Original Research Article

J. Computing & Int. Systems (2021) 187–200

Journal of Computing and Intelligent Systems

Journal homepage: www.shcpub.edu.in

ISSN: 2456-9496

Policy Analysis: Ransomware Impact on the Financial Sector Admist the Covid -19 Pandemic

Yaw Amoah Adum-Attah[#1], K. Saravanapriya[#2]

Received on 3rd JUN 2021, Accepted on 18th JUN 2021

Abstract — This research paper provides a meticulous literature review that focuses on the issues related to the ever-evolving threat malware and ransomware poses to the financial sector admits the 2020 Covid 19 pandemic. Available to the public are research papers providing findings relating to technical analysis and experimentation based on these varying results. Above and beyond ISO/IEC 27032 standards and policies, alongside nations security guidelines, the financial sector cybersecurity policy documentation, focusing on managing the sector vulnerabilities and susceptibilities to Ransomware attacks fails to hold a firm grip on the evolving threat. This study analyses relevant policy documentations these financial institutions use to spurn cyberattacks; we identify their vulnerabilities in the wake of the ever-growing Ransomware landscape. Ultimately, I propose by way of literature the MLAI to help the financial institutions develop suitable framework and structures to fend of Ransomware attacks.

Keywords - VMware, Covid-19, Cybersecurity, SANs Model, Internet of Things, McAfee, Kaspersky, GPcode.AK, SWIFT, CryptoLocker, Global Pandemic.

I. INTRODUCTION

In any organization, policies play an important role; policies are set of concepts used to guide decisions and accomplish objective outcomes. In other words, policies are principles intended to guide actions and produce rational result. Resource allocation and structure growth are often expressed in policy decisions. A governance body within an institution adopts polices, and the financial sector is no exception. Policies have a major impact on the financial sector in a variety of ways. Every element of banking is governed by one policy or the other. From Assets like Bonds, Commodities, Derivatives, Foreign Exchange, Private Equity, and Stocks to Instruments like Cheques, Mortgage, Credit Line, Performance Bonds, to Corporate activities like Audit and Risk Management, to all banking regulations, and the Information System infrastructure upon which these institutions are firmly built. Ransomware poses a significant security risk to the financial sector as criminals uncover new vulnerabilities and susceptibilities to launch attacks. The 2019, 2020 global pandemic skyrocketed malware and ransomware attacks on the financial sector to 148% in March, 2020 alone as the sector shifted to work remotely. The security analysts estimated a 70% rise in remote work between February 4 and April 7. This statistic is focused on information gathered by the VMware Carbon Black Cloud sensor and excludes people who already work from home. And, perhaps unsurprisingly, attacks on the financial sector increased dramatically during this period. According to threat analysts, COVID-19 has been used as a cover by hackers, releasing phishing attacks, bogus apps and maps, trojan horses, rootkits, crypto miners, botnets, and ransomware on the financial sector according to researchers at VMware Carbon Black. The financial sector information security policies for fighting and defending against cyber-attacks are struggling to make firm claim about the challenge. This research paper looks into these regulations and their vulnerabilities admits the pandemic and propose by way of literature Artificial Intelligence and Machine learning to help financial institutions develop suitable framework and structures to fend off Ransomware attacks.

* Corresponding author: E-mail: [1]pyawamoah@gmail.com, [2]priya@shctpt.edu

[1] Department of MCA, Sacred Heart College (Autonomous), Tirupatthur.
[2] Assistant Professor, *Department of MCA, Sacred Heart College (Autonomous), Tirupatthur*

II. Cybersecurity Policy

The protection of computing systems and networks from data leakage, misuse, or harm to devices, applications, or electronic data, as well as service interruption or misdirection, is referred to as cybersecurity. Cybersecurity refers to procedures for preventing unwanted access to databases, networks, and services from both external and internal actors. To operate in a virtual world, it is critical to safeguard the confidentiality and privacy of data. Most organizations are unable to guarantee an adequate collection of software, technology, pedagogy, and methodologies to secure networks, computers, systems, and data against illegal intrusion, resulting in cybersecurity danger. Since it can interrupt banking processes and cause major direct and indirect damages, the cybersecurity challenge has transformed the paradigm of banking operations for many decades in the financial sector. As a result of the rapid introduction of internet operations and deliverables, the sector has become highly vulnerable to security threats. Worse is when most organizations moved work to home as a result of the pandemic. Cybersecurity protocols are used to offer guidelines for operations like email attachment encryption and social media usage restrictions. This has become more crucial because of the vulnerability and exposure to cyberattacks and data breaches, if left unattended can be very costly to the organization, to prevent this cost, cybersecurity precautions are essential. Internal components like employees frequently are the weakest links in an organizations security system. They turn to share passwords, open dangerous URLs and attachments, utilize unapproved cloud services, and neglect to encrypt important data or follow policy instructions to the letter. These human elements are responsible for about 43% of data leaks, half of which were recorded to be an accidental leak according to Grand Theft Data, a McAfee research on Data Exfiltration. On the other hand, should security measures be judged insufficient, the sector or institution faces severe sanctions and fines. The public image and reputation of a corporation are also dependent on cybersecurity measures. Customers, partners, owners, and potential workers all want proof that their sensitive information will be kept safe. A company will not be able to offer such documentation if it does not have a cybersecurity policy. Typically, the first part of a cybersecurity plan usually covers the organization's overall security objectives, roles, and responsibilities for stakeholders. Stakeholders include outside contractors, IT personnel, financial personnel, and others. This part of the policy deals with "roles and obligations" or "data duty and transparency". Cybersecurity Policies also contains sections on antivirus software standards or the use of cloud apps. A remote access policy is also included in the cybersecurity document definition. The SANS Institute has a number of policy cases on cybersecurity. The SANS models additionally include a remote access policy, a wireless networking policy, a password protection policy, an email policy, and a digital signature policy. From network topology to server farm implementations, the regulation explains how to enforce security architecture. The financial cost is suggested by the policy budget, and when it is adjusted, the financial sector applies it. Information security, which has been acknowledged as a major and necessary national policy issue, is the basis to the protecting of computer systems, the integrity, confidentiality, and accessibility of data. The following areas indicate the importance of safeguarding computer systems and data:

- Cyberattacks (Ransomware). The breach of information security seems to be increasing exponentially. Amidst the ever-growing threats, it will be unwise for agencies like the finance sector to ignore the probabilities of worse case eventualities concerning past and future attacks, and the severe consequences they create. Under thing, this will lead to great catastrophe.
- The growing reliance on computers and their integration in to more parts of modern life is expected to continue. (IoT (Internet of Things))

The fundamental issue in both the private and public sectors is whether or not they're devoting enough resources to information security base on the present evolving threat. A part of the solution should return from economic analysis and the costs factor, the other in my opinion is the dependency on current well-made security policies upon which structures and systems are built to fend off attacks. The most queries that require answers are:

- How often can attacks be expected?
- Can the attacks be predicted?
- Is the current policy effective to mitigate attacks?
- Are there fallback systems that can support business continuity?

This research surveys the present ransomware threats by focusing on empirical and historical data, cyberattack cost, and the policies used by these institutions within the current ransomware landscape with emphasis on Ransomware.

III. Proposed approach

First, we summarize studies made on cyberattacks on the financial sector admits 2019, 2020 Covid pandemic, the shift to 'Work from Home' (WFM) and measure the cost of cyber-attacks to victim financial corporations. What's out there is a restricted quantity of survey data because of the confidentiality of information within the banking sector and the threat of public awareness of exposure and vulnerabilities, however, cases are wide reportable within the press. The research realizes substantial short and long-term financial loss to victim firms up to 25% of their annual budget and a drop of costs in the shares securities market after the announcement of an information security violation wherever attackers had gained access to confidential client records. The drop ranges from 1% to 5% of the market capitalization, with losses of up to 15% and more.

Second, the research includes information risk assessment (Cybersecurity policies) practices in financial establishments like banks and outlines the efforts they make to manage cyber-risk in the industry. We tend to analyze the reasons these policies are not efficient in the wake of evolving malware and ransomware attacks on the financial sector.

Third, we offer a literature-based Machine Learning and AI methodology for the sector to build cyber-risk policies inside the ever-changing and evolving Ransomware development technology.

The Evolution of Ransomware – AIDS on Computer Diskette – 1989

Since the inception of ransomware, cybercrime has evolved rapidly, becoming prevalent in the sector. The compromise of device protection, as well as the jeopardization of conventional sector operations (downtime) due to the lucrative demand for ransom charged by victims' businesses, has taken a toll on the financial sector expenditure. Ransomware poses a significant security risk to the financial sector, as criminals uncover new vulnerabilities and susceptibilities to cyber-attacks regularly. Current financial sector information security policies for fighting and defending against cyber-attacks are struggling to make firm claims about the challenge. Ransomware has its roots as far back as 1989 and was first introduced as an AIDS Trojan. Joseph L. Popp, a Harvard educated biologist was the architect of the software. During the June 1989 International AIDS Conference Joseph sent 20000 diskettes which he labelled AIDS Information Introduction Diskette and sent it to the attendees of the conference which was organized by the WHO. The diskette contained compromised (malware - Trojan) information which encrypted the file on his victim's computer by hiding the computer's directories. Affected persons were made to mail the sum of $189 to PC Cyborg Corp before unencrypting their files.

The Internet Age

From 2006 onward has been saw a major surge up of cybercrime, new techniques such as asymmetric RSA encryption was introduced. "Archiveus Trojan3" was launched which also encrypts everything in my Document directory on victims' computers. De-encryption was possible if only victims purchase a 30-digit password from an online pharmacy. That same year saw the introduction of GPcode4, an encryption Trojan which virus spread via email attachment ostensibly as a job application. It used 660-bit RSA public key for it file encryption. Two years down the line GPcode.AK which used 1024-bit RSA encryption key was introduced as the upgrade of GPcode4. The beginning 2011, saw a major surge up of ransomware, 60,000 new ransomwares was detected in 2011, and more than doubled in 2012, to over 200,000. The most worrying and disturbing fact is that 2014 to 2015, ransomware more quadrupled. The major question most malware analysts ask is why the surge up. The figures below show the Malware Statistics from McAfee Labs Threats Report, in 2015, 2016 to 2020 respectively, showing the surge and new strains of malware over the years.

i. First Data Collection [McAfee Labs Threat Report, 2015,2016 – 2020]

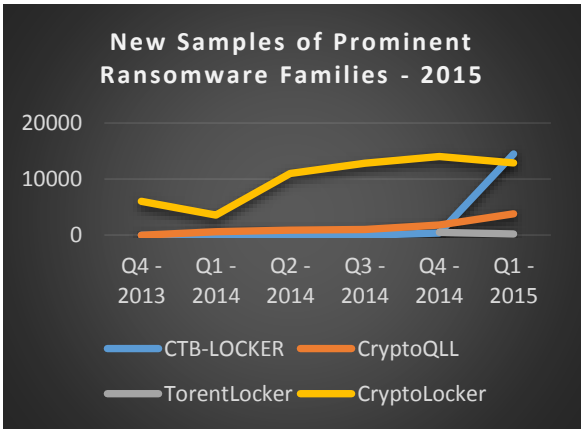

Fig 1: Source: McAfee Labs Threat Report 2015

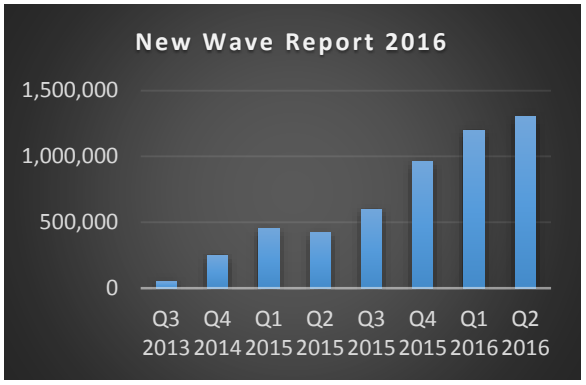

Fig 2: Source: McAfee Labs Threat Report 2016

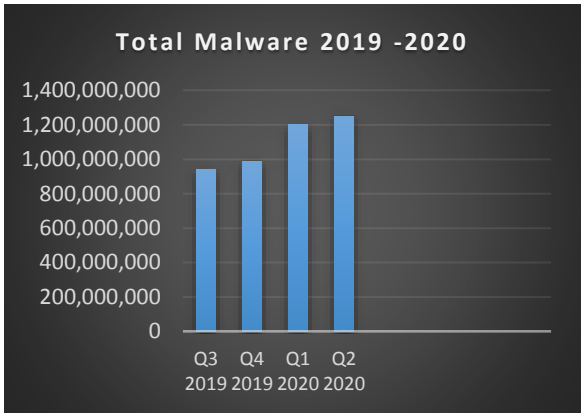

Fig 3: Source: McAfee Labs Threat Report 19 -20

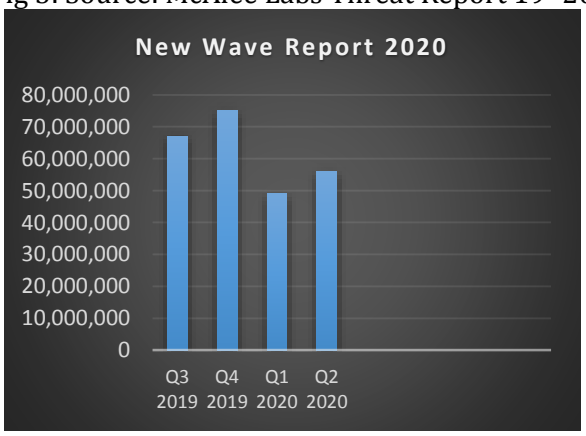

Fig 4: Source: McAfee Labs Threat Report 2020

a. Malware and Ransomware Payouts

From the statistics we can tell clearly that malware development and the engineering of new technologies to propagate it spread has 'just started'. As the economy moves to move sophisticated dependency on computer system so does the doors of malware attacks opened to global business. 2012 saw the worldwide spread of ransomware, the world was taken by surprise as the malware kept transforming into more sophisticated forms, by the end of the first quarter in 2012 over 200,000 ransomwares were discovered among which was the "CryptoLocker" which made its first appearance in September 2013. Copycat software best known as Locker was also introduced in December of that same year. Ransomware is a new type of cybercrime, according to the US Department of Justice, and it has a global impact. Veeam reported that in 2017 businesses had to pay an average of $11.7 due to these attacks. It was estimated that by the end of 2019 $11.5 Billion will be lost to these attacks. In April 2019, IC3 released its annual report to the shock of the world, Cybercrime cost a financial loss of $2.7billion in 2018, and these attacks involved not limited to Investment scams, business email compromise (BEC), and ransomware attacks. According to Accenture Ninth Annual Cost on Cyber studies a rise of 12% was seen as the total cost of cyber-attacks for most victim companies increased from US$11.7 million in 2017 to US$13 Million. The FBI's IC3(Internet Crime Complaint Center) reported that 467,361 complaints where received in 2019 an estimated average of 1,300 each day and a financial loss to individuals and organizations reaching an alarming US$3.5 billion. Business email compromise, confidential fraud, impersonating a person or vendor's account to obtain personal data and financial information, and ransomware were among the complaints with the largest financial damages. Donna Gregory, the director of the IC3, stated that the center did not witness a rise in new sorts of fraud in 2019, but rather witnessed criminals using new methods and strategies to carry out already existing malicious attacks and schemes. Criminals are growing more sophisticated, he added. This makes it more difficult for victims to see red signals and distinguish between real and false. Thousands of organizations around the world have been infected with spyware that forces them to pay a ransom for decryption codes.

ii. Second Data Collection [The Cost and Case Studies]

The Cost Factor - Bangladesh's central Bank Case Study

In 2016, SWIFT hackers hacked Bangladesh's central bank, causing a loss of US$81 million (Gladstone, 2016). For many days in 2013, cyber hackers interrupted South Korean financial networks (Schwartz, 2013). In 2012, denial-of-service (DDoS) attacks were launched against Wells Fargo, JPMorgan Chase, PNC Bank, and Bank of America in the United States (Goldman, 2012). While different institutions give varying statistics for bank losses around the world, the International Monetary Fund (IMF) predicts that yearly losses might be roughly 97 billion dollars, or around 9% of global banking net profits in 2016. (Bouveret, 2018).

Eurograbber Case Study: How Malware Led to the Loss of 36 Million Euros

A case study of a sophisticated, multifaceted, and targeted operation that plundered more than 36 million Euros from over 30,000 bank customers across Europe. The attacks began in Italy, and tens of thousands of online bank customers were discovered in Germany, Spain, and the Netherlands shortly after. Customers who used online banking were fully unaware that they had been infected with Trojans, that their sessions had been hijacked, or that monies had been taken directly from their accounts. This assault effort was detected and named "Eurograbber" by Versafe and Check Point Software Technologies.In a new and very popular variation of the Eurograbber attack, the ZITMO, or Zeus-In-The-Mobile Trojan, is deployed. So far, this hack has only been identified in Euro Zone countries, but a variant of this attack might affect banks outside of the EU as well. Victim banks have been informed as of this writing, and are actively working with law enforcement authorities to stop any existing or potential attacks. The multi-staged attack compromised online banking clients' desktops and mobile devices, allowing the attackers to fully track and control the bank customers' online banking activities once the Eurograbber Trojans were installed on both devices. The attackers even used the two-factor authentication system employed by banks to ensure the security of online banking transactions to validate their unlawful financial transfer. Furthermore, in order to reach a larger "target market," the Trojan used to attack mobile devices was designed for both the Blackberry and Android platforms, and as a consequence, it was able to infect both corporate and private banking users, moving funds out of their accounts in amounts ranging from 500 to 250,000 Euros.

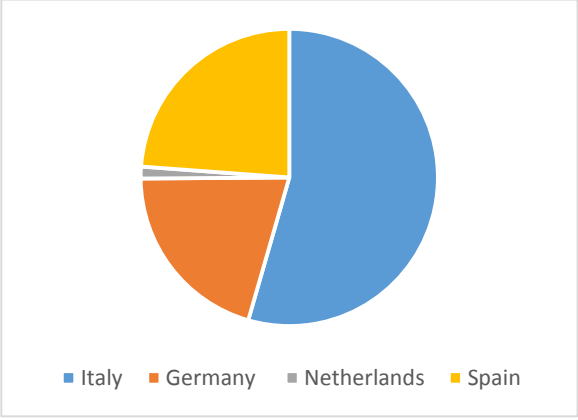

Fig 5: Affected Banks per country

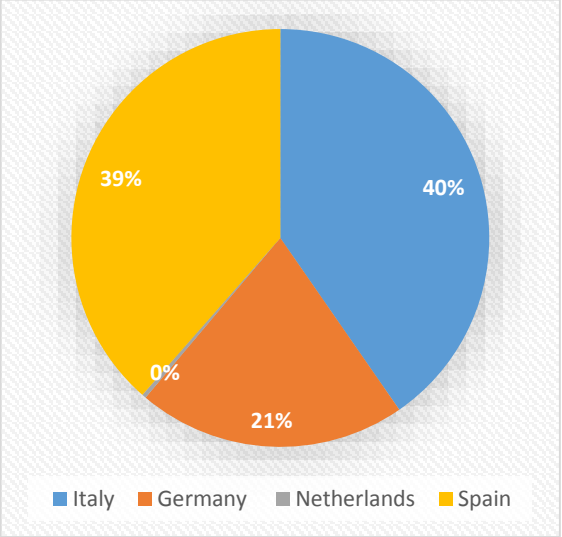

Fig 6: Affected users per country

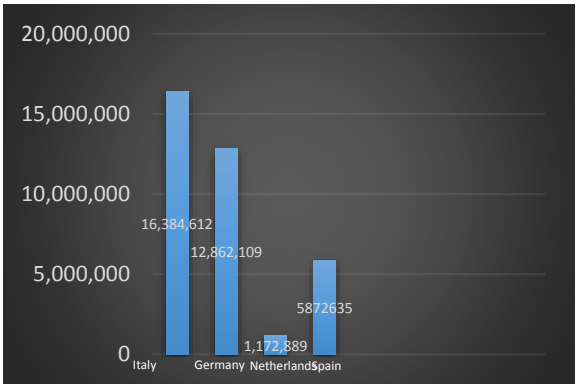

Fig 7: Amount of Euros Stolen per Country

iii. Second Data Collection [The Cost and Case Studies]

192

Japan Ursnif Banking Trojan

Violation Recorded in: 2019-20198, Japan is the intended destination and Phishing is the threat vector. The number of cyber-attacks has increased dramatically in recent years. It is broadening and evolving on a daily basis. “Japanese banks” were the most recent victims of ransomware attacks on March 12th, 2019. The Ursnif Trojan is a malware that is used to steal client credentials from banks. Ursnif's operators have been targeting Japanese banks for the past few years. Ursnif carried out a malware attack close to this one in 2018. For this assault, they primarily used the Dreambot version. They used a new version in “2019” that is primarily based on pilfering data from emails. This malware (Ursnif) is one of the most widespread and powerful forms of malware used for login or system access credential theft. Modules that target banking security items like Phishwall, etc. have been added to this malware. The assault is carried

out by sending the user a phishing text. Malicious attachments, usually an excel spreadsheet, are included in this email. The "Enable Content" button on this sheet will take you to some embedded macro codes if you click it. PowerShell commands are included in these codes, and they will begin downloading them. Ursnif developed the latest variant using ingenious intransigence techniques. They concentrated on eliminating digital traces and thwarting as many cyber security gateways as they could. It also has sophisticated data-stealing modules that target emails and digital wallets. The Ursnif malware attack on Japanese banks resulted in billions of dollars in global financial losses and tens of millions of dollars in individual losses. They've devised a method of targeted attack that exclusively affects Japanese users. Cybereason conducted many researches into location and language settings in order to discover this information.

Failed Security Controls:

- End User Security Awareness
- Spear Phishing and Social Engineering awareness
- Trademark Monitoring of App Stores

The United State Case

2014: According to USA Today, "the federal officers warned organizations on Monday that hackers purloined over 500 million financial data in the last year, effectively stealing into banks without ever entering a building."Another news source reported that, "Distributed Denial of Service (DDoS) assaults targeted 46 large financial organization, during this assault, attackers obtained remote control access to over hundreds of servers and computers, using them to flood a target's server with data, jamming it up and making it unusable." Furthermore, "targets included Bank of America, Capital One ING, the New York Stock Exchange, and PNC Banks," according to court records. According to the study, "FBI and US secret service officers have apprehended a guy charged with the greatest cyber-attack on financial institutions in American history." The company that sustained the most damage as a result of the breach was JPMorgan Chase. Over 83 million of the bank's customers' personal information was exposed as a result of the attack.

Europe Case

2015: The RBS banking firm has revealed that its online services were hit by a cyber-attack that prevented users from logging in for about an hour, just as monthly pay cheques were being deposited into accounts. In late 2015, many cyber-attacks on online trading happened, according to NASDAQ. "On October 1, FXCM Inc., an online foreign exchange trading and related service provider, reported the latest data breach. According to the firm, hackers gained illegal access to client information and made a few transfers from select accounts."

"For the first time ever, in February 2015, a Trojan named Corkow (Metel) grabbed control of a stock market trading terminal and made orders worth hundreds of millions of dollars," said Group-IB in a blog. In just 14 minutes, attackers created exceptional volatility, allowing users to buy dollars for 55 rubles and sell them for 62 rubles. The attack resulted in large losses for a Russian bank, but it was random traders who benefitted rather than the hackers." (a) Hackers attempted to steal $951 million from Bangladesh's Central Bank through the SWIFT system in February 2016, according to Group-IB. Cyberattacks, according to one firm, can lead to more than simply financial damage or data breaches; they can also be used for surveillance and cyberterrorism. Corkow is also known as Metel. 2017: HSBC, one of the world's and Europe's largest banks, was the target of a cyber-attack in early 2017. According to a report from The Week Newsletter, "HSBC clients were unable to use online banking services for the second time in a month today, following an apparent cyber-attack."

Asia Case

2010: Umashankar Sivasubramaniam vs ICICI Bank is one of the most well-known phishing fraud instances. According to the Economic Times, the Tamil Nadu IT secretary on Monday ordered ICICI Bank to pay Rs.12.85 lakh to an Abu Dhabi-based NRI within 60 days for the damage he sustained owing to a phishing fraud in the first case filed under the Information Technology Act.

2017: "Far Eastern on Friday disclosed to the Financial Supervisory Commission that malware had been planted in its computer system, affecting some of its PCs and servers, as well as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network," the Taipei Times reported in 2017. According to Focus Taiwan, "hackers used the planted malware to conduct virtual transactions to transfer roughly US$60 million from Far Eastern Bank customers' accounts to several international destinations such as Sri Lanka, Cambodia, and the United States," according to the bank.

Africa Case

2016: According to the Serianu report, "cyber thieves deployed a very complicated hack targeting 10 institutions in banking, insurance, utilities, and government across three African countries." According to this survey, cyber-attacks caused $206 million in damages to the banking and financial services industry in 2016. (the highest among all sectors). The ransomware virus has infiltrated at least 19 Kenyan companies as part of a global hacking campaign.

Cyberattacks on financial institutions from 2010 – 2018

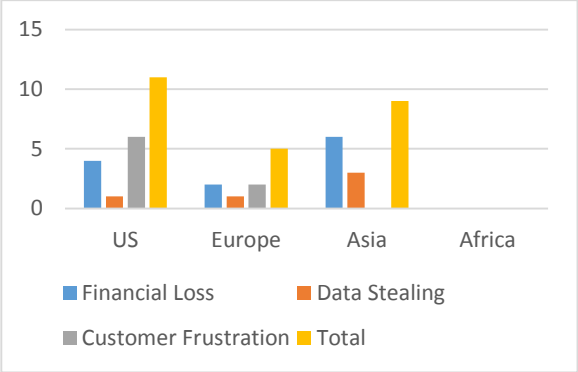

Fig 8: Type of Loss

Type of Losses

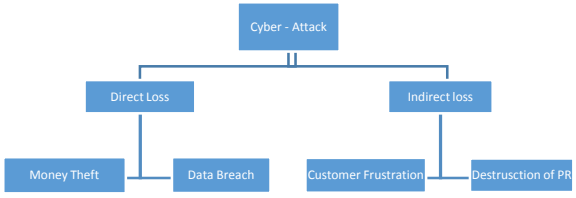

Fig 9: Type of Loss

The Vulnerabilities and Cybersecurity

Publications on cybersecurity risk are available from international organizations such as the International Monetary Fund (IMF), Bank of International Settlements (BIS), World Bank, and Organization for Economic Cooperation and Development (OECD). These publications typically priorities a broader structure for cybersecurity risk management. Similarly, risk assessment analysts and experts argue that a technology strategy alone will not be sufficient to reduce cybersecurity risk. Because no infrastructure is without weaknesses, opportunistic individuals may seek to destabilize the system and create significant losses and financial obligations on financial institutions.

Massive amounts of data are stored on server farms connected to the internet by the banking sector. Additionally, this material is designated as confidential and is not available to the general public. This private data source is processed over the internet, exposing it to a wide range of cyber dangers. This information could readily be abused by a third party. Every internet user's primary focus has shifted to cybersecurity. Cyber-attacks can result in the following outcomes:

- Injection of malware into databases, causing many systems to become infected with viruses
- Spoofing, Phishing, and Spamming
- Denial of existing services, which can lead to multiple attacks
- Password stealing
- Identity sabotage
- Vandalism by different websites
- Privacy misuse via web browsers
- Account hacks and money scams
- Ransomware
- Intellectual Property theft
- Unauthorized access to operating networks and laptops

2019 – 2020 Surge [The Covid 19 Shift Up

Financial organizations were at the forefront of the response to cyber danger during the Covid-19 pandemic. The transition toward more home office or (WFH -Work from Home) and other functional problems have increased their already high vulnerability to cyber risk. Cyber risk is becoming more important as the banking system and economy become more digitally mastered. The word "cyber risk" refers to a wide variety of threats arising from the malfunction or breach of IT networks. According to the FSB Cyber Lexicon, cyber risk is defined as "the amalgamation of the possibility of cyber accidents come about and their consequences" (2019). "Any detectable action in an IS (Information System) that:"

- Hinders a data system's information security or the information it processes, stores, or communicates
- Whether purposefully or inadvertently, breaching security rules, security processes, "To exercise or not to exercise." According to Aldasoro et al. (2020b) and CPMI-IOSCO, cyber risk is one type of operating risk (2016). The cause/method, actor, objective, and effect of cyber risks can all be classified (Aldasoro et al). 2020a

GRC 101(2020)). Also known as cybersecurity risk, is defined as the possibility of failure or destruction originating from an organization's information or communications infrastructure. Cyber menace and data breaches are two types of cyber- menace that have received a lot of attention. Cybersecurity risk, on the other hand, encompasses more than just data loss and monetary loss; it also involves intellectual property theft, productivity losses, and reputational harm. According to Deloitte Advisory Cyber Risk Services, "cyber risk is a concern that happens at the convergence of market risk, regulation, and technology." According to Deloitte's 2019 Future of Cyber Survey, the effects of security incidents ranged from tangible costs such as financial loss attributable to operational delays and regulatory penalties to intangible costs such as loss of consumer interest, reputational harm, or a shift of leadership. Accidental data leakage, as well as installation, setup, and retrieval failures, are examples of the former. Such occurrences are common. Yet, according to Aldasoro et al (2020c), about 40% of cyber threats are deliberate and malicious, i.e., virtual attack [Cyberattack]. In some cyber-attacks, malicious hackers may implant themselves into a secure data exchange. Malware (also known as "malicious malware") is computer software that is created to cause harm and/or steal information (for example, so-called Trojans, spyware and ransomware).

Man-in-the-middle occurs when the attacker implants himself into a two-party transaction and gains access to or changes data or transactions. Cross-site scripting (XSS) is a network security issue that permits attackers to take control of a victim's communications with a hacked software. Phishing is the extortion of personally identifiable information or the installation of malware using malicious emails that look to come from a trustworthy source. Attack by a phishing website. After gaining access, this may aid attackers in obtaining passwords and gaining access to a device. The method of retrieving confidential passwords contained in a database system or broadcast over a network is known as password cracking.

Professional Tools

Professional tools and preparation are used in some assaults. Attack on a program or system flaw detected but not released publicly is known as a zero-day exploit. When a zero-day hack is discovered, all consumers and suppliers of the IT equipment's can become vulnerable to virtual attacks for which there are no remedial patches. Commercial companies who perform research in order to offer zeroday exploits on the open market are exacerbating the problem. Any of these companies, such as Zerodium, provide huge cash incentives for high-risk exploits (up to $2.5 million). DDoS [Distributed Denial of Service] attacks overwhelms data centers with traffic in order to drain limited bandwidth or energy. These threats have the potential to be devastating. Organized criminal and radical groups, industrial hackers, "hacktivists," and governmental actors are all examples of actors. Their ability to damage people is proportionate to their sophistication and financial resources. For example, in 2016, North Korean hackers gained access to Bangladesh Bank's systems and by using the SWIFT network, sent chicanery wire transfer orders (Bangladesh Bank-FRBNY (2019)). The event brought awareness to the increasing cyber vulnerabilities that payment networks and related infrastructures face. The eventual objective could be financial (malware, industrial spying), strategic (state-sponsored attacks on critical infrastructures), or political (sponsored attacks on crucial infrastructures) (e.g., mainstream unrest). Cyber-threats may have far-reaching consequences. Business disruptions and IT system malfunctions can compromise the integrity and supply of assets and resources.

Data breaches jeopardies the security of sensitive information, resulting in financial and reputational damage. Fraud and theft are defined as the loss of money or other stuff like intellectual property that may or may not be entirely private. Cyber-attacks have the potential to have systemic implications and, in some situations, result in considerable economic disruption.

195 ıC Study of Financial Institutions

In a study of financial institutions, FS-ISAC [*the Financial Services Information Sharing and Analysis Center*] reported a considerable increase in phishing, and disruptive behavior against URLs used by WFH employees to gain access into their network [EWS75] EWS. Payment suppliers, bankers, credit unions and insurance companies have all been targeted by hackers. The count of 2019-2020 Covid pandemic related attacks grew from less than 5,000 per week in February to over 200,000 per week in late April as the pandemic stretched out. They grew by almost a third in May and June compared to March and April according to Check Point Research-2020. According to the study, employee of WFH swamped the virtual desktop infrastructure processes in 45 percent of the cases. In

one-third of the situations, organizations ability to sustain IT plans were not for a long-term Work from Home workforce. 1/5 of the financial sector organizations said their system network were attacked or affected during the Covid-19 pandemic.

CrowdStrike Intelligence

According to statistics from the CrowdStrike Intelligence team, ransomware attacks increased dramatically throughout the Covid outbreak, the common tactic used during this period was data extortion in the industries. 1,430 incidents were recorded worldwide in 2020 alone. During the Covid-19 pandemic in 2020, the finance market was one of the most attacked by cybercriminals, at a period when changes in work processes left companies exposed. A total of 86 attacks on the financial sector were registered in 2020, placing the financial sector sixth, on the list of most attacked sectors.

***iv. Forth Data Collection* Financial threats**

Not only are financial threats included in the figures, but also malware for Automatic Teller Machines and POS. In a supplementary paper, statistics on similar mobile dangers are provided. According to the Kaspersky Security Bulletin 2020, malware applications programmed to steal or pillage money from bank accounts infiltrated over 668,619 users' PCs.

Kaspersky Security Bulletin 220 revealed the type of malwares use for banking attacks in November 2019 — October 2020. The following table list the Top 10 financial malware families identified within the scope of the research

Table: 1 - Kaspersky Security Bulletin

SNO	Name	%*
1	Nymaim	2.1
2	RTM	11.1
3	Danabot	3.2
4	SpyEye	3.2
5	Neurevt	3.3
6	Zbot	21.6
7	CliptoShuffler	15
8	Emotet	15.1
9	Nimnul	4.2
10	Trickster	5.1

A proportion of users who were specifically harmed by this malware out of the overall number of people who were harmed by financial malware. Over the reporting time, Kaspersky Lab discovered over 26,700 ransomware updates and 21 new ransomware families.

Mainly such threats are attributed with the default conclusion, that is assigned to brand-new and unblown threats. Each new piece of ransomware was not assigned to a distinct family in our study.

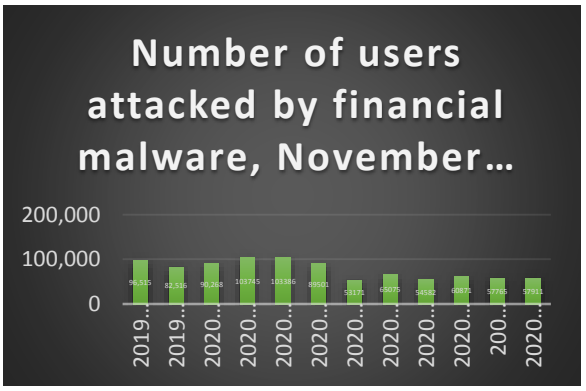

Fig 10: Number of users attacked

The financial sector's total annual cost of cybercrime is calculated to be USD18.5 million. According to recent reports, 82% of financial institutions that have recently reported ransomware attacks believe that attackers' internal knowledge has increased and that tactics have become substantially more advanced. During the preliminary wave of the pandemic, the financial sector gradual transition to remote working created a vulnerability that attackers quickly exploited. As a result, 57% of those polled recently think that cyberattacks are rising uncontrollably as the sector is being tested by the threat the pandemic holds. The extorsion of Data has clearly been the ultimate profitable ransomware tool used by criminals within the cyber space around the globe, and the 2019- 2020 Covid global pandemic has undoubtedly intensified this change. Since the 2019 -2020 pandemic started, cyberattacks on the financial sector have dominated news headlines around the world. During the current COVID-19 pandemic, Moody's warned banks around the world of "increased chances of cyberattacks." VMware Carbon Black conducted a general survey and reported that between February and April 2020, the 2019 – 2020 global pandemic resulted in the Financial sector coming under the weight of cyberattacks. Over the same time frame, ransomware attacks rose nine-

fold. In July 2020, the Reserve Bank of India (RBI) raised concerns about cybersecurity in its financial stability survey. The problems posed by growing cyber threats were highlighted in the study, with the financial sector being a main focus for these attacks. The national security advisor recently stated that "financial frauds grew rapidly as a result of greater reliance on digital payment systems following the 2019 -2020 global pandemic." Others reported that in the last week of June, multinational hackers made headlines by attempting over 40,000 cyberattacks on banks in India and other institutions, over a five-day stretch.

The Proposed Literature Solution

Finally, we identify and present by way of literature the Machine Learning and Artificial Intelligence as a means of fighting back. This involves the use of machine learning to predict future attacks based on historical data and the use of artificial intelligence to revise policies based on the outcome of the predictions taking into consideration new technology proposals.

As attacks increases, detecting attacks early is the best approach forward. Most importantly preventing these attacks should be the main focus of all security policies. We are, without a doubt, living in the most pivotal moment in human history. The dawn of the internet of things, which unites all electronics into a single network. Banks have emerged as one of the most important players in this modern era. Banks depend on technology and its implementations. To understand financial establishment vulnerable and susceptibility to cyberattacks, this study categorizes financial establishment into three vulnerable classes.

Class One: Financial Establishments in this class are referred to in this context as "Timber and Caliber". This class is the least vulnerable and susceptible to cyberattacks as they least depend on network systems like the internet to conduct business.

Class Two: Financial Establishments in this class are referred to in this context as "Sand and Bricks".

These establishments deal with both over the counter and uses the internet to conduct transactions. They are daily faced with high level of vulnerabilities because of how their organizations business outlines are [Online and Offline]. These vulnerabilities are because of the transactions their businesses support online.

Class Three: Financial Establishments in this class are referred to in this context as "Sand and water," have total decency on computer networks, all their business depends on both internal network (intranet) and external networks (internet). These organizations are at the most vulnerable and susceptible to cyber-attacks.

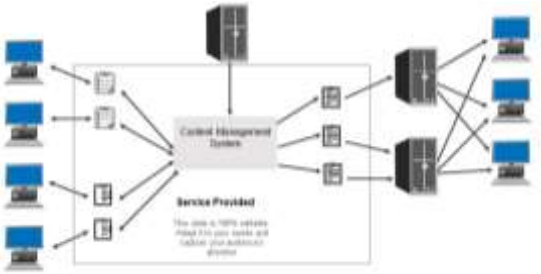

Fig 11: The Banking Architecture (Intranet without Internet)

With Internet Comes the Exposure [Class two and Three]

Sonic-Wall in 2019 researched into certain exposures and reported that 10.52 billion malware attacks occurred between 2018 and 2019 including 217 percent rise in Internet of Things attacks.

They also reported new threat types estimated around 391,689. These numbers have dramatically improved in 2020, and they are expected to rise exponentially by the end of 2021. Furthermore, today's cyber criminals are adapting to new technologies and it's because of this I propose the use of advance tools for the detection and reporting of these attacks. To do this I suggest the use of AI and ML [Artificial Intelligence and Machine Learning]. AI and ML are two of the most hotly debated technological developments that have the potential to completely change the digital defense infrastructure landscape. Any strategy that allows computers to imitate human behavior is referred to as artificial intelligence. The capability to self-sustain intelligence void of direct programming is known as Machine Learning. All of these methods are often used in fields such as hospitals, finance, and storage. DoS and DDoS [Denial of Service and Distributed Denial of Service are the two most used technologies to attack institutions, using Machine Learning algorithm through mining application specific logs we can detect these attacks. To practice and predict if a DoS/DDoS attack has occurred, ML algorithms may be adopted. We will then notify the security engineer via email just when an attack is detected.

197

Any classification algorithm can be adopted to determine whether or not an attack is a DoS or DDoS. SVM [Vector Machine] is a supervised learning system use to analyses data to identify patterns, this is an example of a classification algorithm. AI and ML are both Data driven in their decision-making techniques and they do not require definitive programming. AI

streamlines procedures and voids itself of human involvement. AI is influencing how businesses make decisions. This allows computers to perform tasks that previously required the use of a workforce to run different machines. When AI is used, data and algorithms are provided as feedback, teaching the computer to execute a certain task with extreme precision. Processes are being optimized with AI, and tasks are becoming faster and more error-free. Data is also mined and different patterns dependent on previous trends are pulled out using artificial intelligence and machine learning. These patterns aid in making assumptions about the present and future. Most of those problems ought to be resolved through self-gaining knowledge, AI-primarily based cybersecurity control systems. There is different technology that can be used to effectively train an AI to collect Data from business information uninterrupted. The collected data is then processed, used to conduct patterns correlation across billions of signals that are clear-cut and tailored to the institutions attack surface. In furtherance to this new intelligence are constantly fed to organization categorized in cybersecurity bullets like;

- **Breach Risk Prediction-** The forecasting of when an organization will be compromised can be done using AI based programs. Taking into consideration vulnerabilities so organizations can allocate enough resources to correct the vulnerabilities. Dictatorial recommendations obtained through the research done by the AI will aid organizations to configure, setup, enhance controls and procedures to increase the organization's cyber resilience effectively
- **Threat Exposure –** Hackers track patterns and use them to attack organizations. AI-powered cybersecurity technologies can provide real-time awareness of global and sector-specific dangers, permitting organizations to priorities threats based on the most likely pattern to be used by hackers to attack the organization.

Machine Learning (ML) and Artificial Intelligence (AI) Methods for High-Volume Data Analysis

- Correlating various data sets by arranging them in a certain fashion, scanning various potential attacks, doing a predictive analysis, and predicting the next attack are all things that can be done.
- Continuous auditing of data security techniques can be performed using data cleaning techniques to protect consumers and other interested parties, testing if the controls in place are successful.
- Creating systems to protect data without putting a strain on infrastructure. Cybersecurity experts can reduce costs and prevent unnecessary spending by using machine learning and artificial intelligence.
- Various viruses and pathogens can be quickly identified using artificial intelligence and machine learning by putting in place a security infrastructure with a built-in system for searching large volumes of data, data networks, and recognizing any potential risks.

Machine Learning algorithms are classified to detect Cyber Attacks as:

1. **Supervised Learning:** The Supervised Learning in Machine Learning is to predicts the learning algorithms that is labelled training information. Supervised Learning is including decision tree, linear regression, logistic regression and support vector machine.
2. **Unsupervised Learning:** The Unsupervised Learning in Machine Learning is to find interesting patterns of datasets. It predicts the unlabeled training information for the task of inferring. Unsupervised Learning including clustering and behavioral patterns.

Applications of Machine Learning used in Cyber Security are:

1. **Threat Detection:** Machine Learning is used application in Cyber Security is threat security for using a developed model to identifying the attacks. The models are to monitor and respond to threats and attacks in a real time. It helps to determine and identify the behavior of malware in datasets.
2. **Network Risk Scoring:** Machine Learning is used application in Cyber Security is network risk scoring for quantitative measures in various sections of networks. It can be used by analyzing cyber-attacks datasets and determine certain types of attacks. The risk score is quantifying the impact of attack.

198

3. **Automate and Optimize Security and Human Analysis:** Machine Learning is used application in Cyber Security Automate and Optimize Security and Human Analysis for security activities. It has done by analyzing the reports of attacks and build a model to optimize the security that are performed by humans.

Machine Learning-protect against Cyber Attacks as:

1. **Software keeps up to date:** Machine Learning is required to keep software up to date. It is mandatory and crucial to update and upgrade the software to protect them from cyber-attacks. The outdated software is easy and vulnerable to cyber-attacks. Software patches among others.
2. **Strengthen the Credentials:** Machine Learning can be used to help to strengthen the credentials of employees. It is necessary to determine the strong and complex passwords.
3. **Multifactor Authentication:** Machine Learning is enhancing with multifactor authentication. It basically adds an information to protect from cyber-attacks. It accessing the information by additional requirements.
4. **Protect with Cyber Liability Insurance:** Machine Learning is to protect with cyber liability insurance, join cyber security course online. Cyber liability insurance is to protect the information against sophisticated data breaches.
5. **Evaluating detection by Machine Learning:** Machine Learning is evaluating the detection as main aimed is to classified a threat during systems operations. It is basically done when the data is altered through the testing process.

The brain of AI is ML, it contains an algorithm that permits it to learn and interpret data based in past experiences permitting it to make human like decision. In cybersecurity, machine learning algorithms can diagnose and interpret security events automatically. Machine learning is now used in many modern defense tools, such as threat intelligence. Several ML algorithm exist however most possess the following;

Clustering is a technique for identifying correlations between datasets and grouping them together based on those similarities. Clustering operates on recent evidence without taking prior cases into account.

Classification—Classification algorithms aim to adapt what they've learned from previous observations to current, unobserved results. Objects are classified under one of the names during the classification process. Sorting binary file into groups like lawful applications, spyware, ransomware, or adware, for example.

Vulnerability Management

Organizations are having a difficult time managing and prioritizing the vast number of potential vulnerabilities that they encounter on a regular basis. Vulnerability detection methods used in the past only responded to accidents when hackers had already abused the flaw. Vulnerability databases' vulnerability detection features can be improved using AI and machine learning techniques. Furthermore, as tools like UEBA [User and Event Behavior Analytics] are controlled by AI, AI can monitor user behavior on endpoints and servers to spot irregularities that may signify unseen threat, this can help companies secure themselves before bugs are publicly disclosed or patched.

Hunting Threat

Signatures or attack signs are used by traditional defense tools to detect attacks. This method will quickly detect threats that have already been identified. Signature-based systems, on the other hand, are unable to identify threats that have yet to be identified. In fact, only about 90% of threats are detected by them. Traditional detection rates can be increased by up to 95% using AI. The issue is that you could have a lot of false positives. A mixture of AI and conventional approaches will be the best choice.

This combination of traditional and novel methods will improve identification rates by up to 100%, reducing false positives. By incorporating behavior detection, AI may also enhance threat identification. For example, by analyzing data from endpoints, you can create profiles for any program in your organization's network.

Network security

The two key facets of traditional network management approaches are designing security protocols and observing the network environment. Here are few things to think about:

Security policies may aid in the differentiation between legitimate and fraudulent network links. A zero-trust model can also be enforced by policies. Creating and enforcing rules for a vast range of networks, on the other hand, can be difficult.

Finally, the Revision of Cybersecurity Policy using AI

Analyses current POLICIES in the wake of evolving Malware and Ransomware Landscape using AI and ML

199 come necessary.

The ineffectiveness of the current policies to implement security architecture and structures has left the banks exposed. The current policies used by the financial sector are not effective in the wake of evolving malware and ransomware landscape. This is simply because the policies are not well informed as it takes time to revise them using human efforts as new techniques and encryptions algorithms are developed by cyber bullies and attackers each day, there should be an automatic system void of human interventions that is able to access data, new trends, new technologies and develop security polies that is current and effective against cyber-attacks using AI. In this propose literature, I suggest the use of machine

learning [ML], to predict future attacks by using the banks current security policy and historical data. Once this is done, the predictions which should involve threat analysis based on current vulnerabilities, hackers' technologies and encryptions methods should be fed as input dataset to another AI system which will use those datasets to revise the banks cybersecurity policy. Automating the revision of security policies on a daily basics will help the financial sector fight back as vulnerabilities will be known before attackers gains access through the vulnerability points.

REFERENCES

[1] Sans.org. 2021. Information Security Policy Templates | SANS Institute. [online] Available at: <https://www.sans.org/information-security-policy/> [Accessed 12 April 2021].

[2] Fsb.org. 2019. 7. [online] Available at: <https://www.fsb.org/wp-content/uploads/P121118-1.pdf> [Accessed 12 April 2021].

[3] Bis.org. 2020. BIS Bulletin No 37. [online] Available at:<https://www.bis.org/publ/bisbull37.pdf> [Accessed 12 April 2021].

[4] Ref no: IOSCO/MR/17/2016. 2016. CPMI-IOSCO release guidance on cyber resilience for financial market infrastructures. [online] Available at:<https://www.iosco.org/news/pdf/IOSCONEWS433.pdf> [Accessed 12 April 2021].

[5] Sura Sheth, N., 2020. What is Cyber Risk? [online] Logicgate.com. Available at: <https://www.logicgate.com/blog/grc-101-what-is-cyber-risk/> [Accessed 12 April 2021].

[6] Go.kaspersky.com. 2021. Kaspersky Security Bulletin 2020. Statistics. [online] Available at: <https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf> [Accessed 12 April 2021].

[7] Deloitte United States. 2019. The Future of Cyber Survey 2019. [online] Available at: <https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html> [Accessed 12 April 2021].

[8] En.wikipedia.org. 2021. Bangladesh Bank robbery - Wikipedia. [online] Available at: <https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery> [Accessed 12 April 2021].

[9] Alam, N., 2016. The great Bangladesh cyber heist shows truth is stranger than fiction. [online] Dhaka Tribune. Available at: <https://www.dhakatribune.com/uncategorized/2016/03/12/the-great-bangladesh-cyber-heist-shows-truth-is-stranger-than-fiction> [Accessed 12 April 2021].

[10] FS-ISAC, I., 2020. [EWS75] EWS - Phishing Threats for Remote Workers. [online] Fsisac.com. Available at: <https://www.fsisac.com/resources> [Accessed 12 April 2021].

[11] Check Point Research. 2020. The 2020 Cyber Security Report - Check Point Research. [online] Available at: <https://research.checkpoint.com/2020/the-2020-cyber-security-report/> [Accessed 12 April 2021].

[12] Go.kaspersky.com. 2020. Kaspersky Security Bulletin 2020. Statistics. [online] Available at: <https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf> [Accessed 12 April 2021].

[13] "Financial frauds rising due to dependence on digital payment platforms: NSA Ajit Doval", Money Control, September 19, 2020, https://www.moneycontrol.com/news/india/financial-frauds-witnessing-a-spike-due-to-dependence-on-digital-payment-platforms-ajit-doval-5859641.html

[14] "Rise in cyber attacks from China, Over 40,000 Cases In 5 Days: Official"NDTV, June 23, 2020, https://www.ndtv.com/indianews/rise-in-cyber-attacks-from-china-over-40-000-cases-in-5-days-official-2251111

[15] 2020. The Industrialization of Cybercrime. [online] https://www.imf.org/. Available at: <https://www.imf.org/external/pubs/ft/fandd/2018/06/global-cybercrime-industry-and-financial-sector/gaidosch.htm> [Accessed 12 April 2021].

[16] J. Bates, "High Level-Programs & the AIDS Trojan," In: Wilding E, Skulason F (eds) Virus Bulletin. Virus Bulletin Ltd., Oxon, England, Feb., pages 8–10, 1990.

[17] A. Young, M. Yung, "Cryptovirology: Extortion-Based Security Threats and Countermeasures," In: McHugh J, Dinolt G (eds) Symposium on Security & Privacy. IEEE Computer Society Press, Washington DC, pages 129-141, 1996. "Jahewi's Anti-Malware Information". July 18, 2006. 200 :d from the original on June 11, 2008.

[18] Mcafee.com. 2016. McAfee Labs Threats Report, December 2016. [online] Available at: <https://www.mcafee.com/enterprise/en-us/assets/reports/ rp-quarterly-threats-dec-2016.pdf> [Accessed 12 April 2021].

[19] Institutional Asset Manager. 2021. Data extortion ransomware attacks on financial sector up 350 per cent during Covid-19 pandemic. [online] Available at: <https://www.institutionalassetmanager.co.uk/2021/03/02/296548/data-extortion-ransomware-attacks-financial-sector-350-cent-during-covid-19#:~:text=Sign%20up%20now-,Data%20extortion%20ransomware%20attacks%20on%20financial%20sector%20up,cent%20during%20Covid%2D19%20pandemic&text=The%20global%20Covid%2D19%20pandemic,sectors%20%E2%80%93%20including%20finance%20%E2%80%93%20vulnerable.> [Accessed 12 April 2021].

[20] Www2.deloitte.com. 2021. Cybersecurity in the Indian banking industry. [online] Available at:

<https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-cybersecurity-in-the-indian-banking-industry-noexp.pdf> [Accessed 12 April 2021].

[21] Www2.deloitte.com. 2021. Cybersecurity in the Indian banking industry. [online] Available at: <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-cybersecurity-in-the-indian-banking-industry-noexp.pdf> [Accessed 12 April 2021].

[22] GreatLearning Blog: Free Resources what Matters to shape your Career!. 2021. How will AI and Machine Learning (ML) Affect Cyber Security?. [online] Available at: <https://www.mygreatlearning.com/blog/how-will-ai-and-machine-learning-affect-cyber-security/> [Accessed 12 April 2021].

[23] Horizon 2020 Work Programme 2014-2015. 2015. Leadership in Enabling and Industrial Technologies: Information and Communication Technologies. Retrieved November 25, 2019 from http://ec.europa.eu/research/participants/portal4/doc/call/h2020/common/1587758-05i._ict_wp_2014-2015_en.pdf.

[24] Lozada, L., 2017. Ransomware: Analyzing the Impact on Healthcare and the Economy - ProQuest. [online] Search.proquest.com. Available at: <https://search.proquest.com/openview/74b300065749129c74f4bd3a56cb2238/1.pdf?pq-origsite=gscholar&cbl=18750&diss=y> [Accessed 12 April 2021].

[25] Uddin, M., Ali, M. and Hassan, M., 2020. Cybersecurity Hazards and Financial System Vulnerability: A Synthesis of Literature. SSRN Electronic Journal, [online] Available at: <https://www.researchgate.net/publication/343724670_Cybersecurity_hazards_and_financial_system_vulnerability_a_synthesis_of_literature> [Accessed 12 April 2021].

[26] Icscsi.org. 2015. McAfee Labs Threats Report. [online] Available at: <https://icscsi.org/library/Documents/Threat_Intelligence/McAfee%20-%20Threat%20Report%202015-1Q.pdf> [Accessed 12 April 2021].

[27] Accenture.com. 2019. 2019 Cost of Cybercrime Study | 9th Annual | Accenture. [online] Available at: <https://www.accenture.com/us-en/insights/security/ cost-cybercrime-study> [Accessed 12 April 2021].

[28] Security Affairs. 2021. Cybercrime Statistics in 2019. [online] Available at: <https://securityaffairs.co/wordpress/96531/cyber-crime/cybercrime-statistics-in-2019.html> [Accessed 12 April 2021].

[29] BOUTIN, J. AND CHEREPANOV, A. MODERN ATTACKS AGAINST RUSSIAN FINANCIAL INSTITUTIONS **In-text:** (Boutin and Cherepanov, 2016) **Your Bibliography:** Boutin, J. and Cherepanov, A., 2016. MODERN ATTACKS AGAINST RUSSIAN FINANCIAL INSTITUTIONS. [online] Virusbulletin.com. Available at: <https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-BoutinCherepanov.pdf> [Accessed 15 April 2021].

[30] BOUTIN, J. AND CHEREPANOV, A. MODERN ATTACKS AGAINST RUSSIAN FINANCIAL INSTITUTIONS **In-text:** (Boutin and Cherepanov, 2016) **Your Bibliography:** Boutin, J. and Cherepanov, A., 2016. MODERN ATTACKS AGAINST RUSSIAN FINANCIAL INSTITUTIONS. [online] Virusbulletin.com. Available at: <https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Boutin-Cherepanov.pdf> [Accessed 15 April 2021].

[31] NATIONAL CYBERSECURITY POLICY FRAMEWORK FOR SOUTH AFRICA **In-text: (**NATIONAL CYBERSECURITY POLICY FRAMEWORK FOR SOUTH AFRICA, 2015) SOUTH AFRICA. [online] Available at: <https://www.gov.za/sites/default /files/gcis_document/201512/39475gon609.pdf> [Accessed 15 April 2021].

[32] GLOBAL CYBERSECURITY INDEX (GCI) 2017 **In-text:** (Global Cybersecurity Index (GCI) 2017, 2017) **Your Bibliography:** Itu.int. 2017. Global Cybersecurity Index (GCI) 2017. [online] Available at: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf> [Accessed 15 April 2021].

[33] CONNOR, T. AND WINTER, T. Iranians Charged With Cyber Attacks on U.S. Banks, Dam **In-text:** (Connor and Winter, 2016) **Your Bibliography:** Connor, T. and Winter, T., 2016. Iranians Charged With Cyber Attacks on U.S. Banks, Dam. [online] NBC News. Available at: <https://www.nbcnews.com/news/us-news/iranians-charged-hacking-attacks-u-s-banks-dam-n544801> [Accessed 15 April 2021