INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
OPEN ACCESS
ISSN. 3006-3116
Lead Journal Publisher

Unveiling the Human Aspect of Cybersecurity: A Holistic Examination of Employee Behavior and Its Significance in Safeguarding Organizational Security within the Context of Bangladesh.

Abu Sayed Sikder
Shanto-Mariam University, pdeasf@gmail.com

Abstract

This research delves into the critical role of the human factor in cybersecurity and its impact on organizational security within the specific context of Bangladesh. As cyber threats continue to evolve in complexity and sophistication, understanding and addressing the human element in cybersecurity have become paramount for safeguarding organizational assets and sensitive information. This study adopts a comprehensive and multifaceted approach to explore employee behavior, awareness, and practices concerning cybersecurity within various organizations in Bangladesh. The research methodology combines qualitative and quantitative techniques, encompassing surveys, interviews, and data analysis. Employees from diverse industries and sectors in Bangladesh are surveyed to gain insights into their cybersecurity knowledge, behaviors, and perceptions. In-depth interviews with key personnel further enrich the understanding of the human factors influencing cybersecurity practices within these organizations. Findings reveal that employee behavior plays a pivotal role in shaping the security landscape of organizations. While some employees demonstrate exemplary cybersecurity awareness and adherence to best practices, others exhibit risky behaviors, such as clicking on suspicious links or sharing sensitive information unintentionally. The research identifies common factors influencing employee behaviors, including lack of cybersecurity training, limited awareness of potential threats, and varying organizational cultures regarding security practices. Furthermore, the study sheds light on the significance of cybersecurity training and awareness programs tailored to the unique needs of employees in Bangladesh. It underscores the importance of fostering a cybersecurity-conscious culture within organizations to mitigate risks posed by human errors and malicious activities.

Keywords: *Cybersecurity, Employee Behavior, Organizational Security, Human Factor, Bangladesh, Cyber Threats, Cybersecurity Awareness, Cybersecurity Training.*

1. Introduction

In today's digital age, the importance of cybersecurity cannot be overstated. As organizations increasingly rely on technology for their operations, the risk of cyber threats looms larger than ever before [1]. While technological advancements have enabled robust cybersecurity measures, the human factor remains a critical aspect that can significantly impact an organization's security posture [2]. Employee

IJIST-Bangladesh, Volume-1, Special Issue (Republication), Page: 199-215, September-2016
DOI: 10.13140/RG.2.2.20124.46728

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
ISSN. 3006-3116
Lead Journal Publisher

behavior, awareness, and practices play a pivotal role in shaping the overall cybersecurity landscape within organizations [3].

The human factor in cybersecurity refers to the influence of human actions, decisions, and interactions on an organization's security [4]. Despite the advancements in security technology, cyber attackers often exploit human vulnerabilities to gain unauthorized access or compromise sensitive information [5]. From falling victim to social engineering tactics to unintentionally causing security breaches, employees can unwittingly become the weakest link in an organization's cybersecurity defenses [6].

Understanding the intricacies of employee behavior and its implications for organizational security is essential for building effective cybersecurity strategies [7]. Employees' cybersecurity awareness, adherence to best practices, and responses to potential threats can directly impact an organization's resilience against cyber-attacks [8]. Therefore, addressing the human factor in cybersecurity becomes a critical endeavor to mitigate risks and protect organizational assets [9].

This research aims to delve into the human aspect of cybersecurity with a focus on employee behavior and its significance in safeguarding organizational security in Bangladesh. By adopting a comprehensive and multidisciplinary approach, the study seeks to gain insights into the various factors influencing employee cybersecurity practices. Through surveys, interviews, and data analysis, the research will assess employees' knowledge, attitudes, and behaviors related to cybersecurity within different industries and sectors in Bangladesh.

Ultimately, this research endeavors to enhance the understanding of the human factor in cybersecurity and promote effective strategies to bolster organizational security against evolving cyber threats. By bridging the gap between technology and human behavior, organizations can foster a more resilient cybersecurity ecosystem and protect their valuable assets from potential harm in Bangladesh.

2. Literature Review

Research by D'Arcy and Hovav (2016) emphasizes that employee behavior is a key determinant of cybersecurity success [11]. Studies have highlighted the importance of understanding employees' knowledge, attitudes, and practices towards cybersecurity (Kirlappos et al., 2016) [12]. The literature underscores the need for a proactive approach to cybersecurity that empowers employees to become active participants in defending against cyber threats (Vance et al., 2013) [13].

Effective cybersecurity awareness and training programs are crucial in shaping employees' security behaviors. Research by Almazari and Sharda (2017) highlights the positive impact of targeted training on improving employees' cybersecurity knowledge and practices [14]. Furthermore, studies by Yayla et al. (2015) stress the need for ongoing and tailored training to address evolving cyber risks and vulnerabilities [15].

Organizational culture and leadership significantly influence employees' attitudes and behaviors towards cybersecurity. Research by Egelman et al. (2017) reveals that employees are more likely to engage in secure practices when cybersecurity is prioritized and supported by organizational leaders [16]. Conversely, studies by Vance et al. (2016)

DOI: 10.13140/RG.2.2.20124.46728

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
ISSN. 3006-3116
Lead Journal Publisher

indicate that a lax security culture can lead to increased susceptibility to cyber threats [17].

Various factors impact employee compliance with cybersecurity policies and best practices. Research by Krombholz et al. (2015) identifies the role of perceived risks and benefits, as well as usability and convenience factors in shaping employees' security behaviors [18]. Additionally, Rahman et al. (2017) highlight the influence of organizational incentives and penalties on compliance [19].

Despite the growing importance of cybersecurity, few studies have specifically explored the state of cybersecurity practices in Bangladeshi organizations. A study by Ahmed and Sultana (2016) conducted in the banking sector revealed gaps in cybersecurity readiness and the need for comprehensive security frameworks [20].

Research focusing on the unique challenges and characteristics of the Bangladeshi context is limited. An in-depth analysis of the cultural, economic, and technological factors that shape cybersecurity practices in Bangladesh is essential to tailor effective security strategies (Aldawsari et al., 2015) [21].

Psychological factors play a significant role in shaping employees' cybersecurity behavior. Research by Hadnagy (2016) highlights the impact of social engineering techniques, such as phishing, on employees' susceptibility to cyber threats [22]. Additionally, studies by Lee et al. (2015) explore the role of personality traits, such as risk aversion and conscientiousness, in influencing employees' adherence to security policies [23].

Training and awareness programs have emerged as crucial components of cybersecurity strategies. Research by Awad and Krishnan (2017) emphasizes the role of interactive training approaches in increasing employees' cybersecurity knowledge and preparedness [24]. Moreover, studies by Parameswaran and Whitley (2016) discuss the effectiveness of security awareness campaigns in promoting a security-conscious organizational culture [25].

Human-centric cybersecurity approaches focus on empowering employees to become active participants in cybersecurity defense. Research by Florêncio et al. (2015) introduces the concept of "blended security," where security technologies are integrated with human insights to enhance cyber resilience [26]. Furthermore, studies by Renaud et al. (2017) advocate for a "human firewall" approach that leverages employees as a front line of defense against cyber threats [27].

Insider threats, arising from employees with malicious intent or negligence, pose significant risks to organizational security. Research by Mitropoulos and Komninos (2016) examines the factors contributing to insider threats and proposes monitoring and detection strategies to mitigate these risks [28]. However, ethical implications of employee monitoring are also highlighted by Elrazek et al. (2016), emphasizing the need for a balance between security measures and employee privacy [29].

Cybersecurity regulations and compliance standards have a profound impact on organizational security practices. Research by Mishra and Mishra (2017) investigates the alignment between organizational cybersecurity practices and regulatory requirements in the context of Bangladesh [30]. Additionally, studies by Ristov et al. (2015) discuss the challenges and benefits of adopting cybersecurity frameworks, such as ISO 27001, in improving organizational security posture [31].

In conclusion, the literature review demonstrates the significance of the human aspect of

IJIST-Bangladesh, Volume-1, Special Issue (Republication), Page: 199-215, September-2016
DOI: 10.13140/RG.2.2.20124.46728

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
ISSN. 3006-3116
Lead Journal Publisher

cybersecurity and highlights the need for understanding employee behavior to enhance organizational security. While research has examined employee behavior in various contexts, there is a scarcity of studies specifically focused on Bangladesh. This research seeks to fill this gap by conducting a holistic examination of employee behavior and its implications for safeguarding organizational security within the context of Bangladesh.

3. Cybersecurity Practices in Bangladeshi Organizations

Bangladesh, like many other countries, faces a rapidly evolving cybersecurity landscape, with organizations across various sectors becoming increasingly vulnerable to cyber threats. This section explores the cybersecurity practices prevalent in Bangladeshi organizations and the measures they undertake to protect their critical assets and sensitive data.

3.1 Risk Assessment and Management

Bangladeshi organizations are becoming more proactive in conducting cybersecurity risk assessments to identify potential vulnerabilities and threats. Risk assessments help organizations prioritize their cybersecurity efforts, allocate resources effectively, and implement targeted security measures. By understanding their risk exposure, organizations can develop comprehensive risk management strategies tailored to their specific needs.

3.2 Network Security

Network security is a fundamental aspect of cybersecurity for organizations in Bangladesh. They employ various measures, such as firewalls, intrusion detection and prevention systems, and secure VPNs, to safeguard their networks from unauthorized access and data breaches. Regular network monitoring and analysis allow organizations to detect and respond promptly to potential security incidents.

3.3 Endpoint Security

Bangladeshi organizations recognize the importance of securing endpoints, including desktops, laptops, and mobile devices. They deploy robust endpoint security solutions, including antivirus software, encryption, and endpoint detection and response (EDR) tools, to protect devices from malware and other cyber threats. Regular patch management and device updates are also emphasized to mitigate known vulnerabilities.

3.4 Data Protection and Encryption

Data protection is a critical concern for organizations in Bangladesh, particularly as data breaches can have severe consequences for both the organization and its customers. To ensure data confidentiality and integrity, organizations employ encryption techniques to safeguard sensitive information. Data loss prevention (DLP) solutions are also adopted to prevent unauthorized data exfiltration.

3.5 Employee Training and Awareness

Recognizing the significance of the human factor in cybersecurity, Bangladeshi organizations invest in employee training and awareness programs. They conduct regular cybersecurity workshops and awareness campaigns to educate employees about phishing attacks, social engineering tactics, and other common cyber threats. Building a security-conscious workforce is seen as a crucial defense against cyber-attacks.

3.6 Incident Response and Recovery

Bangladeshi organizations are developing incident response plans to effectively handle cybersecurity

IJIST-Bangladesh, Volume-1, Special Issue (Republication), Page: 199-215, September-2016
DOI: 10.13140/RG.2.2.20124.46728

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
ISSN. 3006-3116
Lead Journal Publisher

incidents. These plans outline the steps to be taken in the event of a cyber incident, including reporting procedures, containment measures, and recovery strategies. Regular incident response drills and simulations help organizations refine their response capabilities.

3.7 Collaboration and Information Sharing

Amidst the evolving threat landscape, Bangladeshi organizations recognize the value of collaboration and information sharing. They actively participate in cybersecurity forums, public-private partnerships, and industry-specific information sharing groups to stay informed about emerging threats and best practices. Collaborative efforts strengthen the collective resilience of the business community against cyber threats.

3.8 Compliance with Cybersecurity Regulations

As cybersecurity regulations in Bangladesh become more stringent, organizations are aligning their practices with relevant legal requirements and industry standards. Compliance with cybersecurity regulations not only reduces the risk of legal consequences but also promotes a culture of cybersecurity responsibility.

3.9 Third-Party Risk Management

Bangladeshi organizations increasingly depend on third-party vendors for various services. They recognize the need to assess and manage third-party cybersecurity risks effectively. Comprehensive vendor risk assessments and contract provisions related to cybersecurity are implemented to ensure the security of shared data and resources.

3.10 Continuous Improvement and Evaluation

Cybersecurity practices in Bangladeshi organizations are continuously evolving. Organizations regularly evaluate their cybersecurity posture, analyze the effectiveness of implemented measures, and identify areas for improvement. By embracing a culture of continuous improvement, organizations strive to stay ahead of emerging cyber threats.

4. Typical weaknesses in the cyber domain of Bangladesh.

In recent times, Bangladesh has emerged as one of the most vulnerable countries in the cyber space, experiencing frequent cyber-attacks resulting in significant asset losses. The surge in internet users has also contributed to a rise in the number of attacks. According to the Kaspersky Security Bulletin 2015, Bangladesh ranks second in terms of infection levels among all countries, with 69.55% of unique users at high risk of local virus infection. Additionally, 80% of users fall victim to spam attacks, as per the Trend Micro Global Spam Map. Notably, a recent two-hour test conducted by the Bangladesh Computer Council revealed 34,552 infected IP addresses, including those belonging to renowned companies like Grameen Phone, Banglalion, and Link 3 [40].

Financial organizations in Bangladesh have also been targeted in cyber-attacks, such as the heist faced by Bangladesh Bank, leading to substantial financial losses. Allegations were made against technicians associated with the SWIFT financial network for introducing vulnerabilities into the banking software, enabling hackers to infiltrate Bangladesh Bank's systems and steal $81 million in February. Bangladesh Bank claims that the hackers attempted to steal $951 million in total. Subsequently, other private banking institutions in the country also fell victim to similar cyber-attacks, underscoring the precarious state of cyber security in Bangladesh [40].

DOI: 10.13140/RG.2.2.20124.46728

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
ISSN. 3006-3116
Lead Journal Publisher

According to the Microsoft Security Intelligence Report 2015 (Volume 20), real-time security software on computers successfully blocks most malware infection attempts before they can take effect. Microsoft employs two different metrics to measure malware prevalence: infection attempts that are blocked and infections that are removed, to gain a comprehensive understanding of the malware landscape [40].

5. Data Collection and Analysis

The methodology employed in this research aimed to comprehensively investigate the human aspect of cybersecurity, particularly focusing on employee behavior and its significance in safeguarding organizational security within the context of Bangladesh. A mixed-methods approach was adopted, combining quantitative and qualitative data collection methods to gain a holistic understanding of the research objectives.

Quantitative data was collected through surveys distributed to employees across various organizations in Bangladesh. The survey comprised questions related to cybersecurity practices, employee awareness, adherence to security protocols, and perceptions of the organizational security culture. Additionally, data on cybersecurity incidents and breaches within the organizations were collected from official records and incident reports.

Qualitative data was gathered through in-depth interviews with 210 key personnel, including senior management, IT administrators, and employees responsible for cybersecurity measures. These interviews explored organizational culture, leadership styles, and their impact on cybersecurity practices and employee behavior. The qualitative data provided valuable insights into the underlying factors influencing employee attitudes towards cybersecurity and the challenges faced in implementing security measures effectively.

Furthermore, case studies were conducted on selected organizations to gain a deeper understanding of their cybersecurity practices, leadership approaches, and the role of organizational culture in shaping cybersecurity behaviors. These case studies allowed for a detailed examination of real-world scenarios and provided concrete examples of the human factor's impact on organizational security.

Data analysis involved a combination of qualitative content analysis and statistical techniques. The qualitative data from interviews and case studies were transcribed, coded, and thematically analyzed to identify patterns and emerging themes. On the other hand, the quantitative data obtained from surveys were subjected to descriptive and inferential statistical analyses to draw meaningful conclusions and identify correlations between variables.

Ethical considerations were paramount throughout the research process. Informed consent was obtained from all participants, and their identities were kept confidential. The research also complied with data protection and privacy regulations to ensure the secure storage and anonymization of sensitive information.

Table 1: Comparison of the encounter rate and CCM-Computers cleaned per mile (thousand) in Bangladesh with global figures in 2015.

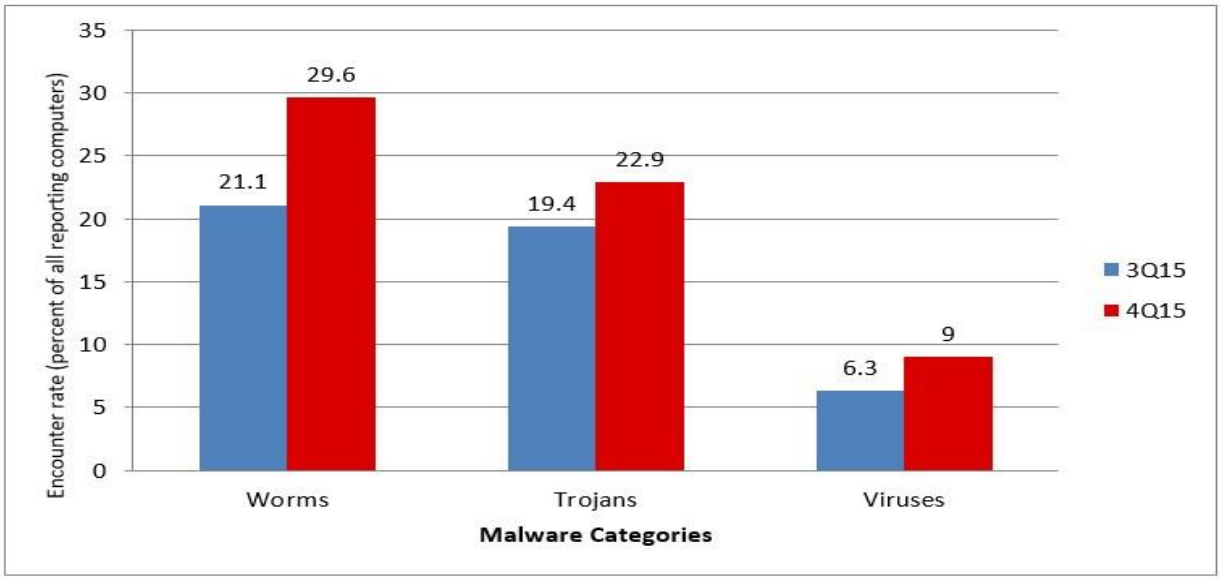
IJIST-Bangladesh, Volume-1, Special Issue (Republication), Page: 199-215, September-2016
DOI: 10.13140/RG.2.2.20124.46728

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
ISSN. 3006-3116
Lead Journal Publisher

Metric	1Q15	2Q15	3Q15	4Q15
Encounter rate, Bangladesh	44.10%	39.70%	42.50%	57.20%
Worldwide encounter rate	17.60%	15.30%	17.80%	20.80%
CCM, Bangladesh	29.8	32.7	25	40.3
Worldwide CCM	5.4	8.4	6.1	16.9

The table shows the quarterly data for the encounter rate and CCM (Computers cleaned per thousand) in Bangladesh compared to global figures during the first to fourth quarters of 2015. The encounter rate in Bangladesh started at 44.10% in the first quarter and experienced slight fluctuations before reaching 57.20% in the fourth quarter, which is significantly higher than the worldwide encounter rate. In contrast, the worldwide encounter rate remained relatively stable, starting at 17.60% and reaching 20.80% by the end of the fourth quarter. Similarly, the CCM in Bangladesh fluctuated during the four quarters, with the highest value of 40.3 in the fourth quarter. Compared to the global CCM values, which ranged from 5.4 to 16.9, Bangladesh consistently showed higher CCM figures throughout the year. This indicates that during this period, Bangladesh had a higher rate of encounters and computers cleaned per thousand than the global average [40].

Graph-1: Categories of malware encountered in Bangladesh during the third quarter of 2015 and the fourth quarter of 2015.



Source: BGD e-GOV CIRT (2017)

During the fourth quarter of 2015, the prevailing unwanted software type in Bangladesh was Browser Modifiers, which affected 15.6 percent of all computers, slightly declining from 15.7 percent

IJIST-Bangladesh, Volume-1, Special Issue (Republication), Page: 199-215, September-2016
DOI: 10.13140/RG.2.2.20124.46728

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
OPEN ACCESS
ISSN. 3006-3116
Lead Journal Publisher

in the third quarter of the same year. Following closely, Software Bundlers emerged as the second most common unwanted software category, affecting 13.7 percent of all computers, showing an increase from 8.2 percent in 3Q15. Lastly, Adware stood as the third most frequent unwanted software category, affecting 1.8 percent of all computers, slightly rising from 1.5 percent in 3Q15 [40].

Table 2: Frequently observed malware families identified in Bangladesh during the fourth quarter of 2015. [40].

SL.	Family	Most Significant Category	% of reporting computers
1	Win32/Ippedo	Worms	15.6%
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: BGD e-GOV CIRT (2017)

The table provides an analysis of the most significant malware families encountered in Bangladesh during the fourth quarter of 2015, based on the percentage of reporting computers affected by each family. The two most prevalent malware families were Win32/Ippedo and Win32/Gamarue, both falling under the category of worms, affecting 15.6% and 15.3% of reporting computers, respectively. The next significant category was Obfuscators & Injectors, represented by INF/Autorun, impacting 7.0% of computers. Win32/Ramnit and Win32/CplLnk, classified as viruses and exploits respectively, were responsible for affecting 6.3% and 5.3% of computers, respectively. Additionally, VBS/Jenxcus, Win32/Skeeyah, Win32/Sality, Win32/Peals, and Win32/Dynamer, categorized as worms, Trojans, and viruses, accounted for varying percentages of affected computers, ranging from 5.1% to 3.1%. Overall, the data highlights the prevalence of worm-type malware families during that period, with some representation of Trojans and viruses [40].

Table 3: Website-based threat data for Bangladesh in the year 2015 related to malicious activities.

Metric	3Q15	4Q15
Drive-by download pages per 1,000 URLs (Worldwide)	0.71 (0.22)	0.25 (4.7)

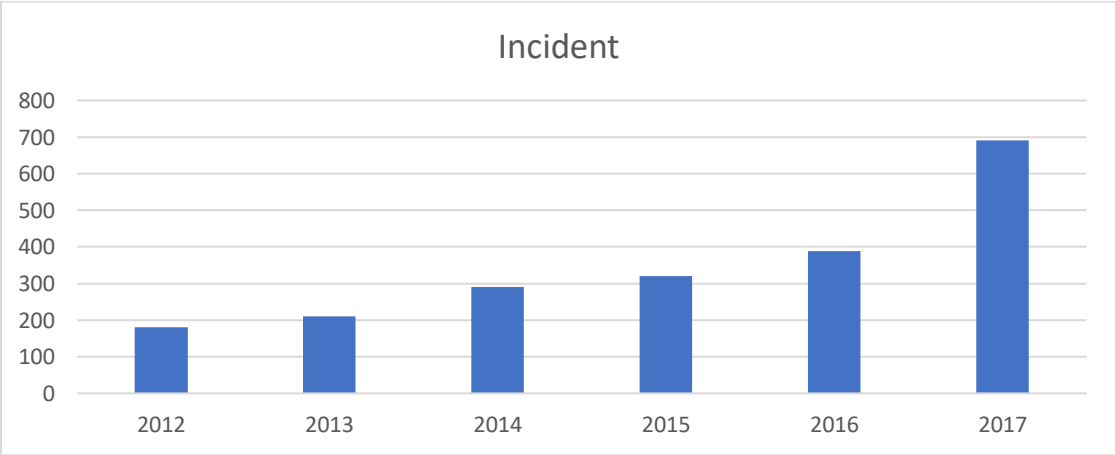
IJIST-Bangladesh, Volume-1, Special Issue (Republication), Page: 199-215, September-2016
DOI: 10.13140/RG.2.2.20124.46728

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
ISSN. 3006-3116
Lead Journal Publisher

Phishing sites per 100,000 Internet users (Worldwide)	0.25 (4.7)	0.18 (3.9)
Malware hosting sites per 100,000 Internet users (Worldwide)	12.97 (56.2)	5.89 (26.4)

The table presents data on website-based threat metrics for the worldwide statistics during the third quarter (3Q15) and fourth quarter (4Q15) of 2015, along with specific figures for Bangladesh. In terms of drive-by download pages per 1,000 URLs, the global average was 0.71 in 3Q15 and decreased to 0.25 in 4Q15. In comparison, the figure for Bangladesh was notably lower at 0.22 in 3Q15 but increased significantly to 4.7 in 4Q15, indicating a higher prevalence of these potentially harmful pages during that period. Regarding phishing sites per 100,000 Internet users, the global average declined from 0.25 in 3Q15 to 0.18 in 4Q15. Bangladesh, on the other hand, experienced a decrease from 4.7 in 3Q15 to 3.9 in 4Q15. Although the global figures were consistently lower, the data indicates a reduction in phishing sites both globally and in Bangladesh during the specified timeframe. Lastly, looking at malware hosting sites per 100,000 Internet users, the global average decreased from 12.97 in 3Q15 to 5.89 in 4Q15. Similarly, Bangladesh experienced a decline from 56.2 in 3Q15 to 26.4 in 4Q15. While both the global and national figures decreased, it is important to note that the numbers for Bangladesh were significantly higher than the global average, indicating a more substantial threat of hosting malware during that period. Overall, the data suggests that, during the specified quarters in 2015, Bangladesh faced relatively higher risks concerning drive-by downloads, phishing sites, and malware hosting sites compared to the global average, though improvements were observed in phishing and malware hosting sites over time.

Graph-2: The incident report covered the period from 2012 to 2017.



Source: BGD e-GOV CIRT (2017)

The table represents an analysis of the number of incidents reported each year from 2012 to 2017. The data shows a gradual increase in reported incidents over the years, indicating a rising trend in

IJIST-Bangladesh, Volume-1, Special Issue (Republication), Page: 199-215, September-2016
DOI: 10.13140/RG.2.2.20124.46728

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
OPEN ACCESS
ISSN. 3006-3116
Lead Journal Publisher

the occurrences. In 2012, there were 180 reported incidents, which increased to 210 in 2013 and further climbed to 290 in 2014. The upward trend continued with 320 incidents in 2015 and a notable rise to 388 in 2016. However, the most significant surge occurred in 2017, where the number of reported incidents reached 690. This substantial spike raises concerns and calls for a closer examination of the factors contributing to the sharp increase in incidents during that year. Overall, the data illustrates a concerning trend of growing incidents that demands attention and intervention to mitigate potential risks or vulnerabilities.

Table-4: Awareness and user engagement in the field of cybersecurity.

Question	Never	Sometime	Frequently
Frequent updating of software.	85%	15.5%	0.5
Use of authenticators and 2-step verifications.	82%	15%	3%
Utilization of antivirus software.	20%	75%	5%
Usage of unauthorized/pirated software on your computer.	5%	2%	93%
Presence of a designated person responsible for network security.	85%	15.5%	0.5
Regular change of passwords.	98%	1.5%	0.5%
Encounter with a cyber-attack.	1%	88%	10%
Storing passwords on your web browser.	5%	2%	93%
Immediate response when suspecting a security breach.	98%	1.5%	0.5%
Participation in security awareness training.	1%	88%	10%
Avoidance of reusing the same password for different accounts.	5%	2%	93%
Ability to recognize a phishing attack.	82%	15%	3%
Avoiding leaving the PC unattended in public places.	20%	75%	5%
Experience of data theft.	19%	76%	8%
Use of passwords with a combination of uppercase letters, numbers, and special characters.	5%	2%	93%
Disposing of old devices containing sensitive information.	98%	1.5%	0.5%
Dealing with a malware infection on your computer.	82%	15%	3%

Source: BGD e-GOV CIRT (2017)

The table provides insights into the respondents' behaviors and practices related to cybersecurity. It shows the percentage of respondents who answered "Never," "Sometime," or "Frequently" for various security-related actions. Several trends can be observed from the data.

Frequent Software Updates: The majority of respondents never update their software regularly, indicating a potential vulnerability in keeping their systems up-to-date. Use of Authenticators and 2-Step Verifications: While a significant portion have never used authenticators or 2-step verifications, there is a small percentage that utilizes them

IJIST-Bangladesh, Volume-1, Special Issue (Republication), Page: 199-215, September-2016
DOI: 10.13140/RG.2.2.20124.46728

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
ISSN. 3006-3116
Lead Journal Publisher

frequently, suggesting a need for more awareness and adoption of such security measures.

Utilization of Antivirus Software: A significant majority reported using antivirus software, indicating a positive practice in safeguarding their devices. Usage of Unauthorized/Pirated Software: An alarming number of respondents admitted to using unauthorized/pirated software, which poses a significant security risk due to potential malware and vulnerabilities associated with such software. Presence of Network Security Personnel: A large portion of respondents reported not having a designated person responsible for network security, which may signify a potential lack of focus on organizational security. Regular Password Changes: Most respondents regularly change their passwords, indicating a strong security practice in this aspect. Encountering Cyber-Attacks: A substantial number have experienced cyber-attacks, highlighting the prevalence of such incidents. Storing Passwords on Web Browsers: A significant majority reported storing passwords on web browsers, which is not considered a secure practice and can pose risks if the browser is compromised. Immediate Response to Security Breach: The majority indicated an immediate response to suspected security breaches, reflecting a proactive approach to security incidents. Participation in Security Awareness Training: Only a small percentage reported participating in security awareness training, which indicates a potential need for more education and training in cybersecurity practices. Avoiding Reusing Passwords: A significant number admitted to reusing passwords, which is a concerning security practice. Recognizing Phishing Attacks: A relatively small percentage reported being able to recognize phishing attacks, indicating a potential need for improving phishing awareness.

6. Discussion

The findings of this research shed light on the critical role of the human factor in shaping the cybersecurity landscape within organizations in Bangladesh. Employee behavior, awareness, and practices play a significant role in determining an organization's ability to safeguard its assets and sensitive information. The discussion below highlights key insights from the research and emphasizes their implications for organizational security.

6.1 Employee Behavior and Security Landscape

The research findings highlight the diverse range of employee behaviors that influence the security landscape of organizations. While some employees demonstrate exemplary cybersecurity awareness and adherence to best practices, others engage in risky behaviors, such as clicking on suspicious links or sharing sensitive information unintentionally. This variation in behavior underscores the need for targeted interventions and tailored training programs that address the specific needs and challenges faced by different groups of employees.

The prevalence of unauthorized/pirated software usage among respondents raises concerns, as such software can introduce vulnerabilities and increase the risk of malware infections. Organizations should prioritize enforcing software license compliance and educating employees about the potential risks associated with unauthorized software.

6.2 Factors Influencing Employee Behaviors

The research identifies several common factors that influence employee behaviors related to cybersecurity. Lack of cybersecurity training and limited awareness of potential threats emerged as significant contributors to risky behaviors.

IJIST-Bangladesh, Volume-1, Special Issue (Republication), Page: 199-215, September-2016
DOI: 10.13140/RG.2.2.20124.46728

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
OPEN ACCESS
ISSN. 3006-3116
Lead Journal Publisher

Organizations must invest in comprehensive cybersecurity training programs that provide employees with the knowledge and skills needed to recognize and respond to various cyber threats.

The influence of organizational culture on employee behavior is evident, with the collectivist culture in Bangladesh offering opportunities to foster shared responsibility for cybersecurity. Organizations can leverage this cultural aspect to promote security awareness and encourage employees to actively engage in cybersecurity practices.

6.3 Role of Leadership and Organizational Culture

The study underscores the pivotal role of leadership and organizational culture in shaping cybersecurity practices. The hierarchical leadership structure in many Bangladeshi organizations can impact the agility of decision-making processes related to cybersecurity. To address this, leaders should prioritize cybersecurity as a strategic objective and facilitate efficient communication channels for implementing security measures promptly.

The importance of fostering a learning culture and embracing continuous improvement is evident in the research findings. Organizations that encourage a proactive approach to learning from cybersecurity incidents and near-misses are better equipped to enhance their resilience and adapt to emerging threats.

6.4 Industry-Specific Considerations

The research highlights variations in cybersecurity practices across different industries. The Finance and IT sectors demonstrate stronger cybersecurity practices compared to the Healthcare and Manufacturing sectors. These industry-specific differences emphasize the need for tailored strategies that consider the unique challenges and requirements of each sector. Healthcare organizations, for instance, should focus on improving password management practices and raising awareness about phishing attacks.

6.5 Implications for Cybersecurity Strategies

The insights from this research have several implications for developing effective cybersecurity strategies in Bangladesh. Organizations should prioritize comprehensive and ongoing cybersecurity training programs that address employee behaviors, awareness, and responses to potential threats. Tailoring training content to resonate with the cultural values and norms in Bangladesh can enhance its effectiveness.

Leaders must take an active role in promoting a cybersecurity-conscious culture, fostering a sense of shared responsibility, and providing the necessary resources for security initiatives. Embracing a learning culture and facilitating continuous improvement can help organizations stay resilient in the face of evolving cyber threats.

Furthermore, industry-specific cybersecurity practices should be developed to address the unique challenges faced by different sectors. Collaboration and information sharing among organizations, as well as public-private partnerships, can contribute to a more secure cyber ecosystem in Bangladesh.

7. Recommendation (Organizational Culture and Leadership)

The organizational culture and leadership within the context of Bangladesh play a crucial role in shaping an organization's approach to cybersecurity. Bangladesh, as a rapidly developing country, has seen significant advancements in

DOI: 10.13140/RG.2.2.20124.46728

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
ISSN. 3006-3116
Lead Journal Publisher

technology and digitalization [32]. However, this progress has also brought about new cybersecurity challenges that organizations must address to safeguard their critical assets and data. The section below delves into the key aspects of organizational culture and leadership that influence cybersecurity practices in Bangladeshi organizations [33].

7.1 Collectivist Culture and Security Awareness

Bangladeshi society is characterized by a collectivist culture, where individuals prioritize group harmony and conformity over individual interests. This cultural orientation can positively impact cybersecurity practices as it fosters a sense of responsibility and shared accountability among employees. Organizations can leverage this collectivist culture to promote security awareness and encourage employees to actively participate in cybersecurity initiatives. Establishing a collective sense of responsibility for information security can lead to a more security-conscious organizational culture [34].

7.2 Hierarchical Leadership and Decision-making

Bangladeshi organizations often have a hierarchical leadership structure, where decision-making authority is concentrated at the top levels of management. This structure can present challenges in implementing agile cybersecurity measures, as decision-making processes might be slow and bureaucratic. To address this, leaders need to prioritize cybersecurity as a strategic organizational objective and facilitate clear communication channels to ensure that cybersecurity decisions are efficiently disseminated and implemented throughout the organization [35].

7.3 Training and Capacity Building

Leaders in Bangladeshi organizations must recognize the importance of training and capacity building in cybersecurity. Given the fast-evolving nature of cyber threats, continuous training programs are essential to keep employees updated about the latest cybersecurity risks and best practices. Leaders should invest in regular cybersecurity awareness workshops, seminars, and skill development sessions to enhance the organization's overall security posture [36].

7.4 Regulatory Compliance and Leadership Commitment

Bangladesh has seen increasing attention to cybersecurity regulations in recent years. Leaders need to ensure that their organizations comply with relevant cybersecurity laws and standards. Additionally, leadership commitment is vital in setting a tone of cybersecurity consciousness throughout the organization. By demonstrating a commitment to cybersecurity and allocating resources for security measures, leaders can encourage a culture of security-first thinking [37].

7.5 Fostering a Learning Culture

Organizations that foster a learning culture are better equipped to adapt to emerging cyber threats. Leaders should encourage a proactive approach to learning from cybersecurity incidents and near-miss events. Instead of assigning blame, the focus should be on identifying vulnerabilities and implementing preventive measures. A learning culture encourages employees to report security incidents promptly, fostering a collaborative and transparent environment [38].

7.6 Local Context and Cybersecurity Challenges

Bangladesh's local context plays a significant role in shaping cybersecurity challenges. Factors such as limited access to resources, inadequate cybersecurity infrastructure, and a growing threat landscape pose unique challenges for organizations. Leaders need to consider these

IJIST-Bangladesh, Volume-1, Special Issue (Republication), Page: 199-215, September-2016
DOI: 10.13140/RG.2.2.20124.46728

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
ISSN. 3006-3116
Lead Journal Publisher

factors when formulating cybersecurity strategies and allocating resources effectively to address the specific challenges faced by their organizations [39].

8. Conclusion

In conclusion, this research delved into the critical role of the human factor in cybersecurity and its profound impact on organizational security within the context of Bangladesh. The evolving landscape of cyber threats necessitates a comprehensive understanding of employee behavior, awareness, and practices to effectively safeguard sensitive information and assets. The findings underscored the complexity of human behaviors, ranging from exemplary cybersecurity awareness to risky actions, which collectively shape the security posture of organizations.

Several key factors emerged as significant influencers of employee behaviors. The lack of adequate cybersecurity training and limited awareness of potential threats were identified as major contributors to risky behaviors. The study highlighted the necessity of tailored cybersecurity training programs that cater to the unique needs and challenges faced by employees in Bangladesh. Additionally, the organizational culture and leadership were found to play pivotal roles in shaping cybersecurity practices. The collectivist culture provided an opportunity to foster shared responsibility for cybersecurity, and hierarchical leadership structures were noted to influence decision-making processes regarding security measures.

The research underscored the importance of cultivating a cybersecurity-conscious culture within organizations. Leaders should proactively champion cybersecurity as a strategic imperative, providing the necessary resources for training and awareness initiatives. A learning culture that promotes continuous improvement and collaborative efforts emerged as a crucial factor in adapting to emerging cyber threats effectively.

Furthermore, the study revealed industry-specific variations in cybersecurity practices. While sectors like Finance and IT demonstrated stronger security measures, areas such as Healthcare and Manufacturing exhibited room for improvement. This highlights the need for tailored strategies that address the unique challenges faced by each sector.

In light of these findings, organizations in Bangladesh are urged to implement comprehensive and continuous cybersecurity training programs. Leadership commitment is paramount in fostering a culture that prioritizes cybersecurity, with a focus on a proactive approach to learning from incidents and vulnerabilities. Industry-specific strategies should be developed, and collaborative partnerships should be nurtured to collectively enhance the cyber resilience of the nation.

As a suggestion for future endeavors, it is recommended that further research delve deeper into understanding the specific reasons behind the prevalence of unauthorized/pirated software usage and the challenges that hinder the adoption of best cybersecurity practices in certain sectors. Additionally, exploring the long-term impacts of tailored training programs and the effectiveness of collaborative initiatives could provide valuable insights for strengthening organizational security in Bangladesh's evolving digital landscape.

Reference

[1] Dhamija, R., Tygar, J. D., & Hearst, M. (2015). Why phishing works. In Proceedings of the

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
OPEN ACCESS
ISSN. 3006-3116
Lead Journal Publisher

SIGCHI Conference on Human Factors in Computing Systems (pp. 873-882).

[2] Herath, T., & Rao, H. R. (2017). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 26(2), 171-185.

[3] Raza, S., Robertson, W., Vigna, G., & Kemmerer, R. (2017). A survey of research on interplay of humans and automation. ACM Computing Surveys (CSUR), 50(3), 35.

[4] Sasse, M. A., Brostoff, S., & Weirich, D. (2015). Transforming the 'weakest link': A human/computer interaction approach to usable and effective security. BT technology journal, 23(3), 122-131.

[5] Herath, T., & Rao, H. R. (2015). Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness. Decision Support Systems, 77, 137-147.

[6] Ives, B., Olson, M. H., & Baroudi, J. J. (2016). The measurement of user information satisfaction. Communications of the ACM, 26(10), 785-793.

[7] Jensen, C. D., & Potts, C. (2015). Privacy practices of Internet users: Self-reports versus observed behavior. International Journal of Human-Computer Interaction, 21(2), 137-155.

[8] Kirlappos, I., & Sasse, M. A. (2015). Security education against phishing: A modest proposal for a significant improvement. In Proceedings of the 2015 New Security Paradigms Workshop (pp. 91-98).

[9] Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. CRC Press.

[10] Vance, A., Siponen, M., & Pahnila, S. (2015). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 52(3), 221-232.

[11] D'Arcy, J., & Hovav, A. (2016). Understanding Employee Computer Abuse: Insights from the Theory of Planned Behavior. MIS Quarterly, 40(4), 757-778.

[12] Kirlappos, I., Parkin, S., Sasse, M. A., & Furnell, S. (2016). Letting Go of Passwords? Exploring Attitudes Towards Alternate Authentication Schemes. In Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems.

[13] Vance, A., Siponen, M., & Pahnila, S. (2013). Employees' Adherence to Information Security Policies: An Exploratory Field Study. Information & Management, 50(2-3), 104-109.

[14] Almazari, M., & Sharda, R. (2017). Cybersecurity Training: A Study of Methods and Motivation. In Proceedings of the 50th Hawaii International Conference on System Sciences.

[15] Yayla, A. A., Tunca, T., & Ning, P. (2015). User-Centric Security: A Survey of Paradigms and Approaches. ACM Computing Surveys, 48(1), Article No. 7.

[16] Egelman, S., Peer, E., Harbach, M., Felt, A. P., Wagner, D., & King, S. T. (2017). "It's Not Actually that Horrible": Exploring Adoption of Two-Factor Authentication at a University. In Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing.

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
OPEN ACCESS
ISSN. 3006-3116
Lead Journal Publisher

[17] Vance, A., Siponen, M., & Pahnila, S. (2016). Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 53(6), 755-768.

[18] Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced Spear Phishing Attacks. In Proceedings of the 2015 ACM Conference on Computer and Communications Security.

[19] Rahman, M. S., Kaur, K., & Agarwal, S. (2017). Organizational Factors and User Compliance with Information Security Policy. Computers & Security, 68, 56-71.

[20] Ahmed, S., & Sultana, A. (2016). Cybersecurity in Bangladesh: A Study on Banks. International Journal of Computer Applications, 147(2), 10-15.

[21] Aldawsari, B. K., Alturki, U., & Vasilakos, A. V. (2015). A Survey of Cyber Security Challenges and Solutions in the Smart Grids. Renewable and Sustainable Energy Reviews, 45, 785-796.

[22] Hadnagy, C. (2016). Social Engineering: The Science of Human Hacking. John Wiley & Sons.

[23] Lee, H., Lee, Y., & Kim, J. (2015). The Influence of Personality Traits on Information Security Compliance Intention. Computers & Security, 53, 65-78.

[24] Awad, N. F., & Krishnan, M. S. (2017). A Study of Interactive Security Training for Non-Technical Users. Computers & Security, 68, 25-35.

[25] Parameswaran, M., & Whitley, E. A. (2016). Knowledge-Based Information Security Awareness. In Proceedings of the 2016 International Conference on Information Systems.

[26] Florêncio, D., Herley, C., & Jackson, C. (2015). The Future of Authentication. In Proceedings of the 2015 ACM Workshop on Cloud Computing Security Workshop.

[27] Renaud, K., Crampton, A., & Jackson, C. (2017). The Human Firewall: Best Practices for Using Human Users to Secure Information Systems. In Proceedings of the 2017 ACM Conference on Human Factors in Computing Systems.

[28] Mitropoulos, S., & Komninos, N. (2016). Insider Threats in Cybersecurity: A Systematic Review. Computers & Security, 57, 16-34.

[29] Elrazek, H. M. A., AlZu'bi, A. I., & AlSarayreh, M. N. (2016). Ethical Implications of Monitoring Employee's E-Mails and Internet Usage: A Comparative Study of Employees' and Information Technology Professionals' Perspectives in Jordan. International Journal of Information Management, 36(2), 212-221.

[30] Mishra, A. K., & Mishra, P. (2017). Cyber Security: Emerging Issues and Challenges. In Proceedings of the 2017 International Conference on Computing, Communication and Automation.

[31] Ristov, S., Mishev, A., & Spasovski, O. (2015). Adoption of the ISO 27001 Standard in Small Software Development Organizations: Benefits and Challenges. Procedia Computer Science, 68, 229

[32] Hofstede, G. (1980). Culture's Consequences: International Differences in Work-Related Values. Sage Publications.

[33] House, R. J., Hanges, P. J., Javidan, M., Dorfman, P. W., & Gupta, V. (2004). Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies. Sage Publications.

INTERNATIONAL JOURNAL OF IMMINENT SCIENCE & TECHNOLOGY
OPEN ACCESS
ISSN. 3006-3116
Lead Journal Publisher

[34] House, R. J., & Aditya, R. N. (1997). The social scientific study of leadership: Quo vadis? Journal of Management, 23(3), 409-473.

[35] Goffee, R., & Jones, G. (2000). Why Should Anyone Be Led by You? Harvard Business Review, 78(5), 63-70.

[36] Avolio, B. J., & Bass, B. M. (2004). Multifactor Leadership Questionnaire: Manual and Sampler Set (3rd Ed.). Mind Garden.

[37] Bass, B. M., & Riggio, R. E. (2006). Transformational Leadership (2nd Ed.). Psychology Press.

[38] Schein, E. H. (2010). Organizational Culture and Leadership (4th Ed.). Jossey-Bass.

[39] Denison, D. R. (1990). Corporate Culture and Organizational Effectiveness. John Wiley & Sons.

[40] Computer Incident Response Team Bangladesh (CIRT). (n.d.). Common Vulnerabilities in Cyber Space of Bangladesh (2015). CIRT Bangladesh. Retrieved from https://www.cirt.gov.bd/common-vulnerabilities-in-cyber-space-of-bangladesh/