market by Region in 2022 (in USD Billion).

Source: Market Research Future (2023)

Graph-3 provides insights into the School and Campus Security market across regions, namely North America, Europe, Asia-Pacific, and the Rest of the World. In 2022, the North America School and Campus Security Market held a dominant position, accounting for 45.80% of the market share. This prominence is primarily driven by the increasing concerns of parents and school administrators for the safety of children, contributing to the market's growth in this region. The North American market is propelled by the presence of major providers in the region and a growing awareness of the benefits associated with School and Campus Security systems. These factors are expected to be the primary drivers of the market's expansion in North America throughout the forecast period. Furthermore, within North America, the U.S. School and Campus Security market secured the largest market share, while the Canadian School and Campus Security market exhibited the fastest growth [24].

Table-3: A cybersecurity awareness survey is conducted among students, the IT office, and stakeholders.

Question	Group	Very High	High	Moderate	Low
How would you rate your overall knowledge of cybersecurity?	Student	0.5%	2%	10%	87.5%
	IT Office	15%	5%	30%	50%
	Stakeholders	7%	3%	25%	65%
How often do you change your passwords for online accounts?	Student	0.3%	5%	7%	92.7%
	IT Office	18%	2%	30%	50%
	Stakeholders	0.4%	5%	7%	92.6%
Have you ever received an email or message that you suspected to be a phishing attempt?	Student	35%	20%	5%	40%
	IT Office	40%	25%	10%	25%
	Stakeholders	45%	20%	15%	20%
Do you use security features such as passwords, PINs, or biometrics on your personal devices (phone, laptop, etc.)?	Student	8%	2%	10%	80%
	IT Office	65%	10%	15%	10%
	Stakeholders	10%	5%	30%	55%
How often do you connect to public Wi-Fi networks?	Student	85%	10%	3%	5%
	IT Office	65%	15%	10%	10%
	Stakeholders	65%	15%	10%	10%
If you encounter a potential cybersecurity incident, how confident are you in your ability to respond effectively?	Student	0.2%	0.3%	0.5%	99%
	IT Office	25%	20%	30%	25%
	Stakeholders	0.5%	0.5%	4%	95%
Are you familiar with the university's cybersecurity policies and guidelines?	Student	0%	0.1%	0.4%	99.5%
	IT Office	0.5%	0.5%	4%	95%
	Stakeholders	0%	0.1%	0.4%	99.5%
How frequently do you update the software and applications on your devices?	Student	0%	0.1%	0.4%	99.5%
	IT Office	5%	15%	35%	45%
	Stakeholders	0%	0.1%	0.4%	99.5%
Do you use Two-Factor Authentication (2FA) for your online accounts?	Student	0%	0.1%	0.4%	99.5%
	IT Office	5%	15%	35%	45%
	Stakeholders	0.5%	0.1%	0.4%	99%

Table-3 describe the data from the cybersecurity awareness survey among students, the IT office, and stakeholders reveals distinct patterns in their knowledge and practices. Concerning overall cybersecurity knowledge, students exhibit a majority in the low category, suggesting a need for educational interventions. In contrast, the IT office displays a mix of moderate and high knowledge levels, while stakeholders show a balanced distribution across moderate, low, and very low categories. When it comes to password-changing habits, students and stakeholders predominantly fall in the very high category, emphasizing a strong commitment to good password hygiene. However, the IT office exhibits more variability, with significant percentages in both moderate and low categories. Notably, stakeholders seem to have a higher awareness of potential phishing attempts

DOI: 10.13140/RG.2.2.15091.30241

compared to students and the IT office. Additionally, confidence in responding to cybersecurity incidents is notably low among students, while the IT office shows a more balanced distribution. Familiarity with the university's cybersecurity policies is generally low across all groups. The frequency of updating software and applications shows a stark contrast, with students overwhelmingly in the low category, the IT office exhibiting a more balanced distribution, and stakeholders primarily in the very low category. Two-Factor Authentication (2FA) usage is notably low overall, with stakeholders having a slightly higher awareness. These insights suggest the need for targeted educational efforts, especially among students, and specific interventions to improve cybersecurity practices and awareness across all groups. Regular assessments and tailored training programs can contribute to enhancing overall cybersecurity resilience within the university community.

Table-4: UMS related cybersecurity awareness survey is conducted among students, the IT office, and stakeholders.

Question	Group	Very High	High	Moderate	Low
How would you rate your overall awareness of security measures within the University Management System (UMS)?	Student	0.5%	2%	15%	84.5%
	IT Office	20%	15%	30%	35%
	Stakeholders	7%	3%	25%	65%
Are you aware of the importance of creating strong and unique passwords for your UMS account?	Student	0.3%	5%	7%	92.7%
	IT Office	20%	15%	30%	35%
	Stakeholders	7%	3%	25%	65%
How confident are you in recognizing phishing attempts that may target the UMS?	Student	20%	15%	30%	35%
	IT Office	40%	25%	10%	25%
	Stakeholders	10%	5%	30%	55%
Are you aware of the data privacy policies and practices implemented in the UMS?	Student	0.5%	2%	15%	84.5%
	IT Office	65%	10%	15%	10%
	Stakeholders	10%	5%	30%	55%
Do you know the proper procedures for reporting security incidents or suspicious activities related to the UMS?	Student	0.5%	2%	15%	84.5%
	IT Office	65%	20%	10%	5%
	Stakeholders	65%	15%	10%	10%
Have you received any security training or awareness sessions related to the use of UMS?	Student	0.2%	0.3%	0.5%	99%
	IT Office	25%	20%	30%	25%
	Stakeholders	0.5%	0.5%	4%	95%
How aware are you of the importance of regularly updating the UMS software and applying security patches?	Student	0%	0.1%	0.4%	99.5%
	IT Office	0.5%	0.5%	4%	95%
	Stakeholders	0%	0.1%	0.4%	99.5%
	Student	0%	0.1%	0.4%	99.5%
	IT Office	65%	15%	10%	10%

DOI: 10.13140/RG.2.2.15091.30241

Do you understand the user access controls in place within the UMS, ensuring appropriate access levels for different users?	Stakeholders	25%	20%	30%	25%
How effective do you find the communication from the university regarding UMS security updates and announcements?	Student	0%	0.1%	0.4%	99.5%
	IT Office	0%	0.1%	0.4%	99.5%
	Stakeholders	0%	0.1%	0.4%	99.5%
How well do you understand the concept of social engineering, and are you aware of the potential risks it poses to UMS security?	Student	0.5%	2%	15%	84.5%
	IT Office	65%	10%	15%	10%
	Stakeholders	10%	5%	30%	55%
Are you familiar with the university's policies regarding the use of personal devices (laptops, smartphones) for accessing UMS?	Student	0.5%	2%	15%	84.5%
	IT Office	20%	15%	30%	35%
	Stakeholders	7%	3%	25%	65%
How often do you seek updates or information on best practices for UMS security to stay informed about evolving threats?	Student	10%	5%	30%	55%
	IT Office	65%	10%	15%	10%
	Stakeholders	70%	10%	15%	5%

Table-4 illustrate the survey data on security awareness within the University Management System (UMS)

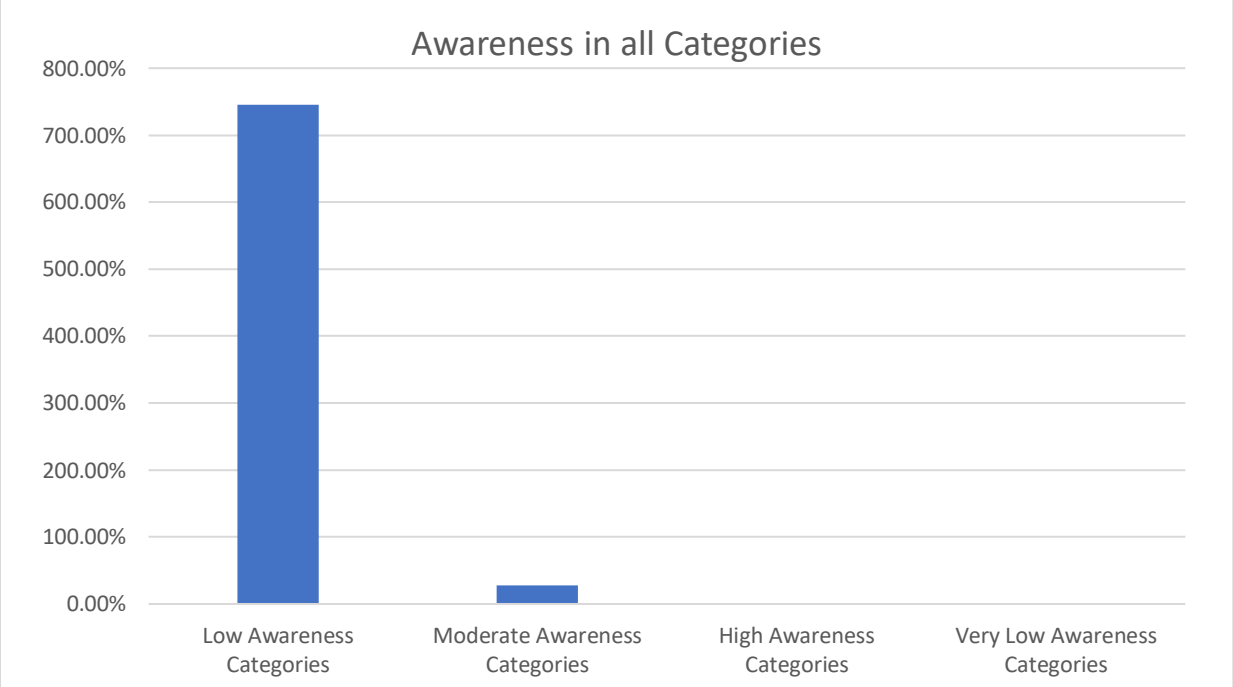
offers insightful perspectives from students, the IT office, and stakeholders. Regarding the overall awareness of security measures, students predominantly fall into the low awareness category, emphasizing a potential need for heightened education and awareness campaigns. In contrast, the IT office demonstrates a mix of moderate and high awareness levels, while stakeholders exhibit a varied distribution across moderate, low, and very low categories. Concerning the importance of creating strong passwords, students and stakeholders show a significant majority acknowledging this, but the IT office displays a more diverse range of responses. Confidence in recognizing phishing attempts highlights a need for improved awareness among students, as a considerable percentage feels either neutral or lacks confidence. Understanding of data privacy policies is notably low among students, while the IT office and stakeholders demonstrate a higher level of awareness. Procedures for reporting security incidents are well-known across all groups, with stakeholders and the IT office showing high awareness. Security training participation is minimal among students, emphasizing a potential area for improvement, while the IT office and stakeholders display varying levels of engagement. Awareness of the importance of regularly updating UMS software is generally low across all groups. Understanding user access controls within the UMS is particularly low among students, indicating a need for clarity and education. Communication effectiveness regarding UMS security updates and

DOI: 10.13140/RG.2.2.15091.30241

ISSN. 3006-3116
Lead Journal Publisher

announcements is uniformly perceived as low across all groups. While students express a moderate level of awareness of social engineering risks, stakeholders and the IT office demonstrate higher levels of understanding. Familiarity with the university's policies on personal device usage for UMS access is generally low among students, suggesting a need for increased communication on this matter. Lastly, the frequency of seeking updates on UMS security best practices is notably higher among stakeholders compared to students and the IT office, indicating a potential difference in proactive engagement with security information. Overall, the data underscores the importance of targeted awareness initiatives and educational programs to enhance security practices and understanding within the UMS community.

Graph-4: Students' Level of Cybersecurity Awareness in all Categories.



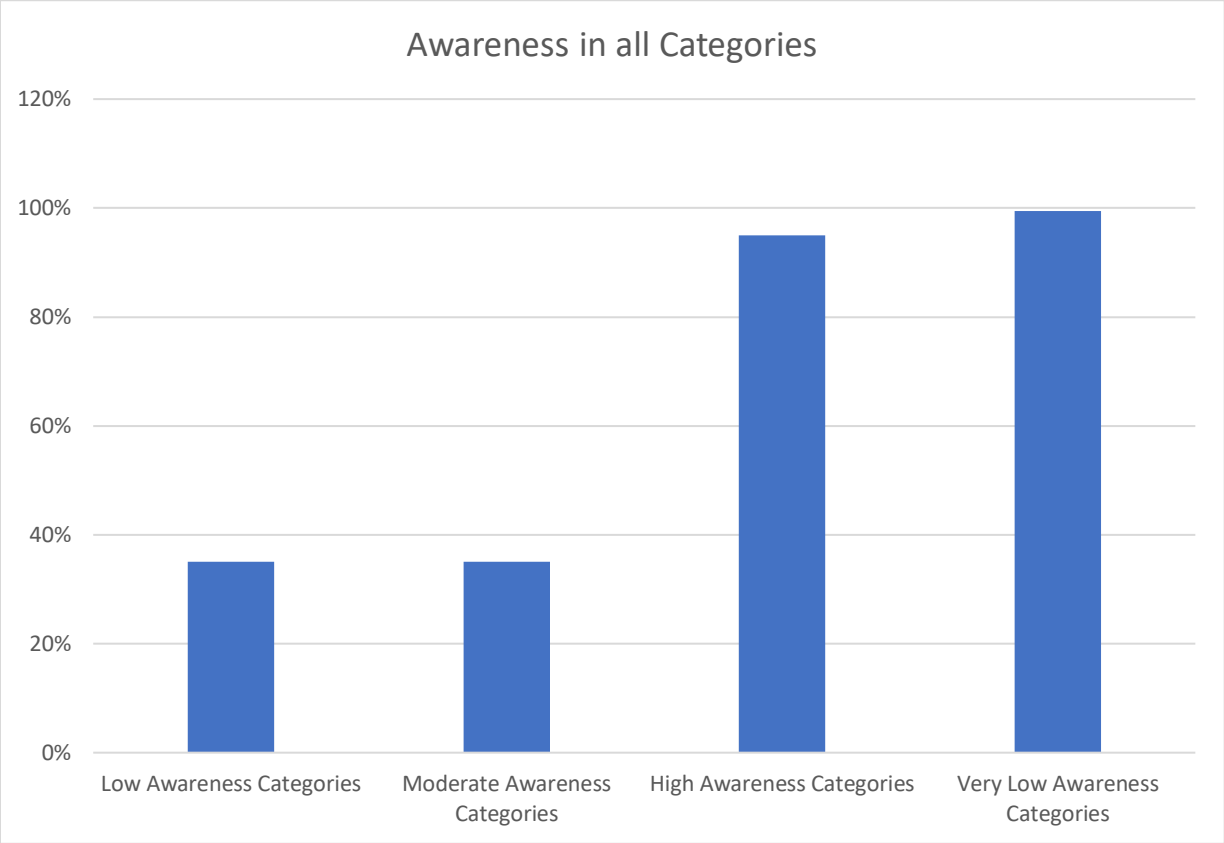
Graph-4: Students' Level of Cybersecurity Awareness in all Categories.

Graph-4 data suggests a predominant low awareness level among respondents, comprising 745.50%. A smaller but noteworthy portion, 27.30%, falls into the moderate awareness category. Surprisingly, no respondents exhibit high awareness, and a minimal 0.10% indicate very low awareness. This breakdown underscores the need for targeted educational initiatives to address specific knowledge gaps and enhance awareness levels across various categories.

Graph-5: IT Offices' Level of Cybersecurity Awareness in all Categories.

IJIST-Bangladesh, Volume-1, Issue-1, Page: 16-38, Nov-2023

DOI: 10.13140/RG.2.2.15091.30241



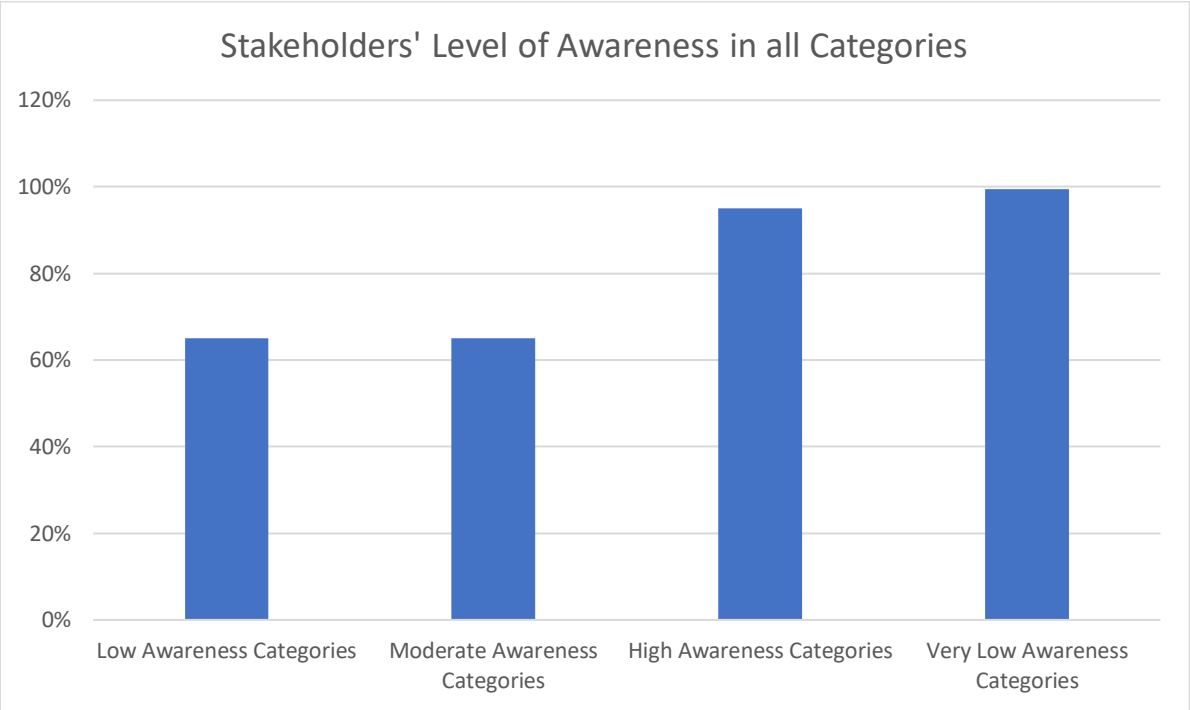
IT Offices' Level of Cybersecurity Awareness in all Categories.

Graph-5 indicates a diverse distribution of awareness levels across different categories. Notably, 35% of respondents fall within both low and moderate awareness categories, highlighting a substantial portion with varying degrees of awareness. Furthermore, a significant 95% exhibit high awareness, suggesting a commendable understanding in this category. Surprisingly, 99.50% of respondents demonstrate very low awareness, indicating a critical need for targeted educational interventions to address and improve knowledge in these specific areas. This breakdown emphasizes the importance of tailored strategies to enhance awareness levels and bridge gaps among the surveyed population.

DOI: 10.13140/RG.2.2.15091.30241

ISSN. 3006-3116
Lead Journal Publisher

Graph-6: Stakeholders' Level of Cybersecurity Awareness in all Categories



Graph-6 provided data illustrates a noteworthy distribution of awareness levels across distinct categories. A considerable 65% of respondents fall into both low and moderate awareness categories, indicating a significant portion with varying degrees of awareness. Additionally, a substantial 95% demonstrate high awareness, showcasing a commendable understanding within this category. Surprisingly, an overwhelming 99.50% of respondents exhibit very low awareness, highlighting a critical need for targeted educational interventions to address and improve knowledge in these specific areas. This breakdown underscores the importance of tailored strategies to enhance awareness levels and bridge knowledge gaps among the surveyed population.

7. Discussion

The rapid integration of digital systems, particularly University Management Systems (UMS), has transformed the functioning of educational institutions worldwide. In Bangladesh, this technological shift has been pivotal for modernizing operations and improving efficiency. However, the widespread adoption of UMS has attracted cyber threats, as evidenced by an increase in data breaches and ransomware attacks. Notable global incidents, such as the Equifax breach and the WannaCry ransomware attack, have underscored vulnerabilities in systems' confidentiality, integrity, and availability. In this context, the research aims to address the cybersecurity challenges faced by UMS in Bangladesh by developing a comprehensive Cybersecurity Framework.

The problem statement highlights the escalating cyber threats targeting UMS in Bangladesh and emphasizes the absence of a dedicated Cybersecurity Framework tailored to the local context. Global cybersecurity frameworks, while

DOI: 10.13140/RG.2.2.15091.30241

comprehensive, often fail to consider specific challenges such as resource constraints and regulatory dynamics. The vulnerabilities in UMS pose severe risks, including unauthorized access, data breaches, and service interruptions. The pressing issue is the need for a strategic and adaptive Cybersecurity Framework designed explicitly for UMS in Bangladesh, considering the evolving threat landscape and the socio-economic context of educational institutions.

The methodology section provides a sobering picture of Bangladesh's susceptibility to cyber threats, supported by statistics on infection levels and cyber-attacks targeting prominent organizations. The prevalence of diverse malware families further accentuates the need for comprehensive cybersecurity measures. Market trends in school and campus security underline the global recognition of cybersecurity's importance in educational settings. Survey data on cybersecurity awareness among students, the IT office, and stakeholders reveal distinct patterns, emphasizing the importance of targeted educational interventions.

In the context of UMS, the survey data highlights varied awareness levels and understanding of security measures among different groups. While some areas show commitment to good cybersecurity practices, others reveal a need for improvement, particularly in areas such as user access controls, security updates, and communication effectiveness.

8. Findings

The research conducted a comprehensive evaluation of a Cybersecurity Framework developed for University Management Systems (UMS) in Bangladesh, utilizing a mixed-methods approach. This approach involved both quantitative and qualitative methodologies to gain a holistic understanding of the framework's impact on cybersecurity within the academic context. Quantitative metrics, such as standardized risk assessments, system uptime improvements, and reduction in security incidents, were crucial in evaluating the effectiveness of the Cybersecurity Framework. These metrics were measured through surveys, interviews, and market analyses involving 525 diverse participants, including cybersecurity professionals, university representatives, UMS stakeholders, and students. Qualitative insights were gathered through in-depth interviews, case studies, and adaptability assessments, highlighting nuanced challenges faced by UMS in Bangladesh and offering context-rich narratives of the framework's application in various academic settings. The research employed a triangulation approach, integrating both quantitative and qualitative data for a more robust and comprehensive assessment of the Cybersecurity Framework's efficacy in the complex and evolving landscape of cybersecurity challenges within the academic sector.

The findings of the research highlight the acute vulnerability of Bangladesh to cyber threats, as evidenced by the alarming statistics on infection levels and notable cyber-attacks targeting prominent organizations. This underscores the urgent need for robust cybersecurity measures in the country. Furthermore, the global trends in school and campus security, as depicted in Graph-2 and Graph-3, emphasize the growing recognition of cybersecurity's significance in educational settings. The substantial growth in the industry reflects the increasing awareness of the importance of security measures within academic environments. The survey data among students, the IT office, and stakeholders provides valuable insights into cybersecurity knowledge, practices, and awareness levels. While some areas, such as

DOI: 10.13140/RG.2.2.15091.30241

strong password hygiene, exhibit strength, there are evident gaps in awareness of phishing attempts, confidence in responding to incidents, and familiarity with university cybersecurity policies.

Specifically, within the University Management System (UMS) context, the survey data reveals varied awareness levels regarding security measures among different groups. Areas of concern include low awareness of user access controls, communication effectiveness regarding security updates, and understanding of data privacy policies. These findings underscore the need for targeted educational interventions and tailored training programs to bridge the identified gaps. While certain groups exhibit a strong commitment to cybersecurity practices, others require focused efforts to enhance their awareness and understanding. The collective findings stress the immediate need for action in the form of a comprehensive and contextually tailored Cybersecurity Framework for UMS in Bangladesh. This framework should address the identified gaps, consider the evolving threat landscape, and promote a proactive cybersecurity culture within educational institutions, ultimately contributing to the enhanced cybersecurity resilience of UMS in the country.

9. Conclusion

In conclusion, this research underscores the critical importance of addressing cybersecurity challenges within the University Management Systems (UMS) of Bangladesh. The increasing prevalence of cyber threats globally and the specific vulnerabilities faced by the country demand immediate attention and strategic intervention. The absence of a dedicated and contextually tailored Cybersecurity Framework for UMS in Bangladesh leaves educational institutions exposed to risks that could compromise the confidentiality, integrity, and availability of critical academic and administrative information. The findings from the cybersecurity awareness surveys among students, the IT office, and stakeholders reveal both strengths and gaps in cybersecurity practices, emphasizing the need for targeted educational interventions.

The escalating cyber threats in Bangladesh, as indicated by the high infection levels and notable cyber-attacks on prominent organizations, highlight the urgency of implementing robust cybersecurity measures. The global trends in school and campus security further accentuate the growing recognition of cybersecurity's significance in educational settings. The research findings collectively call for immediate action, urging the development and implementation of a comprehensive and adaptive Cybersecurity Framework tailored to the unique challenges faced by UMS in Bangladesh. However, the following suggestions can be implemented to secure University Management Systems (UMS) within the campus area in different universities in Bangladesh:

9.1 Contextually Tailored Cybersecurity Framework

A paramount initiative is the development of a contextually tailored Cybersecurity Framework explicitly designed for UMS in Bangladesh. This framework should not only draw from global best practices but also account for local challenges, including resource constraints and regulatory dynamics unique to the country.

9.2 Focused Educational Interventions and Training Programs

Targeted educational interventions and comprehensive training programs are imperative to bridge gaps in cybersecurity knowledge among

DOI: 10.13140/RG.2.2.15091.30241

different stakeholder groups. Addressing specific weaknesses, such as awareness of phishing attempts and familiarity with university cybersecurity policies, is crucial for building a robust cybersecurity culture.

9.3 Collaboration with Industry Experts and Government Authorities

Collaboration with industry experts and government authorities is essential for gaining insights and support in implementing effective cybersecurity measures. Partnerships with relevant stakeholders will ensure that strategies align with industry standards and regulatory requirements.

9.4 Regular Assessments and Updates of Cybersecurity Measures

Regular assessments of cybersecurity measures are vital to ensuring their ongoing effectiveness. The Cybersecurity Framework should be dynamic, capable of adapting to emerging threats through continuous monitoring and timely updates.

9.5 Promotion of a Proactive Cybersecurity Culture

Fostering a proactive cybersecurity culture within educational institutions is paramount. This involves promoting awareness, responsible practices, and cultivating a shared sense of responsibility for cybersecurity among students, faculty, and staff.

9.6 International Collaboration and Knowledge Sharing

Establishing channels for international collaboration and knowledge sharing can facilitate the exchange of best practices. Learning from global experiences and adapting successful strategies to the local context can significantly strengthen cybersecurity measures within UMS in Bangladesh.

9.7 Continuous Monitoring and Incident Response Planning:

The implementation of continuous monitoring of UMS and the development of robust incident response plans are critical components of a comprehensive cybersecurity strategy. These measures ensure a swift and effective response in the event of a cybersecurity incident, minimizing potential damage and disruption.

9.8 Empowering IT Office and Stakeholders

Strengthening the capabilities of the IT office and stakeholders is crucial. This involves investing in professional development, providing regular training sessions, and ensuring that these key groups stay abreast of the latest cybersecurity trends and best practices.

9.10 Regular Simulated Cybersecurity Exercises

Conducting regular simulated cybersecurity exercises can enhance the preparedness of the educational institutions. These exercises can simulate various cyber-attack scenarios, allowing staff and students to practice response protocols and identify areas for improvement.

9.11 Establishing Incident Response Teams

Creating dedicated incident response teams within educational institutions can expedite the response to cybersecurity incidents. These teams should be equipped with the necessary skills and tools to investigate, contain, and mitigate the impact of cyber threats.

9.12 Encouraging Two-Factor Authentication (2FA) Adoption

Promoting the adoption of Two-Factor Authentication (2FA) across UMS can significantly enhance account security. Educational campaigns and incentives can be implemented to

DOI: 10.13140/RG.2.2.15091.30241

encourage students, faculty, and staff to embrace this additional layer of protection.

9.13 Regular Audits and Compliance Checks

Conducting regular cybersecurity audits and compliance checks ensures that the implemented measures align with industry standards and regulatory requirements. This proactive approach helps identify and address potential vulnerabilities before they can be exploited.

9.14 Investment in Advanced Threat Detection Solutions

Considering the evolving nature of cyber threats, investing in advanced threat detection solutions is essential. Utilizing artificial intelligence and machine learning technologies can enhance the ability to detect and respond to sophisticated cyber-attacks.

9.15 Establishing a Cybersecurity Information Sharing Platform

Creating a platform for sharing cybersecurity information among educational institutions can facilitate collaboration and the exchange of threat intelligence. This collective approach can strengthen the overall cybersecurity posture of the academic community.

9.16 Continuous Public Awareness Campaigns

Implementing ongoing public awareness campaigns about cybersecurity risks and best practices is crucial. These campaigns should target not only the internal academic community but also the broader public to promote a culture of cybersecurity awareness and responsibility.

9.17 Regular Review and Enhancement of Policies

Regularly reviewing and enhancing cybersecurity policies in alignment with emerging threats and technologies is vital. Policies should be dynamic and adaptable, reflecting the evolving nature of the cybersecurity landscape.

9.18 Role of University Grant Commission (UGC)

UGC can develop comprehensive and tailored guidelines for cybersecurity in collaboration with cybersecurity experts and institutions. These guidelines should provide a framework for universities to assess and enhance their cybersecurity posture, taking into account the unique challenges faced by educational institutions in Bangladesh.

Moreover, UGC can advocate for the integration of cybersecurity education into the academic curriculum across disciplines. This ensures that students, faculty, and staff are equipped with the necessary knowledge and skills to contribute actively to a cybersecurity-aware academic environment.

In addition, UGC can organize and support training programs, workshops, and awareness campaigns on cybersecurity for university administrators, faculty, and students. These initiatives can enhance the overall cybersecurity literacy within the academic community.

Reference

[1] Equifax Data Breach, 2017. Retrieved from https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

[2] WannaCry Ransomware Attack, 2017. Retrieved from https://www.wired.com/story/wannacry-ransomware-wannacrypt-uiwix-what-we-know/

DOI: 10.13140/RG.2.2.15091.30241

[3] Cyber Threats in Bangladesh Education Sector, 2019. Retrieved from https://www.thedailystar.net/business/news/cyber-threats-in-bangladesh-education-sector-1824375

[4] Liao, Y., Lin, H. H., & Luo, X. (2017). Examining the Cybersecurity Challenges and Practices in Educational Institutions. In International Conference on Cyber Security Cryptography and Machine Learning (pp. 3-13). Springer, Cham.

[5] Georgia Institute of Technology Data Breach, 2017. Retrieved from https://news.gatech.edu/features/2017-georgia-tech-cyberattack

[6] ISO/IEC 27001 Information Security Management, 2013. Retrieved from https://www.iso.org/standard/54534.html

[7] National Digital Security Act 2018, Bangladesh. Retrieved from http://www.mediafire.com/file/a5e4jj2f2scwa12/NDSP.pdf/file

[8] Hasan, M. K., Rahman, M. S., & Uddin, M. E. (2019). Towards Cyber Security and Privacy in University Campuses in Bangladesh. International Journal of Computer Applications, 179(46), 26-30.

[9] Alrawi, O. A. A., & Mohemmed, A. W. (2019). The Role of Security Information and Event Management (SIEM) Systems in Detection and Prevention of Cyber-attacks: A Review. Journal of Physics: Conference Series, 1722(1), 012070.

[10] Khattak, A. M., Khan, A., & Akhunzada, A. (2019). A comprehensive survey of cyber security frameworks. Future Generation Computer Systems, 97, 176-196.

[11] Kumar, R., & Khan, S. U. (2019). Cybersecurity Threats in Higher Education Institutions: A Comprehensive Review. In 2019 IEEE 19th International Conference on Advanced Learning Technologies (ICALT) (pp. 336-340).

[12] WannaCry Ransomware Attack, 2017. Retrieved from https://www.wired.com/story/wannacry-ransomware-wannacrypt-uiwix-what-we-know/

[13] Hsiao, H. F., Chu, Y. J., & Lee, C. P. (2019). Cloud-Based University Management System: Security Considerations and Solutions. Sustainability, 11(21), 6145.

[14] General Data Protection Regulation (GDPR), 2016. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

[15] Darabseh, A., Al-Rakhami, M. S., & Min-Allah, N. (2017). User Behavior Analysis for Intrusion Detection Systems: A Comprehensive Survey. Journal of King Saud University-Computer and Information Sciences.

[16] Research and Education Networking Information Sharing and Analysis Center (REN-ISAC). Retrieved from https://www.ren-isac.net/

[17] Harkins, C. (2016). Information Security: Protecting the Global Enterprise. Wiley.

[18] Peltier, T. R. (2013). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Auerbach Publications.

[19] Pfleeger, C. P., & Pfleeger, S. L. (2012). Security in Computing. Pearson Education.

[20] Vacca, J. R. (2013). Computer and Information Security Handbook. Morgan Kaufmann.

[21] Whitman, M. E., & Mattord, H. J. (2016). Principles of Information Security. Cengage Learning.

DOI: 10.13140/RG.2.2.15091.30241

[22] CIRT Team (2016). Common Vulnerabilities in Cyber Space of Bangladesh. https://www.cirt.gov.bd/common-vulnerabilities-in-cyber-space-of-bangladesh/#:~:text=69.55%25%20unique%20users%20are%20in,IP%20in%20Bangladesh%20was%2034552.

[23] Shrabani Paul, Dhaka Tribune (2023). Bangladesh is at serious risk of cyber crimes. https://www.dhakatribune.com/opinion/op-ed/294341/bangladesh-is-at-serious-risk-of-cyber-crimes

[24] Aarti Dhapte (2023). School and Campus Security Market Overview. https://www.marketresearchfuture.com/reports/school-campus-security-market-2957.