Publisher homepage: www.universepg.com, ISSN: 2663-7804 (Online) & 2663-7790 (Print)

https://doi.org/10.34104/ajeit.023.015025

Australian Journal of Engineering and Innovative Technology

Journal homepage: www.universepg.com/journal/ajeit

Cyber Security Awareness (CSA) and Cyber Crime in Bangladesh: A Statistical Modeling Approach

Mohammad Ahsan Uddin[1]*, Ashrafun Zannat Supti[2], A.S.M. Rafad Asgar[3], Md. Saikat Mridha[4], and Naiem[5]

[1-5]Department of Statistics, University of Dhaka, Dhaka, Bangladesh.

*Correspondence: munna_stat@yahoo.com (Dr. Mohammad Ahsan Uddin, Professor, Department of Statistics, University of Dhaka, Dhaka, Bangladesh).

ABSTRACT

The need to combat cybercrime is becoming more and more urgent. This effect is crucial for developing nations like Bangladesh, which is currently building out its infrastructure in preparation for fully secure digitization. This study aims to identify the numerous factors that contribute to cybercrime, its challenges, the relationships between different cyber security variables, potential solutions to these issues and various behavioral viewpoints individuals and organizations hold regarding cybercrime victimization. A simple random sampling method has been conducted to collect 200 data from individuals on this topic. Factor analysis based on Principal Component Analysis (PCA) was fitted to the data to analyze cyber behaviour, Binary Logistic Regression was fitted to analyze cyber victimization status and Poisson Regression model was fitted to analyze victimization frequency. The research demonstrates that the dependent variable cybercrime victimization is strongly associated with the independent variables which are password sharing status, using a common password, cyber security knowledge Status, personal information online storage status, downloading free antivirus from an unknown source, disabling antivirus for downloading, download digital media from an unknown source, clicking links unauthorized sites, personal info Sharing with stranger over online. According to the regression model's findings, women are more likely than men to experience cybercrime. Cybersecurity knowledge is found to be a key factor in preventing cyberattacks. Additional research on this subject can be conducted utilizing large-scale data to gain more trustworthy conclusions on the underlying factors contributing to cybercrime victimization. Overall, developing a digital Bangladesh where our cyber security is robust can be accomplished by learning about cybersecurity and practicing safe online behavior.

Keywords: Cyber security, Cybercrime, Binary logistic regression model, and Poisson regression model.

INTRODUCTION:

In the era of globalization secure cyberspace plays a significant role in achieving economic prosperity and building a modern, and powerful nation. With the rapid spread of cyberspace and communication technology, cybercrimes have become a considerable security concern. With the progressive increase in the number of internet users in Bangladesh, the percentage of attacks is rising too. According to the Kaspersky Security Bulletin 2015, Bangladesh is in the second position in the level of infection among all the countries. 69.55% of unique users are at the highest risk of local virus infection in Bangladesh. 80% of users are the victim of spam attacks according to Trend Micro Global Spam

Map (N-CERT, 2015). However, when it comes to infrastructure and capacities for cyber-security countermeasures, our nation falls short. For instance, there is a lack of cyber security awareness, a shortage of professionals who have received the necessary training, problems with law enforcement personnel, a subpar judiciary, and so forth.

Cyber security is a set of technologies, techniques, processes, and practices aimed to protect internet connected systems which includes network, hardware, software and data from plausible attacks such as breach, theft, misuse, manifestation, harm, etc (Jeetendra, 2017). The main goal of cyber security is to assure confidentiality, integrity and availability of the system. Cybercrime is the type of crime which involves a network and a computer or any other smart device. The computer can be involved either as a tool or as the target. Cybercrimes can cause serious financial and reputational damage to an organization or an individual. The objective of the study is to identify the numerous factors that contribute to cybercrime, its challenges, the relationships between different cyber security variables, and potential solutions to these issues.

Literature Review

The issue of cyberattacks, which has emerged as one of the most crucial aspects of the Internet of Things (IoT), was discussed in a publication by Ulven & Wangen, (2021). By safeguarding IoT assets and user privacy, IoT cybersecurity aims to lower cybersecurity risk for businesses and consumers. The authors of the paper provided theoretical vulnerabilities faced by the IoT, major security issues, and necessary steps for the protection of cyber security and the IoT (Abomhara & Køien, 2015). Ramirez & Choucri, (2016) researched the 21st-century trends of cyberization and the rising demand for computer security. A recent increase in new technology investment has coincided with an increase in cybercrime, digital currency, and e-governance. Businesses and governments are starting to focus their attention on all-encompassing cybersecurity solutions. Using an integrated approach, Ali *et al.* (2022) investigated the causes of IT system failure in Bangladesh's banking sector. Cyberattacks, database hacks, server failure, network outages, broadcast data mistakes, virus impacts, etc. were the reported factors. Then, to facilitate managers' critical decision-making, these factors were examined. On a few Indian public and private sector banks, Atul *et al.* (2013) exposed the numerous cyberattack techniques used by cybercriminals as well as the various cyber defense strategies and how they relate to cyberattacks. According to the report, 60% of bank executives acknowledged that their bank has discovered internet theft. Scholars examined the cyber threat posed by smart cities, assessed, exposed, and evaluated the advancement of data-driven solutions for situational awareness. The author assessed attack detection approaches, risk assessment methodologies, and ways for modeling relationships across different smart city infrastructures (Neshenko *et al*., 2020). Chen *et al.* (2015) did an exploratory study using the flux-fluctuation law, the Markov state TPM, and predictability measurements to look for patterns and predictability in cyberattacks. Unsurprisingly, they discovered the fundamental pattern of cyberattacks and discovered that just a small number of attacker groups were responsible for practically all the attacks. A comparative analysis of twenty nations' national cyber security strategy was conducted by Shafqat & Masood, (2016). The timeframe of development clearly stated objectives and goals, degree of prioritization, nations' perceptions of cyber threats, organizational overview, incident response capabilities, etc. were used as comparative criteria. It was discovered that while the purposes and objectives of all the strategies were quite similar, their scopes and methods were very dissimilar. Additionally, the UK, USA, and Germany had the best strategy overall. Maalem Lahcen *et al.* (2020) reviewed pertinent theories and ideas and offered insights, as well as a framework that integrates modeling and simulation, behavioral cybersecurity, and human factors. To emphasize the significance of social behavior, environment, biases, perceptions, deterrent, intent, attitude, norms, alternatives, punishments, decision-making, etc. in comprehending cybercrimes, Matyokurehwa *et al.* (2020) studied the Cyber Security Awareness (CSA) perspectives among students at Zimbabwean universities to build a model of the effectiveness of cyber security training programs. They worked on some statistical analysis on their primary data to find any significant relationship between cyberattacks and CSA. They found that malware attacks, social engineering attacks and IoT attacks are positively related to CSA. In addition, they developed a

cross-case analysis which showed that CSA is invariant on age and sex while CSA has a noticeable impact on the level of education and institution. Alqahtani (2022) launched a study about the factors behind cybersecurity awareness among students taking higher study. Based on the CSA data taken from Imam Abdulrahman Bin Faisal University college students, he analyzed and created a module to make the students aware about cybersecurity. Many relevant statistical analyses including ANOVA, multiple regression, correlation test, multicollinearity test was carried out considering password security, browser security, and social media security as three main variables. All the three-security component was found significantly influential on cybersecurity awareness. Kovacevic *et al.* (2020) explored how cyber security behavior is impacted by cyber security awareness. The study defined socio-demographics, cyber security perceptions, previous cyber security breaches, IT usage, and knowledge as CSA factors. Through correlation and regression analysis, knowledge and IT usage was found to be a significant factor in cyber security behavior. Ben-Asher & Gonzalez, (2015) inquired about how knowledge plays a role in the accurate classification of malicious events and prevents damages from cyber-attack. They evaluated the impact of cyber security knowledge on the detection of cyber-attack. A reliable tool for detection is an Intrusion Detection System (IDS) which detects by matching known attack patterns of network events. But 99% of the alerts from IDS are false alerts so a human analyst is required for triage analysis (Monitoring & Detection). And more knowledge about cyber security significantly helps in the correct detection of malicious events and decreases false classification. Haque, (2019) studied public opinion on cyber security condition of Bangladesh. He found that 78.4% internet users thought the condition be vulnerable. He also referred to some cyber threats and recent cyber-attacks specially in financial sectors in our country. Describing the deficiency of awareness in this sector, this paper further discussed some necessary policy regarding cyber security. Mazumder & Hossain, (2022) looked for a connection between board composition and disclosure of cyber security in Bangladesh's banking industry. Multiple linear regression analysis and automated content analysis were employed in the study. Throughout the research period, the cyber security division trend in Bangla-desh's banking sector was up (2014-2020). According to the data, larger boards do not substantially affect CSD whereas increased female involvement is linked to higher CSD. Kundu *et al.* (2018) analyzed cyber-attack in the monetary sector of Bangladesh and investigated the causes of that in Bangladesh. As they found increasing trend of cyber-attack, they suggested available framework against cybercrime in this paper. Hadlington, (2017) made a survey on attitude towards cybercrime as well as cyber security in business scale, Internet addiction and risky cyber security behaviors. By regression analysis the research shown that employee attitudes towards cyber security correlated negatively with which they engaged in risky cyber security behavior self-reporting is the Limitations for the study.

Research highlights employee attitudes & knowledge can play vital role in cyber security. Astromskis (2017) developed a conceptual cyber security regulation framework, based on the fundamentals of transaction cost theory. The study evaluated it in the context of emerging legal technologies. Bowen *et al.* (2011) conducted an experiment on randomly selected 4000 students and staffs using forged phishing emails to investigate a new method to measure, quantify and evaluate the security state of large corporation organizations and government agencies. According to them, computer security depends on the people who operate the system aside technology and systems. Nifakos *et al.* (2021) aimed a review study to find out the factors causing cyber-attacks in healthcare sector. They analyzed and reported human behavioral causes of cyber threats in health organizations. They also researched the possible policies and measures which could be taken by the healthcare-providing organizations. In order to understand the mechanics of cyber-attack campaigns, Lallie *et al.* (2021) examined the cyber-attacks that occurred during the COVID-19 epidemic.

Additionally, it showed how cybercriminals use actual crises and tragedies as cover for opportunistic assaults. Finally, the effects of these attacks on persons who work from home were explored, along with some future planning ideas. Sardi *et al.* (2020) studied by giving a special emphasis on one of the main challenges in the healthcare sector during the COVID-19

pandemic, the cyber risk. Since the beginning of the Covid-19 pandemic, the World Health Organization has detected a dramatic increase in the number of cyber-attacks. Information security and cyber security are two different concepts, according to Von Solms & Van Niekerk, (2013). They contended that these two aren't quite interchangeable or similar. The safeguarding of information assets is known as information security. However, cyber security is the defense of the internet's physical infrastructure, its users, and the assets that can be accessed through it. Consequently, cyber security has a further component. Staheli *et al.* (2014) surveyed and categorized the visualization evaluation metrics, components and techniques for cyber security that were utilized in the previous decade of VizSec (A research community that focuses on visualization of cyber security) research literature. They also defined existing methodological gaps in evaluating visualization in cyber security as well as suggested potential avenues for future research. Švábenský *et al.* (2020) studied the fact that cybersecurity is now more important than ever, and so is education in this field.

However, the cybersecurity domain encompasses an extensive set of concepts, which can be taught in different ways and contexts to understand the state of the art of cybersecurity education and related research. Klimburg *et al.* (2011) had outlined a cyberstrategy that provided the stance of the United States of America (USA) on cyber-related issues and outlined a unified approach to the USA's engagement with other countries on cyber issues. They analyzed about technologies that might be used to protect the cyber environment and organization and user's assets. Becker & Quille, (2019) studied about cyber-Security issues that needed to be integrated in the educational process in the beginning at an early age (Mia *et al*., 2022).

This study focuses on cyber security emerging trends while adopting new technologies such as mobile computing, cloud computing, e-commerce, and social networking. The paper also described the challenges due to lack of coordination between Security agencies and the Critical IT Infrastructure. Lebek *et al.* (2014) provided an overview of theories used in the field of employees' information systems (IS) security behavior by analyzing and synthesizing previous literature.

MATERIALS AND METHODS:

Data Collection and Processing

Questionnaires were used as the data collection tool for this cross-sectional study. Both personal interviews and mail questionnaires through google forms were used for this purpose. Internet users who are greater than 16 years old were the target population of this study. Simple random sampling was adopted in collecting data from individuals. For large samples, the formula for estimating sample size through Simple Random Sampling is-

$$n = \frac{Z^2_{1-\frac{\alpha}{2}}\, pq}{d^2}$$

$$\therefore \text{n} = \frac{1.96^2 * 0.5 * 0.5}{0.07^2} = 196$$

Here, in this study,

P, Assumed proportion in target population =0.50; q=1-p =0.50; d, Degree of accuracy expected in the estimated population =.07; Z, Standard normal deviate = 1.96. Accordingly, 200 data from Dhaka city was gathered for the study. Data were analyzed using SPSS software in computer.

Principal Component Analysis

By turning a set of values for correlated variables into a set of values for linearly uncorrelated variables, PCA is used to reduce the number of dimensions. Old dimensions are changed into new dimensions. These new dimensions indicate that since the majority of the information is included in the first few dimensions, it is acceptable to eliminate other dimensions containing less information/variance and instead choose the most significant ones, which results in dimensionality reduction. In this project, orthogonal transformation is used in variance reduction.

Binary Logistic Regression Model

Let us define the binary random variable

$$Z = \begin{cases} 1 \text{ if the outcome is a success} \\ 0 \text{ if the outcome is a failure} \end{cases}$$

with probabilities Pr (Z = 1) = π and Pr (Z = 0) = 1− π, which is the Bernoulli distribution B(π). If there are n such random variables Z_1,..., Z_n, which are independent with Pr(Z_j = 1)

$= \pi j$, *then their joint probability is*

$$\prod_{j=1}^{n} \pi_j{}^{z_j}(1-\pi_j)^{1-z_j} = \exp[\sum_{j=1}^{n} z_j \log\left(\frac{\pi_j}{1-\pi_j}\right) + \sum_{j=1}^{n} log(1-\pi_j)],$$

Which is a member of the exponential family.

Next, for the case where the π_j's are all equal, we can define

$Y = \sum_{j=1}^{n} z_j$

So that Y is the number of successes in n "trials." The random variable Y has the distribution Bin (n, π): Pr (Y = y) $=\binom{n}{y}\pi^y(1-\pi)^{n-y}$, y = 0,1,...,n.

For i^{th} random variable Y_i, $\mu_i = E(Y_i) = n_i\pi_i$ is the expected number of successes. We can allow μ_i to depend on x_i (vector of explanatory variables) via the link function

$g(\mu_i) = \boldsymbol{x}_i^T\boldsymbol{\beta}$,

Where **β** is a vector of parameters.

Finally, we consider the general case of N independent random variable Y_1, Y_2,...,Y_N corresponding to the numbers of successes in N different subgroups or strata. If $Y_i \sim$ Bin (n_i ,π_i), the log-likelihood function is

$$l(\pi_1,...,\pi_N;y_1,...,y_N) = \sum_{i=1}^{N}\left[y_i \log\left(\frac{\pi_i}{1-\pi_i}\right) + n_i log(1-\pi_i) + log\binom{n_i}{y_i}\right]$$

Where, $\pi_i = \frac{e^{x_i^T\beta}}{1+e^{x_i^T\beta}}$.

The parameter vector **β** can be estimated numerically using numerical methods.

Finally, the model can be written as

$\log\left(\frac{\pi_i}{1-\pi_i}\right) = \boldsymbol{x}_i^T\boldsymbol{\beta}$.

Odds ratio, $OR_j = e^{\beta_j}$.

Poisson Regression Model

Let us consider $Y_1,...,Y_N$ be independent random variables with Y_i denoting the number of events observed from exposure n_i for the i^{th} covariate pattern. The expected value of Y_i can be written as $E(Y_i) = \mu_i = n_i\theta_i$.

The dependence of θ_i on the explanatory variables is usually modelled by $\theta_i = e^{x_i^T\beta}$.

Therefore, the generalized linear model is $E(Y_i) = \mu_i = n_i e^{x_i^T\beta}$;

$Y_i \sim Po(\mu_i)$.

The natural link function for the Poisson distribution, the logarithmic function, yields a linear component

$\log E(Y_i) = \text{constant} + x_i^T\beta$.

For a binary explanatory variable denoted by an indictor variable, $x_j = 0$ if the factor is absent and $x_j = 1$ if it is present. The rate ratio, RR, for presence vs. absence is

$$RR = \frac{E(Y_i \mid \text{present})}{E(Y_i \mid \text{absent})} = e^{\beta_i}.$$

When the response variable is over dispersed, more sophisticated model such as Negative Binomial Regression Model can be used.

RESULTS AND DISCUSSIONS:

Factor analysis using principal component analysis on cyber behavior

The goal of the traditional principal component analysis is to reduce the number of m variables to a smaller number of p uncorrelated variables known as principal components which account for the variance of the data as much as possible. PCA is suitable for continuous variables, and it assumes a linear relationship between variables, it is not an appropriate method for dimension reduction in categorical variables. Alternatively, categorical principal component analysis (CATPCA) has been developed for data having mixed measurements such as nominal, ordinal, or numeric which may not have linear relationships with each other. We refer to Gifi, (1990) for a historical review of CATPCA using optimal scaling. We compute the Bartlett's test for sphericity and find the Kaiser-Meyer-Olkin measure of sampling adequacy before proceeding to factor analysis.

Table 1: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		**.751**
Bartlett's Test of Sphericity	Approx. Chi-Square	381.804
	df	91
	Sig.	.000

Here, the Kaiser-Meyer-Olkin measure is .751 which indicates the dataset is valid for factor analysis. Bartlett's test for sphericity tests the hypothesis that a correlation matrix is an identity matrix, which means the variables are unrelated. For our data, we have p-value .000 for Bartlett's test for sphericity. Therefore, we have enough evidence to conclude that the factor analysis is useful for the data. Now we can approach for the factor analysis in our dataset. The initial values of commonalities are set to 1. The highest extracted value is for the variable "Sharing password" is .693 indicating that a 69.3% variation in "Sharing password" is explained by the principal factors. 65.6% variation in "Same password multiple use" is explained by principal components. The least explained variable is "Insecure payment info online storage" which has an extraction value of about .294. As all values here are greater than .25, the communalities are acceptable (**Table 2**).

Table 2: Communalities and extracted values (Extraction Method: Principal Component Analysis).

Communalities	Initial	Extraction
Sharing password	1.000	.693
Common password	1.000	.465
Same password multiple use	1.000	.656
Personal info online storage	1.000	.544
Insecure payment info in website	1.000	.294
Using free access Wi-Fi	1.000	.346
Free antivirus with unknown source	1.000	.396
Disabling antivirus for downloading	1.000	.499
Downloading digital media from unknown source	1.000	.370
Sharing location on social media	1.000	.547
Friend request accepting by photo in social media	1.000	.540
Clicking links unauthorized	1.000	.574
Personal info with strangers over Internet	1.000	.451
Storing company info on personal device	1.000	.536

Table 3 shows the eigenvalues and percentage of variance in the original variables. From eigenvalues of component, we can see that 1st 4 components' eigenvalue is greater than 1. So, 1st four components are considered as four factors that are altogether explaining about 49% of the total variance which is moderate.

Table 3: Total variance explained (Extraction Method: Principal Component Analysis).

SN	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.196	22.829	22.829	3.196	22.829	22.829	1.929	13.778	13.778
2	1.439	10.278	33.107	1.439	10.278	33.107	1.817	12.979	26.757
3	1.224	8.746	41.853	1.224	8.746	41.853	1.685	12.035	38.792
4	1.049	7.493	49.346	1.049	7.493	49.346	1.478	10.554	49.346
5	.999	7.136	56.482						
6	.940	6.717	63.199						
7	.838	5.989	69.188						
8	.771	5.506	74.694						
9	.725	5.175	79.870						
10	.704	5.030	84.899						
11	.601	4.292	89.191						
12	.565	4.037	93.228						
13	.506	3.612	96.841						
14	.442	3.159	100.000						

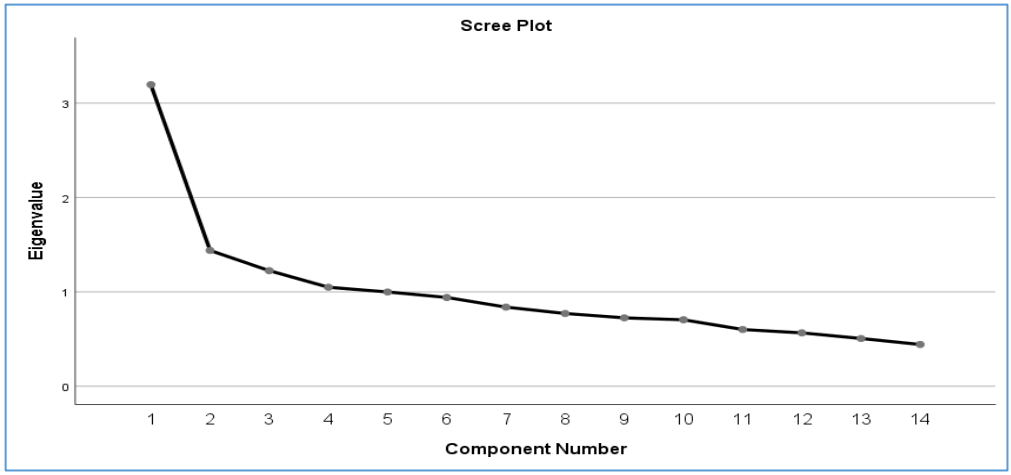

Fig. 1: Scree plot for eigenvalues of the components.

The scree plot shows that eigenvalues drop somewhat rapidly from components one to four. As 4 components are above one, four components are selected.

Table 4: Table for Rotated Component Matrix (Extraction Method: Principal Component Analysis).

Rotated Component Matrix[a]	Component			
	1	2	3	4
Same password multiple use	.770			
Personal info online storage	.659			.315
Downloading digital media from unknown source	.560			
Free antivirus with unknown source	.419	.392		
Insecure payment info in website	.418			
Using free access wifi	.369	.337		
Sharing password		.827		
Clicking links unauthorized		.715		
Friend request accepting by photo in social media			.719	
Storing company info on personal device			.706	
Sharing location on social media			.696	
Disabling antivirus for downloading				.683
Common password		.320		.564
Personal info with strangers over Internet		.426		.515

Rotation Method: Varimax with Kaiser Normalization[a]
a. Rotation converged in 6 iterations.

Variables that are most strongly correlated with each component are selected in **Table 5** from the rotated factor matrix (**Table 4**). We assume 0.5 as a threshold value and select the variables for each principal component accordingly.

Table 5: Variables included in the factors.

Factors	Included Variables
Factor 1	Same password multiple use, Personal info online storage, Downloading digital media from unknown source,
Factor 3	Sharing password, Clicking links unauthorized
Factor 3	Friend request accepting by photo in social media, Storing company info on Sharing location on social media
Factor 4	Disabling antivirus for downloading, Common password, Personal info with strangers over Internet

As the factors cannot explain the total variance more than 60%, we may fit our statistical models with individual variables.

Fitting Binary Logistic Regression Model to assess victimization status

In **Table 6**, the odds ratio is discussed to show the effect of the covariates on victimization status. The odds ratio describes the odds that an event occurs given a particular exposure is present compared to an event that occurs given the exposure is absent. Controlling for all other variables in the model, cybercrime victimization is 3.028 times more likely for those who use common password than those who do not (p-value=.012). Also controlling for every other variable, the odds of cybercrime victimization is 2.526 times higher as person shifts from not storing personal data online to storing them online (p-value=.034). For persons leaving payment information on website with no clear security compared to those who do not, the odds of victimization are significantly 66.3% lower (p-value=.02). However, this seems illogical and may be observed due to our sample data. Having the habit of disabling antivirus while downloading significantly increases the victimization odds by approximately 3 times (p-value=.014). The practice of downloading digital media from unknown sources significantly rises the victimization odds by 2.398 times (p-value=.041). The likelihood of cybercrime victimization when a person shares personal information to strangers over the internet is 4.422 times greater than that of their counterparts. The p-value here is .002 which refers to the factor being highly significant at a 5% significance level. The significant outcomes support the research hypothesis I. All the other covariates are statistically insignificant at 5% level of significance.

Table 6: Binary Logistic Regression Model for victimization status.

Covariates	Estimate	SE	OR	P-value	95% CI for OR	
					LB	UB
Sharing password (1)	0.585	0.8297	1.795	0.481	0.350	9.367
Common password (1)	1.108	0.4410	3.028	0.012	1.275	7.256
Same password multiple use (1)	0.321	0.4414	1.379	0.467	0.580	3.310
Personal info online storage (1)	0.927	0.4368	2.526	0.034	1.083	6.064
Insecure Payment information in website (1)	-1.118	0.4995	0.327	0.025	0.117	0.840
Using free access WiFi (1)	0.006	0.4045	1.006	0.988	0.449	2.213
Free antivirus with unknown source (1)	-0.521	0.4909	0.594	0.289	0.219	1.517
Disabling antivirus for downloading (1)	1.011	0.4101	2.747	0.014	1.230	6.198
Downloading digital media from unknown source (1)	0.875	0.4275	2.398	0.041	1.046	5.645
Sharing location on social media (1)	-0.015	0.4444	0.985	0.974	0.407	2.350
Friend request accepting by photo in social media (1)	-0.233	0.4464	0.792	0.601	0.328	1.909
Clicking links unauthorized (1)	0.581	0.5304	1.788	0.273	0.625	5.073
Personal info with strangers over internet (1)	1.487	0.4685	4.422	0.002	1.783	11.347
Storing company info on personal device (1)	-0.338	0.4372	0.713	0.439	0.297	1.663
Constant	-2.599	0.4889	0.074	0.000	0.027	0.183

*Here No (0) is the reference category for all the regressors.

Fitting Poisson Regression Model to assess victimization frequency

Table 7 shows the results from the Poisson regression model for the frequency of cybercrime victimization. Since the frequency of victimization is over-dispersed, the Negative Binomial model would be a better fit for this scenario. Its AIC is 465.131, whereas the AIC of the Poisson regression model is 540.994. However, a Poisson regression model is fitted here for ease of use. Here, we only describe the results which are statistically significant at 5% level of significance.

We have found women more vulnerable than men. The mean victimization rate of men is 35.2% less than that of women (p-value=.015). For one unit increase in social cite number, the mean frequency of victimization increases by 15.2% (p-value=.013). Users who spend more than 6 hours online experience an average rate of victimization that is 89.9% higher than those who spend less than 2 hours online (p-value=.044). The findings of the study by Cornelius (2016) demonstrated a positive, substantial, causal link between users' intention to adopt safe technology and their knowledge of cyber hazards. Similarly, in this study, Knowledge

of cyber security has been demonstrated to be a critical component in protecting against victimization. When compared to their counterparts, those with an understanding of cyber security are 44.7% less likely to experience cybercrime victimization (p-value =.001). This finding supports the research hypothesis II. When the p-value is less than 0.05, the odds of victimization rate increase by 16% for every unit increase in the number of social sites. Therefore, social site number is a highly significant factor.

Table 7: Poisson Regression Model for frequency of victimization.

Variables	Estimate	SE	IRR	P-value	95% CI for RR	
					LB	UB
Constant	-1.471	0.7790	0.230	0.059	0.048	1.034
Age	0.032	0.0176	1.032	0.073	0.995	1.067
Gender						
Male	-0.433	0.179	0.648	0.015	0.456	0.921
Female						
Education						
Graduate	-0.051	0.5509	0.950	0.926	0.275	2.512
Undergraduate	0.129	0.2137	1.137	0.547	0.754	1.747
Secondary						
Skill Level						
Advance	0.025	.3746	1.025	0.948	0.507	2.227
Intermediate	0.443	0.3304	1.558	0.180	0.852	3.147
Beginner						
Daily internet usage time						
More than 6 hours	0.642	0.3178	1.899	.044	1.043	3.650
4 to 6 hours	0.292	0.3182	1.339	0.359	0.735	2.578
2 to 4 hours	-0.188	0.3189	0.829	0.556	0.454	1.597
Less than 2 hours						
Cybersecurity Knowledge Status						
Yes	-0.593	0.1771	0.553	0.001	0.392	0.786
No						
Social site number	0.149	0.0544	1.160	0.006	1.042	1.290

CONCLUSION AND RECOMMENDATIONS:

Cyber facilities have brought a wave of change in our modern life. The purpose of the study is to see the behavior of cybercrime victimization, knowledge of cyber security, and causes of cybercrime victimization and to find some possible solutions and recommendations for this problem. The most common sort of cybercrime happening around is found to be hacking, identity fraud, phishing, monetary loss, computer virus and so on. The research demonstrates that the dependent variable cybercrime victimization is strongly associated with the independent variables which are password sharing status, using common password, cyber security knowledge Status, personal information online storage status, downloading free antivirus from unknown source, disabling antivirus for downloading, download digital media from unknown source, clicking links unauthorized sites, personal info Sharing with stranger over online. However, not all other variables have significant impact on cybercrime victimization. According to the regression model's findings, women are more likely than men to experience cybercrime. It is also evident from the views of the respondents that women are not very protected online. The study also contributes to some important opinions on cybercrime in the industrial sector. 69.5% of respondents strongly agree that management has the responsibility to ensure a company is protected from cybercrime. 65.2% of respondents strongly agree everyone in the company has a role to play in protecting against threats from cyber criminals. 56.52% of respondents agree that they don't have the right skills to be able to protect the organization from cybercrime. 52.1% of respondent agree that the Police cannot deal with cybercrime effectively.

39.13% of respondents were neutral that they worry that if they report a cyber-attack to the Police, it might damage the reputation of the company. The economic & digital development of the world along with our country is going on in a rapid speed. For this purpose, it is cyber security that is playing a vital role and contributing in these sectors. So, after conducting the study and recognizing reasons for cybercrime, we recommend following suggestions.

1) The Govt. should initiate cyber training programs.
2) The prevailing Law of Cybercrime should be implemented.
3) Strict cyber law should be imposed.
4) More and more seminars should be arranged to raise awareness among people.
5) Back dated software are unable to protect the device from cyber-attack. So, users should use up to date software in their devices.
6) For cyber security passwords is an exigent object. To avoid hacking, users should use strong & unique passwords.
7) Users should backup the data & review online accounts regularly.
8) Unauthorized & unknown sites contain viruses. So, downloading any content from unknown sources should be avoided.
9) There is a high risk of identity theft, making fake accounts, harassment for sharing personal information. Therefore, sharing personal information with anyone should be avoided.

ACKNOWLEDGMENT:

First and foremost, the author is grateful to Almighty Allah. The author is also thankful to anonymous reviewers and editors for their helpful comments and suggestions.

CONFLICTS OF INTEREST:

The author declares no conflict of interest.

REFERENCES

1) Abomhara, M., & Køien, G. M. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *J. of Cyber Security and Mobility*, **4**(1), 65-88. https://doi.org/10.13052/jcsm2245-1439.414
2) Ali, S. M., Hoq, S. M. N., Kabir, G., & Paul, S. K. (2022). Evaluating factors contributing to the failure of information system in the banking industry. *PLOS ONE*, **17**(3), e0265674. https://doi.org/10.1371/journal.pone.0265674
3) Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences*, **12**(5), 2589.
4) Astromskis, P. (2017). Legal technologies and cyber security in the singularity age. *Law Rev*, **16** (2), 34-57. https://doi.org/10.7220/2029-4239.16.3
5) Bahalul Haque, A. (2019). Need for critical cyber defence, security strategy and privacy policy in Bangladesh- hype or reality? *Inter J. of Managing Information Technology*, **11**(01), 37–50.
6) Becker, B. A., & Quille, K. (2019). 50 Years of CS1 at SIGCSE. *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*. https://doi.org/10.1145/3287324.3287432
7) Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, **48**, 51-61.
8) Bowen, B. M., Devarajan, R., & Stolfo, S. (2011). Measuring the human factor of cyber security. *IEEE Inter Conference on Technologies for Homeland Security (HST)*. https://doi.org/10.1109/ths.2011.6107876
9) Cornelius, (2016). Online identity theft victimizeation: An assessment of victims and non-victims level of cyber security knowledge. *Colorado Technical Univ. ProQuest Dissertations Publishing*.
10) Chen, Y. Z., Huang, Z. G., Xu, S., & Lai, Y. C. (2015). Spatiotemporal Patterns and Predictability of Cyberattacks. *PLOS ONE*, **10**(5), e0124472. https://doi.org/10.1371/journal.pone.0124472
11) Dobson & Barnett. (2018). An Introduction to Generalized Linear Models (4th ed.). *Taylor & Francis Group, LLC*.
12) Gifi, A. (1990). Nonlinear multivariate analysis. *Wiley-Blackwell*.
13) Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, **3**(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346
14) Kovacevic, A., Putnik, N., and Toskovic, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Access*, **8**, 125140-125148.

15) Kilmburg Cabaj, Zbigniew Kotulski, and Ana Respício. (2018). Cyber-security education: Evolution of the discipline and analysis of master programs. *Comp. & Sec.*, **75**(2018), 24-35.
16) Kundu, S., Hossain, M. A., & Chowdhury, I. H. (2018). Cybercrime trend in Bangladesh, an analysis and ways out to combat the threat. *2018 20th Inter Conference on Advanced Communication Technology (ICACT)*. https://doi.org/10.23919/icact.2018.8323799
17) Lallie, H. S., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, **105**, 102248.
18) Lebek, B., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, **37**(12), 1049-1092. https://doi.org/10.1108/mrr-04-2013-0085
19) Maalem Lahcen, R. A., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, **3**(1). https://doi.org/10.1186/s42400-020-00050-w
20) Matyokurehwa, K., Rudhumbu, N., Gombiro, C., & Mlambo, C. (2020). Cybersecurity awareness in Zimbabwean universities: Perspectives from the students. *Security and Privacy*, **4**(2).
21) Mazumder, M. M. M., & Hossain, D. M. (2022). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter? *J. of Accounting in Emerging Economies*.
22) Mia MM, Rahman MA, and Siddiqua T. (2022). Fear of crime and victimization: an explorative study, *Br. J. Arts Humanit*., **4**(6), 171-182. https://doi.org/10.34104/bjah.02201710182
23) N-CERT. (2015). Common Vulnerabilities in Cyber Space of Bangladesh.
24) Neshenko, N., Bou-Harb, E., & Furht, B. (2020). A survey of methods supporting cyber situational awareness in the context of smart cities. *J. of Big Data*, **7**(1).
25) Nifakos, S., Panaousis, E., & Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors*, **21**(15), 5119. https://doi.org/10.3390/s21155119
26) Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber Risk in Health Facilities: A Systematic Literature Review. *Sust*, **12**(17), 7002.
27) Staheli, D., Yu, T., Harrison, L. (2014). Visualization evaluation for cyber security. *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*. https://doi.org/10.1145/2671491.2671492
28) Sunil k. & Vikas S. (2018). Social Media Security Risks, Cyber threats and risks prevention and mitigation techniques, *International J. of Advance Research in Computer Science and Management,* **4**(4),2018, pp:125-129.
29) Švábenský, V., Vykopal, J., & Čeleda, P. (2020). What are cybersecurity education papers about? *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*. https://doi.org/10.1145/3328778.3366816
30) Tanner J. Burns, Thomas K. Jordan, Qijun Gu, and Trevor (2020). Cyber security challenges for society, *ACM Digital Library*.
31) Thomas h. Becker and Keith Quille. (2019). 50 Years of CS1 at SIGCSE: A Review of the Evolution of Introductory Programming Education Research. In Proceedings of the 50th ACM Technical Symposium on Computer Science Education (SIGCSE '19). ACM, NY, USA https://doi.org/10.1145/3287324.3287432
32) Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet.*
33) Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, **38**, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Citation: Uddin MA, Supti AZ, Asgar ASMR, Mridha MS, and Naiem. (2023). Cyber security awareness (CSA) and cyber crime in Bangladesh: a statistical modeling approach. *Aust. J. Eng. Innov. Technol.*, **5**(1), 15-25. https://doi.org/10.34104/ajeit.023.015025