Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021: 5466 - 5482

Research Article

COVID – 19 and Cyber Crimes: Developing Insights by Qualitative Inquiry of Global Cases

Aastha Verma

Assistant Professor, Department of Management Studies, Netaji Subhas University of Technology
Email – aastha.verma@nsut.ac.in

Abstract

The Internet has renovated the way business is done in India. This is especially true in the current pandemic scenario. COVID -19 has increased the dependence of business on digital mode. E – Commerce is growing like never before. Indian e-commerce market is predicted to grow to US$ 200 billion by 2026 from US$ 38.5 billion as of now. This may be attributed to increasing internet and smartphone penetration. At the same time there are many security concerns involved in E-Commerce system posing threat to both buyer and the merchant. Cyber safety has become a constant and mounting issue as new Internet-based technologies and applications are developed. Therefore, the present paper makes a qualitative attempt to prepare a guiding framework to deal with possible security threats and for achieving the same, this paper investigates a number of case studies at globe level. A detailed combined analysis of all the cases synthesizes a suggestive guiding framework for the customers, merchants, researchers and policy makers. In order to investigate the big literature (*Case Studies*), this research uses qualitative data analysis software for generating a protection framework. This helps on going digital businesses and is potent to avert a security threat.

Keywords: Cybercrime, Case Studies, Qualitative Research, Word Cloud, Word Tree, Single case model.

1. Introduction

The COVID – 19 pandemic has accelerated digital transformation of business. In an attempt to preserve the revenue, flow many firms adopted digital business models (OCED, 2020). We have entered in a new phase of globalization driven by digital connectivity. The flow of data and information is paving the way to a much greater global connectedness than attained by any other driver of globalization. As per a report of Mc Kinsey 2017 this connectivity with respect to e-commerce and growth of new digital platforms means consumers are less restricted by physical borders than ever, and they are happily shopping across national lines. Moreover, with the onslaught of COVID pandemic customers feel safer in shopping online. However, one of the major issues surrounding the electronically enabled business transactions today is of security and privacy. The manner in which cyber-criminal flow through their target networks is very similar to how a virus such as Covid-19 flows through the human body (Scroxton, 2020). Further, Increased reliance on digital technology to grow business is marred by security threats. This is one of the main and ongoing concerns that deter customers and organizations to engage in digital transactions. The safety in digital operation is the central issues in an E-commerce transaction (Wen and Zhou 2008). Web applications tend to assimilate other-party services. The assimilation put forth new security challenges due to the complicacy of an application which coordinate its component service with web clients through the internet. A potent barrier to internet buying over the coming years will be the burgeoning danger of cybercrimes, and a crime always has a negative effect on commercial growth. There are many types of scams customers face in an online transaction, a commonly occurring fraud is called the merchandise scam which takes place when a consumer purchases a product through internet using mobile or laptop. In this case a customer places the order but the product is never delivered. Another common type of fraud which frequently occurs online is Credit card fraud, in this type of fraud credit card information is stolen and used fraudulently for online purchase (Segal et. al. 2011). In another scam, scammers send an email to customers which channelize them to a spoof website which prompt them to divulge their financial information for purchase. Sometimes customers are persuaded to divulge their date of birth, driver's license number, debit card number etc. Cyber fraud hampers both customers and organizations. The information database of the companies becomes victim (Berkowitz, 2003). The aim of this study is to explore all the important cases occurred globally where digital security was compromised resulting into loss of customers, money, data, goodwill etc. so that a collective learning lead to creation of a protective framework potent in averting future e – commerce crimes. Along with manual examination of cases this research employs the use of qualitative data analysis software– MAXQDA Analytics Pro 2020 for handling the (big literature) cases. As stated by Verma (2021) – "Qualitative research has been greatly advanced with the development of qualitative analysis software, it allows more extensive and comprehensive review of big literature free from human bias and other limitations".

1. Theoretical Background

Business Standard, 2021 highlights a report by Data Security Council of India (DSCI) mentioning that Covid-19 pandemic forces consumers to opt for digital payments leading to a rapid rise in cybercrimes such as web-skimming, malware campaigns and phishing scams in the country. This shatters the trust of a consumer in digital transactions ultimately resulting in decreased organizational revenue. Researchers and corporations involved in e – commerce either for research or business, over the years have created a list of characteristics that defines the trust of a consumer in online transactions (Cassell and Bickmore, 2000; Friedman et al., 2000; Urban et al., 2000). One widely quoted study recognized 6 features of a Web portal which augment consumer perceptions of trust in online transactions (Cheskin and SA, 1999). These features are as following: (1) Safety assurance (2) The organizations' status (3) Easy interface (4) On time order delivery (5) Expertise (6) Design of website. Beyond capturing these important Web features, authors argued that "the first and most essential step in forming consumer trust is providing assurances that the consumers personal information will be protected". Other authors working in same domain strengthened this belief asserting that "only after security concerns have been addressed, consumers consider other web features as important" (Dayal et al., 1999; Hoffman et al., 1999; Ovans, 1999).

An online safety threat has been explained as a "circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service fraud and abuse" (Kalakota and Whinston, 1996). Security is the safety against such dangers. These are characterized by attack on network and data or by unauthorized access by fake confirmation. Safety in Business - to - consumer electronic commerce depends on the technologies used in protecting and securing consumer data. Safety concerns of consumers may be addressed by many of the same technology protections as those of businesses, such as encryption and verification. There are consumers' apprehensions regarding giving information online due to worry of threats to online security, including panic of hackers and informational theft. The most common security threats in the E-commerce environment are malicious code threats. This usually includes viruses, worms, and Trojan horses. Most of the time virus corrupts the files on the web portal. They are unsafe as they destroy the computer systems and can harm the normal working of the computer. Almost in the similar way like Corona virus infects humans, computer virus also requires a host to multiply. Despite efforts from industry and research communities to deter it this remains a viable security threat (Singh et al. 2020). Worms differs from viruses. They are also considered more dangerous from the virus. Hacker transmits it directly through the internet. It can contaminate millions of systems in about few hours (Marin et al., 2021). Robertson et al (2017) attempted to analyze the functioning of malicious hacking market in an attempt to curtail it and presented some interesting insights about the nature of virus and the extent of its destruction. Second type of security threat is "Hacktivism" also known as hacking activism. As described by Krapp (2005) hacktivism grounded on the hacker's approach of hacking as discovering, testing, and forming solutions to technical limitations which are not legally accepted. The third threat is Phishing – It is a type of online identity theft that uses both social engineering and technical trick to take away customers' important information both personal and financial (Vittal, 2005). The other type of threat is of Distributed Denial of Service or DDoS attacks which impose serious danger to the integrity of the Internet. Ansari and Shevtekar, 2011 highlights that the attackers are professionals and they engage themselves in such activities because of the financial incentives. Further, Kumar (2004) in his research article presented the case of highly disastrous and massively distributed DoS attack in which millions of Internet servers were exploited as packet reflectors. The author concluded by highlighting the need to protect innocent internet servers. The last threat of discussion is Malware - It is the mischievous software that invaders/hackers put into webpages after gaining entree to the organization's site. The proliferating rate of malware attacks on computers, computer networks, and mobile phones has highlighted the need for aggressive measures to tackle the malware threat (Imran et al., 2017). Malware is found on a person's system in case they have been themselves become the prey of a phishing attack or otherwise been compromised. Malwares can be installed on website if there is a server with other compromised websites. Ecommerce platforms are chiefly vulnerable to malware infections because of their proliferation in the market. Malware poses many threats like stealing information from credit card and other accounts. Malware also perform spam activities by connecting to sites selling medicines or other goods, readdressing pages to other sites.

2. Objective of the Study

The main objective of this study is to

- Analyze the possible threats and major security issues which surround the cyber space/ digital business.
- Categorize these threats/security concerns through a guiding protective framework for organizations.
- Synthesize protection measures and techniques after detailed analysis of cases occurred at global level to avert companies to fall prey of internet threats.

3. Research Methodology

This paper adopts a qualitative research methodology. The research is conducted in two phases in order to generate insight about cyber-crimes occurred at global level. Phase – I includes integration of the cases obtained from the time period of 2011 – 2020. The case details are obtained from authentic online sources for analysis. Each case after careful analysis produces information such as case details, affected party /loss, and damage control measures. Phase II of the research employs CAQDAS "Computer assisted qualitative data analysis software - MAXQDA Analytics Pro 2020". Codes are generated to contain common information related to Cyber - crime and Cyber –Security. This is used for creation of word cloud, word tree and single case model through the software so that common themes can be identified. Post analysis cyber-crime protection prevention framework is generated.

4. Cases of E-Commerce Security Threat

CASE: 1	
Name of the organisation	Health Care Organizations
Country	Globally
Date	November, 2020
Type of security threat	Distributed denial-of-service (DDoS) attacks
Case details	While healthcare organizations are focusing on treating COVID -19, they are fighting to stay ahead of proliferating cybersecurity threats. Pandemic has in many ways made them more vulnerable to cyber breaches and attractive target for hackers. In this case hackers took advantage of the critical hospital data. There were fraudulent emails sent to patients with subject line – "test result and PPE availability" channelizing them to a scam.

Affected party/loss	Patients and hospitals losing their medical case history, criminals demand ransom.
Damage control measures	Make sure systems are strengthened, have right monitoring in place, and have an appropriate antivirus – which is frequently updated so that new set of guidelines can be downloaded on time, System isolation in their own network, instructions to staff and making them aware about common risks. Investing in automated technologies. Installing Artificial Intelligence solutions are helpful because of their continuous learning capabilities.
Source	Reference 9

CASE: 2	
Name of the organisation	Global Information solutions company, EQUIFAX
Country	USA
Date	July 2017
Type of security threat	Data breach
Case details	Malicious hackers won access to EQUIFAX systems by exploitinga - "website application vulnerability". Data of 147.9 million customers was leaked. Initially Equifax was reluctant to inform how many PINs and other important information was leaked. Equifax stated that – "the delay was due to the time which went into finding out gravity of the intrusion and how much personal data is involved".
Affected party/loss	Cyber criminals got access to 146.6 million names, 145 social security number, 99 addresses, 27 million phone numbers, 17 million driving license number, 1 million email addresses.
Damage control measures	Financial regulators intervened and Equifax obliged to follow the security rules as per a consent order with eight state financial regulators. The order from regulatory authority laid down steps to abide like conducting regular security audits, creating written data protection policies and guides, close monitoring of outside technology dealers, and improvement in software patch management controls.
Source	Reference 25

CASE: 3	
Name of the organisation	Deloitte
Country	US
Date	September 2017
Type of security threat	Hacking
Case details	Hackers obtained the particulars from the company's blue-chip clients. The attack went unnoticed for months. It was found that Deloitte did not have two-step authentication set up and access needed only a single password. The hacker invaded the firm's global email server with a false account that gave them advantage and unobstructed admission to all areas.
Affected party/loss	Hackers had possible admission to usernames, passwords, IP addresses, confidential models and other information. Various electronic mails had add-ons with highly secured security and design details.
Damage control measures	Government authorities intervened. Deloitte committed to ensure that best cyber-security defence is placed. It invested profoundly in protecting sensitive information and continually reviewed and enhanced cyber-security.
Source	Reference 4

CASE: 4	
Name of Organisation	TSMC, National Health Care Service
Country	Taiwan
Date	May 2017
Type of security threat	Malware, England, Scotland
Case details	This was ransom ware attack held on May 2017. It was a worldwide attack by the wanna cry ransomware crypto worm. This worm mainly attacks on the computers running the Microsoft windows operating system. The attackers demanded ransom payments in the bitcoin crypto currency. A similar variant of malware made Taiwan semiconductor manufacturing company to shut down its operations temporarily in 2018.

Affected party/loss	The estimated loss by the attack was more than 200,000 computers, across 150 countries. The loss amounted to hundreds of billions of dollars. National health service hospital in England was worst hit; seventy thousand medical devices which included computers, MRI scanners and other medical equipment were affected.
Damage control measures	The attack was controlled only after some days of its discovery. Emergency signals were sent by Microsoft to destroy and prevent the spread of Wanna cry.
Source	Reference 18

CASE: 5	
Name of the organisation	Ebay
Country	Worldwide
Date	May 2014
Type of security threat	Database threat
Case details	The cyber-attack was reported by the online auction giant. They stole names, addresses, date of birth and encrypted passwords of one hundred forty-five million users. It was reported that hackers used the credentials of three corporate employees to gain access of company's system for many days. Using the same they accessed user database and a lot of sensitive information was compromised.
Affected party/loss	Hackers accessed email addresses and encrypted passwords belonging to all eBay users.
Damage control measures	Company initiated the program in which they requested 145 million customers to change their passwords. This was followed by securing the personal information as precautionary measure.
Source	Reference 7

CASE: 6	
Name of the organisation	JP MORGAN CHASE
Country	USA
Date	JULY 2014
Type of security threat	Hacking

Case details	In this case of hacking, hackers somehow obtained the login ID and password of JP Morgan employee. JP Morgan mistakenly ignored the double authentication protection system which gave room to hackers to commit this cyber-crime. Security team neglected two factor authentication process. The company stated "It exposed contact information for 76 million households and 7 million small businesses. The major threat in case was that criminals could take on the identities of these 83 million businesses and people".
Affected party/loss	Compromised the data of almost 50 % of all US households – 76 million, plus 7 million small businesses.
Damage control measures	JP Morgan IT team could able to identify the cyber criminals behind the hacking. The company stated that "perpetrators are charged for unauthorized access of computers, identity theft, securities & wire fraud and money laundering". Thereafter bank also implemented the double authentication scheme.
Source	Reference 26

CASE: 7	
Name of the organisation	Yahoo
Country	World Wide
Date	2014
Type of security threat	Data Theft
Case details	YAHOO discovered a major cyber-attack in 2014, in which data of one billion users compromised. The scale of the loss made this case largest in history. The company accused those hackers were working on behalf of government. They planned to use "forged cookies" these allow an intruder to access user's account without a password. This enables them to become the owner of an email account. The execution of this crime is based on bits of code which tend to stay in user's cache and login details are not required in every visit.
Affected party/loss	The information leaked included "names, email addresses, telephone numbers, dates of birth and hashed passwords". In few cases security unencrypted questions and answers were compromised".

Damage control measures	FBI accused this 2014 breach to 4 men, along with the involvement of two Russia's Federal Security Service (FSB) employees. They were imprisoned.
Source	Reference 31

CASE: 8	
Name of Organisation	HOME DEPOT
Country	USA
Date	SEPTEMBER, 2014
Type of security threat	Malware
Case details	Home Depot announces that - "56 million credit cards information compromised in a breach that lasted from April to September 2014". It made this the biggest retail breach. Home Depot stated that "malware used in the attack has not been seen in previous attacks, describing the malware as unique and custom-built". The company said that "the hackers' method of entry has been closed off, the malware eliminated from its network, and that it had rolled out enhanced encryption of payment data".
Affected party/loss	US customers lost $ 19.5 which Home Depot agreed to makeup. US customers bore huge loss. The breach affected more than fifty million card holders. Home improvement retailer announced –" $13 million fund will be used to reimburse shoppers for out-of-pocket losses." The retailer also sponsored 5 million card holders protection service for a year worth $6.5 million.
Damage control measures	Home Depot stated that it - taken multiple steps to recover from its data breach; one of them is to enable the use of EMV Chip-and-PIN payment cards". Second is "implementation of P2P encryption and proper network segregation" Home Depot also agreed and stated to "improve data security over a two-year period, and hire a chief information security officer to oversee its progress". Home Depot separately pay legal fees and related costs for affected consumers.
Source	Reference 1

CASE: 9	
Name of the organisation	Uber
Country	USA

Date	November 2014
Type of security threat	Hacking
Case details	In this case hackers made their way into GitHub repository and stole password protected credentials; these were then used to reach the account of Amazon web services. This compromised the information stored inside it.
Affected party/loss	Uber announced that "hackers stole names, email addresses, and phone numbers of 57 million Uber riders around the world, along with data on more than 7 million drivers, which included over 600,000 drivers' license records".
Damage control measures	Uber took some urgent remedial actions to avoid future occurrence of such instances. Uber took immediate action to secure the data. It completely halted further authorizations. Thereafter Uber decided to submit frequent audit reports to FTC as opposed to submitting initial audit report. At the time of the incident, Uber took prompt steps to secure the data and shut down further unauthorized access by the individuals, Uber now submits every audit report of its privacy program to the FTC, as opposed to only submitting the initial audit report.
Source	Reference 27

CASE: 10	
Name of the organisation	Sony
Country	New York/ Boston
Date	April 2, 2011
Type of security threat	Server Threat (database threat)
Case details	As stated by Sony – "It began with anonymous term used by hacktivists. They attacked Sony's servers with distributed denial of service attacks. This attack by the perpetrators seemed more revenge based. The attackers were upset by Sony's legal action against PS3 jail breakers. The group eventually halted its attacks, accepting they were only hurting Sony's end users: the gamers".
Affected party/loss	As disclosed by Sony – "Personal details of millions of its customers have been compromised including users' names, home addresses, email addresses, birth dates, PSN passwords, usernames, PSN profile data, purchase history and billing address and security question answers".

Damage control measures	Sony hired a Chief Information Security Officer. The officer was assigned to see new efforts of Sony which consisted of monitoring against the attack, enhanced data encryption. Further, Sony expedited the move of the system that houses the PlayStation Network to a new data Centre in a different location than its current place.
Source	Reference 24

5. Computer Aided Qualitative Data Analysis

This section presents the output after analysis of cases with MAXQDA software. Figure 1 presents the word cloud after analysis of cases text. Codes are created for “cyber-crime” and “cyber - security” to contain common information in a structured format as presented in Figure 2 and Figure 3 in the form of word tree. Further, after composite analyses of cases a single case model is generated that links the two

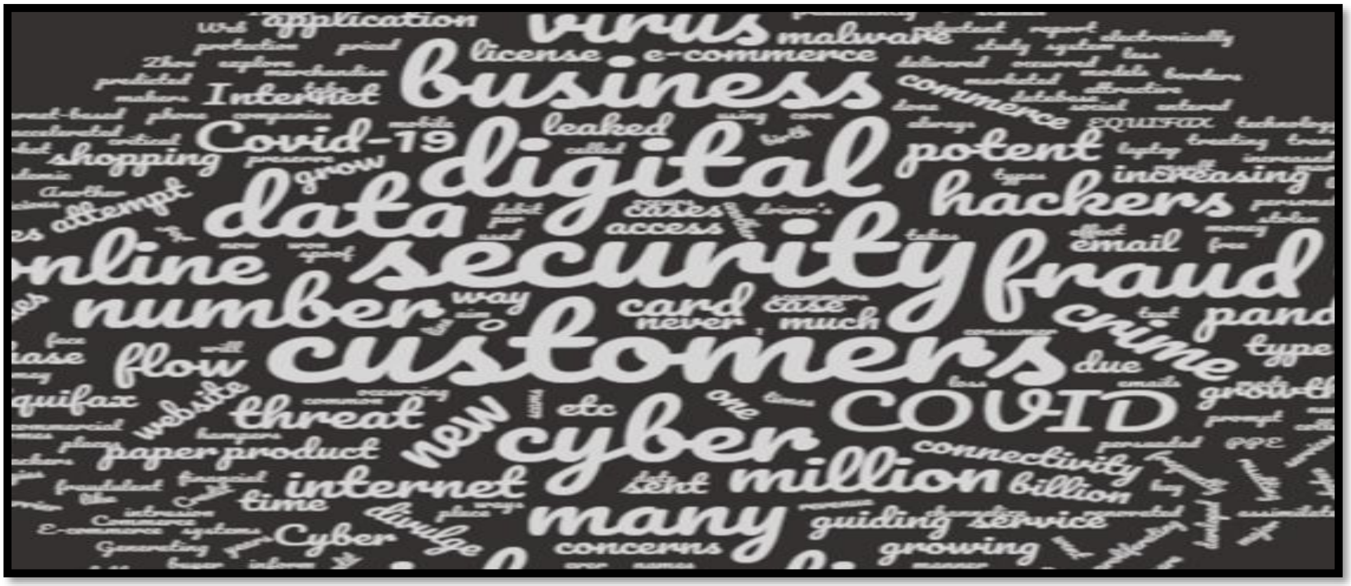
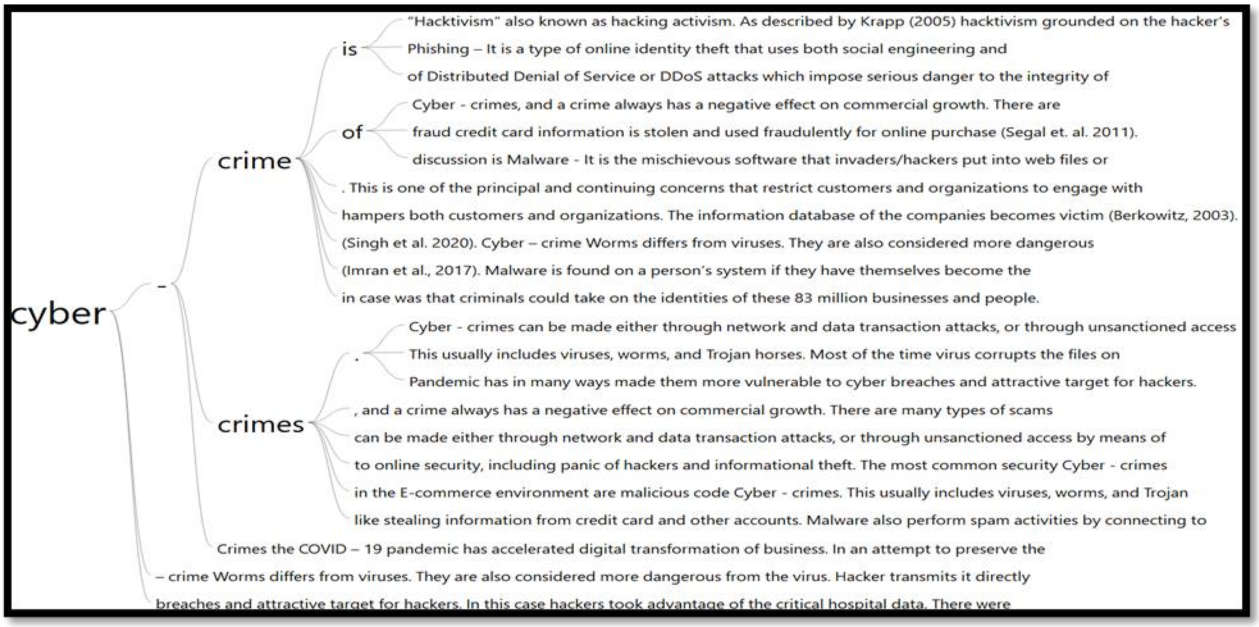
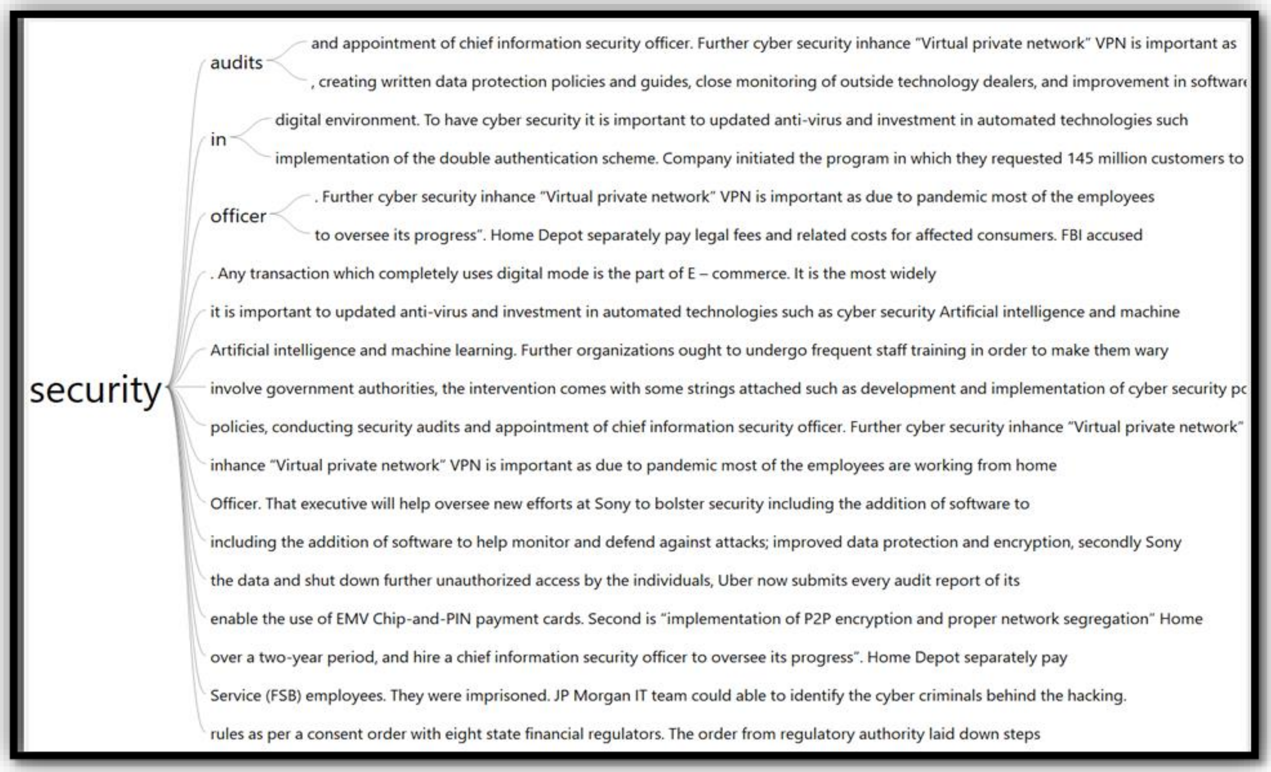


Figure 1: Word Cloud of Text
(Source: Generated by software)



"Hacktivism" also known as hacking activism. As described by Krapp (2005) hacktivism grounded on the hacker's
Phishing – It is a type of online identity theft that uses both social engineering and
of Distributed Denial of Service or DDoS attacks which impose serious danger to the integrity of
Cyber - crimes, and a crime always has a negative effect on commercial growth. There are
fraud credit card information is stolen and used fraudulently for online purchase (Segal et. al. 2011).
discussion is Malware - It is the mischievous software that invaders/hackers put into web files or
. This is one of the principal and continuing concerns that restrict customers and organizations to engage with
hampers both customers and organizations. The information database of the companies becomes victim (Berkowitz, 2003).
(Singh et al. 2020). Cyber – crime Worms differs from viruses. They are also considered more dangerous
(Imran et al., 2017). Malware is found on a person's system if they have themselves become the
in case was that criminals could take on the identities of these 83 million businesses and people.
Cyber - crimes can be made either through network and data transaction attacks, or through unsanctioned access
This usually includes viruses, worms, and Trojan horses. Most of the time virus corrupts the files on
Pandemic has in many ways made them more vulnerable to cyber breaches and attractive target for hackers.
, and a crime always has a negative effect on commercial growth. There are many types of scams
can be made either through network and data transaction attacks, or through unsanctioned access by means of
to online security, including panic of hackers and informational theft. The most common security Cyber - crimes
in the E-commerce environment are malicious code Cyber - crimes. This usually includes viruses, worms, and Trojan
like stealing information from credit card and other accounts. Malware also perform spam activities by connecting to
Crimes the COVID – 19 pandemic has accelerated digital transformation of business. In an attempt to preserve the
– crime Worms differs from viruses. They are also considered more dangerous from the virus. Hacker transmits it directly
breaches and attractive target for hackers. In this case hackers took advantage of the critical hospital data. There were

Figure 2: Word Tree for Cyber – Crime
(Source: Generated by Software)



security

audits

and appointment of chief information security officer. Further cyber security inhance "Virtual private network" VPN is important as

, creating written data protection policies and guides, close monitoring of outside technology dealers, and improvement in softwar

in

digital environment. To have cyber security it is important to updated anti-virus and investment in automated technologies such

implementation of the double authentication scheme. Company initiated the program in which they requested 145 million customers to

officer

. Further cyber security inhance "Virtual private network" VPN is important as due to pandemic most of the employees

to oversee its progress". Home Depot separately pay legal fees and related costs for affected consumers. FBI accused

. Any transaction which completely uses digital mode is the part of E – commerce. It is the most widely

it is important to updated anti-virus and investment in automated technologies such as cyber security Artificial intelligence and machine

Artificial intelligence and machine learning. Further organizations ought to undergo frequent staff training in order to make them wary

involve government authorities, the intervention comes with some strings attached such as development and implementation of cyber security pc

policies, conducting security audits and appointment of chief information security officer. Further cyber security inhance "Virtual private network"

inhance "Virtual private network" VPN is important as due to pandemic most of the employees are working from home

Officer. That executive will help oversee new efforts at Sony to bolster security including the addition of software to

including the addition of software to help monitor and defend against attacks; improved data protection and encryption, secondly Sony

the data and shut down further unauthorized access by the individuals, Uber now submits every audit report of its

enable the use of EMV Chip-and-PIN payment cards. Second is "implementation of P2P encryption and proper network segregation" Home

over a two-year period, and hire a chief information security officer to oversee its progress". Home Depot separately pay

Service (FSB) employees. They were imprisoned. JP Morgan IT team could able to identify the cyber criminals behind the hacking.

rules as per a consent order with eight state financial regulators. The order from regulatory authority laid down steps

Figure 3: Word Tree for Cyber Security
(Source: Generated by Software)

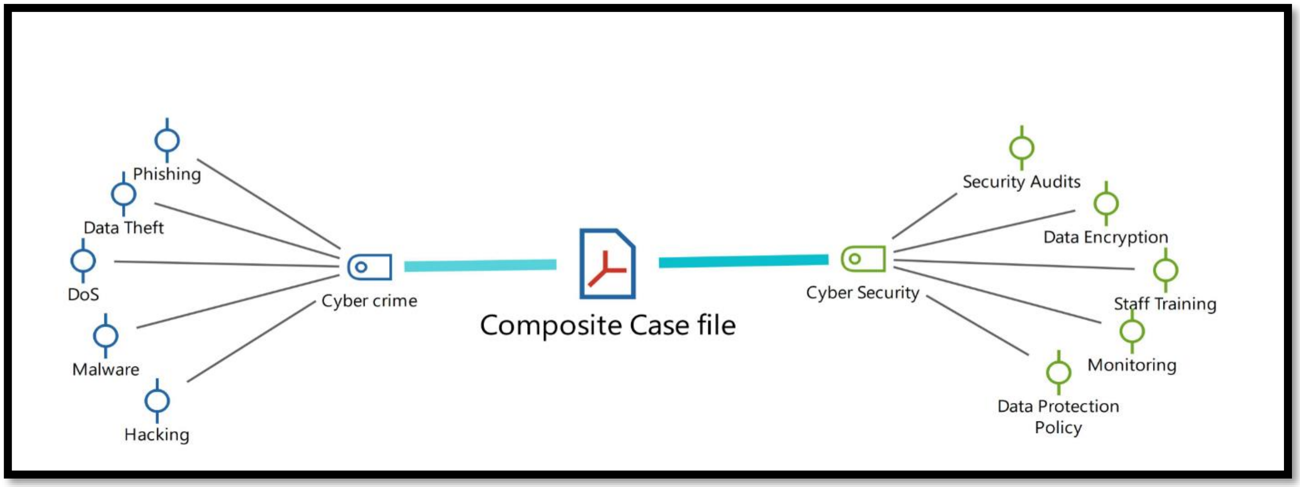
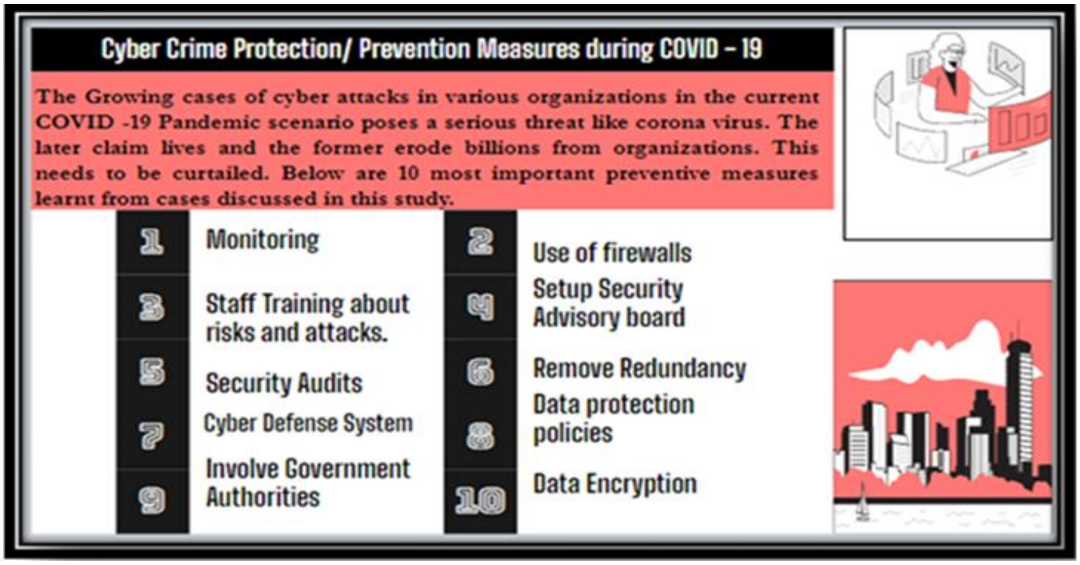


Figure 4: Single Case Model

(Source: Generated by Software)

6. Discussion and Conclusion

It is imperative to have the policies and structure in the organization which minimizes the risk of unsolicited cyber-attacks. Any transaction which completely uses digital mode is the part of E – commerce. It is the most widely used mode today and the same is especially true during the current circumstances of COVID – 19 pandemic. In these challenging times when the organizations are already struggling for their survival a cyber-attack can completely collapse its position in the market. Therefore, the current paper after the manual and qualitative software analysis of cases as discussed in study above, presents a ten-pointer framework as a guiding tool for organizations to avert such attacks. The same is as in Figure 5 below.



Cyber Crime Protection/ Prevention Measures during COVID – 19

The Growing cases of cyber attacks in various organizations in the current COVID -19 Pandemic scenario poses a serious threat like corona virus. The later claim lives and the former erode billions from organizations. This needs to be curtailed. Below are 10 most important preventive measures learnt from cases discussed in this study.

1 Monitoring

2 Use of firewalls

3 Staff Training about risks and attacks.

4 Setup Security Advisory board

5 Security Audits

6 Remove Redundancy

7 Cyber Defense System

8 Data protection policies

9 Involve Government Authorities

10 Data Encryption

Figure 5: Cyber-crime Prevention / Protection framework
(Source: Created by Author)

Digital space is extensively used these days for all type of business operations. A large amount of sensitive information is stored electronically by company's which requires protection from invaders. They can use this information illegally rendering irreparable damage to the organization sometimes. Businesses can avail complete benefit from digital transformation once they are fully equipped to fight proliferating cybercrimes. While companies expand and discover new opportunities and innovations, a big challenge is maintaining a secure digital environment. To prevent cyber-attacks regular monitoring of system is essential; this involves installing suitable updated anti-virus and investment in automated technologies such as Artificial intelligence and machine learning. Further organizations ought to undergo frequent staff training in order to make them wary of common cyber risks and attacks. In the event of an occurrence of cyber-attack organizations should involve government authorities, the intervention comes with some strings attached such as development and implementation of cyber security policies, conducting security audits and appointment of chief information security officer. Further installing a "Virtual private network" VPN is important as due to pandemic most of the employees are working from home accessing the work server remotely. VPN generates safe encrypted connection. Next is avoiding data redundancy as it takes more storage space on server render more power at the hand of hacker to misuse it in case of an attack. Organizations can capitalize from digitization of business provided they are completely equipped to fight

proliferating cyber-crimes. While companies expand, innovate and discover new opportunities a big challenge of maintaining secure digital environment can be attained through planning and organization

7. Limitations and Future Scope

The main limitation of the study is that it employs qualitative research methodology to derive the model. A mixed method analysis could have generated more insightful directions. The generated framework works as a potent tool for organizations consisting the learning gained from the recent major cyber-crime cases. This adds to the existing body of literature, it can be inferred through this paper that cyber security is the part of growing and emerging research owing to the increased dependence on digital transactions. Eventually, the author hopes that the current research serves as a foundation to further augment the domain of cybersecurity.

References

1. 56 million cards compromised Home Depot breach is bigger than target. (2014) Retrieved from https://www.forbes.com/sites/katevinton/2014/09/18.

2. Ansari, N., & Shevtekar, A. (2011). *Cyber Infrastructure Protection* (pp. 279-306, Rep.) (Saadawi T. & Jordan L., Eds.). Strategic Studies Institute, US Army War College. Retrieved July 1, 2021, from http://www.jstor.org/stable/resrep11979.15.

3. Berkowitz, B.S. (2003). Cyber security: who's watching the store? *Issues in Science and Technology,* Vol. 19 No. 3.

4. Big four accounting firm Deloitte confirms (2017) Retrieved from https://www.forbes.com.
5. Cassell, J., Bickmore, T., 2000. External manifestations of trustworthiness in the interface. Communications of the ACM. December, 50–56.
6. Cheskin Research and Studio Archetype/Sapient. ECommerce Trust Study, January 1999.

7. Cyber thieves took data on 145 million e Bay customers by hacking 3 corporate Employees (2014) Retrieved from https://www.businessinsider.in.
8. Dayal, S., Landesberg, H., Zeisser, M., 1999. How to build trust online. *Marketing Management*, 8 (3), 64–71.
9. Fearn, N. (2021). How Can Healthcare Fight Cyber Crime? *Computer Weekly*, 21–25.
10. Friedman, B., Kahn, P.H. Jr., Howe, D.C., 2000. Trust online. Communications of the ACM December, 34–40.
11. Imran, M., Afzal, M. T., & Qadir, M. A. (2017). A comparison of feature extraction techniques for malware analysis. *Turkish Journal of Electrical Engineering & Computer Sciences*, *25*(2), 1173–1183. https://iproxy.inflibnet.ac.in:2092/10.3906/elk-1601-189.
12. Kalakota, R., Whinston, A.B., 1996. Frontiers of Electronic Commerce, Addison-Wesley, Reading, MA.
13. Krapp, P. (2005). Terror and play, or What Was Hacktivism? *Grey Room,* (21), 70-93. Retrieved July 1, 2021, from http://www.jstor.org/stable/20442704.
14. Kumar, V. (2004). Sophistication in distributed denial-of-service attacks on the Internet. *Current Science, 87*(7), 885-888. Retrieved July 1, 2021, from http://www.jstor.org/stable/24109391
15. Marin, E., Almukaynizi, M., Sarkar, S., Nunes, E., Shakarian, J., Shakarian, P., & Amoroso, E. G. (2021). Exploring Malicious Hacker Communities: Toward Proactive Cyber-Defense. Cambridge: Cambridge University Press.
16. OECD (2020), Digital Transformation in the Age of COVID-19: Building Resilience and Bridging Divides, Digital Economy Outlook 2020 Supplement, OECD, Paris, www.oecd.org/digital/digital-economy-outlook-covid.pdf.
17. Ovans, A., 1999. Is your web site socially savvy? *Harvard Business Review* 77 (3), 20–21.
18. Ransom ware what is wanna cry ransomware how does it infect and who does it infect and who was responsible (2017) Retrieved from https://www.csoonline.com.
19. Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., & Shakarian, P. (2017). Analyzing Products and Vendors in Malicious Hacking Markets. In *Darkweb Cyber Threat Intelligence Mining* (pp. 56–66). chapter, Cambridge: Cambridge University Press.
20. Saban, K.A., McGivern, E. and Saykiewicz, J.N. (2002). A critical look at the impact of cyber-crime on consumer Internet behavior. *Journal of Marketing Theory and Practice*, Vol. 10 No. 2, pp. 29-37.
21. Scroxton, A. (2020). What Cisos Can Learn from Covid-19. *Computer Weekly*, 11–15.
22. Segal, L., Ngugi, B., & Mana, J. (2011). Credit Card Fraud: A New Perspective on Tackling an Intransigent Problem. *Fordham Journal of Corporate & Financial Law*, *16*(4), 743–781.
23. Singh, P., Tapawsi, S., Gupta, S. Malware Detection in PDF and Office Documents: A survey. *Information Security Journal: A Global Perspective*, Vol. 29, No. 3, pp. 134–153, 2020. DOI 10.1080/19393555.2020.1723747.

24. Sony PlayStation. (2011) Retrieved from https://www.nytimes.com/2011/04/27/technology/27playstation.html.
25. The Equifax security breach affected millions more people than we originally thought. (2017). Retrieved from https://www.bbc.com/news/business.
26. What lies behind the JP Morgan Chase Cyber Attack (2014). Retrieved from https://www.economist.com/finance-and-economics.
27. Uber concealed cyber-attack that exposed 57 million people data. (2017). Retrieved from https://www.bloomberg.com/news/articles/2017.
28. Urban, G.L., Sultan, F., Qualls, W.J., 2000. Placing trust at the center of your internet strategy. *MIT Sloan Management Review* (1), 39–48.
29. Verma, A. (2021). Battling COVID-19 with Process Model of Integrated Digital Technology: An Analysis of Qualitative Data. In Niranjanamurthy, M, Bhattacharyya, Siddhartha, Kumar, Neeraj (Eds.) Intelligent Data Analysis for COVID-19 Pandemic. pp 55 -81. Springer.
30. Vittal, J. (2005). Phishing, Pharming, and Other Scams. *GPSolo, 22*(8), 26-32. Retrieved July 1, 2021, from http://www.jstor.org/stable/23672964.
31. Wen,Y. Zhou, C. Ma, J and Liu, K, (2008). *Research on E commerce Security Issues*, International seminar on Business and Information Management, pp. 186 – 189. doi: 10.1109/ISBIM.2008.168.
32. Yahoo hack security of one billion accounts breached (2014). Retrieved from https://www.theguardian.com/technology.