An Analysis of Risk Management in the Technology Industry

Gau Meng Yew (11324766)

FINA20201 – Risk Management

Professor: Pierre Saint-Laurent

11 Pages

1. Introduction

The technology sector has experienced major changes and growth in recent decades, and it shows no sign of slowing down. With growth, the level and number of risks associated increases proportionately, and it leads to more unique risk management methods arising in order to mitigate the impacts on the company. In this paper, we aim to explore said risks and management methodologies and provide both an assessment to their effectiveness and areas for improvement.

2. Industry Analysis

The technology industry comprises of many sectors, and it spans a wide array of use cases. Furthermore, with the rapid digitalisation and emergence of industry disruptors, the definition of a classification of a tech company is becoming blurry. For the sake of simplicity, we define a tech company as an IT service company that provides a software (E.g., Cloud services, CRMs, etc.) or internet service (E.g., Search Engine, E-Commerce, etc.).

As of 2021, global IT spending has exceeded USD 4,000 billion (Figure 1). By 2023, this number is expected to approach USD 5,000 billion. The emergence and immense growth of the technology industry has sent waves through the entire world. It has become one of the primary pillars supporting the global economy, transformed societal norms, and blurred the lines between our professional, private, and public lives.

Due to its permeating effects in society and the economy, the call to manage risks effectively in these companies has become much greater than ever. Any failure to manage risks could lead to severely disruptive consequences for both the company and the economy. For example, the recent collapse of the digital cryptocurrency exchange company FTX is a result of mismanagement of both financial and business risks. The resulting crash cost investors millions of cash and caused a domino effect that threatened the life savings of many working-class people, as pension funds and banks with exposure to FTX suffered setbacks as well. In addition, the company's value virtually evaporated within 10 days, a crash with striking similarities to the demise of the investment banking giant Lehman Brothers. Three of the Top 10 Fortune 500 companies are multi-trillion tech companies (Fortune, 2022). Hence, with their size and reach, it is incredibly important to employ bespoke methodologies to manage risks in these companies.

3. Industry risks

Before we can effectively measure and manage risks, it is imperative to first identify what are the main risks inherent to the company and prioritise them. In this section, we will explore what are the common risks tech companies face, and the methods used to minimise the impacts of these risks.

3.1 Business and Industry Risks

While there are multiple business and industry risks for each tech company, we will only look at the most common risk, which is intellectual property risk.

3.1.1 Intellectual Property (IP) and Piracy Risks

In the technology industry, patents, trademarks, trade secrets and copyrights are incredibly valuable. This is because if the competition has access to the assets protected by copyrights, the product of the company is easy to replicate. Furthermore, with enough software engineering expertise, products can be easily made with a striking resemblance and functionality to the original.

For example, piracy is a common method of intellectual property infringement. Piracy has increased more than 20% from 2021 to 2022 (TorrentFreak, 2022), and as "Software Cracking" becomes more sophisticated, pirated products are becoming more easily accessible. Between 2015 and 2017, the software sector lost USD 46.3 billion to piracy (Spajic, 2022), and 2 in 5 copies of software products in global distribution are unpaid for (Spajic, 2022).

A more common and recent example of piracy is password piracy, or more commonly known as password sharing. It is reported that streaming giant Netflix loses over billions yearly to password sharing, and the company has resorted to extreme measures such as charging more per user to tackle this problem (Chirinos, 2022).

In essence, the most common business and industry risks for tech companies would be intellectual property and piracy risks, and competitive risk. While these risks are common to other industries as well, it does not discount its importance in the technology industry particularly.

3.2 Data Governance and Cybersecurity Risks

Data leaks, hacks, and poor data practices are a major problem in tech companies. The global average cost of a data breach in 2022 is USD 4.35 million, and whenever there is a critical infrastructure breach, the cost to the company is USD 4.82 million (IBM, 2022). Most critically, when ranked by industry, the technology industry is the 4th most costly sector (Figure 2) when there is a data breach.

Besides the cost of managing a data breach, poor data governance and cybersecurity practices are damaging to the reputation of a company, which may cause significant liabilities and weaken its brand name. The impact of this risk is large as the technology industry is saturated with competition, and having a strong reputation is paramount to gaining an edge over competitors. In the 2018 Facebook Cambridge Analytica scandal, the social networking giant lost more than USD80 billion in two weeks, as advertisers and users alike left Facebook, which is now reputed for its poor privacy and data governance practices (Monica, 2018).

Moreover, third-party risks are a related threat to data governance and cybersecurity. As of 2021, 74% of organisations who have experienced a data breach have cited privilege third-party access as the main cause (Security Magazine, 2021). Despite this, more than half have stated that the cybersecurity and privacy practices of the third party are not properly assessed or checked before providing privileged access. Similarly, in the Facebook Cambridge Analytica scandal, Cambridge Analytica was a third party given privileged access to Facebook's data. It shows that no matter the size of the organisation, third-party risk is inherent if the company becomes complacent in conducting its checks.

To combat this risk, companies such as Alphabet, Microsoft, and Amazon have opted for **cyber insurance**. This offering has been extended to their customers as of 2021 (Alspach, 2022), partnering with Allianz, Cowbell, and other reputable insurers who use data driven insights to assess the cyber risk of the organisation.

3.3 Qualitative and Quantitative Market Risks

Tech companies tend to operate across borders, as the nature of their products do not particularly require physical delivery, such as Google, Facebook, etc. However, because of cross-border operations, they are subjected to a wide variety of market risks, which differs from

country to country. In addition, they must mitigate cross-border risks such as forex risks and interest rate risks, both of which are challenging to manage.

Furthermore, tech companies manage intense competition through buyouts and investments. This expands their investment portfolios, but will also be affected by forex, interest rates, and equity investment risks.

3.3.1 Forex Risks

For multinational tech companies such as Apple (Apple AR, 2022), foreign exchange (Forex) risk carries significant impact on the company. Forex volatility is the biggest challenge faced by corporate treasurers, and it is consistently a major concern (Deloitte, 2017). As a case study, companies like Apple hedges with foreign currency swaps to convert the currency into U.S. dollar notes (Apple AR, 2022). While the swaps are dependent on the effective interest rates, its fair value has been increasing since 2021, displaying that using alternative investments are an effective way of managing forex risks. We will explore management methodologies for forex further in depth in Section 4.2.2.

3.3.2 Interest Rate Risks

Similarly, due to a large investment portfolio and cross-border transactions, tech companies are also exposed to changes in interest rates. Tech companies with operations based in U.S. such as Apple are most affected by changes in U.S. interest rates (Apple AR, 2022), likely due to holding most of their cash equivalents and marketable securities in their home currency. It also affects the costs of hedging and debt, potentially increasing liabilities for the company.

Apple and Amazon usually invest in safe and high-grade market instruments, in order to minimise the potential risk (Apple AR, 2022), (Amazon AR, 2021). Furthermore, Apple also uses interest rate swaps, outstanding floating/fixed rate notes that are convertible to one another to hedge their position.

3.3.3 Equity Investment Risks

The companies in the investment portfolio are occasionally in the start-up or development stages, and it would be complicated to accurately value them as there is a lack of readily available market data for private companies. This creates equity investment risks, where the market value of these private holdings are **not reflective of their true value**.

3.4 Other Risks

The number of risks in the technology industry is non-exhaustible, and it is without a shadow of a doubt that we have not covered all of them. Other risks that plague tech companies include **seasonality risk, human capital risk, political/socioeconomical disputes, and more.** These risks are important, but they are not explored in depth in this paper as they may be uncommon to tech companies, require strategies that focus on culture management or are completely outside of the company's control.

3.5 Prioritisation

3.5.1 Medium Risks

Each of the three risks classified as **medium** are equally significant. Although their impact can be high and they would have disastrous consequences, their frequency and severity greatly diminish their long-term impact on businesses.

Data governance and cybersecurity risk has a **high impact but low frequency** of occurrence. This is in part due to an arms race between cyber defense and cyberattack technologies. The impact of data breaches and cyberattacks is still great, and we recommend various methods such as **Cyber Value-At-Risk (Cyber VaR),** to gauge the level of impact, and supplementing it with **Incident Response Plans** to react effectively to the threat.

Equity investment risks also have a lower frequency of occurrence, as tech companies' investments, as mentioned above, are in highly rated market instruments in order to minimise their exposure to risks.

IP and piracy are classified as medium impact due to their effects on the technology industry. While piracy hurts the bottom-line profits of the company, in the long run, with the correct management strategy, it becomes a business opportunity for the company, particularly those in the software sector such as Adobe and Microsoft. As then Microsoft Group President, Mr Jeff Raikes, mentioned, piracy builds a base of people who are using their software in the long term, and the challenge becomes converting them into paid users (Mondok, 2007). It eliminates the issue of these users turning to their competitors instead. This shift in paradigm reduces piracy risks' impact and reduces their level of competition, as more consumers are loyal to their brand

despite not paying for it. The application for patents and copyrights also serves to cushion the impact of IP risks, hence it is not as significant now.

3.5.2 High Risks

Forex and interest rate risks create a large fiscal impact, and they have a high frequency of occurrence, especially in the current socioeconomic conditions of the world. The impact on the company is further accentuated by the cross-border nature of tech companies. It is therefore no wonder that both are classified as a high-level risk and would require attention by the company. Despite so, some companies, such as Netflix, has opted to not hedge their exposures to fluctuations at all (Netflix AR, 2021). There is inherent difficulty in forecasting the rates with reliable accuracy, but we will explore some methods to hedge part of the position for the companies in Section 4.

4. Risk Management Methods

4.1 Employed Methodologies

As discussed above, tech companies have already employed some strategies to combat risks. The employed strategies are summarised below, and in this section, we will recommend underemployed strategies that can improve the effectiveness of risk management in tech companies.

Risk	**Employed Strategy**	**Risk Level**
Forex	Swaps are uncommon, tend to be left alone	**High**
Interest Rates	Swaps are uncommon, tend to be left alone	**High**
Data Governance and Cybersecurity	Cyber Insurance	**Medium**
Equity Investment	Diversification and clear investment objectives	**Medium**
IP and Piracy	Changing strategical approach or crackdowns	**Medium**

4.2 Strategy Recommendations and Evaluation

4.2.1 Measuring data and cyber risks with Cyber Value-At-Risk

To hedge losses against cyberattacks and data breaches, tech companies are **opting for Cyber Insurance**. It covers a wide array of impacts caused by cybersecurity breach, ranging from data restoration costs to privacy liability. While its effectiveness is well-pronounced, a challenge arises from the difficulty in measuring the impact of the breach. Estimation of potential losses to reputation and others is hard to quantify, and the company may incur a risk of overpaying for insurance or being underpaid when collecting their pay-outs.

To properly measure the impact of this risk, the **Cyber Value-At-Risk (CVaR)** is recommended. It is an aggregated framework designed to account for the potential harm arising from cyber threats and quantifying it using data driven insights. The implementation of CVaR is similar to the conventional Value-At-Risk (VaR), except it is based on four factors (Assets, Harms - losses resulting from cyber threats, Controls, Threats) instead (Figure 5). CVaR's effectiveness has been validated in academic studies and adopted by reputable insurers such as Marsh Insurance to assess the cyber and data threats posed to companies.

With an accurate and reliable way to measure data and cybersecurity risks, the vulnerable technology industry would be able to optimise their **incident response plans** and **cyber insurance** coverage, hence minimising their losses.

4.2.2 Foreign Currency Swaps

As established, tech companies tend to have cross-border transactions and they also have diverse investment portfolios in different markets in order to keep their products competitive and diverse. With an uncertain socioeconomic situation and fluctuating exchange rates, it becomes more crucial to manage currencies to ensure the market value of the company is not diluted.

As an example, the USD has been appreciating against the CAD in the past year. By adopting currency swaps, U.S. tech companies ensure their cash equivalents and marketable securities in the Canadian market can be converted back to USD at a more favourable exchange rate rather than the prevailing rates. This **optimises** their **investment profits** and hedges them against any sudden dramatic exchange rate fluctuations.

4.2.3 Interest Rate Swaps

It is no secret that tech companies are heavily financed by debt. In fact, the global technology industry has a debt ratio of 26%. Due to being heavily financed by debts, when interest rates fluctuate, the interest on debt would either increase or decrease accordingly. This can lead to heavy repercussions for tech companies that are over-leveraged and growth aggressive.

To protect their positions, companies such as Microsoft, Google, and Cisco opted to hoard cash reserves (Richardson, 2015). Conversely, other companies such as Apple elected for alternative investments such as interest rate swaps. While hoarding cash reserves has its benefits, interest rate swaps are more effective in protecting against future rises of interest rates. A case study of a tech company that has utilised this strategy effectively is Apple. Apple has swaps for both fixed and floating rate interest payments (Apple AR, 2022), and it has allowed them to control their debt interests effectively.

Hence, interest rate swaps are particularly effective for tech companies, especially start-ups or growth aggressive firms. This is because they tend to be highly leveraged, and with a tumultuous economic situation and changing interest rates, these swaps will hedge their position and provide consistency.

To accurately determine the potential effect of fluctuations of interest rate, tech companies can follow Alphabet's lead and use Value-At-Risk (VaR) analysis to measure the level of exposure (Alphabet Annual Report, 2021).

4.2.4 Managing Equity Investment Risk

From the annual reports, the equity investment risks have been managed well so far, whereby some companies may use derivatives to hedge their market price risk. To bolster the hedging position, it is also recommended to use put options to protect the company from sudden drops in equity values.

4.2.5 Paradigm Shift towards Piracy

In Section 3.3.1, the strategy mentioned in combating piracy is to adopt a paradigm shift towards piracy. This approach is qualitative in nature, but it is an important strategy as this risk also reduces business risk as well.

By viewing pirated users as customers, the problem will shift from competition to conversion into licensed users. It solidifies a base of loyal customers for the product, and without the need to compete, the likelihood of the company being forced into a price or innovation war is lower. Furthermore, the company can use data driven insights to find the ideal price point and level of R&D to convert the pirated users into licensed ones. As such, this approach hits two birds with one stone, mitigating both competitive risk, and IP and piracy risks.

4.2.6 Enterprise Risk Management

Enterprise risk management would be the most effective way to control overall risks in a tech company. By aggregating all risks in a single, unified framework, the effectiveness of risk management increases.

A firm can also opt to blend this approach with other recommendations presented, such as CVaR, swaps, etc., to tackle as many angles as possible. However, the caveat of this approach is that it may be extremely costly to implement, and for highly leveraged tech companies, there may not be enough capital for investment to implement this framework.

4.3 Evaluation

While the tech industry has employed various strategies to assist them in risk management, it is not as optimised as it can be. There is certainly room for improvement, especially since the industry is highly globalised. We recommend using **CVaR** to measure accurately the level of data and governance risk present, and using swaps to protect themselves against the high-level risks of foreign exchange rate and interest rate fluctuations.

5. Conclusion

Unlike industries such as Finance, FMCG and F&B, the technology industry is relatively new. Yet, its unprecedented growth rate has brought with it a lot of new risks, without the time nor experience to adjust to them. By adopting conventional risk management methods such as swaps, we can dynamically adjust them to fit the context and manage risks more effectively. New methods to measure threats in the technology industry have also emerged, such as CVaR, and its effectiveness has been proven.

To close it off, the approach to risk management should start with identification, followed by prioritisation, and ending with coming up with the appropriate strategies to measure and control these risks. As there are multiple risks present in the technology industry, companies should be agile in their mindset, and capitalise on measures such as VaR and CVaR to gauge the level of risk and determine an ideal solution.

6A. Appendix

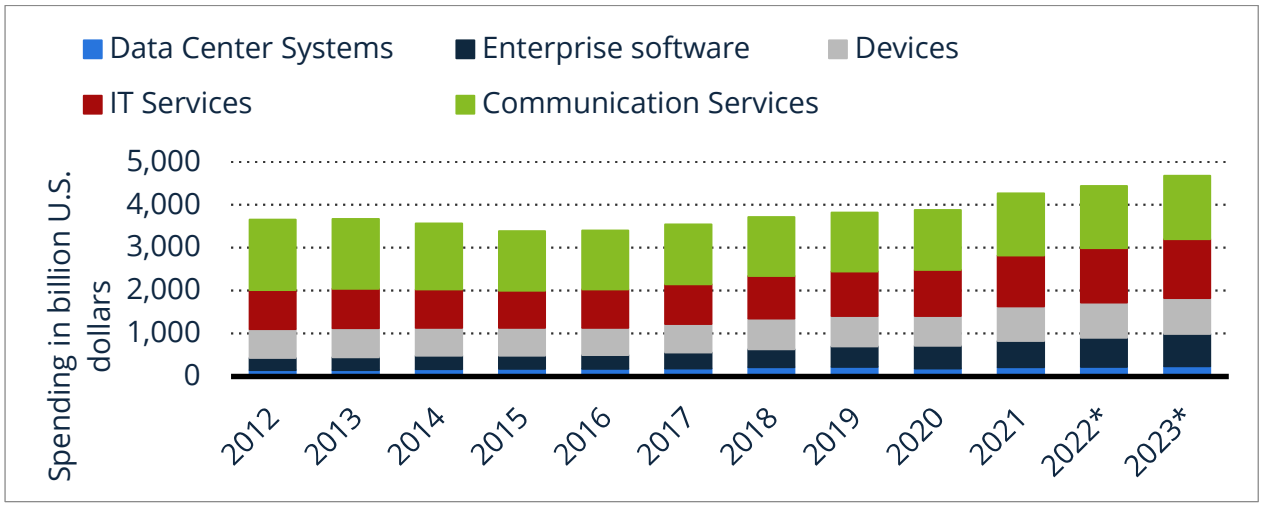

Figure 1 Size of IT Spending (Statista, 2022)

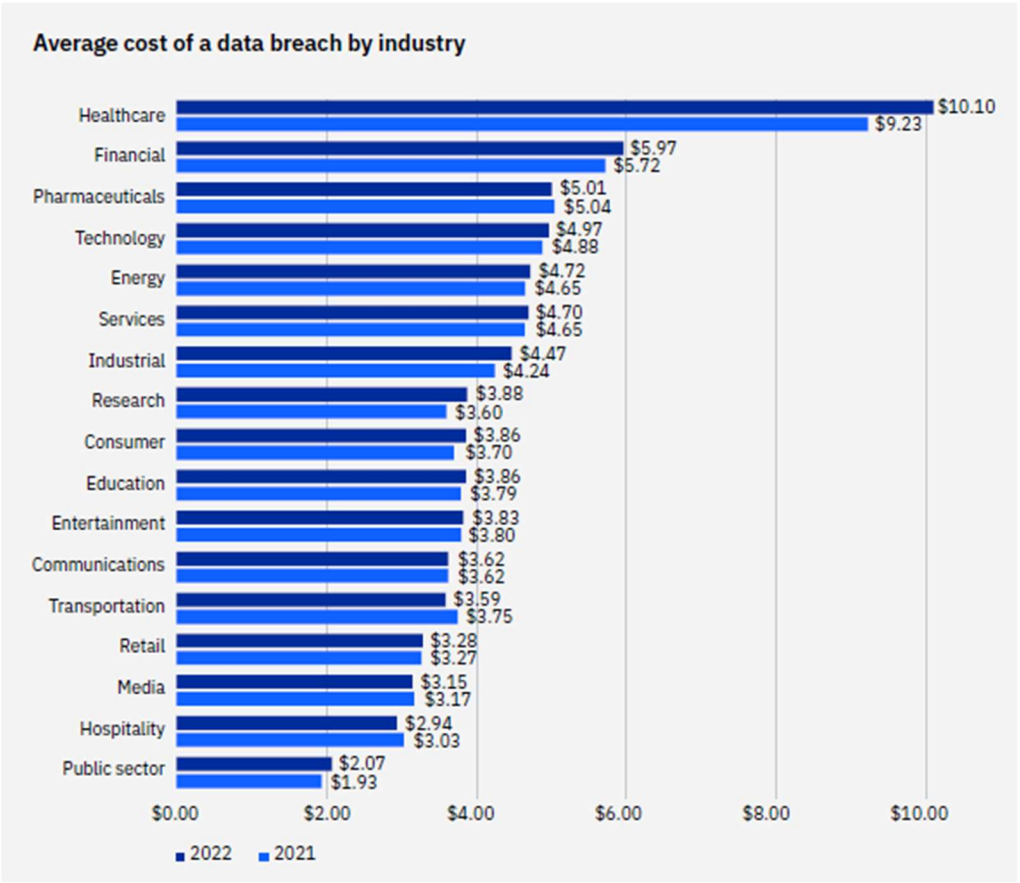

Figure 2 Cost of Data Breach by Industry (IBM, 2022)

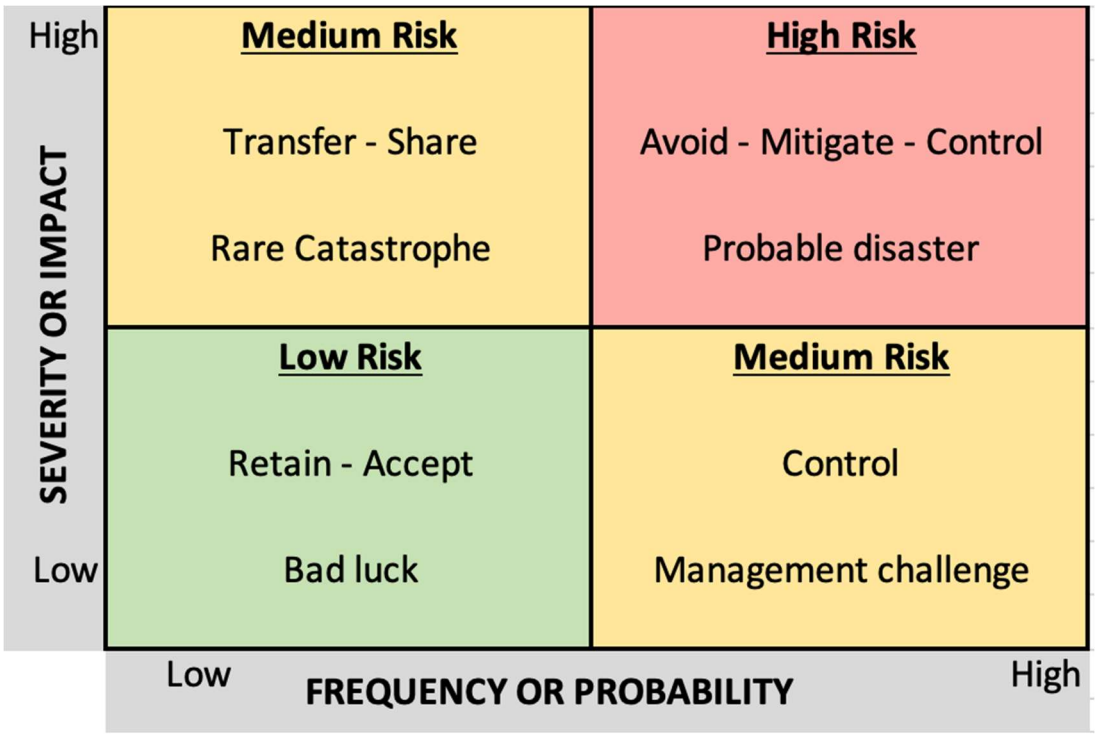

Figure 3 Risk prioritisation matrix

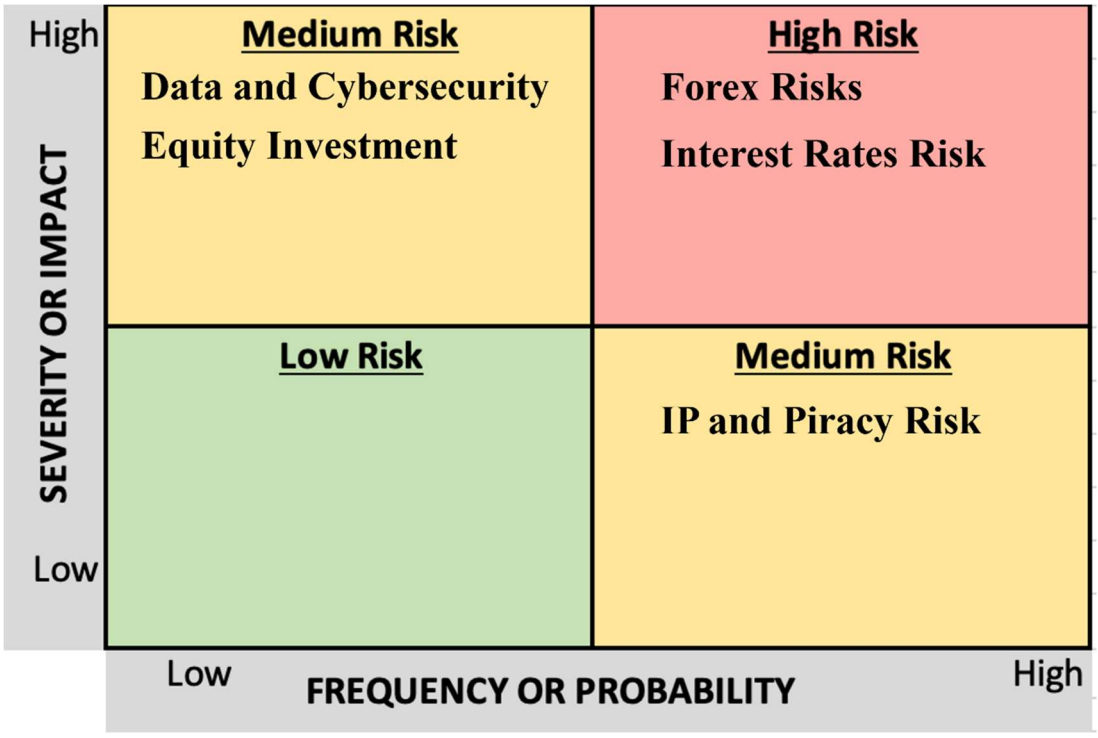

Figure 4 Tech Industry Risk Matrix

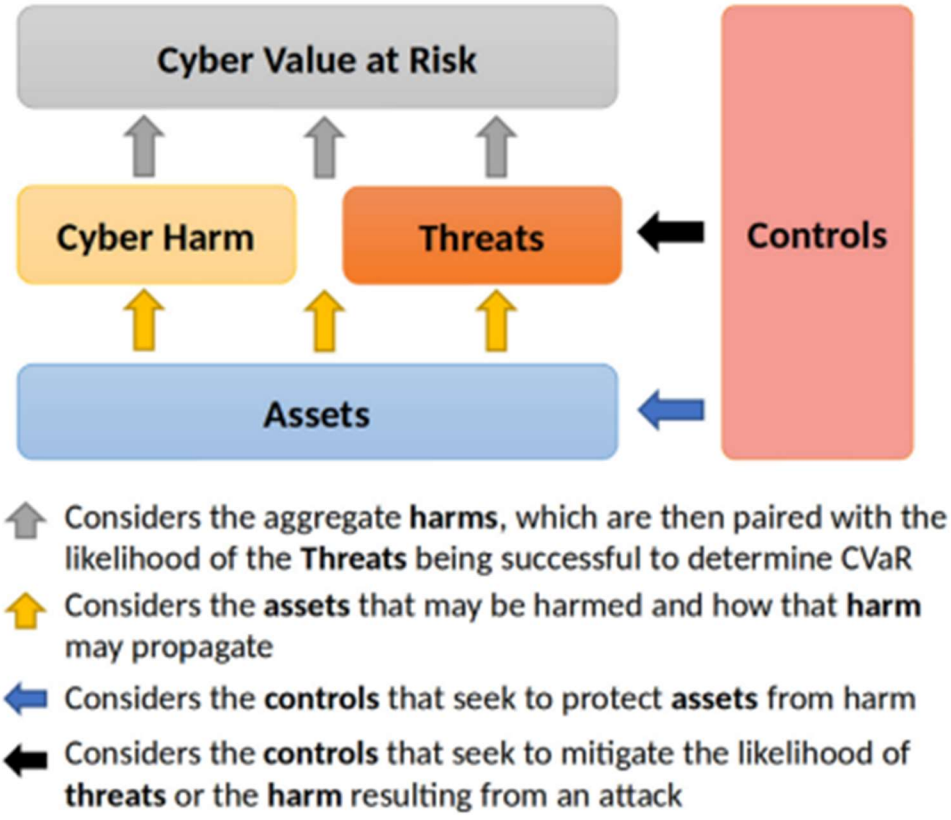

Figure 5 Association between CVaR and Threats, Assets, Harms, and Controls (Erola, 2021)

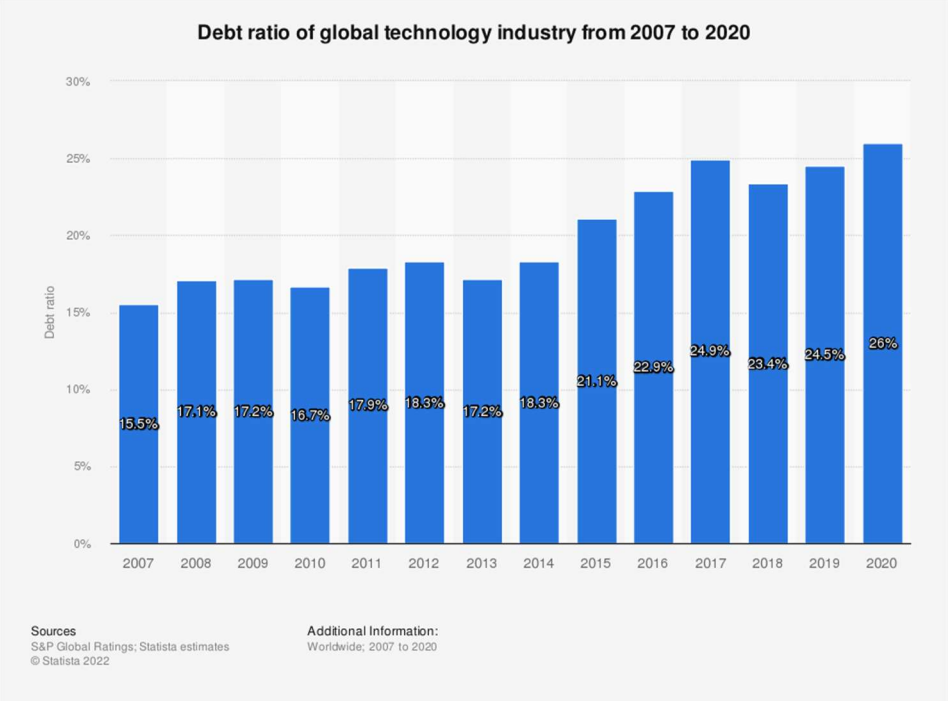

Figure 6 Debt Ratio of Tech Industry

6B. Bibliography

Jocelyn, V., & Biagi, L. (2022.). It services. Statista. Retrieved December 5, 2022, from https://www.statista.com/study/31341/it-services-statista-dossier/

Editors, F. (2022, May 24). Fortune 500. Fortune. Retrieved December 5, 2022, from https://fortune.com/fortune500/

TorrentFreak. (2022, October 11). Online piracy continues to rise with the US firmly in the lead. Go to TorrentFreak. Retrieved December 5, 2022, from https://torrentfreak.com/online-piracy-continues-to-rise-with-the-us-firmly-in-the-lead-221011/#:~:text=Piracy%20is%20on%20the%20rise,after%20the%20Covid%20release%20slowdown.

Spajic, D. J. (2022, October 4). Piracy is back: Piracy statistics for 2022. Dataprot. Retrieved December 5, 2022, from https://dataprot.net/statistics/piracy-statistics/

Chirinos, C. (2022, April 18). Netflix is losing billions a year to password sharing. here's how it plans to fight back. Yahoo! Finance. Retrieved December 5, 2022, from https://finance.yahoo.com/news/netflix-losing-billions-password-sharing-211933200.html

IBM. (2022). IBM - United States. Cost of a Data Breach Report 2022. Retrieved December 5, 2022, from https://www.ibm.com/downloads/cas/3R8N1DZJ

Monica, P. R. L. (2018, March 27). Facebook has lost $80 billion in market value since its data scandal. CNNMoney. Retrieved December 5, 2022, from https://money.cnn.com/2018/03/27/news/companies/facebook-stock-zuckerberg/index.html

Security Magazine. (2021, September 2). 51% of organizations have experienced a data breach caused by a third-party. Security Magazine RSS. Retrieved December 5, 2022, from https://www.securitymagazine.com/articles/95143-of-organizations-have-experienced-a-data-breach-caused-by-a-third-party

Alspach, K. (2022, August 30). Need cyber insurance? get ready to show your data. Protocol. Retrieved December 5, 2022, from https://www.protocol.com/enterprise/cyber-insurance-google-microsoft-aws#:~:text=Google%20Cloud%20and%20its%20insurance,data%2Dpowered%20cyber%20insurance%20market.

Deloitte (2017). Deloitte 2017 Global Corporate Treasury Survey. Retrieved December 5 2022, from https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-global-corporate-treasury-survey-report-2017-210817.pdf

Mondok, M. (2007, March 13). Microsoft Executive: Pirating software? choose Microsoft! Ars Technica. Retrieved December 5, 2022, from https://arstechnica.com/information-technology/2007/03/microsoft-executive-pirating-software-choose-microsoft/

Alphabet (2021) Annual Report. Retrieved from . https://abc.xyz/investor/static/pdf/2021_alphabet_annual_report.pdf?cache=3a96f54

Amazon (2021) Annual Report. Retrieved from https://s2.q4cdn.com/299287126/files/doc_financials/2022/ar/Amazon-2021-Annual-Report.pdf

Netflix (2021) Annual Report. Retrieved from https://s22.q4cdn.com/959853165/files/doc_financials/2021/q4/da27d24b-9358-4b5c-a424-6da061d91836.pdf

Apple (2022) Annual Report. Retrieved from https://s2.q4cdn.com/470004039/files/doc_financials/2022/q4/_10-K-2022-(As-Filed).pdf

Erola, A., Agrafiotis, I., Nurse, J. R. C., Axon, L., Goldsmith, M., & Creese, S. (2022). A system to calculate cyber value-at-risk. *Computers & Security*, *113*, 102545. https://doi.org/10.1016/j.cose.2021.102545

Sava, J. A. (2022, September 2). *Global Tech Industry: Debt ratio 2007-2020*. Statista. Retrieved December 5, 2022, from https://www.statista.com/statistics/787756/worldwide-technology-industry-debt-ratio/

Richardson, H. (2015, March 13). *Relatively low leverage gives tech companies flexibility*. Yahoo! Finance. Retrieved December 5, 2022, from https://ca.finance.yahoo.com/news/relatively-low-leverage-gives-tech-140601608.html