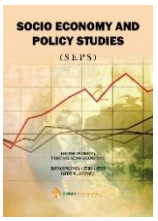
ZIBELINE INTERNATIONAL™ PUBLISHING

ISSN: 2785-8715 (Online)
CODEN: SEPSCJ

Socio Economy and Policy Studies (SEPS)

DOI: http://doi.org/10.26480/seps.01.2025.05.12



REVIEW ARTICLE

STATISTICAL APPRAISAL OF THE FINANCIAL IMPACTS OF CYBERCRIMES ON CORPORATE GOALS IN NIGERIA

Fidelis I. Onah[a*], H.C. Inyiama[b]

[a] *Department of Computer Science, University of Cross River State, Calabar, Nigeria.*
[b] *Department of Electronics and Computer Engineering, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria.*
**Corresponding Author. E-mail: ikonah80@yahoo.com*

ARTICLE DETAILS

Article History:

Received 6 December 2024
Revised 13 January 2025
Accepted 19 January 2025
Available online 24 February 2025

ABSTRACT

As technology advances, the need to assess the devastating impacts of Cybercrime and alert rational policy-makers at all levels, businesses and individuals of its subsequent financial implications become a growing concern. The objective of this study is to statistically investigate the financial implications of Cybercrime on organization's goal as perceived by shareholders, investors and key executives; and then proffer proactive steps to curb the menace. Questionnaires, interviews and discussions were the methods used to gather the opinions of the target audience. The Chi-Square method was then employed as a very useful predictive tool to determine the implications of a wide range of costs of online fraud to the businesses. It was established that online fraud management will reduce revenue leakages and bring businesses in line with the realization of corporate goals and objectives. The results of this study should be of interest to government and rational policy-makers charged with the responsibility of security in various quarters to coordinate law-enforcement action and give top spending priority to the most targeted sectors of the economy. It should also raise awareness amongst computer and information systems security designers, computing educators as well as consumers of online systems about developments in the cyber world and the need to institute an effective Cybercrime risk management system.

KEYWORDS

Cybercrime, online fraud, financial firm, financial impact, statistical appraisal, cybercrime detection system

1. INTRODUCTION

Cybercrime is a worldwide problem that cost countries, businesses, government and individuals billions of dollars in lost revenue annually. As more and more business services migrate to the cloud, larger quantities of the organization's critical assets, data and operational environments continue to be vulnerable to attacks by fraudsters. The case for more rigorous policing is stronger than ever (Financial Crime Academy LLC, 2024). Cybercrimes and the attendant clean-up required drive-up overhead costs in the organization. Huge financial costs posed to the global economy are increasingly being reported by the day. Phishing/spoofing, for example, has remained a top tactic used by cyber criminals to steal sensitive information. These attacks often come disguised as legitimate communications such as emails, phone calls or text messages aimed at tricking individuals into sharing personal data or clicking malicious links. In Ireland, Phishing complaints rose by 45% during the period March 1 to May 31 2020, compared to the same time in 2019 from the Garda Siochana figures released in June 2020 (Thornton, 2021).

Fraud loss via Internet Banking in Nigeria increased by 325% between 2022 and 2023 (Internet Crime Control Center, 2023). The top five States with the highest values are Lagos State, Abuja (FCT), Rivers State, Ogun State and Kaduna State in that sequence (NIBSS, 2024). A research report by Ponemon Institute (2016) shows that, Cybercrime cost in six countries (U.S.A, Japan, Germany, U.K, Brazil and Australia) in 2016 ranged from USD$4.3 million to USD$17.3 million annually. As new attack methods, new vulnerabilities, and new risks appear every year, the cost of a data breach continues to rise. According to IBM's Cost of a Data Breach Report 2023, the average cost of a data breach rose from $4.35 million in 2022 to USD $4.45 million in 2023; representing a 2.3% increase from 2022 to 2023 (UpGuard Inc, 2024; IBM Cost of a Data Breach Report 2023). The costs are expected to reach $5 million within the next few years. In 2022, the IC3 has seen an increase in an additional extortion tactics used to facilitate ransomware – a type of malicious software designed to block access to a computer system until money is paid. Cyber-criminals use this means to steal data off the system, hold the data hostage and threaten to publish the data if a ransom is not paid (Internet Crime Complaint Center (IC3), 2023). According to Verizon Data Breach Investigations Report 2023, nearly 35% of ransomware attacks originated from a breached email account (Internet Crime Complaint Center, 2022).

The daily reports of Cybercrime attacks on organizations around the world are endless. These have significant negative consequences which can ultimately jeopardize the survival of the organization. Among the traumatic financial impacts of Cybercrime on organizations are: devastating financial losses causing depletion of profitability, irreparable damage to brand reputation, potential legal and regulatory costs, lost opportunities, distorted markets and erosion of public trust on online business. A country that harbors online Cybercrime activities drives away potential investors and tourists. The rest of the world perceive the citizens as scammers and thus discriminates against them. Other negative consequences of cybercrime include the consumption of computer and network resources, and the cost in human time and attention of deleting unwanted messages (Ibrahim, 2019).

There is thus the need to awaken the case for better funding and coordinated law-enforcement action. According to IBM Cost of a Data Breach Report 2023, organizations affected by a ransomware attack but did not involve law enforcement experienced an average of $470,000 higher costs and damages. Government at different levels wants to know how much should be spent on cyber security. Policy-makers want to

Quick Response Code	Access this article online	
	Website: www.seps.com.my	**DOI:** 10.26480/seps.01.2025.05.12

Cite The Article: Fidelis I. Onah, H.C. Inyiama (2025). Statistical Appraisal of The Financial Impacts of Cybercrimes on Corporate Goals in Nigeria. *Socio Economy and Policy Studies, 5(1): 05-12.*

understand the total impact of Cybercrime to enable organizations to make more informed decisions. Is Cybercrime a reality? How does it impact on people, industries, entities, services and the environment? Government and rational policy-makers charged with the responsibility of security in various quarters, therefore, need to be reminded that resources should be adequately directed at more vulnerable activities. Gaining a better understanding of both prevalence and costs of Cybercrime would also help to raise awareness amongst computer and information systems security designers, computing educators as well as consumers of online systems about developments in the cyber world and the need to institute an effective Cybercrime risk management system (NDIC, 2020; Financial Crime Academy LLC, 2024).

In response to these threats, the adoption and implementation of cost-saving cybercrime detection, analysis and prevention systems have generally improved in emerging markets and developing economies of the world. However, enhancing the cyber resilience of notable entities in Nigeria and several other countries remain inadequate. This research paper carried out an empirical investigation of the costs and risks posed by Cybercrimes to the Nigerian economy as perceived by stakeholders, investors and key executives of some corporate entities. For network designers and administrators, demand per day is uncertain. If he invests unwisely, he looses the profit he could have made. Correlation analysis is conducted to analyze relationships between attacks and financial losses on corporate goals in Nigeria. The survey represents reality in mathematical terms to help planners and decision makers determine their policies and actions scientifically. The study will help people to understand better how severe the current threat on computer information system is. It is a call for rational policy-makers to concentrate more on catching and punishing perpetrators of Cybercrime and less on preventive measures (antivirus, firewalls, etc). A multi-agent system that cooperates to detect frauds in real time was proposed.

2. Review of Related Literature

The term "Cybercrime" or "online crime" refers to criminal activities that are carried out using computers, networks, or digital technologies. These offenses often involve the unauthorized access, manipulation, or theft of digital data, as well as the disruption or sabotage of computer systems and online networks for illicit purposes (Ajibade, 2024). Cybercriminals take advantage of security holes and vulnerabilities found in systems and exploit them in order to take a foothold inside the targeted environment. The security holes can arise from using weak authentication methods and passwords and also from lack of strict security models and policies (Talents, 2024). Cyber attack incidences continue to increase every year as Internet usage expands and cyber-criminal techniques become more sophisticated. (Australian Federal Police, 2024; Fortinet, Inc., 2024).

The most common cybercrimes include: use of tricks or malicious software to get sensitive information from a target system (email phishing scams), identity theft, ransomeware attack, unauthorized access to a computer for malicious purpose, and Internet fraud. Other types of cybercrimes include: Online harassment (bullying), using unwanted and intimidating calls and messages (cyberstalking), software piracy, use of social media fake accounts, online drug trafficking, electronic money laundering, cyber extortion, Online intellectual property infringements, and online recruitment fraud (Talents, 2024). It is important to also note the existence of the following cybercrime attacks: greeting card scams, credit card scams, online dating scams, lottery fee fraud, the Nigerian prince scam, online bank fraud, cryptocrime, counterfeit software, copyright theft (which include copyright for academic publications), fake antivirus, impersonation fraud, website defacement (replacement of a website's main page with images and content of the attacker's choosing), advance fee fraud, business email compromise, etc. (Financial Crime Academy LLC, 2024; Fortinet, Inc., 2024).

The total costs incurred by businesses all over the world as a result of cybercrimes may be categorized as follows:

- Costs in anticipation of crime: These are costs incurred by individuals and businesses in providing defensive (or preventive) measures like spam filters, antivirus software, firewalls, browser extensions, insurance and compliance.
- Costs as a consequence: These refer to costs that occur as an immediate result of a crime. It normally takes the form of property damage, money lost or emotional and physical costs from crime. Time and effort to reset account credentials (for banks and consumers); missed business opportunity, training or awareness security services provided to individuals, and overwhelming systems with spam messages which consume bandwidth are yet other costs incurred as a consequence of crime. It also includes public loss of trust in a business which leads to reduced revenues from electronic transaction fees.
- Costs in response to crime: These refer to costs of handling complaints and queries, etc from a crime incident, costs from 'goodwill' compensation payments to victims, discounts provided to customers and fines paid to regulatory bodies, police forces and the criminal justice system. They also include costs due to loss of business relationships, lost investor or funder support.

3. Methodology

The methodology adopted is to survey experts from within the industry as to what proportion of turnover is lost to Cybercrime. The study was conducted in three state capitals namely: Enugu, Calabar and Awka - the capital cities of Enugu, Cross River and Anambra States of Nigeria respectively. These cities offered sufficient availability of network resources, and vibrant individuals who were knowledgeable on the concept, universality and potential danger of Cybercrimes. Opinions of stakeholders were gathered through discussions, observations, interviews and the use of questionnaires. (See Table 1). The study population were thus drawn from government agencies/ministries/parastatals; private businesses (major shops, hospitals, industries, proprietors of schools, etc); telecommunication network operators; banks/financial institutions; Universities, media houses (radio and television houses); and many more local and international business organizations.

The field survey spanned a period of one week and four days in each study area (Enugu, Calabar and Awka). The multi-stage sampling technique was used to collect individual data using both stratified and simple random sampling methods (Owie, 1996). The individuals in the metropolis were grouped into two main strata (network operators and stakeholders) which exhibited definite characteristics such as age and educational levels (Tables 2 and 3). The simple random sampling method was then used to select individuals from each stratum. The reason for the use of simple random sampling method was that every element or stakeholder had an equal chance of being selected from the population (Owie, 1996).

A total of 140 questionnaires were randomly distributed to the respondents during the field surveys. Out of this, only 135 datasets were usable while 5 units of data were excluded from further statistical analysis due to faulty entries.

3.1 Data Analysis

In our research problem, answer options are classified into five mutually-exclusive categories namely: Strongly Agree, Agree, Neutral, Disagree, and Strongly Disagree. The dependent variable – Quest/Rank – is classified into the various research questions. With this information, we can design the frequency distribution of answer options for 135 questionnaire respondents.

3.2 Geographical Location of Respondents

To present the data in a more manageable and comprehensible form, frequency distribution was used to tabulate the frequency of occurrence of each measure. The **s**tudy populations by area of location are shown in Table 2 below:

Table 2: Study Population by area of Location

Location	No. of Respondents	Percentages
Enugu	65	48.15
Calabar	40	29.63
Awka	30	22.22
Total	135	100.00

3.2.1 Age Distribution of Respondents

The ages of the respondents are shown in Table 3 below.

Table 3: Age distribution of Respondents

Age of Respondents	No. of Respondents	Percentages
25-30	20	14.81
31-35	27	20.00
36-40	49	35.56
Above 40	39	29.63
Total	135	100.00

The analysis indicates that the respondents are vibrant, matured individuals who understand the impact of fraud in organizations and businesses.

3.2.2 Educational Qualifications of Respondents

The educational qualifications of the respondents are shown in Table 4 below.

Table 4: Respondents Educational Qualification

Qualification of Respondents	No. of Respondents	Percentages
WASC/GCE	14	10.37
NCE/OND	19	14.07
HND/B SC	34	25.19
M.SC/MBA/PhD	27	20.00
Professional Cert.	41	30.37
Total	135	100.00

The analysis here indicates that the respondents have adequate and relevant education qualification to understand the concept and universality of the research topic.

3.3 Research Questions and Hypotheses

To realize the objectives of this study, the following research questions and hypotheses are formulated and will be tested to examine them for correctness and completeness.

3.3.1 Research Questions

The following research questions are formulated and answered in this paper:

- Is cybercrime a reality?
- Is cybercrime a significant source of financial losses to businesses and organizations?
- Does cyber attack against network systems erode the public's confidence in the security of online transactions?
- Does cybercrime cause a traumatic damage to the organization's brand and reputation?
- Is the establishment of systems and controls to prevent or detect Cybercrimes and safeguard network systems the concern of Policy-makers and government at all levels?
- Will online business transactions give service operators a competitive edge in terms of customer care and retention, marketing and revenue assurance?
- Will cybercrime management bring businesses and organizations in line with the realization of corporate goals and objectives through reduction of revenue leakages?

3.3.2 Research Hypotheses

The research hypotheses below are formulated and will be tested to ascertain their viability and reliability. They comprise the null hypotheses (designated as H_0) and the alternative hypotheses (symbolized by H_1, H_2, H_3, etc.).

3.3.2.1 Test of hypothesis 1

H_1: The existence of cybercrime is a reality and constitutes a major source of lost revenue to the financial sector.

H_0: The existence of cybercrime is not real and does not constitute a major source of lost revenue to the financial sector.

3.3.2.2 Test of hypothesis 2

H_1: Cyber attacks erode the public's confidence in the security of online transactions and safeguarding network systems should be the concern of government at all levels.

H_0: Cyber attacks do not erode the public's confidence in the security of online transactions and safeguarding network systems should not be the concern of government.

3.3.2.3 Test of hypothesis 3

H_1: Cybercrime management will bring businesses and organizations in line with the realization of corporate goals and objectives through reduction of revenue leakages.

H_0: Cybercrime management will not bring businesses and organizations in line with the realization of corporate goals and objectives through reduction of revenue leakages.

3.4 Statistical Analysis

To establish the appropriateness of the audience, we compute summaries and derived values from the data collected. Without proper processing and analysis, data is quite useless for decision making (Oppenheim, 1992).

The Chi-Square, symbolized by X^2, test of independence will be used in this analysis because of the nature of the data (quantitative). The formula is given by:

$$X^2 = \frac{\sum (f_0 - f_e)^2}{f_e}$$

Where f_0= observed frequencies in a category (Generated from sample data),

f_e = expected frequencies in the same category (provided by population parameters).

Σ = sum of this ratio over all columns and rows.

For the two-tailed test:

H_0: $f_0 = f_e$ – Mean of A = Mean of B

H_1: $f_0 > f_e$ – Mean of A $\neq$ Mean of B

The sampling distribution of the X^2 is a function of the associated degrees of freedom (df),

where df = No. of categories, K – 1.

The method we shall use before applying the general X^2 formula is to determine the expected frequencies f_e for each cell as follow:

$$f_e = \frac{(\text{Row total})(\text{Column total})}{N}$$

where N = no. of frequencies in the distribution (or sample size)

= 135; for this research.

The three hypotheses formulated will be tested at 5% level of significance with (r-1) (c-1) degree of freedom to ascertain their viability and reliability. If X^2 calculated is greater than X^2 tabulated, we reject the null hypothesis (H_o), else we accept otherwise. We are concerned with both tails of the distribution of sample means (H_0 and H_1) and this is thus called a two tail test of significance. The null Hypothesis is the one which is tested. If H_0 is accepted, H_1 is rejected whilst if H_0 is found to be false, H_1 is accepted.

4. Results and Discussion

The data collected based on these hypotheses are presented in Tables 4, 5, and 6, respectively. In each cell, the numbers in brackets are the expected frequencies while the numbers without brackets are observed frequencies. The expected frequencies are obtained using the formulae:

Eji = (Ri*Cj)/N,

Where;

R1 = Row total,

Cj = Column total,

N = Grand total

The number of rows equals the number of questions that represent each null hypothesis. The number of columns also equals the ranks of the respondent's position about each question.

The respondent's position is shown as follows:

4.1 Test of hypothesis 1

H_1: The existence of cybercrime is a reality and constitutes a major source of lost revenue to the financial sector.

H_0: The existence of cybercrime is not real and does not constitute a major source of lost revenue to the financial sector.

Table 5: The existence of Cybercrime is a reality and constitutes a major source of lost revenue to the financial sector.

Quest/Rank	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Row total (Ri)
1	41(41)	51(46)	17 (19)	15 (16)	11 (13)	135
2	41(41)	41(46)	21 (19)	17 (16)	15 (13)	135
Column Total (Cj)	**82**	**92**	**38**	**32**	**26**	**270**

Expected frequencies are obtained thus:

Designing a 10-cell contingency table:

Table 6: Contingency Table for Test of Hypothesis 1

CELL	F_o	F_E	$F_o - F_E$	$(F_O - F_E)^2$	$(F_O - F_E)^2/F_E$
A: $r_i c_i$	41	41	0	0	0.0000
B: $r_i c_2$	51	46	5	25	0.5435
C: $r_i c_3$	17	19	-2	4	0.2105
D: $r_i c_4$	15	16	-1	1	0.0625
E: $r_i c_5$	11	13	-2	4	0.3077
F: $r_2 c_i$	41	41	0	0	0.0000
G: $r_2 c_2$	41	46	-5	25	0.5435
H: $r_2 c_3$	21	19	2	4	0.2105
I: $r_2 c_4$	17	16	1	1	0.0625
J: $r_2 c_5$	15	13	2	4	0.3077
					$\sum X^2$ = 2.2484

Where r = number of rows, c = number of columns

X^2 cal = 0 + 0.5435 + 0.2105 + 0.0625 + 0.3077 + 0 + 0.5435 + 0.2105 + 0.0625 + 0.3077

$\simeq$ **2.248**

df = (r – 1)(c – 1)

= (2 – 1)(5 – 1)

= 1*4

= 4

With 4 df, the critical X^2 value required for significance at .05 significance level is 9.488 (from Table 7, Appendix 11).

That is, X^2 (tabulated) = X^2 (r-1)(c-1); 0.05 = X^2 df, 0.05 = 9.488.

Decision: Since X^2 calculated (i.e. 2.248) is less than X^2 tabulated (i.e. 9.488), we accept H_0 and conclude that the existence of Cybercrime is a reality and constitutes a major source of lost revenue to the financial sector. As businesses take measures to reduce the chances of attacks by securing their networks (like buying security software applications), overhead (operating) cost increases while profit margins and productivity reduces.

4.2 Test of hypothesis 2

H_1: Cyber attacks erode the public's confidence in the security of online transactions and safeguarding network systems should be the concern of government at all levels.

H_0: Cyber attacks do not erode the public's confidence in the security of online transactions and safeguarding network systems should not be the concern of government.

Table 8: Cyber attacks erode the public's confidence in the security of online transactions and safeguarding network systems should be the concern of government at all levels.

Quest/Rank	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Row total (Ri)
3	46(46)	41(46)	26 (21)	11 (11)	11 (11)	135
4	46(46)	51(46)	16 (21)	11 (11)	11 (11)	135
Column Total (Cj)	**92**	**92**	**42**	**22**	**22**	**270**

Expected frequencies are obtained thus:

Designing a 10-cell contingency table:

Table 9: Contingency Table for Test of Hypothesis 2

CELL	F_O	F_E	$F_o - F_E$	$(F_O - F_E)^2$	$(F_O - F_E)^2/F_E$
A: $r_i c_i$	46	46	0	0	0.0000
B: $r_i c_2$	41	46	-5	25	0.5435

Table 9(cont): Contingency Table for Test of Hypothesis 2					
C: $r_i c_3$	26	21	5	25	1.1904
D: $r_i c_4$	11	11	0	0	0.0000
E: $r_i c_5$	11	11	0	0	0.0000
F: $r_2 c_i$	46	46	0	0	0.0000
G: $r_2 c_2$	51	46	5	25	0.5435
H: $r_2 c_3$	16	21	-5	25	1.1904
I: $r_2 c_4$	11	11	0	0	0.0000
J: $r_2 c_5$	11	11	0	0	0.0000
					$\sum X^2$ = 3.4678

where r = number of rows, c = number of columns

X^2 cal = 0 + 0.5435 + 1.1904 + 0 + 0 + 0 + 0.5435 + 1.1904 + 0 + 0

≃ 3.468

df = (r – 1)(c – 1)

= (2 – 1)(5 – 1)

= 1*4

= 4

With 4 df, the critical X^2 value required for significance at .05 significance level is 9.488 (from Table 7, Appendix 11).

X^2 (tabulated) = X^2 (r-1)(c.1); 0.05 = X^2 c,0.05 = 9.488

Decision: Since X^2 calculated (i.e. 3.468) is less than X^2 tabulated (i.e. 9.488), we accept H_0 and conclude that Cyber attacks erode the public's confidence in the security of online transactions and safeguarding network systems should be the concern of government at all levels. The decline in the public's morale and trust in a business causes irreparable damage to the organization's brand and reputation, increase in financial losses from electronic transaction fees and the risk of exposure to potential legal and regulatory sanctions. The result of this also includes lost opportunities and distorted markets where fraudsters obtain a competitive advantage and drive out legitimate businesses.

Government and policy-makers must adequately fund and coordinate law-enforcement action to put an end to impunity and focus on more informed decisions concerning their business goals. While organizations must spend much on preventive measures (on antivirus, firewalls, etc), government should spend more on catching perpetrators and throwing them in jail.

4.3 Test of hypothesis 3

H_1: Cybercrime management will bring businesses and organizations in line with the realization of corporate goals and objectives through reduction of revenue leakages.

H_0: Cybercrime management will not bring businesses and organizations in line with the realization of corporate goals and objectives through reduction of revenue leakages.

Table 10: Cybercrime management will bring businesses and organizations in line with the realization of corporate goals and objectives through reduction of revenue leakages.

Table 10: Cybercrime management will bring businesses and organizations in line with the realization of corporate goals and objectives through reduction of revenue leakages.						
Quest/Rank	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Row total Ri
5	49(47)	42(43)	20(19)	12(14)	12(12)	135
6	46(47)	41(43)	19(19)	17(14)	12(12)	135
7	46(47)	46(43)	18(19)	13(14)	12(12)	135
Column Total (Cj)	141	129	57	42	36	405

Expected frequencies are obtained as follows:

$$e_{11} = ((135x141)/405) = 47 \quad e_{21} = ((135x141)/405) = 47 \quad e_{31} = ((135x141)/405) = 47$$
$$e1_{12} = ((135x129)/405) = 43 \quad e_{22} = ((135x129)/405) = 43 \quad e_{32} = ((135x129)/405) = 43$$
$$e_{13} = ((135x57)/405) = 19 \quad e_{23} = ((135x57)/405) = 19 \quad e_{33} = ((135x57)/405) = 19$$
$$e_{14} = ((135x42)/405) = 17 \quad e_{24} = ((135x42)/405) = 17 \quad e_{34} = ((135x42)/405) = 17$$
$$e_{15} = ((135x36)/405) = 12 \quad e_{25} = ((135x36)/405) = 12 \quad e_{35} = ((135x36)/405) = 12$$

Designing a 15-cell contingency table:

Table 11: Contingency Table for Test of Hypothesis 2					
CELL	F_o	F_E	F_o - F_E	$(F_O - F_E)^2$	$(F_O - F_E)^2/F_E$
A: $r_i c_i$	49	47	2	4	0.0851
B: $r_i c_2$	42	43	-1	1	0.0233

Table 11(cont): Contingency Table for Test of Hypothesis 2					
C: $r_i c_3$	20	19	1	1	0.0526
D: $r_i c_4$	12	14	-2	4	0.2857
E: $r_i c_5$	12	12	0	0	0.0000
F: $r_2 c_i$	46	47	-1	1	0.0213
G: $r_2 c_2$	41	43	-2	4	0.0930
H: $r_2 c_3$	19	19	0	0	0.0000
I: $r_2 c_4$	17	14	3	9	0.6429
J: $r_2 c_5$	12	12	0	0	0.0000
K: $r_3 c_i$	46	47	-1	1	0.0213
L: $r_3 c_2$	46	43	3	9	0.2093
M: $r_3 c_3$	18	19	-1	1	0.0526
N: $r_3 c_4$	13	14	-1	1	0.0714
O: $r_3 c_5$	12	12	0	0	0.0000
					$\sum X^2$ = 1.5585

where r = number of rows, c = number of columns

X^2cal = 0.0851 + 0.0233 + 0.0526 + 0.2857 + 0 + 0.0213 + 0.0930 + 0 + 0.6429 + 0 + 0.0213 + 0.2093 + 0.0526 + 0.0714 + 0

≃ 1.559

df = (r – 1)(c – 1)

= (3 – 1)(5 – 1)

= 2*4

= 8

With 8 df, the critical X^2 value required for significance at .05 significance level is 5.507 (from Table 7, Appendix 11).

X^2 (tabulated) = X^2 (r-1)(c.1); 0.05 = X^2 c,0.05 = 15.507

Decision: Since X^2 calculated (i.e. 1.559) is less than X^2 tabulated (i.e. 15.507), we accept H_0 and conclude that Cybercrime management will bring businesses and organizations in line with the realization of corporate goals and objectives through reduction of revenue leakages (i.e., financial losses, reputation and brand damage and other costs incurred by the businesses). This includes giving service operators a competitive edge in terms of customer care and retention, marketing and revenue assurance. An organization can lose its competitive advantage and suffer losses when a hacker steals its confidential information and future plans and sells it to a competitor.

5. Conclusion

As many social and economic interactions keep migrating from the physical world to cyberspace, larger quantities of personal and business information are exposed to cyber attacks. This paper has shown that the security and privacy of network systems should be the concern of government at all levels. Statistical studies suggest that government and rational policy-makers should concentrate more on catching and throwing perpetrators to jail and less on preventive measures (antivirus, firewalls, etc).

A better funded and coordinated law-enforcement action from government and stakeholders is recommended for a stable, safe and resilient cyberspace. The survey also highlighted that larger organizations can manage cyber security better than small-sized firms, and are thus less vulnerable to cyber incidents. The paper further established that cybercrime management will reduce revenue leakages and bring businesses in line with the realization of corporate goals and objectives. A multi-agent system that cooperates to detect frauds in real time is recommended to effectively manage and protect the networked systems using different techniques.

The paper contributed to knowledge by alerting businesses, computer and information systems security designers, computing educators and consumers of online systems about Cybercrimes and their impacts on corporate goals. It calls on governments and policy-makers to coordinate law-enforcement action and channel resources to strengthen the cyber security frameworks of the financial sector. This is proven to promote economic vitality and national security.

References

Ajibade, A.A., 2024. What is Cybercrime? Thomas Adewumi University, Oko-Irese, Kwara State , Nigeria. Accessed from https://www.tau.edu.ng on 27/10/2024.

Australian Federal Police, 2024. Cybercrime. Accessed from www.police.act.gov.au on September 29, 2024.

Cyber Talents, 2024. What is Cybercrime? Types, Examples, and Prevention. Accessed from https://www.cybertalents.com on 27/10/2024.

Financial Crime Academy LLC, 2024. Understanding the Impact of Fraud: Types, Risks, and Management Strategies. Accessed from https://financialcrimeacademy.org/impact-of-fraud/ on Sep 26, 2024.

Fortinet, Inc., 2024. What is Cybercrime? Types of Cybercrime. Accessed from https://www.fortinet.com on Sep 29, 2024

Hooper, C., 2024. From losses to lessons: Assessing the full spectrum of the cost of fraud. Retrieved from https://www.veriff.com/fraud/learn/the-cost-of-fraud on Sep 22, 2024.

Ibrahim, U., 2019. The Impact of Cybercrime on the Nigerian Economy and Banking System. NDIC-Quarterly-Vol-34-No-12-2019

Internet Crime Complaint Center (IC3), 2022. Federal Bureau of Investigation Internet Crime Report 2022 Retrieved from: https://www.xxxxxxxxxx

Internet Crime Complaint Center (IC3, 2023. 2022 Internet Crime Report. Accessed from: https://www.ic3.gov on 03/10/2024.

NDIC, 2020. Understanding the costs of cyber crime. Accessed from: https://assets.publishing.service.gov.uk on 03/10/2024.

NIBSS, 2024. 2023 Annual Fraud Landscape. Accessed from: https://nibss-plc.com.ng on 03/10/2024.

Oppenheim, A.N., 1992. Questionnaire Design, Interviewing and Attitude Measurement, Wellington House, London: Pinter Pub Ltd.

Continuum The Tower Building, 11 York Road, London SEl 7NX 370 Lexington Avenue.

Owie, I., 1996. Fundamentals of Statistics in Education and the Social Sciences, United City publishing company, Benin City, Third print.

Thornton, G., 2021. The Economic Cost of Cybercrime. Retrieved on 03/10/2024 from https://www.grantthornton.ie. Ireland

UpGuard, Inc., 2024. Cybersecurity - What is the Cost of a Data Breach in 2024? Retrieved from: https://www.upguard.com on 03/10/2024.

Appendix 1

Sample Questionnaire on Cybercrimes

Screening Questions:

(Please tick (√) to one which is applicable to you)

1. Sex: (a) Male ( ) (b) Female ( )

2. Age: (a) 25 – 30( ) (b) 31 – 35( ) (c) 36 – 40( ) (d) Above 40 ( )

3. Religion: (a) Christian ( ) (b) Moslem ( ) (c) Traditional ( )

4. Marital Status: (a) Single ( ) (b) Married ( )

5. Qualification: (a) WASC/GCE ( ) (b) NCE/OND ( ) (c) HND/B.Sc ( ) (d) M.Sc/MBA/PhD ( ) (e) Professional Cert. ( )

Table 1: Sample Questionnaire

S/N	Test Questions	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
6	The existence of cybercrime is a reality and constitutes a major source of lost revenue to businesses.					
7	Cyber attacks erode the public's confidence in the security of online transactions and safeguarding network systems should be the concern of government at all levels.					
8	Better funding and coordinated law-enforcement action from government and policy-makers should be prioritized to cut down the devastating impact of Cybercrimes.					
9	Cybercrime management will bring businesses and organizations in line with the realization of corporate goals and objectives through reduction of revenue leakages.					

10. What is the estimated size of your organization? A. small size (<= 500 people)

B. mid-size (< 5000 people) C. Large size (> 5000 people)

11. Are you aware that information resources maintained in computer network infrastructures are plagued by various online frauds? Yes ( ) or No ( )

12. Are you aware that most cyber attacks are perpetrated through the Internet?

Yes ( ) or No ( )

13. There is a dramatic increase in online fraud that specifically targets consumers, enterprises and government. Yes ( ) No ( ) Don't know ( )

14. Do you think that online business transaction gives service operators a competitive edge in terms of customer care and retention, marketing and revenue assurance? Yes ( ) No ( ) Don't know ( )

15. Cybercrimes can result to distorted market where criminals obtain a competitive advantage and drive out legitimate business.

Yes ( ) No ( ) Don't know ( )

16. Have you ever participated in any seminar, training or workshop on security awareness?

Yes ( ) or No ( )

17. Cybercrime prevention systems allow businesses and organizations to make better informed decisions and realize corporate goals.

Yes ( ) No ( ) Don't know ( )

18. The economic vitality and security of any nation largely depend on a stable, safe and resilient cyberspace.

Yes ( ) No ( ) Don't know ( )

19. Is your Organization highly effective at reducing online fraud?

Yes ( ) or No ( )

20. Any other comments please state below:

……
……
……
……
……
……
……
……
……
……

Appendix 11

Excerpts from Chi-Square Distribution Table

The following are excerpts from chi-square (X^2) distribution table for the first 10 degrees of freedom (df).

Table 7: Excerpts from Chi-square Distribution Table

Degrees of Freedom	0.995	0.99	0.975	0.95	0.90	0.10	0.05	0.025	0.01	0.005
1	0.000	0.000	0.001	0.004	0.016	2.706	3.841	5.024	6.635	7.879
2	0.010	0.020	0.051	0.103	0.211	4.605	5.991	7.378	9.210	10.597
3	0.072	0.115	0.216	0.352	0.584	6.251	7.815	9.348	11.345	12.838
4	0.207	0.297	0.484	0.711	1.064	7.779	9.488	11.143	13.277	14.860
5	0.412	0.554	0.831	1.145	1.610	9.236	11.071	12.833	15.086	16.750
6	0.676	0.872	1.237	1.635	2.204	10.645	12.592	14.449	16.812	18.548
7	0.989	1.239	1.690	2.167	2.833	12.017	14.067	16.013	18.475	20.278
8	1.344	1.646	2.180	2.733	3.490	13.362	15.507	17.535	20.090	21.955
9	1.735	2.088	2.700	3.325	4.168	14.684	16.919	19.023	21.666	23.589
10	2.156	2.558	3.247	3.940	4.865	15.987	18.307	20.483	23.209	25.188