Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 1s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Analyzing the risk of cyberattacks on pharmacy information systems

Ashish Agrawal[1], Kunal Chandrakar[2]

[1]Assistant Professor, Department of Pharmacy, Kalinga University, Raipur, India.
[2]Research Scholar, Department of Pharmacy, Kalinga University, Raipur, India.

Cite this paper as: Ashish Agrawal, Kunal Chandrakar, (2025) Analyzing the risk of cyberattacks on pharmacy information systems. *Journal of Neonatal Surgery*, 14 (1s), 542-547.

ABSTRACT

As the world moves closer to a cashless and paperless economy, digitization is essential for any firm to succeed. Although initiatives to encourage digitization have been started, cyber risk was overlooked, and the danger of cyberattacks has been rising and is far more than the perceived risk of cyber. Globally, there has been a startling rise in cyberattacks of all kinds, which have in certain cases caused some businesses to become unstable and taken days or months to recover. In addition to the other operational problems, the recovery period resulted in cost and market share loss. This study aimed to determine the factors that influence an individual's readiness to manage cyber risks by examining the role of respondents' online behavior, awareness of cyber risks, experience with cyber risks, and attitude toward cyber risks in lowering the incidence of cyber risks. 385 respondents were given a structured questionnaire by the researcher, and the information gathered was coded and revised for additional analysis. The data was subjected to univariate, bivariate, and multivariate analysis, and the researcher employed regression, t-test, and Anuva to highlight the study's framework. The findings show that an individual's online behavior and awareness of cyber hazards contribute to their readiness to manage those risks. An individual will be able to improve their readiness to manage cyber hazards with the help of the findings.

Keywords: *health, digitization, medical, identifying, cyber risk.*

1. INTRODUCTION

With technology constantly evolving and the economy becoming more digitalized, as well as with online marketing and e-commerce becoming the norm for both business and daily life, cyber risks are the biggest threat that many people face [1]. Digitization has emerged as a key word for all organizations, large and small, startups and established businesses alike, as well as for individuals looking to advance in their careers or improve their businesses, find knowledge, and manage and complete daily tasks more easily in both their personal and professional lives [2]. Every person wants to be able to easily handle all of their life's activities including friends and family from the comfort of their home or place of employment. This has led to the emergence of cyberbullies who watch for any weak spot that could be exploited [16]. other incident involving a data breach or other criminal activity carried out via a computer connected to the internet is considered cyber-crime [15]. The first step in managing cyber risks is for a person or organization to determine where they are at risk so that all of the exposures can be addressed to lower the likelihood of a cyberattack [11]. Both numerically and as a proportion, the number of cybercrimes that occur in India and around the world has been trending upward [3]. More cases of these crimes, together with the writing on the walls stating that the next world war will undoubtedly be fought online, call for more research and studies to be done in order to control cyber threats and ensure cyberspace security [9]. Any person who is careless puts themselves, their family, their enterprise, or even their nation at risk of a cyberattack. This study aims to comprehend the exposures to cyber risks and the elements that influence a person's readiness to manage cyber hazards. An individual's online activity, attitude toward cyber risks, understanding of cyber risks, experience with cyber risks, and preparedness to manage cyber risks are all factors that the study seeks to ascertain. All age categories of internet users in Bengaluru were included in the survey, starting with students, professionals, those working in the public and commercial sectors, independent contractors, freelancers, and retirees [4].

2. AIM AND OBJECTIVES

Cybercrime, Ransomware, Data Breach, Third-Party Liability, Identity Theft, Financial Loss, Cyber Risk, Cybercrimes, etc. In the digital economy, these are the terms that we hear most frequently. In order to prevent virus attacks and handle system failures, organizations used to benefit from having a secure network and security system [12]. However, despite the significant investments made in IT security, cyber dangers and cyberattacks still exist today. Cyber hazards are unavoidable,

and organizations need to be ready to handle and successfully manage them. Financial loss, identity theft, ransomware, data breaches, third-party liability, cybercrime, cyberrisk, etc. These are the terms we hear the most in the digital economy. Organizations used to profit from having a safe network and security system to handle system outages and prevent virus attacks [6]. However, cyberthreats and cyberattacks persist today in spite of the large investments made in IT security. Organizations must be prepared to deal with and effectively manage cyber threats because they cannot be avoided [5]. Despite being one of the most promising areas for the present and the future, not many insurance companies have entered and expanded into the cyber insurance business [13]. This led to the inquiry. Why? After a more thorough review of the literature, it was determined that the lack of measures to determine the extent of cyber risks and the lack of historical data make it even harder for insurance companies to determine premiums that will guarantee that businesses and individuals have enough coverage to overcome their financial liabilities and maintain their market share and operations while also ensuring that the financial implications to the insurance companies are well within the liquidity norms [7]. Finding cyber risk exposures and evaluating them in relation to an individual's level of readiness for cyber hazards is the first step in the research process [8]. The organizations do not know how much coverage they should get to protect themselves financially and guarantee that their business runs smoothly and error-free. In order to lessen the impact of direct losses brought on by cyber threats, the organizations are primarily focusing on two factors: third-party financial liability, which is extremely challenging to evaluate. Finding cyber risk exposures and evaluating them in relation to an individual's level of readiness for cyber hazards is the first step in the research process. Generally speaking, "cybercrime" refers to any unlawful or abnormal behavior that uses a computer as a tool, a target, or both [14]. Any unpleasant, undesired, illegal, and deviant behavior carried out through a system or other devices connected to the internet is also included in this term. The statistics that are currently available indicate that cybercrime is becoming more common in India, but they are unclear on the various types of cybercrime.

3. PROPOSED METHODOLOGY

The primary objective of the study is to determine how the dependent variables—awareness, readiness, attitude, online behavior, and experience with cyber risks—relate to the independent demographic variables—gender, age, income, and education—in a population. According to Singh (2007), there are two types of quantitative research designs: exploratory and conclusive. According to his explanation, this study is exploratory in nature since it helps the researcher identify specific research issues. It may be said that it is the foremost research as it paves for conclusive research. According to [10], the primary goal of conducting exploratory research is to satisfy the researcher's curiosity and their comprehensive understanding while confirming the area that warrants additional investigation. The study's participants are Bengaluru residents who use the internet for a variety of reasons, including as social media, online shopping, e-commerce, business, financial transactions, surfing, entertainment, education, and communication. Bengaluru, the capital of Karnataka and the center of India's IT sector, has been the perfect place for this study because it is populated by people from all over the country, representing a diverse spectrum of educational and cultural backgrounds. Bengaluru has accounted for roughly 47% of the cybercrime instances recorded from our nation's metro areas, according to data from the National Crime Records Bureau (NCRB). Therefore, the majority of internet users have either been victims of cybercrime or are intimately connected to people who have been victims of cybercrime, as cybercrimes are on the rise and about half of instances originate from Bengaluru. The research has selected this city for the study based on these criteria.

3.1 Research methodology

According to the literature review, investing in system and network security has become more significant, and cyber insurance is essential for controlling cyber risks. In order to prevent system compromise and lower risk, insurance companies look for companies with strong network security. A number of models and frameworks have been proposed to illustrate how cyber insurance may be a way to protect the system against online threats. According to all of these studies, the market for cyber insurance is enormous and is expected to grow even faster in the years to come. However, not enough research has been done on cyber risk exposures and how to evaluate them in relation to the organization's financial liability. Since there is no historical data on the frequency, type, and financial loss—information that is essential for determining premiums—insurance firms are reluctant to offer policies that cover these risks. The study aims to supplement previous research by creating a model based on the evaluation of operating system risk exposures and how they affect the firm's financial obligation. The study's conclusions will help actuaries estimate premiums

3.2 Data Collection

Data for this study was gathered from 389 internet users in Bengaluru using a straightforward random sample technique. To get their answers, the respondents were contacted directly via phone calls and mail. Both physical forms and Google Forms were used to administer the questionnaire. To get their answers, the link was distributed by email and social media. The option to complete the questionnaire whenever it was most convenient for them was provided to the respondents. The researcher gathered information from Statistia.Com, which provided the trend of rising cybercrimes in India over the past ten years, and the National Crime Records Bureau (NCRB), which provided the number of cybercrime cases in India. Furthermore, information from secondary sources has been gathered to fulfill the study need for comprehending cyber dangers.

3.3 Sample Design

The respondents in this survey are people from Bengaluru who use the internet for all of their communication needs and conduct the majority of their everyday activities online.

4. EXPERIMENTAL RESULTS

This study uses exploratory factor analysis (EFA) in its multivariate analysis to identify the factors impacting internet users' attitude toward cyber risks, experience with cyber hazards, readiness to manage cyber risks, and online activity. Confirmatory Factor Analysis (CFA) determines Construct Reliability (CR), Average Variance Extracted (AVE), and Discriminant Validity (DV) in relation to cyber risk awareness, experience, readiness to manage cyber risks, attitude toward cyber risks, and online behavior. Determine the connections between their online behavior and their understanding of, familiarity with, preparedness for handling, and attitude toward cyberthreats using the structural equation model (SEM). 48 items were added to the poll in order to measure how people become ready to manage cyber hazards. The purpose of the factor analysis was to reduce these numerous components to a small number of primary ones.

4.1 Statistical Tool Application

Descriptive statistics have employed frequency and percentile, and the results are displayed in the form of tables and figures. b. Statistics for Inference: The hypotheses put out for the current study have been tested using both bi-variate and multi-variate techniques. c. The association between awareness, readiness, experience, online behavior, and attitude about cyber dangers and variables such as gender, income, and qualifications was examined using the t-test. ANOVA was used to look at the relationship between age and occupation and cyber risk awareness, readiness, experience, online behavior, and attitude. The statistical association between people's online behavior, attitudes toward cyber risks, willingness to manage cyber risks, experience with cyber risks, and awareness of cyber risks was ascertained by regression analysis.

4.2 Statistical Analysis

Based on the previously evaluated literature, the study's conclusions have been analyzed. We start the chapter by examining the demographic factors before moving on to the variables that have been examined in the study, including awareness of cyber risks, attitude toward cyber risks, online behavior of individuals, readiness to handle cyber risks, and the experience of an individual with cyber risks. The study's goals are to identify different cyber risk exposures and evaluate the factors that affect a person's readiness to manage cyber hazards. To collect the data, a structured questionnaire was created and administered. The data was then categorized and tabulated to continue the research. Respondents from Bengaluru City, who were people who use the internet every day for a variety of reasons, were given the questionnaire.

Table 1: Awareness of cyber risks

Cyber Risks and Appropriate Actions	Strongly Agree		Agree		Neutral		Disagree		Strongly Disagree	
	Count	%	Count	%	Count	%	Count	%	Count	%
There are risks concerned whenever I am at work online	95	24.7	197	48.1	85	18.6	5	1.0	3	0.6
It is all the time advisable to register in as a user instead than an administrator whenever going online.	67	17.4	226	55.2	78	17.0	12	2.5	2	0.4
Utilizing the same passcode for various accounts carries no risk.	67	17.4	80	19.5	78	17.0	86	18.1	74	15.5
I must frequently or routinely change my password.	180	46.8	108	26.4	64	14.0	22	4.6	11	2.3
Any passwords I use needs to be at minimum eight characters long and should contain a mix of letters, numbers, and symbols.	210	54.5	114	27.8	42	9.2	12	2.5	7	1.5
I am aware of the different computer crimes I could potentially encounter when working online.	112	29.1	205	50.0	57	12.5	9	1.9	2	0.4

Table 1 illustrates the respondents' awareness of a variety of cyber risks, such as the dangers of working online, the need to log in as a user rather than an administrator when online, the dangers of using the same code word for multiple accounts, the dangers of not changing passwords frequently, the dangers of not using appropriate characters, numbers, and special characters to strengthen passwords, and the various crimes and risks we face when using the internet. According to the table, the majority of respondents (292) strongly agree or agree that there are risks of cybercrimes when using the internet, while 85 respondents are neutral about the statement. Only 8 respondents disagree or strongly disagree with the statement that there

are risks when using the internet.

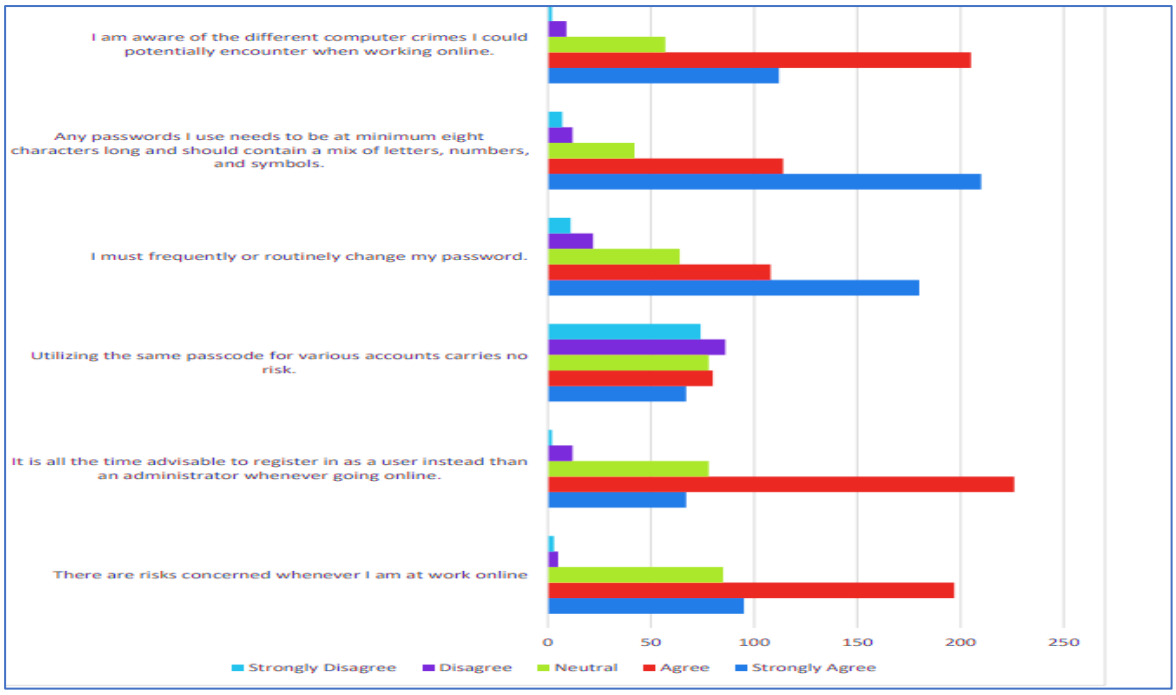

Figure 1: Awareness of Cyber Risks

In order to determine the respondents' readiness to manage cyber threats, the study asked them a number of questions on their readiness to do so. This was one of the primary topics of the investigation. We can gain an understanding of this from the tables and data provided below.

Table 2: Preparedness to handle cyber risks

Preparedness to Handle Cyber Risks	Strongly Agree		Agree		Neutral		Disagree		Strongly Disagree	
	Count	%	Count	%	Count	%	Count	%	Count	%
On my PC,Iought to only have authentic operating systems installed.	136	35.1	176	45.5	65	16.9	9	2.1	3	0.5
Antivirus and firewall software should be required for my personal PC.	184	47.5	158	40.8	39	10.1	4	0.8	4	0.8
I should always update my PC's operating system and antivirus software.	161	41.6	158	40.8	51	13.2	13	3.1	6	1.3
Another type of protection programme should be added to my computer in addition to the antivirus	73	18.7	150	38.7	131	34.0	26	6.5	9	2.1
software already there.										
At the very least once every week, I should run a full system virus protection scan on my computer.	130	33.5	153	39.5	85	22.1	16	3.9	5	1.0
I must regularly back up my files to prevent data loss in the event of a computer crash.	169	43.6	151	39.0	43	11.2	22	5.5	4	0.8

The study's third component looked at how equipped the respondents were to deal with cyber dangers. It has been said that the battle is half won if you are ready to take a chance. Only 12 respondents disagreed with the assertion that they should only have a legitimate working system installed on their PC, while 312 respondents agreed with it, and 65 respondents had a neutral opinion. This demonstrated that some people still need to make sure they're using the original operating system

instead of a pirated one. The study's conclusions have been examined in light of the previously reviewed literature. We start the chapter by examining the demographic factors before moving on to the variables that have been examined in the study, including awareness of cyber risks, attitude toward cyber risks, online behavior of individuals, readiness to handle cyber risks, and the experience of an individual with cyber risks. The study's goals are to identify different cyber risk exposures and evaluate the factors that affect a person's readiness to manage cyber hazards. To collect the data, a structured questionnaire was created and administered. The data was then categorized and tabulated to continue the research. Respondents from Bengaluru City, who were people who use the internet every day for a variety of reasons, were given the questionnaire.

5. CONCLUSIONS

Due to the rapidly evolving technology, the digitalization of the economy, and the fact that e-commerce and online marketing are now a part of life, cyber risks are the main risk that many people are currently facing. Cybercrime is a generic phrase that refers to an illegal or data breach or any immoral conduct that is committed with the use of a computer which is used as a tool to commit the crime or is the target point of the attach through the internet. Computers, mobile phones, and the Online world have become an integral part of our daily lives in the age of globalization. As a result, online processing data is made accessible over the internet, introducing new dangers in the form of cybercrime. Such risks not only have various expressions, but also differ in their execution methods, making it challenging for cyber professionals to find an effective solution. Because of the high rate of threats, governments around the world have become particularly worried about their citizens' online safety and have enacted a number of parliamentary acts and International Instruments. The information compiled indicates that India has a high percentage of cybercrime, but the numbers do not differentiate between the varied types of cybercrime. However, previous studies in India and around the world show that there are various kinds of illegal activity carried out by using computers and other related devices with a Connection to the internet. Hence this study has been carried out to ensure preparedness of individuals to handle cyber risks.

REFERENCES

[1] Kwon J, Johnson ME. Healthcare security strategies for regulatory compliance and data security. In2013 46th Hawaii International Conference on System Sciences 2013 Jan 7 (pp. 3972-3981). IEEE. https://doi.org/10.1109/HICSS.2013.246

[2] Kelly B, Quinn C, Lawlor A, Killeen R, Burrell J. Cybersecurity in Healthcare. Trends of Artificial Intelligence and Big Data for E-Health. 2023 Jan 2:213-31. https://doi.org/10.1007/978-3-031-11199-0_11

[3] Majid UMA, Atan NA, Rukli R, Khan A. Framework of computer science learning through hybrid service-learning oriented visual toward the continuum of visualization thinking and generic skills. Indian J Inf Sour Serv. 2024;14(3):192-206. https://doi.org/10.51983/ijiss-2024.14.3.25

[4] Thomasian NM, Adashi EY. Cybersecurity in the internet of medical things. Health Policy and Technology. 2021 Sep 1;10(3):100549. https://doi.org/10.1016/j.hlpt.2021.100549

[5] Aziz B. A note on the problem of semantic interpretation agreement in steganographic communications. Journal of Internet Services and Information Security. 2021 Aug 31;11(3):47-57. https://doi.org/10.22667/JISIS.2021.08.31.047

[6] Lechner NH. An overview of cybersecurity regulations and standards for medical device software. InCentral European Conference on Information and Intelligent Systems 2017 (pp. 237-249). Faculty of Organization and Informatics Varazdin.

[7] Caviglione L, Wendzel S, Mileva A, Vrhovec S. Guest Editorial: Multidisciplinary Solutions to Modern Cybersecurity Challenges. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl. 2021 Dec;12(4):1-3.

[8] Anderson S, Williams T. Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge?. Computer Standards & Interfaces. 2018 Feb 1; 56:134-43. https://doi.org/10.1016/j.csi.2017.10.001

[9] Sharma N, Rajput A. Development of a Genomic-based Predictive Model for Warfarin Dosing. Clinical Journal for Medicine, Health and Pharmacy. 2024 Jun 28;2(2):11-9.

[10] Marotta A, Madnick S. Cybersecurity as a unifying factor for privacy, compliance and trust: The Haga Hospital case. Issues in Information Systems. 2022 Jan 1;23(1). https://doi.org/10.48009/1_iis_2022_108

[11] Saranya N, Geetha K, Rajan C. Data replication in mobile edge computing systems to reduce latency in internet of things. Wireless Personal Communications. 2020 Jun;112(4):2643-62. https://doi.org/10.1007/s11277-020-07168-7

[12] Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, Bonacina S. Influence of

human factors on cyber security within healthcare organisations: A systematic review. Sensors. 2021 Jul 28;21(15):5119. https://doi.org/10.3390/s21155119

[13] Lee CD, Ho KI, Lee WB. A novel key management solution for reinforcing compliance with HIPAA privacy/security regulations. IEEE Transactions on Information Technology in Biomedicine. 2011 May 12;15(4):550-6. https://doi.org/10.1109/TITB.2011.2154363

[14] Abraham C, Chatterjee D, Sims RR. Muddling through cybersecurity: Insights from the US healthcare industry. Business horizons. 2019 Jul 1;62(4):539-48. https://doi.org/10.1016/j.bushor.2019.03.010

[15] Udayakumar R, Pansambal SY, Gajmal YM, Vimal VR, Sugumar R. User Activity Analysis Via Network Traffic Using DNN and Optimized Federated Learning based Privacy Preserving Method in Mobile Wireless Networks.

[16] Busdicker M, Upendra P. The role of healthcare technology management in facilitating medical device cybersecurity. Biomedical Instrumentation & Technology. 2017 Nov;51(s6):19-25. https://doi.org/10.2345/0899-8205-51.s6.19