International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Evolution of Compliance and Cybersecurity: A Risk Management Perspective in Financial Markets

Bruna Veiga

Abstract: ***This paper has the purpose to investigate how cibersecurity can impact at the way that the compliance's standards are being developed. This frame considered the background of the regulation and the laws provided by the american legislators and regulators. Also, it aims to explore how a company shall develop the risk management and build the continuity of the business. It is important to highlight that this concern is revelant for companies with any size and assets under management. Specially for companies that provides financial services, this relationship must reflect on the way that the data will be protected, using an analyze to take care of this protection and fullfilling with all the standards required by the regulation in force. At least, the paper will also reflect about the consequences – as warnings and fines – for non-compliance with standards imposed by the regulation and the laws provided by the american legislators and regulators.***

Keywords: compliance, cybersecurity, financial companies, regulations, risk management

1. Introduction

The compliance department has developed some standards and obligations from the past years until nowadays, specially from the decade of 1970s. For some years, even if this department has started to be built, it was not still a priority for most of the companies. At the begginings – from 1970s to 1980s – the main concern for the compliance department was on ethics.

Specially due to some scandals investigated by the US Securities and Exchange Commission (SEC), dirty money, terrorism and drug traffick were the specific topics to be handled by the regulation. That is why te Currency and Foreign Transactions Reporting Act of 1970 was referred to as the Bank Secrecy Act (BSA).

At this time, the Department of the Treasury was allowed to impose requirements on financial companies to detect and prevent money laundering. Also, in 1977, the Foreign Corrupt Practices Act (FCPA) was signed into law. In 1990s, the companies have began to be held liable and be prosecuted for the criminal acts of their employees. Combining with this development, some of the internal control procedures have been created, requiring all companies at the financial market to adhere to stringent rules.
The criminal meaning for liability got more clear after the case United States v. Hilton Hotels Corp.[1] This case stablished that companies must be liable for the criminal attempts of employees. It is important to highlight that this responsability started to be defined even if all policies and manuals on behalf of the company defines that this behaviour is not allowed.

By the beggining of 2000s, some guidelines started to be built to prevent and detect crimes, implement new procedures for due diligence, monitor and report suspect behaviours and promote compliance as a culture for the company through the training schedule. Also, Sarbanes-Oxley Act of 2002 developed measures, increasing corporate responsibility and protecting investors. Due to the subprime crisis in 2008, SOX also included a provision in order to protect whistle-blowers at publicly traded companies.

How cibersecurity started to be related to compliance and risk management

As a consequence of all events described above, at 2010s, US DOJ and SEC significantly updated the regulatory schemes as long as the accountability and transparency were provided in corporate accounting. This was an huge step in order to promote financial stability, fulfilling all gaps that the regulatory and the laws still had at the time.

The next chapter about the concern at a perspective for compliance and risk management was guaranting that all companies seek to accomplish with parameters for cibersecurity. It is important to define that "*the term cybersecurity refers to the practice of protecting computer systems, networks, programs, and data, specifically from digital attacks, unauthorized access, damage, or theft. Cybersecurity also has to do with the processes and technologies that assist in this endeavor*."[2]

Actaully, since 1980s – when the using of computers started to be more wide for personal use – the whole world deals with attacks from hackers. Due to this market shift, a lot of systems have developed abroad (such as the The Domain Name System), and all security challenges became bigger as well.

Also, it is important to highlight that the internet ascends in the 1990s impacted also in the way that digital technologies started to be more used at the corporate's daily routines. That is the reason why many companies started to have firewalls as a necessary defense. However, since 2010s – and even more during the COVID-19 pandemic –, the whole world

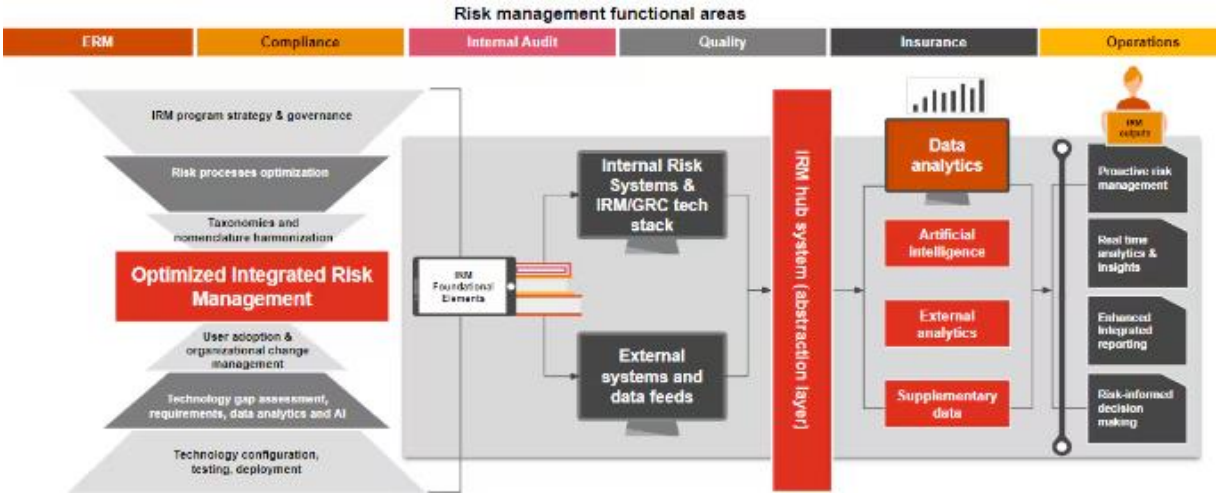
[1] "*The preoccupation of Congress with corporate liability was only emphasized by the adoption in 1914 of section 14 of the Clayton Act to reaffirm and emphasize that such liability was not exclusive, and that corporate agents also were subject to punishment if they authorized, ordered, or participated in the acts constituting the violation*." SKELTON, Chris. 1973. *United States v. Hilton Hotels Corp., 467 F.2d 1000 (9th Cir. 1973)*. JUSTIA US LAW. Available from https://law.justia.com/cases/federal/appellate-courts/F2/467/1000/154124/. [Accessed on 10/10/2024]

[2] CORO. *A History of Cybersecurity and Cyber Threats*. Available from https://www.coro.net/blog/history-of-cybersecurity-and-cyber-threats. Accessed on 10/10/2024]

became more ware about archieving all documents and data in cloud systems.

Considering that financial companies provides services and products for clients, all of them are obligated to be aware about (i) how to do a data mapping frequently, (ii) accomplishing a data loss prevention, (iii) doing annually a penetration test and (iii) concluding all the evidences found at a risk analyze, to be reported to all partners and directors in time.

As a consequence, all stakes of the compliance department became bigger in accordance with this development. Also, these events required that the financial companies must prove that all regulations and laws in force are being envisioned and organized. For that reason, the subjects to be carried by the compliance department have been updated, in accordance with the keys to risk management, as shown below.[3]



Putting together all the development of the matters for compliance and risk management in terms of historical records, the landscape became more focused on dealing with cibersecurity and data protection. Otherwise, any hacker attack can put all the business in risk – even because the clients' data can be involved and demaged in this scenario.

2. Conclusion

The american background about cibersecurity imposes consequences in diferente Acts, considering the business and the data involved in the real case. The most important one for the financial market is Cybersecurity Information Sharing Act (CISA) of 2015. Also "*S.754 - To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes*" is being analyzed by the Senate.

At least, the General Data Protection Regulation (GDPR) involves all companies with business related to european companies and people. "*For especially severe violations, listed in Art. 83(5) GDPR, the fine framework can be up to 20 million euros, or in the case of an undertaking, up to 4 % of their total global turnover of the preceding fiscal year, whichever is higher"*.[4]

The purpose of this study henceforth is to understand cybersecurity awareness to have an inventory IT hardware and software, anazyling annually all risks assessment that the company is envolved with, perform a gap analysis and implement controls to accomplish with the security properlly.

All this obligations must be supported by the compliance department, guaranting that it will be done in accordance with the regulation in force. Also, the results of these projects must be scored in a risk basead approach annually. Regardless of the company's business, size and purposes on the financial market, this risk management must be accomplished, building and maintaining this relationship between compliance, risk management and cybersecurity.

References

[1] CISA. 2015. *Cybersecurity Information Sharing Act 2015*. Available at https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520Information%2520Sharing%2520Act%2520of%25202015.pdf.
[2] CORO. 2024. *A History of Cybersecurity and Cyber Threats*. Available at https://www.coro.net/blog/history-of-cybersecurity-and-cyber-threats.
[3] CYBERINSURE ONE. Cibersecurity Laws and Penalties. https://cyberinsureone.com/laws-penalties/.
[4] INTERSOFT CONSULTING. "*GDPR Fines / Penalties*". Available at https://gdpr-info.eu/issues/fines-penalties/#:~:text=For%20especially%20severe%20vi

[3] PWC. *Tech Enabled Integrated Risk Management (IRM)*. Available from https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/risk-control-security-transformation/integrated-digital-governance-risk-compliance.html. [Accessed on 10/10/2024]

[4] INTERSOFT CONSULTING. "*GDPR Fines / Penalties*". Available from https://gdpr-info.eu/issues/fines-penalties/#:~:text=For%20especially%20severe%20violations%2C%20listed,fiscal%20year%2C%20whichever%20is%20higher. [Accessed on 10/10/2024]

olations%2C%20listed,fiscal%20year%2C%20whichever%20is%20higher.

[5] PWC. *Tech Enabled Integrated Risk Management (IRM)*. Available at https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/risk-control-security-transformation/integrated-digital-governance-risk-compliance.html.

[6] SKELTON, Chris. 1973. *United States v. Hilton Hotels Corp., 467 F.2d 1000 (9th Cir. 1973)*. JUSTIA US LAW. Available at https://law.justia.com/cases/federal/appellate-courts/F2/467/1000/154124/.

[7] WONG, Lai-Wan Wong; LEE, Voon-Hsien ; TAN, Garry Wei-Han; OOI, Keng-Boon; SOHAL, Amrik. 2022. *The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities*. Available at https://www.sciencedirect.com/science/article/abs/pii/S0268401222000548.