Estimating the Cyber Risk of the Financial Sector in Portugal

José Barbosa

Lusófona University, Porto - Portugal
josepmbarbos@gmail.com

Abstract. In a world where technology has taken over most aspects of our daily lives, the financial sector is not an exception. In the same way that our information and data can be stolen, intercepted or even tampered with, the financial sector is subject to a much higher cybersecurity risk than any other sector. From banks to the stock market, even insurance companies, no one in this sector is immune to attacks in the technological department. On this paper, we will be focusing on the cybersecurity threats to the financial sector worldwide, and then we will focus on the case of Portugal. We will also discuss the risks, vulnerabilities and the means to prevent attacks and intrusions to promote cybersecurity.

Keywords: Technology, Financial sector, Cybersecurity risk, Stock market, cybersecurity.

1 Introduction

With the invention of the computer and the exponential technological advances that followed it, most industries and services were able to implement such advancements, that provided them with certain advantages such as the automatization of certain tasks and serving as an aid in others. These advancements proved themselves incredibly useful.

They were followed by another invention that would change the way we go about our daily lives, a way to connect all our computers and many of our devices, the internet. With an impact reminiscent of the industrial revolution, these new discoveries launched us into the cyber era and changed business and life altogether.

One of the biggest profiteers of these technological advancements was the financial sector in general. From banks, ATM's (Automated Teller Machine) and even the stock market all relies on cutting edge technology. [1] [2]

With these new opportunities, came new means of to carry out criminal activities, relying on the communication between these systems. Either for espionage in order to gain advantage over the competition or even theft, given that these systems handle monetary transactions, with the digitalization of the financial sector, a door was opened for those with knowledge and criminal intentions, making these new advancements as damaging as they are rewarding. [3]

10.11228/dpsc.03.01.007

2 Cybersecurity threats to the financial sector

2.1 Definition of the financial sector

The financial sector is a section of the economy made up of firms and institutions that provide financial services to commercial and retail customers. This sector comprises a broad range of industries including banks, investment companies, insurance companies, and real estate firms. [4]

2.2 Cybersecurity threats that target the financial sector

Being one of the biggest sources of income in multiple countries, the financial and the insurance industry are also one of the most desirable targets for hackers and cyber criminals [5]. For this reason, this sector is subject to several threats, such as:

- **Malwares**: short for malicious software, a malware consists of a harmful computer program that aims to get access to privileged information. A malware is essentially a program design to cause harm to a system and can do so in several ways [6]. In this case, it is common the use of information stealing malwares, such as key loggers able to steal passwords [5].
- **Phishing**: phishing consists of a fraudulent message, in form of a text message or an email, that tries to trick the receivers into believing that they are going to win something or that they have debts to pay, and will try to convince them to download an attachment or click on a link. What makes these attacks particularly effective is the fact that the attacker disguises himself as someone who the victim trusts or might even do business with. It is one of the oldest forms of cyber-attack [7]. This results in the disclosing of financial and personal information, identity theft, identity fraud and theft of personal information [5].
- **Theft or loss of proprietary or confidential information or hardware**: A data breach, harmful to the company who suffered it both financially and in terms of reputation, that can be divided into two categories, physical breaches, when using, for example, stolen data storage devices, and non-physical breaches, such as network intrusions [5].
- **Insider abuse of access**: This happens when someone who has authorized access, use their knowledge of the business's vulnerabilities to carry out illicit or malign activities, such as theft, eavesdropping, modification of information or even for their personal advantage by selling the information to the competition or using it for their personal advantage [5].
- **Denial-of-service**: The denial-of-service consists of an attack directly upon the computer or system that one aims to render useless. These attacks are made by flooding a system with requests, making it so that normal traffic cannot be processed, thus denying services to its users. These can be divided into two categories, buffer overflow attacks, which is when an overflow consumes all the hard disk space, memory, or even CPU time,

and flood attacks, when a designated server is flooded with packets, thus saturating the server, and rendering it useless [8].

2.3 Measures to prevent cyberattacks

Within the financial sector and when it comes to cybersecurity threats, attacks share one of two natures, being either internal or external.

The internal attacks are known to be more dangerous and damaging, and according to the 2014 U.S. State of Cybercrime Survey [10], 37% of organizations have suffered an insider attack and 32% go as far to say that these attacks were more damaging than the outsider attacks. In 82% of the cases, sensitive or private information was released to the public unintentionally and in 72% of the incidents, confidential data was stolen. In 71% and 63% of these incidents, respectively, customer and employee records were compromised or stolen.

These numbers, while worrying, are only referring to the known cases of insider attacks, since most of these transgressions usually go unnoticed. They are mostly handled internally and very rarely they involve legal actions, mostly due to the lack of evidence usually attributed to these cybercrimes and the difficulty to prove malicious intent. [9]

These attacks happen mostly due to lack of awareness and the negligence of basic security measures such as password sharing practices, unlocked devices, unsecure Wi-Fi networks and weak passwords.

Some of the best ways to prevent insider attacks are:

- **Educating employees –** By showing employees the importance of cybersecurity and the correct practices, resources and measures for safe networking.
- **Encrypting data –** Making our data unreadable and useless to those who access it without permission.
- **Implementing proper password managing practices -** Enable two-factor-verification and use complex passwords to add a second layer of security and reconfirm a user's identity every time they log in. Change passwords every six months and make sure they contain upper and lowercase letters, numbers and symbols.
- **Installing antivirus software –** Antivirus scan the whole system in search of malicious files or even virus and in most cases can even handle spyware and malware.
- **Updating all devices –** Outdated devices are usually more vulnerable to all types of unauthorized accesses. [11]

Outsider attacks however are when individuals or group tries to steal protected data or more, by infiltrating the system or organization in question. They can be individual hackers, organized crime groups or even government entities. The attack itself can also be divided into active or passive. An active attack generates packets or participates in the network while a passive attack is eavesdropping the network or tracking users. The motive behind these attacks can be Cyber Espionage, Cyber Warfare, and Hacktivism. [12]

The following measures may reduce the risk of suffering an outsider attack:

- **Using multi-factor authentication –** This system makes it so that more than one factor is required to access our data. If the only mean of protection we have is a password, it can easily be compromised through phishing attacks for example. If the system is protected with more than just a password, but also a card, or an email verification it becomes harder to access it without authorization.
- **Responsibilities of third-party security –** if it is crucial that third parties must access our systems, such as vendors or other companies, it must be done in a safe way. In this case, it is necessary to monitor the networks, creating tight security controls and to identify potential cyber threats.
- **Educating employees –** this measure is important for both outside and inside threats. Employees may be victims of scams, phishing attacks or many other schemes, that may be avoided if they are prepared to face such issues. This can be done through seminars, or even annual training sessions.
- **Creating data backups –** creating data backups is essential to assure that the business in question maintains its productivity, even in the wort case scenarios. this prevents us from losing our data and even helps with some ransomware cases.
- **Keeping the systems updated –** Outdated systems are usually easier to access. For this reason, keeping the systems updated, even if there is some financial cost attached to it, is crucial to the security of the business. Updates patch vulnerabilities that previous versions might have had and protect against potential security threats.
- **Installing antivirus and firewalls –** Possibly the most important step in what comes to protection from outside attacks, is to install antivirus software in every system that accesses the private network of a business and regularly update it. And for further protection a firewall should also be installed, in order to prevent threats from the outside. [13]

3 The cyber risk to the financial sector in Portugal

3.1 Financial institutions in Portugal

According to a study by Banco de Portugal [14], in 2018, financial institutions were the victims of 25,7% of all malicious cyberattacks, in the first three months of 2019, the number of credit card thefts increased by 212%. There was an increase of 129% of client's credentials being compromised and there was an increase of 102% of malicious apps, including bank related apps for mobile devices.

In a country where the financial sector grows daily, cybercrime is still one of the most damaging factors to the economy, almost as much as geopolitical uncertainties and NPL's (Non-Performing Loan).

Figure 1 – The growth of cybersecurity risk as a concern to the global economy. [15]

Cybersecurity incidents may be responsible for the following impacts:

- **Financial risk –** Cybercrime results in major monetary losses, it may involve judicial costs, expropriation of funds, the costs associated with the safety of the damaged systems and taxes or sanctions for non-compliances of contractual obligations.
- **Reputational risk –** Companies and service providers will lose the trust of their clients for the mediatic exposure associated with security issues. The non-compliance of security measures may lead to sanctions and even further defamation of the business in question. Critical data may also be exposed to the public.
- **Operational risk –** The company may be unable to provide essential services to the public. Inability to integrate systems and networks in outsourcing.
- **Legal risk –** Non-compliance of deadlines, inability to comply with legal and contractual obligations. Inability to obey the AML/CTF (Anti-Money Laundering, Counter-Terrorism Financing) legislation. Loss of data integrity and confidentiality. Possible occurrence of disputes.

These risks all lead to monetary lost and to the disruption of services, and all may lead to financial instability.

Due to growing threat of cybercrime, Portugal has qualified authorities that assist those who have been victims of these crimes. The CNCS (Centro Nacional de Ciber Segurança), is the national centre of cybersecurity, and is the entity to whom all types of cybercrime must be reported by law. And the UNC3T (Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica), the operational unit that helps prevent and overall fight cybercrime. This unit handles prevention, detection and investigation of cybercrime.

Banco de Portugal divides authority approach in three fundamental pillars:

- **Regulation**
- **Supervision**
- **Cooperation**

3.2 Report obligations

If a financial institution was to fall victim of a cybercrime, the incident must be reported to legal authorities. Once it occurs, we must evaluate first if its impact was relevant. In order to evaluate it, we must answer questions such as:

- How many users did it affect?
- Was it damaging economically?
- Was it damaging towards the business' reputation?
- Did it activate the crisis management mechanisms?
- Was it attributed internal relevance?
- Were there any legal or regular non-compliances?
- Is it a systemic risk?

By answering these questions, we can determine if an attack was relevant or not. If the attack was considered relevant, it should be reported to the CNCS in three phases:

- **Initial (< 2 hours)** – A brief notification and description of the attack.
- **Intermediate (< 10 days) –** Details and relevant actualizations.
- **Final (> 30 days)** – Causes and corrective measures applied.

If the attack wasn't relevant however, then, the CNCS does not need to be informed of the transgression or should be notified voluntarily. [14]

4 Denial of Service (DoS)

A denial of service attack is a type of cyber-attack where a malicious individual or group tries to render a computer or any other system unavailable and therefore, useless to its intended users by interrupting the device's normal functioning. They usually function by flooding or overwhelming the targeted system with requests until normal traffic can no longer be processed, resulting in denial of service to the users. In a DoS attack only one computer is used to start the attack. These attacks usually target the infrastructure layer; however, they may also target the application layer.

Another attack of the same nature as DoS is the DDoS which stands for distributed denial of service. It consists of a DoS attack that comes from multiple sources.

DoS attacks are usually divided into two categories:

- **Buffer overflow attacks –** It is an attack in which a memory causes the system to consume all available hard disk space, memory or CPU time. This attack usually results in system crashes, sluggish behaviour and other inconveniences that ultimately lead to denial of service.
- **Flood attacks –** These attacks work by saturating a targeted server with an overwhelming number of packets, saturating server capacities, and causing denial of service. For these attacks to work, the attacker must have a wider bandwidth than the victim.

Some of the biggest DoS attacks so far have been:

- **Smurf attacks –** Attacks where an individual utilizes the broadcast address of a vulnerable network by sending spoofed packets resulting in the flooding of the targeted IP address.
- **Ping flood –** A simple form of DoS is based on flooding the target with ICMP (ping) packets. By feeding the target more pings than it is able to respond, we may cause denial of service. This attack can be qualified as a DDoS.
- **Ping of death –** Often confused with ping flood, the ping of death consists in sending the targeted system a malformed packet, that results in harmful behaviour, such as system crashes. [16]

4.1 Real cases of DoS in the financial sector

On September and October 2012, a group by the name "Izz ad-Din al-Qassam Cyber Fighters" attacked several financial institutions. On December that same year, the group attacked six banks in three days, by causing severe slowdowns and blocking access to the banks. Luckily, the previous attacks encouraged banks to prepare themselves for future attacks, thus making the attacks less impactful than they might have been. [17]

More recently, a series of Hungarian banks and telecommunication companies were also attacked by powerful DDoS attacks, launched from servers in Russia, China and Vietnam. [18]

4.2 How to prevent DoS attacks

In order to reduce the risk of suffering a DoS attack, the following measures should be implemented:

1. **Reducing the area of the attack surface –** By minimizing the surface that can be attacked, we limit the attackers' options and allows us to focus our protection in one place. We do this by making sure that our devices don't communicate with doors, protocols or apps that are not supposed to communicate with it.

10.11228/dpsc.03.01.007

2. **Planning –** The two main aspects that should be planned are bandwidth and server capacity. In terms of bandwidth, we must make sure that the provider offers a broad connectivity that can handle great volumes of traffic. In what comes to the server capacity, since DoS attacks are meant to consume resources, it is important that we can control our resources when needed. We do this by running larger computing resources or those that have features like more extensive network interfaces or enhanced networks that support larger volumes.
3. **Knowing the difference between normal and abnormal traffic –** Whenever an excessively large amount of traffic is detected, the host must process it without affecting the system's availability. Advanced protection techniques are able to accept only the legitimate traffic by analysing individual packages.
4. **Implementing firewalls –** Firewalls can protect us from all sorts of attacks, namely SQL injection or request forgery between sites, which attempt to exploit a vulnerability in the application itself. Firewalls can filter packages by country, by size or even IP, which makes us able to choose the traffic that we will receive.

5 Conclusion

Without any doubt, the market and industries will continue to grow with the aid of networking and technology in general. The exponential evolution we've gone through over the last decades brought over numerous advantages but on the other side, it also cursed us with other ways to damage, steal or harm us.

The financial sector is no exception, as it is the sector that is the most subject to all cybersecurity threats, whether they come in the form of unauthorized accesses, phishing scams or even the much-dreaded DoS attacks.

While writing this paper I gained a more serious notion that cyber security is not just something that is advised, it is essential in order to safely benefit from all types of networking, namely when handling monetary transactions or large monetary amounts.

References

1. R. Gourlay, A., J. Pentecost, E.: The Determinants of Technology Diffusion: Evidence from the UK Financial Sector. Economic Research Paper No. 00/9. (2000).
2. Lagazio, Monica, Sherif, Nazneen and Cushman, Mike (2014) A multi-level approach to understanding the impact of cyber crime on the financial sector. Computers & Security, online . pp. 1-32. ISSN 01674048 (In Press)
3. ERIKSSON, J., GIACOMELLO, G.: The Information Revolution, Security, and International Relations: (IR)relevant Theory?. International Political Science Review. 27, 221–244 (2006).
4. Kenton, W.: Financial Sector, https://www.investopedia.com/terms/f/financial_sector.asp.

5. Choo K 2011. Cyber threat landscape faced by financial and insurance industry. *Trends & issues in crime and criminal justice* no. 408. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi408
6. Fruhlinger, J.: Malware explained: How to prevent, detect and recover from it, https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html.
7. Fruhlinger, J.: What is phishing? How this cyber attack works and how to prevent it, https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html.
8. What is a Denial-of-Service (DoS) Attack?, https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/.
9. Kul, G. and Upadhyaya, S., 2020. Towards A Cyber Ontology For Insider Threats In The Financial Sector. State University of New York at Buffalo, Buffalo, NY, USA.
10. C. I. T. Center, "2014 U.S. State of Cybercrime Survey," July 2014.
11. Grinavich, J., n.d. Business Security: How To Prevent Insider Attacks. [online] Vector Security. Available at: <https://www.vectorsecurity.com/blog/business-security-how-to-prevent-insider-attacks> [Accessed 16 December 2020].
12. JA, A., 2015. Insider Vs. Outsider Threats: Identify And Prevent |. [online] Resources.infosecinstitute.com. Available at: <https://resources.infosecinstitute.com/topic/insider-vs-outsider-threats-identify-and-prevent/> [Accessed 17 December 2020].
13. Managed IT Services & Technology Consulting | OSIbeyond. 2020. How To Prevent Cyber Attacks On Businesses In 2020 | Osibeyond. [online] Available at: <https://www.osibeyond.com/blog/7-methods-to-prevent-cyber-attacks/> [Accessed 17 December 2020].
14. Costa Ferreira, L., 2019. Ciber-resiliência no setor bancário A perspetiva do Banco de Portugal.
15. Lagarde, C., 2020. Estimating Cyber Risk For The Financial Sector. [online] IMFblog. Available at: <https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/> [Accessed 18 December 2020].
16. Cloudflare. 2020. What Is A Denial-Of-Service (Dos) Attack?. [online] Available at: <https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/> [Accessed 18 December 2020].
17. Felter, B., 2020. 7 Of The Most Famous Recent Ddos Attacks. [online] Vxchnge.com. Available at: <https://www.vxchnge.com/blog/recent-ddos-attacks-on-companies> [Accessed 18 December 2020].
18. Carnegie Endowment for International Peace. 2020. Timeline Of Cyber Incidents Involving Financial Institutions. [online] Available at: <https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline> [Accessed 18 December 2020].
19. Amazon Web Services, Inc. 2020. O Que É Um Ataque Ddos E Como Proteger Seu Site Contra Um Deles. [online] Available at: <https://aws.amazon.com/pt/shield/ddos-attack-protection/> [Accessed 19 December 2020].
20. B. Panja, D. Fattaleh, M. Mercado, A. Robinson and P. Meharia, "Cybersecurity in banking and financial sector: Security analysis of a mobile banking application," *2013 International Conference on Collaboration Technologies and Systems (CTS)*, San Diego, CA, 2013, pp. 397-403, doi: 10.1109/CTS.2013.6567261.
21. *Catota, F., Morgan, M. and Sicker, D., 2018. Cybersecurity incident response capabilities in the Ecuadorian financial sector. Journal of Cybersecurity, 4(1).*

22. *Journal of Xidian University, 2020. The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector. 14(7).*
23. *Didenko, A., 2020. Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond. Uniform Law Review, 25(1), pp.125-167.*
24. *Calliess, C. and Baumgarten, A., 2020. Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective. German Law Journal, 21(6), pp.1149-1179.*
25. *Smith, S., 2020. EMERGING TECHNOLOGIES AND IMPLICATIONS FOR FINANCIAL CYBERSECURITY. International Journal of Economics and Financial Issues, pp.27-32.*