International Journal of Research in Engineering, Science and Management
Volume 6, Issue 5, May 2023
https://www.ijresm.com | ISSN (Online): 2581-5792

Main Determinant Factors of Cyber Crime – A Case Study for Online Business in Punjab

Sahil Baghla[1*], Kamalpreet Kaur[2]

[1]*Research Scholar, Department of Management, CT University, Ludhiana, India*

[2]*Assistant Professor, Department of Management, CT University, Ludhiana, India*

***Abstract*: In modern society, the role of IT information and computer systems in the use of the Internet is essential and well-recognised. Many businesses from small to big get benefited from the development of networking and cyberspace to prevent cybercrime. This kind of development in Punjab concerning unethical activity online creates legal issues. Cybercrimes impact the many businesses by damaging their customers' data and operating systems online and also hamper the financial condition of the company. Such incidents lead to significant reputational damage and large-scale cyber-attacks on the company's brand equity in the trading market. As a result, it reduces the institutional trust drop in the market value. Therefore, cybercrime in India constantly rising and many businesses increase the cyber security costs to handle this unfortunate situation and reduce fraud cases. The study covers the cyber security determinants and how it affects business in Punjab. The research study shaded light on the ways in which the company can prevent this cybercrime during their online business operation.**

***Keywords*: cybercriminal behaviour, cybercrime investigation, cyber security, cyber security cost, cyber security cell in Punjab, determinants, government campaign, online business in Punjab, toll-free number.**

1. Introduction

Cybercrime is an evolving form of digitalisation that is mainly transnational crime in recent times. Cybercrime has a complex nature that takes place in the borderless realm of cyberspace by the increasing involvement of the crime group. In recent times, the Global economic crime survey reported that cybercrime is ranked one of the four economic crimes globally that affect many businesses. In the new digitalisation period as the economy increases based on the internet as a result it is exposed to all threats which are possessed by cybercriminals. Cybercriminals often use computers and do hacking, spamming and phishing. It totally does so remotely with the use of a certain application. This research study evaluates cybercrime and its main determining factors that contribute to the legal problem. Also, this research study considers different ways to overcome server crime in the online business of Punjab so that it can combat this issue in present-day internet uses and applications.

2. Literature Review

According to the Tribune News Service, (2023), Chandigarh witnessed an increasing criminalisation of daily business life with information technology that indicates a case of cyber fraud. It has increased four times in Punjab during the past year, from 24 in 2020 to 21. In recent years the number has reached 98 in 2021-2022. This data is enlisted on the complaints register on the national helpline. The service provides the reply by Electronics and Information Technology Minister Ashwani Vaishnav to a query by Member of Parliament Sanjay Haribhau during the Question Hour in Lok Sabha (Tribune India, 2023). The newspaper also forecast that the IG of Cybercrime RK Jaiswal said that this kind of criminal activity typically uses my computer network to generate financial profits by hacking the data or harming the computer programming which is proudly covered by the cybercrime. As well as there are many events where cybercrime increases the spread of wrong information or distorted image to alter the truth in the case of online business processes. This kind of unethical activity involves infecting computers with viruses to spread to interlink computers which gastrically affects the businesses and their operation that lead to a negative downfall of their sales.

It also leads to the increasing number of police records so that people are more aware of cyber fraud. From the Police Ministry department, different warning messages were promoted and different kinds of TV advertisements showing to increase awareness among the mass media. Earlier many of the victims passed their personal details to the cyber-criminal. They flash on their computer with the wrong information but now the police department carefully handles this. This kind of public awareness increases through variant promotional activity so that the UN individual cannot pass their personal information without verifying the seeker. The Punjab Police Department organized a portal for cybercrime that links to the National Cyber Crime Reporting Portal so that it takes cautious steps to prevent cybercrime against the online business process.

According to the Hindustan Times news article, (2022), It is seen that with the rise of online financial fraud cases in Punjab the cyber security cell of the Punjab police has launched a toll-free helpline number. There is a well-equipped and trained cyber team that works the whole day to save hard-earned money for online businesses. The Punjab DGP introduced a new helpline number that was replaced by the Union Home Ministry under the citizen Financial Cyber Fraud Reporting and

[*] Corresponding author: sahil.baghla@gmail.com

Management System (Hindustantimes, 2022). In 2019 many companies lost nearly 1.8 billion to cybercrime. Many companies massively represent their products and operation service online heavily target by these criminals which lead to a loss in their Financial Service, Technology, energy and manufacturing sector.

As per Datta *et al.* (2020) view, the development of technology and advancement of the technological solution with the use of the internet creates a significant cybercrime that is a real threat to society in recent times globally. Cybercrime in India is exponentially rising and this kind of offence is related to the Information Technology Act 2000 which is further amended by the IT Amended Act 2008. Phishing and denial of service attract (DOS) other most popular types of Cybercrime in India that increase online harassment and leak the sensitive information of the business. The crime investing branch of Punjab established many cyber-crime cells that take care of different reports and investigations of the cyber offences which significantly damage the online business procedure. FIR for a cybercrime is the first step to getting a solution from these offences and the businesses can also approach the Commissioner of the Punjab Judicial Magistrate.

As per Kethineni, (2020) opinion, with the cyber-attack the company lost their reputational value and customer trust to not control the customer data which led to a settlement claim to pay a million bucks. For instance, in 2010 hackers sympathetic to WikiLeaks fought back against credit card gents Visa and master cards by arranging attacks that caused temporary crashes of their websites.

3. Methodology

In this research study, the methodology plays a huge role that is associated with the current digitalisation issues. Also, the study significantly aligns with the research topic with the help of prominent justification which leads to the research paper's success and transparency. This research methodology maintains different policies and criteria to increase the research journal's validity and authenticity so that it makes a reliable approach to its consumers. This research methodology chooses the positivist research philosophy which draws the different evidence closely so that it significantly evaluates the cyber security determinants and how they affect the businesses in Punjab. The researcher also selects the deductive research approach to create a strong framework so that it progresses with different ethical information regarding the cyber security costs in which the business can prevent the cyber-attack on the online business operating side.

The qualitative research strategy in the methodology part is widely chosen which especially helps to avoid cyberstalking to keep a low profile, high internet protocol, maintaining good digital hygiene and updating the antivirus program to save the sensitive information of the consumer. Social engineering attack is another cybercrime that leaks customer personnel information such as account numbers, PAN cards and Aadhar card numbers. Some common forms of digital social engineering cyber-attacks are vishing, water holing and baiting (Kagita *et al.* 2022). ATM cloning and privacy is another attack that is popular in recent times. Privacy is the kind of unauthorized cropping of some business data from the license users then the cybercriminal supplies it to other people. It creates a problem in an official product that leads to mistrust in the consumer and people do not agree to spend their money on the company's services.

This kind of secondary data and qualitative research strategy helps the researcher to collect the reliable information from different online news articles and online journals so that he can make the proper interpretation flexibly. In this way, the researcher can obtain authenticity and transparency in his research work the dynamically approaching the different aspects of the cyber security program in Punjab (Kethineni, 2020). It significantly promotes the awareness that the mass media and different investigation and complaint lodging information create opportunities for businesses in Punjab so that the management team can take successful financial decisions regarding its cyber security.

4. Result and Analysis

In the table 1, a frequency table of total number of gender who have participated in the survey has been represented. From the above frequency table, it has been observed that about 50.2% of males have participated. On the other hand, 47% are female participants and 2.8% of the participants have selected the option of 'prefer not to say'.

The table 2 shows a frequency table of the ages of the participants. It appears that 277 participants are in the age range of 18 to 25 years. On the other hand, 97 participants are between the age of 26 to 35 years. In addition, it has been analysed that 98 participants are in the age group of 36 to 45yaers. On the

Table 1
Analysis based on gender factor

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	251	50.2	50.2	50.2
	Female	235	47	47	97.2
	Prefer not to say	14	2.8	2.8	100
	Total	500	100	100	

Table 2
Analysis based on age factor

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-25 years	277	55.4	55.4	55.4
	26-35 years	97	19.4	19.4	74.8
	36-45 years	98	19.6	19.6	94.4
	46-60 years	28	5.6	5.6	100
	Total	500	100	100	

contrary, 28 participants belonged to 46 to 60 years age group.

In table 3, a frequency table of region or area from which the participants belong has been represented. It has been observed that 150 participants belong to Ludhiana and 150 participants belong to Jalandhar. On the other hand, 100 participants belong to Mohali and 100 participants belong to Bathinda.

Table 3
Analysis based on region belong

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ludhiana	150	30	30	30
	Jalandhar	150	30	30	60
	Mohali	100	20	20	80
	Bathinda	100	20	20	100
	Total	500	100	100	

Table 4
Descriptive analysis

	N	Minimum	Maximum	Mean	Std. Deviation
Gender	500	1	3	1.53	0.553
Age	500	1	4	1.754	0.9567
Belong Area	500	1	4	2.3	1.101
Cybercrime	500	1	2	1.21	0.405
Phishing Scam	500	1	5	1.66	1.181
Ransomware and Malware	500	1	5	1.79	1.091
Inadequate Cybersecurity Measures	500	1	5	1.79	1.091
Weak Passwords and Insecure Systems	500	1	3	1.35	0.636
Lack of Proper Training and Education on Cybersecurity	500	1	5	1.79	1.088
Use of Pirated Software and Unsecured Networks	500	1	5	1.3	0.841
Lack of regular updates and patches	500	1	5	1.81	1.11
Business transactions	500	1	5	1.63	1.035
Strong passwords	500	1	5	1.69	1.215
Firewalls	500	1	5	1.65	1.12
Endpoint protection	500	1	5	1.77	1.255
Knowledgeable about cybercrime	500	1	3	1.37	0.588
Business suffered cybercrime	500	1	2	1.25	0.433
Business place prevent cybercrime	500	1	4	1.96	0.962
Business conduct employee training cybercrime prevention	500	1	4	2.15	0.922
Business ability prevent cybercrime	500	1	3	1.91	0.686
Phishing attempt	500	1	2	1.26	0.438
Pirated software business	500	1	2	1.17	0.376
Software used business	500	1	3	1.65	0.808
Passwords used business sensitive accounts	500	1	3	1.55	0.704
Fallen phishing attempt	500	1	2	1.33	0.471
Change passwords used business	500	1	3	1.79	0.833
Backup data used business	500	1	3	1.69	0.755
Knowledgeable employees cybercrime prevention	500	1	3	1.75	0.729
Awareness campaigns cybercrime prevention beneficial businesses	500	1	2	1.32	0.468
Government industry work together prevent cybercrime online business community	500	1	4	2.68	1.194
Valid N (listwise)	500				

Table 5
One-Sample T-Test

	Test Value = 0					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Strong passwords	31.141	499	0	1.692	1.59	1.8
Firewalls	32.947	499	0	1.65	1.55	1.75
Endpoint protection	31.472	499	0	1.766	1.66	1.88
Knowledgeable about cybercrime	52.059	499	0	1.368	1.32	1.42
Business suffered cybercrime	64.485	499	0	1.25	1.21	1.29
Business place prevent cybercrime	45.496	499	0	1.958	1.87	2.04
Business conduct employee training cybercrime prevention	52.036	499	0	2.146	2.06	2.23
Business ability prevent cybercrime	62.16	499	0	1.906	1.85	1.97
Phishing attempt	64.227	499	0	1.258	1.22	1.3
Pirated software business	69.578	499	0	1.17	1.14	1.2
Software used business	45.664	499	0	1.65	1.58	1.72
Passwords used business sensitive accounts	49.336	499	0	1.554	1.49	1.62
Fallen phishing attempt	63.183	499	0	1.332	1.29	1.37
Change passwords used business	48.095	499	0	1.792	1.72	1.87
Backup data used business	50.194	499	0	1.694	1.63	1.76
Knowledgeable employees cybercrime prevention	53.733	499	0	1.752	1.69	1.82
Awareness campaigns cybercrime prevention beneficial businesses	63.196	499	0	1.324	1.28	1.37
Government industry work together prevent cybercrime online business community	50.211	499	0	2.68	2.58	2.78

In table 4, descriptive statistics have been highlighted by considering the independent and dependent variables. The skewness value for the "gender" variable is 0.396, indicating that the data is evenly distributed within the dataset. As the skewness value lies between the ranges from +1 to -1, therefore, it can be said that the data for this particular variable is reliable and valid as well as can be considered for further statistical analysis.

It has been identified that "business ability to prevent cyber-crime" has a greater t-value as compared to its critical value. Therefore, from these findings, it can be summarised that in case of H1 the null hypotheses can be rejected. On the other hand, "strong passwords", "firewalls" and "endpoint protection" have a greater value as compared to their critical

Table 6
Correlation analysis

		Change passwords used business	Backup data used business	Knowledgeable employees cybercrime prevention	Awareness campaigns cybercrime prevention beneficial businesses	Government industry work together prevent cybercrime online business community
Business transactions	Pearson Correlation	-.262**	-.231**	-.115*	-.317**	-0.043
	Sig. (2-tailed)	0	0	0.01	0	0.337
	N	500	500	500	500	500
Strong passwords	Pearson Correlation	-.248**	-.239**	-.190**	-.169**	-.385**
	Sig. (2-tailed)	0	0	0	0	0
	N	500	500	500	500	500
Firewalls	Pearson Correlation	-.360**	-.321**	-.379**	-.230**	-.436**
	Sig. (2-tailed)	0	0	0	0	0
	N	500	500	500	500	500
Endpoint protection	Pearson Correlation	-.397**	-.410**	-.351**	-.249**	-.326**
	Sig. (2-tailed)	0	0	0	0	0
	N	500	500	500	500	500
Phishing attempt	Pearson Correlation	.856**	.779**	.741**	.852**	.653**
	Sig. (2-tailed)	0	0	0	0	0
	N	500	500	500	500	500
Pirated software business	Pearson Correlation	.657**	.784**	.775**	.654**	.501**
	Sig. (2-tailed)	0	0	0	0	0
	N	500	500	500	500	500
Software used business	Pearson Correlation	.910**	.912**	.859**	.861**	.786**
	Sig. (2-tailed)	0	0	0	0	0
	N	500	500	500	500	500
Passwords used business sensitive accounts	Pearson Correlation	.859**	.889**	.846**	.815**	.760**
	Sig. (2-tailed)	0	0	0	0	0
	N	500	500	500	500	500
	N	500	500	500	500	500

Table 8
Chi-Square test

Backup data used business		**Value**	**df**	**Asymp. Sig. (2-sided)**
Rarely	Pearson Chi-Square	.^{b}		
	N of Valid Cases	242		
Occasionally	Pearson Chi-Square	55.586^{c}	2	0
	Likelihood Ratio	68.759	2	0
	Linear-by-Linear Association	49.619	1	0
	N of Valid Cases	169		
Regularly	Pearson Chi-Square	.^{b}		
	N of Valid Cases	89		
Total	Pearson Chi-Square	547.414^{a}	6	0
	Likelihood /Ratio	640.827	6	0
	Linear-by-Linear Association	384.663	1	0
	N of Valid Cases	500		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 8.48.
b. No statistics are computed because software_used_business is a constant.
c. 0 cells (.0%) have expected count less than 5. The minimum expected count is 5.23.

values. Considering this, it can be stated that in terms of H2, the null hypothesis is rejected.

Table 7
Cronbach's Alpha

Reliability Statistics	
Cronbach's Alpha	N of Items
0.758	30

The correlation between different variables has been shown. From the above analysis, it can be identified that cybercrime and phishing scam has a negative correlation as the observed value of cybercrime is 1 and phishing scam is -0.241. Therefore, it can be said that in case the value of variable is positive then it can be stated that there is a positive correlation between the independent variable and dependent variable.

It has been observed that the Cronbach's alpha score of 0.758 for a scale or survey instrument with n=12 items suggests that the scale or instrument has moderate to good internal consistency or reliability. A Cronbach's alpha score falls on a scale from 0 to 1, with higher values indicating higher reliability. A score of 0.7 or above is generally considered to be good, while a score below 0.7 may indicate that the scale or instrument is not measuring a single underlying construct and may be unreliable.

In table 8, the Chi-square test has been performed considering an independent variable that ransomware and malware. It can be observed that Phi value is 0.600. On the other hand, it has been identified that the Cramer's value is 0.600.

An R-value of 0.652 suggests a moderate to strong positive linear relationship between the predictors and the dependent variable. A value of 0.652 means that about 65.2% of the variance in "Cybercrime" can be explained by the predictors in the model. A significant value of .000b means that the relationship is statistically significant and unlikely to have occurred by chance. In this case, the F-value of 40.442 suggests that the model fits the data well. Based on the significant value of the regression analysis both two null hypotheses of this study can be rejected. Therefore, it can be said that alternative hypotheses can be accepted based on the regression test which states inadequate cybersecurity measures, ransomware and malware attacks, phishing attacks, weak passwords, lack of proper training, use of pirated software and lack of regular software updates are the main determinant factors of cyber-crime in online businesses in Punjab.

In terms of cyber security attacks in Punjab, this research reveals that it has a very negative relation to Punjab business. In India Punjab is the most vulnerable state, witnessing near about 98 cases per year of cyber-attacks and it is consistently rising so the huge access to the information technology and the internet in online business operations. Additionally, this research report is based on a large amount of authentic data that gives an effective result that aligns with the research topic and the researcher illustrates different statistical tests which are related to the qualitative research modes. Therefore, cybercrime hampering the business to date and stealing customer status online and increasing the vulnerable situation. The businesses are tackling the cyber security cost in the form of higher prices to the consumer which disbalances the total business systems and affects their profit and sales margin (Ch *et al.* 2020). Newly 6% of the company reported the control of critical IT Systems to handle the cyber-attack which severely disrupted the operational systems and altered the business practice.

5. Discussion

Cyber security increases product cause and the IT software department prevents criminals from exiting the company's private and authentic data. With the help of cyber security technology and expertise the company paid more to prevent victims of an attack as a result its damaged cyber security regulation and increased operational transparency. Cybercrime is progressing with the help of vast fields of technology and

Table 9
ANOVA test

	Model	Sum of Squares	df	Mean Square	F	Sig.
1	Regression	34.73	10	3.473	36.094	.000[b]
	Residual	47.052	489	0.096		
	Total	81.782	499			

a. Dependent Variable: Cybercrime
b. Predictors: (Constant), pirated software business, Strong passwords, Business transactions, Lack of regular updates and patches, knowledgeable about cybercrime, business suffered cybercrime, business conduct employee training cybercrime prevention, business ability prevent cybercrime, business place prevent cybercrime, phishing attempt

Table 10
Coefficients

	Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.491	0.087		17.069	0
	Lack of regular updates and patches	0.071	0.019	0.196	3.786	0
	Business transactions	-0.09	0.015	-0.23	-6.121	0
	Strong passwords	0.121	0.013	0.364	9.19	0
	Knowledgeable about cybercrime	-0.098	0.065	-0.143	-1.518	0.13
	Business suffered cybercrime	-0.008	0.164	-0.009	-0.051	0.959
	Business place prevent cybercrime	0.265	0.045	0.631	5.888	0
	Business conduct employee training cybercrime prevention	-0.183	0.047	-0.417	-3.862	0
	Business ability prevent cybercrime	0.031	0.061	0.052	0.502	0.616
	Phishing attempt	-0.279	0.164	-0.302	-1.704	0.089
	Pirated software business	-0.138	0.079	-0.129	-1.757	0.08

a. Dependent Variable: Cybercrime

communication technology. That is a major category of cyber-crimes that happened in the form of cyber defamation and harassment that significantly lead to an adverse situation. It has a negative impact on the economic downturn and creates financial crises as well as potentially lead to cyber harm in the online business process which is a growing problem and recent times with the help of the internet or computer (Chudasama *et al.* 2020). The second category of cybercrime is a crime against property such as intellectual property including software piracy, illegal copy of a program, credit card fraud, copyright infringement and trademark violation.

6. Conclusion

From the above discussion, it can be concluded that cybercrime is the most critical problem in the digitalisation business period that altered the business practice to hack customers' financial and personal information. As a result, it attacks not only the online business operation in Punjab but also threatens many individuals' financial property. Punjab DGP is vocal regarding it adequate to protect against cyber-attacks so that it patronizes the business and gives safety from the temporarily crashed website.

References

[1] Ch, R., Gadekallu, T.R., Abidi, M.H. and Al-Ahmari, A., 2020. Computational system to classify cyber-crime offenses using machine learning. *Sustainability*, *12*(10), p. 4087.

[2] Chudasama, D., Patel, D., Shah, A. and Shaikh, N., 2020. Research on Cybercrime and its Policing. *American Journal of Computer Science and Engineering Survey*, *8*(10), p. 14.

[3] Datta, P., Panda, S.N., Tanwar, S. and Kaushal, R.K., 2020, March. A technical review report on cyber-crimes in India. In *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)* (pp. 269-275).

[4] Hindustan Times, (2022). Punjab: Call 1930 to report cyber frauds. Available at: https://www.hindustantimes.com/cities/chandigarh-news/punjab-call-1930-to-report-cyber-frauds-101649252022820.html [Accessed on 6 May 2023]

[5] Kagita, M.K., Thilakarathne, N., Gadekallu, T.R., Maddikunta, P.K.R. and Singh, S., 2022. A review on cyber-crimes on the internet of things. *Deep Learning for Security and Privacy Preservation in IoT*, pp. 83-98.

[6] Kethineni, S., 2020. Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pp. 305-326.

[7] Shah, R., 2019. Cyber Crimes in India: Trends and Prevention. *International Journal of Research and Analytical Reviews (IJRAR)*, *6*(1).

[8] Tribune India, (2023). Cybercrime up 4 times in Punjab in a year. Available at: https://www.tribuneindia.com/news/punjab/cybercrime-up-4-times-in-punjab-in-a-year-418577 [Accessed on 6 May 2023].