مجلة الأصيل للبحوث الاقتصادية والإدارية
El - Acil Journal for Economic and Administrative Research
ISSN: 2571-9866
EISSN: 2661-7854
Volume: 5 /N °1./June2021, PP448-464

The importance of cyber security in the financial sector in the age of digital transformation

أهمية الأمن السبراني في القطاع المالي في ظل التحول الرقمي

***Sanaa Laib**
Emir Abd Elkader University For Islamic Science (Algeria)
Laibsana89@gmail.com

***Received**: 04 /05/2021* ***Accepted**: 27/06/2021* ***Published**: 30/06/2021*

Abstract :
The present article aims to determine The importance of cyber security in the financial sector in the age of digital transformation, by getting an overview of the cyber security as it is defined by specialized literature, international legislation, and perform an analysis of attacks reported in the financial sector over the last view years until the covid-19 crisis, in order to determine patterns and trends in cyber-crime.

Based on the results of the analysis, we find that the hackers chose financial institutions as easy targets due to the fact that they can spread the attack quickly through the interconnected financial system, and because most of the financial institutes still use legacy digital systems. In this context the international authorities insist on the collective work to enhance the Cyber-risk awareness culture.

Keywords :cyber security, cyber attacks, cyber risk, financial sector,digital transformation.
JEL classification codes:D8,P43.

ملخص:
نهدف من خلال هذا البحث إلى التعرف على مدى أهمية الأمن السبراني في القطاع المالي في ظل التغيرات الرقمية، من خلال عرض مفهوم الأمن السبراني وعلاقته بالمفاهيم الأمنية الأخرى، وكذا عرض أنواع الهجمات السبرانية وتحيل أثرها على القطاع المالي خلال السنوات الماضية وصولا إلى أزمة كوفيد-19 لرصد اتجاه الجريمة السبرانية. واستنادا لنتائج التحليل وجد أن القطاع المالي يعد الأسهل اختراقا نظرا لقدم الأنظمة الرقمية المستعملة، وبالتالي فإن انتشار الهجمات السبرانية يعد أمرا سهلا لترابط النظام المالي، وفي هذا الإطار حثت الهيئات الدولية على ضرورة العمل الجماعي لنشر الوعي حول الخطر السبراني ومواجهته.

الكلمات المفتاحية: الأمن السبراني، الهجمات السبرانية، الخطر السبراني، القطاع المالي، التحول الرقمي.
تصنيف JEL: D8,P43

Corresponding author

1. Introduction

Internet and information technology has transformed the world and has created new opportunities for the global economy and humanity at the globe. The financial sector is undergoing massive changes in the age of the digital transformation, which enabled improving market efficiency, providing more efficient and faster services, improving financial inclusion and enhancing customer experience.

The sector is witnessing the negative aspects of this development, breaches and hacking operations are increasing dramatically, threatening the confidentiality and integrity of financial data. Due to these attacks the economic losses is reached at 3500 million dollars, Losses increased during the Covid-19 crisis, like what is happened to 'Dave' banking app on July 25, 2020when hackers published data and personal information of 7.5 million users **(carnegie endowment for international peace, 2021)**. Given the rising of data breaches, the topic of cyber security has launched to the top of the priority list for boards of directors and different internationl authorities at the globe to enhance the protection of confidentiality, integrity, and availability of information.

By this study we aim to determine the importance of cybersecurity in the era of digital transformations and its impacts on the financial industry. Accordingly we have to set answers for the following questions:

1. Whyis the financial sector most vulnerable from hackers?
2. Are the cyber attacks related to territorial boundaryand development of countries?
3. Why are the cyber security frameworks ineffective facing cyber attacks?

To achieve the aim of study, we were formulatingthe answers for the previous questions:

1. The financial sector is greater vulnerable from hackers due to their vibrant role.
2. The cyber attacks related to the development degree of each country.
3. The individualwork makes the cyber security frameworks ineffective facing the common cyber attacks.

To clarify the previous points, we werestructuring the study in four axes:

1. Conceptual framework
2. Types of cyber attacks
3. Cyber attacks statistics.
4. International cyber security frameworks

2. Conceptual framework

2.1. What is cyber security?

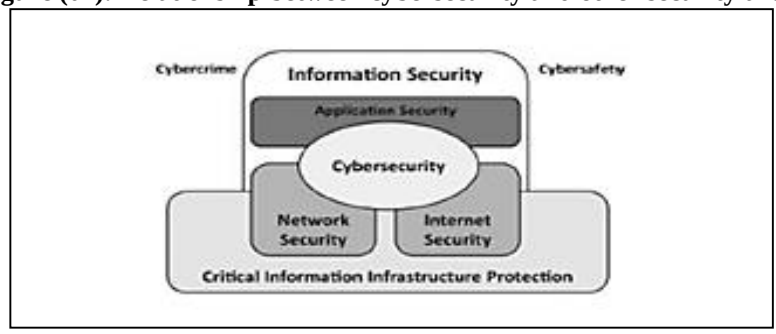
Due to the wide spread of the Internet and its versatility, our protection in the cyber space becomes a necessity whether at home or at work. Cyber security is one of the most prevalent topics in our days. Many literatures have dealt with the topic of cyber security. Among the definitions contained therein are the following:

- "A set of technologies, processes and practices used to protect networks, computers, programs and data from attack or unauthorized access"**(Center, 2018, p. 11)**
- It can be said that it is: a set of policies, guidelines, processes and procedures necessary to enable the implementation of electronic transactions with minimal risks of hacking, intrusion or theft.
- CS in the financial sector has appeared as "an operational issue since onlinebased criminal activities, frauds, and system failures can disrupt banking functions"**(Hamid Uddin & al, Auguste 2020, p. 14)**

2.2. Relationship between cyber security and other security areas:

As we mentioned the cyber security is concerned with the confidentiality, integrity, and availability of information in the cyber space. In parallel the information security interpreted as preservation of the confidentiality, integrity, and availability of information.

Figure (01): Relationship between cybersecurity and other security areas



Source: (Laurent & Bobin, 2019, p. 16).

By comparing the two concepts together, we find that the cyber security is part of information security, like the figure shows, we find that the information security has many aspects, including cybersecurity which is narrowed to protect the digital assets.

In confirmation of the foregoing, the Basel Committee urged (within the principles of cyber governance) the necessity of adopting policies and procedures to protect information security in order to ensure the good management of risks, and this confirms the relationship between information security and cyber security.

We can point that the same committee recognized the necessity of establishing safety controls for all major information systems in the bank to maintain the correctness, integrity and confidentiality of information and for more safety; all major systems must be reviewed by other external parties with competence in the risk management framework.

From what has been presented previously, weconclude that cybersecurity is part of the risk management process.

2.3. types of cyber attacks:

The terms cyber attacks, cyber crimes, and other related terms which means an unauthorized access made by a person to cracking the systems or an attempt to bypass the security mechanisms, by hacking the banking sites or accounts of the customers**(kumudha & Rajan, 2018, p. 1561)**. Among the international literature that has dealt with the types of cyber attacks are the following:

- **Spam emails:** are unsolicited emails or junk newsgroup postings. Spam emails are sent without the consent of the receiver potentially creating a wide range of problems if they are not filtered appropriately **(Manisha M & al, December 2015, p. 745).**
- **Denial-of-service (DoS):** This attack is performed over the network user's computer to make it inaccessible to the user by flooding them with messages to trigger the crash **(Adharsh & Dhatchina, Decemder 2020, p. 02).**
- **Fiscal fraud:** By targeting official online payment channels, cyber attackers can hamper processes such as tax collection or make fraudulent claims for benefits **(Manisha M & al, December 2015, p. 745).**

- **Malware:** is a generic term describing types of malicious software, used by the attacker to compromise the confidentiality, availability and integrity of data. **(Bendovschi, 13-14 April 2015, p. 03)**Most common types of malware are:
  - ✓ **Viruses and worms:** are computer programs that affect the storage devices of a computer or network, which then replicate information without the knowledge of the user **(Junaido & Mua'zu, 2015, p. 07)**
  - ✓ **Trojan:** is a malicious computer program designed to steal sensitive and confidential information stored or processed through online banking systems. **(Bulueliv, 2019, p. 20)**
  - ✓ **Spyware:** It is malicious software installed in a user's computer without their knowledge hacker can access all the files and their stored file in the system **(Adharsh & Dhatchina, Decemder 2020, p. 03).**
  - ✓ **Ransomware:** are caused by a type of malicious software or malware designed to deny access to a computer system or data until a ransom is paid. Such an attack on a financial institution can cause monetary damage **(RSBP for Central Asia, 2020, p. 02).**
  - ✓ **Adware:** is a security threat that is usually employed to accumulate marketing data or show adverts in order to create revenue **(Yilamaz & Zavrak, 2015, p. 5599).**
  - ✓ **Scareware:** some cyber criminals compel users to download certain software. While such software is usually presented as antivirus software, after some time these programs start attacking the user's system. The user then has to pay the criminals to remove such viruses **(Manisha M & al, December 2015, p. 745).**
  - ✓ **Keyloggers:**this programs are building for Keystroke logging and creating records of everything typing on computer Keyboard, this programs can used for controlling the devices while it is used. Some criminals used Key loggers to steal the data. **(Kaspersky, 2021)**
- **Carders:** Stealing bank or credit card details are another major cyber crime. Duplicate cards are then used to withdraw cash at ATMs or in shops **(Junaido & Mua'zu, 2015, p. 08).**
- **Spoofing:**Through this type of attack the hacker tries to use a computer, device, or network to trick other computer networks by masquerading as a legal entity **(Kaspersky, 2021)**
- **Phishing:**it is a social engineering technique that aims to influence the target to reveal his personal information, such as email, password, or any other financial information through which a hacker can take over the target balances **(Alabdan, 2020, p. 01).**

Due to the variety and sophistication of the cyber attacks, it can target any part in the financial sector (banks, financial market, etc.). The following are some of the possible scenarios **(Boer & Vasques, september 2017, p. 04):**

1. Attack on Payment Systems.
2. Integrity of data.
3. Failure of wider infrastructure.
4. Loss of confidence.

From the previous definitions of the types of cyberattacks we can say that this practices can makes a cyber risk, since it is caused by the human factor, in this regard it is classified as: "one of form of operational risk" **(Aldasaro & al, 14 january 2021, p. 03)**, more clearly it is defined as: "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems" **(Bouvert, 2019, p. 78).**

3. Cyber attacks statistics:

The Exposure Classification according to the **CSI** is based on data collected from publicly available sources in the dark web and deep web and from data breaches. From this data, signs of sensitive disclosures, exposed credentials and hackergroup activity against companies are identified. Companies are ranked based on the number of findings and identifiedrisks divided by their employee counts **(cyber Intelligence House, 2021).**

A study from Frisby contained out of 108 countries, to reveal the most/least exposure countries. The CSI provides an exposure classification scale (very high, high, moderate, low, very low) as the table below shows:

Table (01):Exposure Classification Distribution

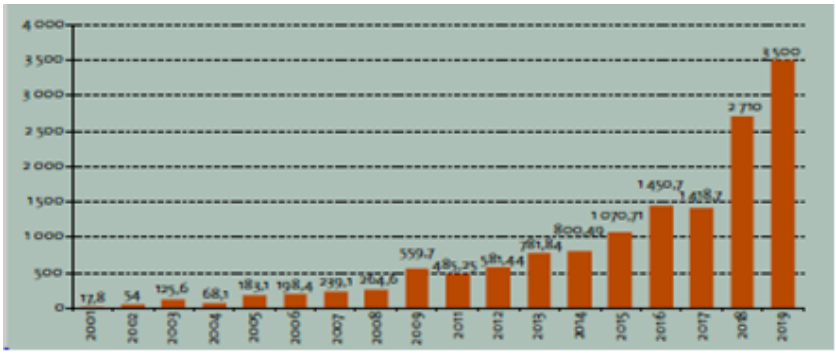
Continent	Very High	High	Moderate	Low	Very Low
Europe	0	2	10	21	8
North America	0	3	4	1	1
South America	1	3	5	1	0
Asia-Pacific	3	11	8	7	3
Africa	1	11	3	1	0
Global	**5**	**30**	**30**	**31**	**12**

Source: (Frisby, 2020)

The study found that:

- ✓ **Africa:**Classified in the **high** exposure group with 0.643 point (**Ethiopia**is the most country exposure with 0.866p;**Mauritius** is the least country exposure with 0.200p).
- ✓ **Asia-Pacific:** Classified in the **moderate** exposure group with 0.483 point (**Afghanistan** is the most country exposure with1.000p;**Australia** is the least country exposure with 0.131p).
- ✓ **South America:**Classified in the **moderate** exposure group with 0.541 point (**Venezuela**is the most country exposure with 0. 807p; Uruguay is the least country exposure with 0.348p).
- ✓ **North America:** Classified in the **moderate** exposure group with 0.207 p (**El Salvador**is the most country exposure with0.517p;**USA**is the least country exposure with 0.145p).
- ✓ **Europe:**Classified in the **low** exposure group with 0.207 point (**Armenia**is the most country exposure with 0.655p;**Finland**is the least country exposure with 0.110p).

Figure (02) : Annual economic losses due to cybercrime

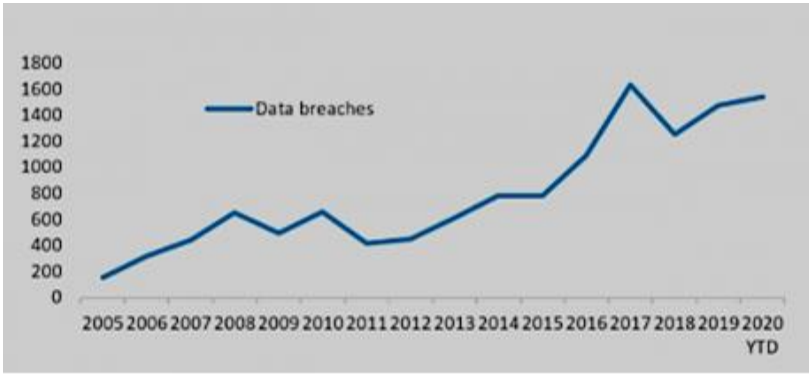


Source: ECLAC report, 2020, p10.(Fal, 2020, p. 10)

The financial losses resulting from cyber attacks are rising at the digitalization of processes advanced, it is reached their peak within 2019 at nearly 3500 million dollars. These figures represent only reported incidences. More than 90% of incidences are not reported in order to avoid damaging organization's reputation,

Study of cyber security Venture expects that the global cyber attacks costs grows by 15% per year over the next 5 years, reaching 10.5 billion dollars annually by 2025 **(Morgan, january 21, 2021, p. 01),** it means that according to the cyber attacksincreases since the technology revolution growths.

Figure (03): The rise of cyber attacks

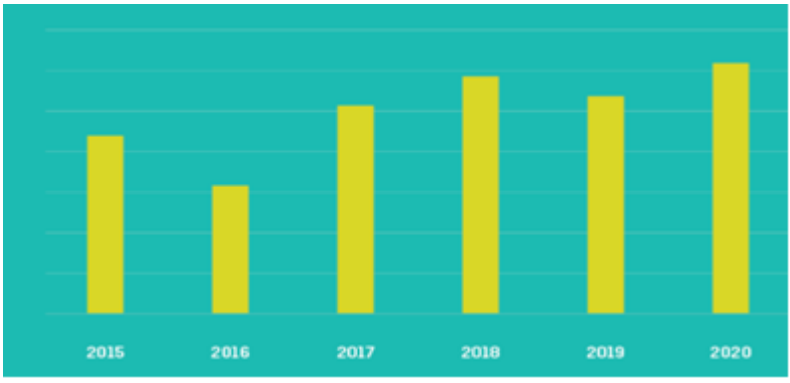


Source : (Bouveret, June 2018, p. 08)

During the period (2005-2020), the financial sector is undergoing massive cyberattacks, increased in severity due to the increasing use and spread of the Internet, as well as the expansion in the use of digital payments and the spread of financial technology companies.

Among financial institutions, banks account for the bulk of the attacks (%91 of the attacks), followed by insurance companies (%7). Among banks, retail banking activities (%39) and credit cards services (%25) were the main business lines targeted.Thestatisticsreflects theunwillingness to face cyber attacks, duo to weak risk governance, and reliance on old mechanisms that are easy to penetrate. Theinterconnected of financial system facilitate the transmission of risks from one institution to another. That is makes the financial system more vulnerable to cyber incidents **(Velieva & Al, 2021).**

Figure (04): phishing incidents during the period (2015-2020)

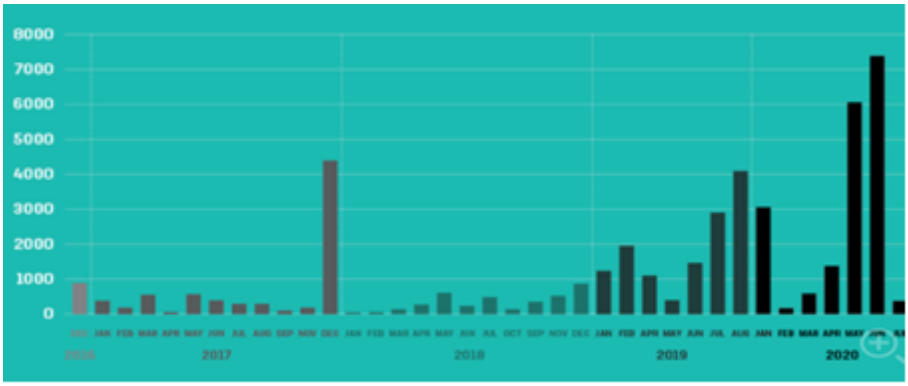


Source: (Warburton, 2020, p. 04)

The finance sector became the most attacked sector globally, despite a 46 % drop in attack volume in APAC. Attacks against finance were characterized by extensive use of spyware and keyloggers, as well as application-based attacks **(NTT, 2018, p. 05)**

The overall number of phishing detectionsin 2019 stood at 467,188,119 cases, 51.4% of thosewas financerelated attacks. The number is increased in 2020 by 15% compared with last year. In the **USA** 52% of all attacks were due to remote work which facilitated the hacking operations especially for institutions that are lack of preparedness to face hackers **(SecureList, 2020).** In **UK**, phishing accounted for 28% of all cases reported during the period of April 2019-Match 2020,according to the **(OAIC)**data the number of phishing reached at %36 of all hacking events which related to thefts credentials(the most initial channels of attacks with %29 of all cyber events) **(Warburton, 2020, p. 04).**It should be noted that **USA**, **UK**, Australia were classified in the moderate exposure zone, however they witnessed a high cyber breaches percentage. We can say that the cyber risk is not related to the territorial boundary or development degree of each country, but rather is related to the hacking mechanisms.

Figure (05) : quantity of stolen cards from during the period (2015-2020)



Source:, https://www.f5.com (Warburton, 2020, p. 16)

The stolen cards have been decliningat the peak in 2016, 97.2% of all cards had full names related with them. In 2020 this number has dropped to 84.9%. Likewise, card validity has also fallen. At its worst in 2017, 76% of cards were in date at the time of discovery. This had dropped to just 32.8% in 2020.

A study from Juniper Research in 2016 expected that the value of online fraudulent transactions is to reach $25.6 billion by 2020, up from $10.7 billion in 2019. This means that by the end of the decade, $4 in every $1,000 of online payments will be fraudulent **(Guechi, 2020, p. 349)**

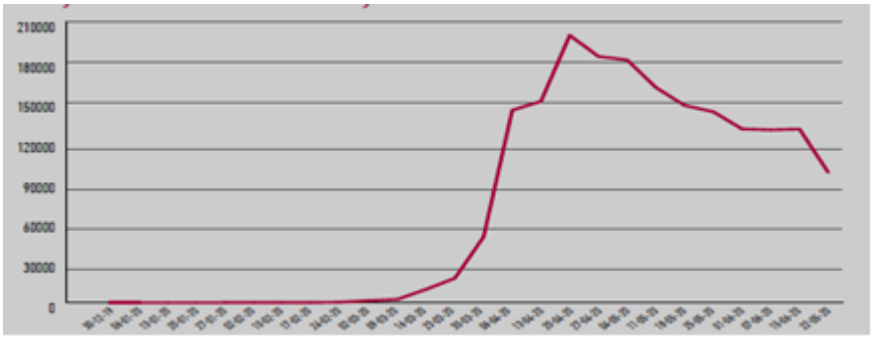
Within the **COVID-19**crisis, the increased number of people working from home and using digital channels for banking has created an ultimate environment for cybercrime to grow and for cybercriminals to use their mechanisms in a more aggressive manner**(RSBP for Central Assia, 2020, p. 02).**

Figure (06): Covid-19-related cyber events by sector

Source: (Aldasaro & al, 14 january 2021, p. 06)

The listed statistics show the degree to which each sector is affected individually during the period of **covid-19**, and it was found that the financial sector is the most affected with 25.3%, followed by the service sector with 24.4% Out of total reported cyber-attacks. According to a report by Keeper security, 70% of reported attacks are real and successfully implemented. The affected businesses attribute these attacks to circumstances related to the pandemic **(Muncaster, 2021).**

Figure (07): Cyber attacks since the appearance of COVID-19



Source: (Chek Pouint Software Technologies, 2020, p. 04)

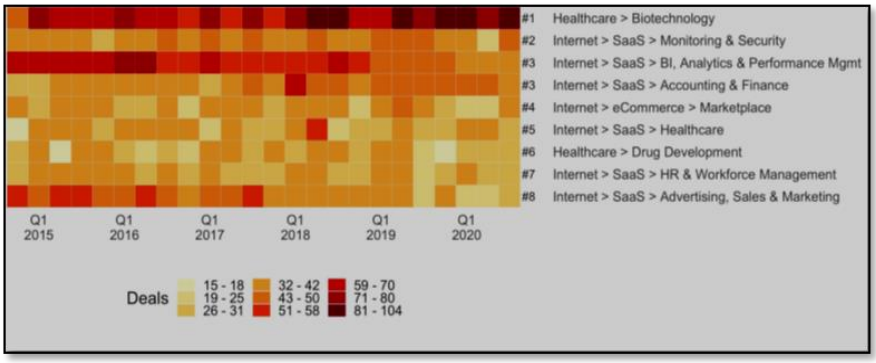
At the beginning of the second quarter of 2020, cyber attacks witnessed a significant escalation, where it reached nearly 21,000 attacks on various sectors on April 20, 2020. Due to ECLAC 2020 report, on an annual basis, ransoware attacks increased up to 108%,

while attacks on the Internet of things increased to 833%. This growth reflects the exposed weaknesses due to the raise in unexpected demands that cover a large number of people in a short time. **(Fal, 2020, p. 10)**

4. Investing in cyber security:

In a published report by **CB** insights &**PwC**, about capital investment, it is found that during the third quarter of 2020, surveillance and security deals grew more than double what they did in the second quarter of the same year. This caused by the increasing frequency of cyber attacks on various sectors, most of which are considered successful attacks. **(Colombos, 2020):**

Figure (08): That monitoring and security deals in Q3 2020



source: (PwC CB Insights, 2020, p. 18)

Meanwhile, 92% of financial services firms increased their cybersecurity investment over the previous 12 months. The primary investment priorities for the cyber information security officers (CISOs) over the next 12 months include secure file transfer (64%), protecting the remote workforce (63%) and cloud/Office365 (56%) **(Security Brief, 2020).**

The global cyber security market size was valued at 156.5 billion USD in 2019 and is expected to expand at a compound annual growth rate (**CAGR**) of 10.0% from 2020 to 2027 **(Grand View Reaserch, 2021).**In parallel the spending on cybersecurity reached at 131 billion Dollars in 2020, it is expected to reach174 billion Dollars by 2022; this expansion is due to the organizations' awareness of the need to find more effective ways to ensure protection, confidentiality of data against future attacks.

In 2019 a survey study of out of 580 senior executives from **IT** Information Security, Cybersecurity and **IT** Operations in 7 sectors

across 10 countries (The least exposure countries), include the investment in Artificial Intelligent (**AI**) to enhance cyber security, found that 69% of organizations believe that they will not be able to respond to cyberattacks without AI, 81% of banks from the banking sector believe in AI **(Tolido & al, 2019, p. 05).**

Several cyber security institutions demonstrated their competence and ability to adapt, and attract clients. From the most important institutions that were ranked among the top 20 cybersecurity start-ups to watch in 2020: **Axis Security**and **Cato Networks** which are a **SASE** (Secure Access Service Edge) provider, their products were built on the zero trust security framework **(Colombos, 2020).**

Since the **Q2**of 2020 the cyber security posed major challengesfor investors that look to achieve serval unique goals in 2021 **(Guercio, 2021):**

- ✓ Scalability and lean research and development
- ✓ Investors looks to have an air tight business plans that will enable to solve real, large scale problems.
- ✓ Achieve regulatory compliance to maintain customer's compliance with general regulations, in order to ensure their privacy data.
- ✓ Support Remote Work and impact the remote worker.

5. International cyber security frameworks:

5.1. Guidelines of different countries:

A study from **IMF** in 2021 has found that 50% countries have no cyber security strategy in place, only 38% of countries have published their guidelines, and just 12% are in the process of developing one.

- **Singapore:ASEAN** countries developed their cyber security policy to enhance public trust on online transaction with ensuring open internet to promote innovation, Combating cyber crimes to protect their citizen privacy **(Sunkpho & al, 26-28 Match 2018, p. 02).** In this context the Cyber Security Agency (**CSA**) of Singapore posed major guidelines to protect information confidentiality on the private/public sector**(Hamid Uddin & al, Auguste 2020, p. 296):**
  - ✓ Build a resilient cybersecurity infrastructure.
  - ✓ Develop safer cyberspace.
  - ✓ Promote a vibrant cybersecurity ecosystem.
  - ✓ Enhance international partnership and cooperation.

- **Australia:** The Australian Cyber Security Centre (**ACSC**) submits several guidelines, such as **(Jenkins, 2020):**
  - ✓ Defendingcritical infrastructure.
  - ✓ Setting new methods to investigate and shut down cyber crime.
  - ✓ Strengthening defences for government networks and data.
  - ✓ Improving sharing of threat information.
  - ✓ Enhancingcollaboration with industry through the **JCSC** (Joint Cyber Security Centres) program.

The measures taken by each country seem to be general measures to strengthen national security and not to protect financial systems. This is owing to the fact that cyber security is not included in the risk management policies. The thing that elucidates the difficulty of accessing loss data related to cyber risks, since it is treated as an operational risk.

5.2. Basel Committee on Banking Supervision (BCBS):

In December 2018 **BCBS** published a report on the range of cyber-resilience practices, which contained cyber-governance principals. **(BCBS, December 2018, pp. 11-15):**

- ✓ Cyber risk strategy should beincluded within risk management policy that setting by board of direction.
- ✓ The committee insists on assigning the task of CR management to the cyber information security officer (**CISO**) who reports to the cyber risk officer.
- ✓ Most of banks do not include special requirement to address cyber security workforce skills.Therefore, the committee urged on spreading awareness of cyber risk, promoting a common risk management culture in the banking industry

5.3. The International Monetary fund (IMF):

In November 2020 the **CEIP** released a report titled "International Strategy to Better Protect the Global Financial System against Cyber Threats". Developed in collaboration with the **WEF**, the report included major principles **(Maure & Nelson, Spring 2021):**

- ✓ More clarity about roles and responsabilities.
- ✓ Given the financial losses resulting from cyber attacks, banks/ financial institutions should unified international **CS** framework, urge common collaboration to stop cyber crime.
- ✓ Focusing on the financial sector by setting more effective protection frameworks provides better protection of other sectors in the future.
- ✓

6. CONCLUSION

The purpose of this study is to discover the role of cybersecurity in protecting the confidentiality of financial data in light of digital transformations, which makes major changes in the financial sector, we have found that the concept of cyber security falls under the concept of information security (as it is broader and comprehensive), which in turn falls under the concept of risk management. These risks, which varied and multiplied by the multiplicity of methods of piracy and penetration, since it is caused by the human factor, it is classified as one of form of operational risk, and are managing within this scope.

The financial sector is hard fragile facing of cyber attacks, due to the fact that the hackers can spread the attack quickly through the interconnected financial system, and because most of the financial institutes still use legacy digital systems, 91% of attacks detected in the banks, more than 68% was phishing attacks during 2020.

Most countries that were hacked, were not necessarily classified within the most exposure group, likewise North America which wasexposure to more than 52% of the total attacks during 2020, it means that the cyber attacksarenot related to the territorial boundary or development degree of each country, but rather is related to the hacking mechanisms.

Cybersecurity posed a major challenge to the financial sector during the Covid-19 period; the attacks increased and caused huge losses to the economy as a whole. The cybersecurity market has expanded dramatically in order to develop mechanisms that ensure the preservation and integrity of data confidentiality. Investment in this field was not only limited to specialized institutions, the financial institutions worked to develop this aspect, by using height technologies (eg: Artificial Intelligent, Internet of Things).

The losses resulting from the cyber attacks still increased, in the absence of unified policies of cybersecurity at the global level, the **BCBS** and **IMF** insist on the collective work to enhance the Cyber-risk awareness culture, sincethe individual work is very costly, and the continuous spending on enhancing data protection in light of technological development is in itself a financial burden.

Bibliography:

I Journal articles:

1. Alabdan, R. (2020, September 30). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. future Internet Journal, vol 12(Issue 10), 01-39.
2. Bouvert, A. (2019, April). Cyber Risk for the Financial services Sector. Journal of Financial Transformation, vol 49.
3. Hamid Uddin, M., & al. (August 2020). Cyber security hazards and financial system vulnerability: a synthesis of literature. Risk Management N22.
4. Junaido, B. M., &Mua'zu, A. S (2015). Cyber-Attacks: The legal response,. International Journal of International Law, Vol 01(Issue 02).
5. Guechi, M. (2020, June 30). The Future of the banking industry in the era Of digital transformation. (U. A. Draya,) Journal of Economic Integration, vol 08(N 02), 341-353.
6. Manisha M, M., & al. (December 2015). Online Banking and Cyber Attacks: The Current Scenario. international Journal of advanced research in Computer Science and Software Engineering, VOl 5(Issue 12).
7. Yilamaz, S &Zavrak, S (2015). Adware: Are view. International Journal for Computer Science and Information Technology, vol 06(N 06).

II Seminar articles:

1. Adharsh, M., &Dhatchina, M. (December 2020). Cyber Attacks in banking industry. cyber attacks in banks; Bournemouth Project: cyber crime in banking.
2. Sunkpho, J., & al. (26-28 Match 2018). Cyber security Policy in ASEAN Countries. Dans G. D. Samonas, 17th Annual security Conference-Securing the interconnected world, (01-07). Las Vegas.

III Reports:

1. Aldasaro, I., & al. (14 January 2021). Covid-19 and cyber risk in the financial sector. Bulletin, Bank of International Settlement, Basel.
2. BCBS. (December 2018). Cyber-resilience: Range of practice. Bank for International Settlement, Basel.
3. Boer, M., &Vasques, J. (september 2017). Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system. The Institution of International Finance (IIF), Washington.

4. Bouveret, A. (June 2018). cyber security for the financial sector: A Framework for Quantitive Assessment. Working paper, IMF.
5. Bulueliv. (2019). cyber threat intelligence for Banking &Financial services. spain: Bulueliv.
6. Center, D. I. (2018). Islamic Fintech Report 2018 Current Landscape & Path Forward. Dubai.
7. Check Point Software Technologies. (2020). Cyber attacks trends: 2020 MID-YEAR REPORT. San Carlos.
8. Fal. (2020). Cybersecurity in the time of COVID-19 and the transition to cyber immunity. Spain: Facilitation of transport and trade in Latin America and Caribbean.
9. Maure, T., & Nelson, A. (Spring 2021). the global cyber threat. IMF.
10. Morgan, S (January 21, 2021), Cyber warefare in the c-suite, Cyber Security Venture, California.
11. NTT, S. (2018). Global Threat Intelligence Report. Buenos Aires.
12. PwC CB Insights. (2020). Money Tree Report Q3 2020. New York.
13. RSBP for Central Asia. (2020). COVID-19: cybersecurity challenges for financial institutions.
14. Tolido, R., & al (2019). Reinventing Cybersecurity with Artificial Intelligence: The frontier in digital security. Capgemini Research Institute, Paris.
15. Warburton, D. (2020). 2020 phishing and fraud report. F5Labs, Seattle.

IV Internet websites:

1. Carnegie endowment for international peace. (2021). Timeline of cyber incidents Involving Financial institutions. Retrieved 02 17, 2021, from Carnegie endowment for international peace: http:// carnegieendowment.org
2. Colombos, L. (2020, 11 29). The Top 20 Cybersecurity Startups To Watch In 2021. Retrieved 01 21, 2021, from Forbs: www.Forbs.com
3. cyber Intelligence House. (2021). Cyber Exposure Index. Retrieved 01 29, 2021, from cyber Intelligence House: http://cyberexposureindex.com
4. Frisby, J. (2020, JUNE 02). Cyber security Exposure Index (CEI). Retrieved 02 24, 2021, from Passwordmanagers.co: http://passwordmanagers.co
5. Goud, N. (s.d.). Cyber Attacks incur $100 billion losses to Financial Institutions. Retrieved 01 21, 2021, sur http://www.cybersecurity-insiders.com

6. Grand View Research. (2021, April). Cyber Security Market Size, Share & Trends Analysis Report By Component, By Security Type, By Solution, By Services, By Deployment, By Organization, By Application, By Region, And Segment Forecasts, 2021 - 2028. Retrieved April 27, 2021, from Grand View Research: http://www.grandviewreaserch.com
7. Guercio, K. (2021, 01 29). Top 22 Cybersecurity Startups to Watch in 2021. Retrieved 03 23, 2021, from eSecurity Planet: www.esecurityplanet.com
8. Jenkins, S. (2020, August). 2020 Cyber Security Strategy calls for centralization of federal agency network. Retrieved 02 03, 2021, from the mandarin: http://www.themandarin.com
9. Kaspersky. (2021). What is IP spoofing? Retrieved 01 28, 2021, from Kaspersky: http://www.Kaspersky.com
10. Kaspersky. (2021). What is Kstroke Logging and Keyloggers. Retrieved 06 05, 2021, from Kaspersky: http://www.Kaspersky.com
11. Muncaster P. (2021, 01 19). Most Financial Services Have Suffered COVID -Linked Cyber attacks. Retrieved 03 11, 2021, from Infosecurity Magazine: http://www.Infosecurity Magazine.com
12. Secure List. (2020, April 16). Retrieved 03 05, 2021, Financial Cyber threats in 2019, https://securelist.com/financial-cyberthreats-in-2019/96692/
13. Security Brief. (2020, 11 07). 92% of financial services Firms increased cyber security investment this year. Retrieved 02 16, 2021, from Security Brief: http://SecurityBrief.co.nz
14. Velieva I, & Al. (2021, May 24). Cyber risk in new Era: The effect on bank ratings. Retrieved June 18, 2021, from S& P Global Ratings: http://www.spglobal.com/ratings