Facultad de Ciencias Económicas y Empresariales

How should MNCs respond to a data breach to protect their reputation and relationship with consumers? An analysis of case studies.

Author: 202121225

Director: Raúl González Fabre

MADRID | junio 2023

Table of Contents

Chapter 1: Introduction

1.1 Research Question

Data drives businesses, governments, and individuals to make informed decisions, understand consumers' preferences, and develop new products and tools. Data refers to any information that is collected, processed, stored, or transferred. In the context of consumer data privacy, data can be categorized as non-personally identifiable information (non-PII) which does not allow for the direct identification of an individual, only an indication towards behaviours and preferences. For the purpose of this paper, it will discuss primarily personally identifiable information (PII), which has a direct link to an individual thus having the potential to lead to more significant consequences like identity fraud and financial corruption.

Cyber resilience is becoming an increasingly common term used from industry to industry in the protection of corporate interests. The widespread application and necessity of electronic devices for both consumers and businesses have brought our generation into the Cyberage. This is a period characterized by the population's dependence on technology in all aspects of life from education and health to e-commerce, hence the presence and wide use of computers and the internet. Cyber resilience is defined as the capacity to identify computerized risks and respond with effective and efficient cybersecurity to protect the critical activities and information systems of the business; it refers to the prevention, detection, and management of cyber risk. An information system (IS) is a "set of activities, involving people, processes, data and/or technology, which enable the organization to obtain, generate, use and communicate transactions and information" (Galligan and Rau, p.6, 2015). The purpose of an information system is to measure the progress and performance of the organisation and assess it in relation to its objectives.

Entities are focusing on organisational cyber safety for numerous reasons. The progressively interconnected world due to the "continued adoption of Web, mobile, cloud, and social media technologies has increased the opportunity for exploitation by the perpetrators of cyber attacks" (Galligan and Rau, p.23, 2015). This is exacerbated by third-party interactions, outsourcing and offshoring, whereby data is being shared with an external entity, broadening the horizon in which they can be exploited. Also, technology continues to evolve; cyber

resilience will only become more difficult to manage as businesses expand their operations, opening new avenues for exploitation, and perpetrators become more skilled and sophisticated. The COVID-19 pandemic is a clear example of the difficulties associated with cyber resilience. This will be investigated further under the heading Secondary Research.

This paper will advise multinational corporations (MNCs); it will provide a strategic management guide to be used to mitigate the effects of data breaches. The report will focus on the reparation of reputation and the relationship with consumers with consideration for long-term endurance. In order to satisfy the primary research question, this paper will respond to the following questions:

1. What is the current situation of data breaches in MNCs operating in Spain?
2. What are the key factors that determine the extent of the reputational damage caused by data breaches for MNCs?
3. What are the potential long-term effects of a data breach on the reputation and relationship of MNCs with consumers?
4. What are the legal and regulatory requirements for data breach management in Spain?
5. What are the best practices for MNCs to respond to a data breach to protect their reputation and relationship with Spanish consumers?

The final proposed recommendations, developed from the secondary research, will be used to analyse three case studies. Through this method, it will investigate the similarities and differences between the MNCs management of the data breach and the proposed methodology; whether the outcome, in terms of the MNCs reputation and relationship with Spanish consumers, was affected positively or negatively.

The research of this paper will be based on a literature review and a case study analysis. There is a great availability of information on this topic and therefore secondary research will provide a sufficient foundation for the investigation and recommendations.

The following chapter, Secondary Research, will begin to investigate the supporting questions.; it will introduce the climate of data breaches in Spain. Chapter 3 will discuss the

key factors that determine the extent of reputational damage caused by a data breach and the potential long-term effects of a data breach and the way it can affect a business' relationship with consumers in the long-term. Chapter 4 will summarize the legal and regulatory requirements for data breach management. It will address the legal responsibilities of a business from the moment they discover that a data breach has occurred according to the National Institute of Cybersecurity (INCIBE), Organic Law on Data Protection and Digital Rights Guarantee (LOPDGDD) and General Data Protection Regulation (GDPR) as Spain is a member of the European Union. Before finalizing the most suitable strategy, Chapter 5 will research the best practices for MNCs to protect their relationship and preserve their relationship with consumers. Finally, based on the research undertaken, Chapter 6 will propose a solution for MNCs to best manage a data breach in order to protect their reputation and relationship with consumers.

1.2 Research Methodology

In Chapter 7, the proposed methodology will be used to compare against the case studies of Iberdrola, CaixaBank and Hotel Meliá. These examples will begin with an overview of each data breach and the actual management strategy which was utilized. It will be followed with a comparison to the proposed methodology to understand how the outcome of the MNCs reputation and relationship may differ, this will allow us to conclude, based on the three case studies, whether the proposed methodology is the most suitable data breach management strategy. The results of the case study analysis will be addressed in Chapter 8. In the following chapter, we will consider how the research from the literature review and the learned knowledge from the application of data breach management strategies overlap. Chapter 9 will discuss the positives and negatives of the proposed methodology as identified in the case study analysis; it will ascertain whether there are any limitations to the proposed data breach management strategy. The paper will conclude with Chapter 10 which will finalize the most suitable strategy for data breach management.

Chapter 2: Secondary Research

2.1 The Current Situation Of Data Breaches In MNCs Operating In Spain

The proliferation of digital technologies has made data breaches a common occurrence in the modern business landscape. Therefore, data breaches in corporations are a growing concern in Spain. The Spanish National Cybersecurity Institute (INCIBE, 2021) reported it is expected that incidents will continue to grow. According to a report by the INCIBE, the number of cybersecurity incidents reported by companies in Spain in 2020 increased by 19.1% compared to the previous year (INCIBE, 2021). Data breaches are becoming increasingly prominent with 1,500 data breaches being reported in Spain in 2021 alone (20minutos, 2021). All regions in Spain have been subject to cyber-attacks; 2022 studies show that Catalonia is the region most highly victimised by cybercrime in Spain with 35,000 cases, and Madrid follows closely with 30,000 cases (Comparitech, 2022).

The most common types of data breaches in corporations in Spain are phishing attacks and ransomware attacks. In 2020, phishing attacks accounted for approximately 48% of all incidents reported to the INCIBE by companies (INCIBE, 2021). These attacks involve cybercriminals using fraudulent emails to obtain sensitive information, such as login credentials or financial information. Ransomware attacks are another significant threat, with the INCIBE reporting an increase of 200% in ransomware attacks in 2020 compared to the previous year (INCIBE, 2021). These attacks involve cybercriminals encrypting data and demanding payment in exchange for the decryption key. Distributed denial of service (DDoS) attacks are also common in Spain, with the banking sector being a prime target. According to a report by the Spanish National Police, DDoS attacks on Spanish banks increased by 95% in 2020 compared to the previous year (El País, 2021).

Numerous sectors have been affected by data breaches in Spain, with the banking and finance sector being particularly targeted, followed by energy and healthcare. In 2020, the banking sector was the most affected sector, accounting for 40.5% of all cybersecurity incidents reported to the INCIBE (INCIBE, 2021). Healthcare organizations have also been targeted, with cybercriminals stealing sensitive patient information. The education sector has experienced an increase in ransomware attacks, with cybercriminals targeting online learning platforms. Government agencies have also been targeted, with cybercriminals attempting to steal confidential information and disrupt government services. Similarly, the European Union

Agency for Cybersecurity (ENISA) reported that finance, healthcare and energy sectors were the most targeted sectors for cyber-attacks across Europe, aligning with that of Spain (ENISA, 2020). INCIBE determined that these sectors are attractive targets due to their high level of regulation and handling of sensitive information (INCIBE, 2021). If there is a greater priority for the privacy of the data, for example, individuals' financial information, it identifies a weak point in the organisation that can be targeted for financial gain in the form of extortion.

The Spanish government has taken several measures to address the increasing threat of cyber-attacks. In 2019, the government created the National Cybersecurity Institute (INCIBE) to help businesses and individuals prevent and respond to cyber-attacks. The government has also implemented various regulations, such as the General Data Protection Regulation (GDPR), to protect personal data and ensure that organizations are held accountable for data breaches. Additionally, the government has increased its investment in cybersecurity to improve its ability to respond to cyber-attacks. In 2021, the Spanish government announced that it would invest €2.5 billion in cybersecurity over the next five years (El País, 2021).

Corporations in Spain have also had to increase their cybersecurity, enhancing their measures to both prevent and respond to data breaches if the case arises. Examples of new protection policies include stronger firewalls, intrusion detection systems and multi-factor authentication. Arguably the most important effort is the increased investment into cyber security for employees at all levels; employees and third parties are access points for attacks by cybercriminals. The education and training of a workforce to raise awareness of the possible threats to the organisation and the associated risks reduces the initial danger. Companies are also increasingly investing in cybersecurity technologies, such as endpoint protection and threat intelligence platforms. Furthermore, companies now have greater consideration for their response to data breaches as it is a significant possibility and threat to their success. Although, this is not the case with every company, particularly smaller businesses; PWC identified that many Spanish companies still do not prioritise cybersecurity or invest in the necessary resources to protect against cyber-attacks (PWC,2020). The prioritization of cybersecurity is key to mitigating the risks associated with data breaches.

The COVID-19 pandemic is another factor to be considered in the increasing severity of the current situation of data breaches in Spain. The majority of businesses, all those which were able, were forced to transfer their products and services offered to e-commerce. Also, the

Spanish government implemented a series of restrictions on the population to minimise the spread of COVID-19. As a result, Spain experienced a drastic increase to nearly 2 million non-essential employees working from home, a growth of more than 100% (Statista, n.d.). Spain, along with many countries worldwide, was pushed into a heightened digital age where all activities from family contact to work-life involved technology. Therefore, the amount of data stored on devices increased exponentially and this data was not secured in a working environment but on personal devices in the homes of workers. There was not sufficient infrastructure for this overnight transformation, and by 2021, there was a recorded internet penetration of 83% (Statista, n.d.). This digital transformation meant many organisations had to implement new technologies and develop new security policies and procedures after the transition when employees were accessing the company and consumers' information from home. This created new vulnerabilities and opportunities for cybercriminals to exploit (El Confidencial, 2021).

In 2021 Spain was above the global average for countries attacked by ransomware, they stand at 44% which is 7% greater than the average figure (Comparitech, 2022). Despite being ranked 59th out of 75 countries for its cybersecurity efforts, Spanish companies have paid a total of €14,490,094 in GDPR fines. This is significantly less than other European countries with the UK, France, Germany, and Italy paying between €44M and €66M. The majority of European countries, including those listed prior, are bound by the same GDPR regulations and so they all have the same tolerance and response to incidents of data breaches. Spain's cybersecurity efforts mean that they are not positioned as Europe's worst country for data breaches; however, there is a significant improvement to be made to minimise corporations' risk, reputation and corporate integrity, and relationship with consumers. This paper will propose recommendations to address this gap in knowledge.

Chapter 3: Reputational Damage Of Data Breaches

3.1 Key Factors

The global rise in cybersecurity threats and data breaches can be attributed to varying factors including the increasing sophistication of cyber-attacks. The advances in technology, most notably artificial intelligence (AI), have also seen a rise in advanced techniques like social engineering, which allows cybercriminals to bypass security measures to gain access to sensitive information (EFE Empresas, 2021).

Data breaches can cause significant damage to the reputation of all companies, specifically multinational corporations as the effect is often compounded by the media response. Public perception and media attention can amplify the reputational damage caused by a data breach; it is more significant in cases when the company's response is considered as inadequate or insensitive (Wang, et al., 2018). There are other key factors which determine the extent of the reputational damage caused by data breaches.

The industry in which the multinational corporation operates is a strong influence on how the public perceives the data breach. Industries like telecommunications, finance and, health are responsible for more sensitive information of consumers like financial and medical details. Consumers entrust confidential and sensitive information to companies that they believe will store it and protect it responsibly and effectively; it can be considered a duty of care. Data breaches in these industries are likely to cause greater concern and reputational damage compared to other industries. Companies in other industries may be responsible for personally identifiable information, like contact information and addresses, but they are associated with other business in the eyes of consumers. Therefore, these companies will usually have an easier time of distancing themselves from a data breach.

Another key factor is the severity of the breach; this refers to the quantity of individuals affected, the type of data compromised and the consequences this will have for consumers. Data breaches can affect consumers in a number of ways, the consequences can be short-term minor inconveniences or long-term substantive problems like financial debt, inability to work and long-term physical or psychological effects (Mike Muha, 2020). The way in which the consumer is impacted will be reflected in the extent of the reputational damage. Similarly,

when a data breach compromises a large proportion of consumers' data, it is more likely that the media will focus on and report this incident. This will further damage the organisation's reputation.

Is this data breach the first or one of many? Consumers are less forgiving of companies that have a poor reputation for cybersecurity, which can be signified by a previous data breach. Whereas companies with a strong record of reliability and clean record from previous data breaches are more likely to be able to mitigate the reputational damage. The prior reputation and trust can be influenced by other factors like customer service, quality of product or service and work culture. If a consumer has loyalty to a brand or company, it will take a greater incident to damage the relationship than if the consumer was previously either unhappy or undecided of their ties.

The main factor which is in the control of the company at the time of the data breach is the timing and response. How quickly and effectively did the company respond to the data breach? There is a perceived correlation between an inadequate response that was not reported in a timely manner and a lack of care for consumers' data. This will damage the reputation. On the other hand, a timely and transparent response, coupled with effective communication with customers, can help to restore trust and minimize reputational damage (Wang et al., 2018).

3.2 Measures

The extent of reputational damage can be measured in both qualitative and quantitative data; it is important that a company is aware of all methods of monitoring the impacts of the data breach. A full and comprehensive understanding of how the company is affected will allow for a targeted and more appropriate response which will improve the likelihood of acceptance on behalf of consumers.

Qualitative measurements

The qualitative analysis will primarily be the responsibility of the marketing team. It is common for MNCs to have a solid presence on social media which is used by the population to contact and remain updated on current events of the company. Spain is one of the biggest social media markets in Western Europe with more than 40 million social networking users in 2022 (Statista, 2022). The most popular social media channels frequently used by the Spanish population include Facebook, Instagram and WhatsApp, thus these are the most important networking sites to be utilised by MNCs to have a direct

link to Spanish consumers. Following a data breach, it can be expected that consumers will reach out using social media, the population will use platforms to discuss the data breach, and reports will be uploaded online by news entities. Therefore, the MNC should monitor social media platforms for mentions of the data breach. Tools like social listening software can track the volume and tone of online conversations; it will also provide valuable insight into public perception. Another substantial qualitative method is the analysis of media coverage, which has a direct correlation with consumers' social media responses. The way in which the incident is being reported will set the tone for whether the company was a victim of a data breach or whether it should face the blame. Qualitative analysis will give an insight into consumers and the public's response to the data breach and management. To clearly understand the reaction of consumers in a private environment, companies can encourage customer feedback. The company can survey its consumers to understand how their level of trust in the company has been affected. The more specific the questions, the clearer it is for the company on the actions they need to take to remedy the relationship.

Quantitative measurements

The quantitative analysis will primarily be the responsibility of the finance team. MNCs should be aware of the financial impact derived from the data breach. The company can compare the cost of remediation, legal fees, and lost revenue resulting from the data breach to previous quarters or years to determine the extent of reputational damage. Also, in the case of public companies, the value of the share price can be analyzed to determine how shareholders and investors are responding to the incident. If a share price significantly falls in the aftermath of a data breach, it is evident that there is not a positive response. As the MNC manages and responds to the situation, it should expect the share price to steadily increase on average.

Qualitative and quantitative metrics can be compared to the previous history, the expected achievements for the next period and the position of competitors. These measurements will be used in the consideration of case studies [refer to section titled Case Study Analysis] to analyze the strategic management of data breaches by Iberdrola, CaixaBank and Hotel Meliá.

3.3 Potential Long-Term Effects

Data breaches can have significant long-term effects on a company's reputation and relationship with its consumers. In the event of a data breach, consumers' personal information can be compromised, such as names, addresses, and financial data, resulting in a loss of trust and confidence amongst consumers. This loss of trust can be challenging to overcome and may have a lasting impact on a company's reputation and financial performance. Once a data breach becomes public, especially if the media intervenes and publicises articles on the incident, it will not disappear from the public space: the internet. Negative publicity will have a more serious impact; however, any publicity will remind consumers of the data breach keeping it as current affairs. Long-term effects of a data breach can include:

- Damage to company reputation
- Loss of business and revenue
- Internal rifts between teams
    - Higher employee turnover
    - Less attractive to new employees, especially in tech positions
- Legal penalties/ ramifications

Damage to company reputation

One of the most significant long-term consequences of a data breach is the impact on a corporation's reputation. A report by Forbes identified data loss as "the fourth most common threat to reputation" and that 46% of organisations "experienced damage to their reputation and brand value" (Forbes, 2013). The initial aftermath after a data breach was likened to a burning build by Dan Erwin, Security Officer of Dow Chemical Co. (Scheidies, 2019); this highlights the high severity and high-pressure scenario that unfolds following a cyberattack. However, a company's reputation and corporate integrity can suffer negative connotations years after the data breach occurred. Some studies suggest that reputational damage can persist for up to three years or more following a data breach. This is verified by a survey conducted that found 44% of consumers would avoid doing business with a company, even two years after the incident.

The long-term impacts devolve from the initial consumer reaction and 'poisoned search results' on your corporate brand (Poremba, 2021). A marketing team can spend years attempting to control the online narrative after a data breach; this includes search engines and social media. It will be a continuing responsibility as new articles or online comments emerge discussing the breach in a negative way.

Loss of business and revenue

Data breaches can have a significant impact on a company's bottom line and the effects can be long-lasting as new costs emerge. The loss of revenue can be attributed to a variety of factors including the loss of business opportunities; halt of operations; loss of sales; loss of intellectual property; investment in employee education and cybersecurity; and unexpected costs. The extra costs of remedying the data breach must also be included; there will be an increased expenditure in all functions: marketing, finance, human resources, sales, and strategy.

Business collaboration can bring substantial financial gains for both parties as they share resources and knowledge to work together towards a common aim or purpose. It can also be used to create innovative ideas, more efficient processes, improved communication and many more advantages. Businesses want to partner with organisations that have strong reputations, a focus towards a clear goal and the capacity to invest in the partnership in terms of finance and time. To partner with an organisation facing a data breach would most likely implicate yourself in negative publicity and the following chaos; businesses and other consumers want to conduct business with companies that they consider safe (lowest risk possible). Similarly, it will make it more difficult for the company to acquire new customers. New potential customers may be hesitant to do business with a company that is unable to protect their consumers' privacy. A study by Kaspersky Lab indicates that there is a strong correlation between a data breach and reduced new customer acquisition. It can take an MNC two years to recover the lost business following a data breach (Kaspersky Lab, 2018). Ponemon Institute and IBM determined that 38% of the averaged total financial costs derived from a data breach, is attributed to lost business.

Typically, the size and capital of MNCs allow them to maintain operations during and following a data breach whereas 60% of small and medium-sized businesses will shut down within six months of a cyberattack. In 2022, IBM concluded that the global average total cost of a data breach is $4.35 million, a 2.6% increase from 2021, and a 12.7% from 2020. IBM states the average cost of a ransomware attack is $4.54 million and this figure does not include the cost of the ransom itself. Ransomware costs refer to the money demanded by cybercriminals to return the company's intellectual property. This amount cannot be predicted and so falls into the category of unexpected costs. The State of Ransomware 2022 report ascertains that 11% of businesses paid ransom amounts greater than $1 million in 2021, an increase of 5% from the previous year. It also concludes that the average ransomware cost is between $570,000 to $812,360. It should also be noted that paying ransomware is unlawful in most cases and law enforcement does not encourage nor endorse the payment of ransoms.

Cybercriminals' intentions, in the case of ransomware, are to make it fundamentally impossible or at least extremely difficult for the company to continue functioning. The halt in operations forces the company into a position where they must pay the ransom to return to work, otherwise, they face the risk of losing more sales and business. Therefore, cybercriminals will steal files and confidential documents, the fundamental information, to prohibit the continuation of work. If there are no backups for the documents, it can take years for the company to rebuild the documents, costing the business time and money. The IBM report summarised the costs accrued from a data breach: on average, 24% of costs arose in the first three to six months; 52% of costs occurred in the first twelve months; 29% in the second year; and the final 19% arose more than two years after the breach (IBM, 2022). It is also noted that the higher costs in the years after the data breach are composed of greater regulatory and legal costs. These statistics confirm that the financial responsibilities resulting from a data breach are long-term consequences for the company.

Internal rifts between employees

Chief Executive Officers' (CEO) hold the responsibility of being the face of the company. Such responsibility includes being held at fault for company wrongdoings; this is also pertinent to data breaches. Although the Chief Information Security Officer (CISO) will bear some of the fallout, as it can be perceived as an error in performance, it is the CEO who is responsible

for the overall running and management of a company. CEOs will be penalised for "a lack of support" (Poremba, 2021). The management team and the security team will often propose diverse solutions to a data breach. The CISO has a greater understanding of the technical risks and possibilities, whereas the CEO will likely primarily consider short-term solutions like increased spending on marketing campaigns to shift the narrative. CEOs will also have the pressure of responding in a way that protects their career, which is why an immediate remedy may be preferred. The contrasting opinions can lead to internal rifts; the stakes are high, and this can cause a power struggle which, in turn, is reflected in the company culture.

The IT team is usually the most affected within a company. Carbonite reported that among IT professionals 24% witnessed a decrease in office morale and a further 21% were subject to micromanagement. As the company looks to find the root cause of the data breach, it can often set departments against one another as they want to protect their team and themselves. Furthermore, 15% of IT professionals reported they saw employees being fired, and of the remaining, 11% saw employees quit. The lack of trust between the employer and employee because of the breach can cause dissatisfaction in the working environment.

Investment in employee education and cybersecurity

Once a data breach has occurred, it is evident that the technical infrastructure is not secure and will require updating and improving to mitigate the option of another cyberattack. The GDPR recommends organisations to increase investments in their cybersecurity governance technologies (IBM, 2022). Worldwide, 40.7% of companies reported being "frequent victims" of a cyberattack that deals with six or more successful attacks annually, thus highlighting the fundamental need for the best cybersecurity. The money that is not invested in improved cybersecurity or technological employee training will be required to pay the costs listed in response to a data breach. As technology continually adapts, systems will require improvements and the workforce will necessitate an upgraded education to ensure they are aware and prepared for attempted attacks and the protocol following a data breach. IBM named human error "the threat with the highest economic impact" as it is responsible for nearly a third of IT disruptions and it is important to remember "how vulnerable an entire system can be to one person making a mistake" (IBM, 2022). As the leading cause of IT disruptions, it is

fundamental that there is an increased and continued investment into employee education on how to prevent and manage a data breach.

Legal penalties

The legal and regulatory consequences of a data breach will affect multiple functions of the business directly and indirectly. The direct effects could be catastrophic on capital and reputation. The legal result of a data breach typically involves investigations by regulatory bodies, auch as the GDPR in Spain, to determine the cause of the breach and whether the company was compliant with GDPR laws and regulations. In the case that a company is deemed to have violated any data protection laws or regulations, it may be subject to fines and legal action. GDPR has strengthened the legal framework for data protection and so can be fined at least €20 million or up to 4% of the company's global annual revenue due to non-compliance. Non-compliance with data protection regulations can have a detrimental effect on a company.

Legal action will take time to investigate, follow court proceedings and issue consequences in the case of non-compliance. Other long-term effects include significant financial losses, thus affecting a company's ability to invest in new projects or expand operations. The legal and regulatory proceedings are compulsory following a data breach and so this keeps the incident as a matter of current affairs; therefore, it can remain in media coverage.

Chapter 4: Legal and Regulatory Requirements for Data Breach Management In Spain

Spain follows the General Data Protection Regulation (GDPR) which is a regulation implemented by the European Union (EU) to strengthen and unify data protection for all individuals within the EU (Voigt & Von Dem Bussche, 2017). In addition to the GDPR, Spain also has its own national data protection laws, which are based on the GDPR and provide further guidance and regulations for data protection in Spain. LOPDGDD (2018) states the Spanish data protection laws are primarily governed by the Organic Law on Data Protection and Digital Rights Guarantee (LOPDGDD), which was implemented in December 2018 to replace the previous Spanish data protection law, the Organic Law on Data Protection (LOPD). The LOPDGDD sets out the framework for data protection in Spain and establishes the Spanish Data Protection Agency (Agencia Española de Protección de Datos or AEPD) as the regulatory body responsible for overseeing data protection compliance in Spain.

The framework outlined by both GDPR (Voigt & Von Dem Bussche, 2017) and LOPDGDD (2018) includes the following legal and regulatory requirements. In the instance of a data breach, it is compulsory to notify the Spanish Data Protection Agency (AEPD) within 72 hours of becoming aware of a data breach. This is to protect the rights and freedom of individuals. Furthermore, the company must notify affected individuals, those whose data has been compromised, without undue delay. The notification should clearly and concisely state information regarding the nature and scope of the breach, the types of affected data and the steps that the company is taking to mitigate the breach. However, this does not apply if the data has been rendered unintelligible, it is no longer personally identifiable information (PII) or the risk of harm is low. The following step after notification is the investigation into the data breach on behalf of the company to determine its scope and cause. Within this stage, companies will gain a more complete understanding of the nature of the data involved; the scope of the breach including the individuals involved; the cause of the breach and any vulnerabilities within the organisation’s systems or processes; finally, the response to the breach to mitigate the risk of harm to affected individuals. At this point, the company has an opportunity to demonstrate its commitment to data protection and to its consumers by meeting its legal and regulatory obligations.

Throughout the process, the GDPR (Voigt & Von Dem Bussche, 2017) and LOPDGDD (2018) state the necessity to cooperate with themselves and the AEPD. Both regulatory entities require companies to maintain records of data breaches and their management; transparency regarding their data breach practices, breach notification and risk mitigation; and the steps taken to manage breaches. Therefore, it is essential companies have or instate clear policies and procedures for data breach management. If a company fails to maintain the required records, it may be subject to legal and regulatory consequences, in addition to the financial liability derived from the data breach itself: €20 million or up to 4% of global annual revenue by AEDP (AEPD, 2021b). Under GDPR, companies can be fined up to 2% of their annual global revenue or €10 million, whichever is higher (GDPR, 2022). Finally, the company must consider and prepare its response to the data breach, ensuring that all decisions and steps are documented.

This paper will exclusively propose the most appropriate and effective data breach management strategy for multinational corporations (MNCs). In Spain, there are no specific laws or regulations that singularly apply to MNCs; all companies operating in Spain, regardless of size, must wholly comply with GDPR which protects the personal data of EU citizens. The obligations defined by GDPR (Voigt & Von Dem Bussche, 2017) include the implementation of appropriate technical and organizational measures in relation to company size to ensure data security, notification of authorities and involved individuals, and the correct and accurate completion of all records. The other factor to consider in relation to MNCs is that they have a higher global annual revenue, therefore they will be subject to a more significant fine for non-compliance as they are calculated on a percentage basis. Also, the media coverage will be more inclined to report on a more well-known company; the expected media response for an MNC is more severe and damaging unless well-managed.

Chapter 5: Most Suitable Data Breach Management

This Chapter will identify the most effective strategy for data breach management and so it will assume that the legal and regulatory requirements, accounted in Chapter 4, are already satisfied. Companies operating in Spain follow the official guideline proposed by the AEPD (AEPD, 2021b); they are responsible for overseeing the application of data protection laws and ensuring that individuals' personal data is protected in accordance with Spanish law. AEPD (2021b) highlights some important factors in the successful mitigation of response from a data breach. In the aftermath of a data breach, it is essential to act quickly and transparently to minimise the negative impact of the breach on affected individuals and the company's reputation because the delay or hiding of information can lead to distrust and further harm to the brand's image. It was recorded that on average a data breach took more than two months to be contained in 2022 (Chin, 2023). Therefore, it is essential that from the moment an internal data breach is identified, the MNC acts quickly and introduces its data breach management strategy immediately. A quick response and transparency can help to restore trust and credibility not only with consumers but with all stakeholders.

According to Chin (2023), the response to a data breach can be categorised into three main broad goals:

1. Containment of the situation
2. Notification of the affected parties
3. Fixing the breach and remediating risks

These three goals encompass all the activities an MNC should undertake to address a data breach, including legal responsibilities and those that will repair its reputation and relationship with consumers. MNCs should always comply with the AEDP laws and regulations at a minimum *[consult the previous section for this guideline]*. Further efforts should be undertaken to repair the relationship with existing consumers, especially those who suffered from the data breach with their data compromised. Primarily, a risk assessment needs to be undertaken to assess the impact of the breach and to determine the appropriate reactions that reflect the level of damage they experienced. The MNC must take responsibility for their actions and any harm inflicted. Depending on the type of data involved, consumers can face a variety of consequences that range from identity theft to financial harm (Muha, 2020). It must

also consider the sensitivity of the data and the potential harm to vulnerable groups, ie. children or individuals with disabilities; this would require a greater outreach by the MNC. Potential outreach may include credit monitoring services, identity theft protection, fraud alert services or other methods of support. To mitigate the diminished and negative relationship with consumers, consumers must not suffer any consequences from the data breach, or be inconvenienced, for example by needing to chase the company to receive their support. "Reputational damage suffered by companies who fail to protect personal data can translate directly into a loss of business" (Drinkwater, 2016).

Another key trait the MNC should embody is proactivity in response. The root cause of the data breach must be addressed to remove any vulnerabilities from the system or processes so a second incident cannot arise. MNCs can achieve this by implementing additional security measures and conducting a thorough investigation to identify the source of the breach. If consumers are not reassured that cybercriminals do not maintain an access point to the company and their data, they will revoke their relationship with the company, thus losing sales for the MNC.

All stakeholders of a business will be affected by a data breach. It is crucial for the MNC to communicate in a timely and transparent manner with its stakeholders, including shareholders and managers, as well as customers and regulators. Open communication is fundamental for building and maintaining trust. Effective communication involves not only informing stakeholders of the breach, but also providing them with information about the potential impact on their data and any steps they should take to protect themselves. The company must also provide information on the measures it is taking to prevent future breaches. In some cases, companies may also consider engaging external communication experts or consultants to assist with breach management and communication. This can provide the company with additional expertise and resources to effectively manage the communication process and ensure that stakeholders receive accurate and timely information about the breach.

Above all, a data breach is an opportunity for the company to complete an internal assessment to identify vulnerabilities and weaknesses; ensure all members of the company are well-versed in how to prevent and identify a data breach; and improve overall cybersecurity and data protection measures. The company being perceived as stronger after the data breach is a significant factor influencing whether consumers will maintain their relationship with the

company and whether new business will be generated. The perception of a stronger, more prepared company is in the interest of all stakeholders and the aim following a data breach.

In order to ensure the management of a data breach in Spain is consumer-centric, the values and behaviours of Spanish consumers must be considered. The economic crisis in the 1980s and the high rate of unemployment, measured at 13.26% in January of 2023 (TRADING ECONOMICS, 2023), have led to price being the most influential factor in purchasing decisions (*Reaching the Spanish Consumer - Santandertrade.com*, n.d.). Furthermore, due to this price hypersensitivity, there is a lack of brand loyalty in Spain. The report by Santander Trade (2023) states that 75% of the Spanish population search for the most cost-effective offer before buying and that 25% will switch their regular provider if they find a lower-priced substitute. This signifies that there is even greater pressure on a suitable response to a data breach in order to preserve relationships with consumers and retain their consumer base as they will be more willing to take their custom to another business due to a lack of loyalty.

On the other hand, a report conducted by Marcas con Valores, a Spanish marketing and communication agency, identified a change in consumer behaviour. The article discusses that there has been a rise in Spanish consumers who no longer prioritise price, especially the younger generations, "the younger, the more optimistic you are towards brands" (Haz, 2018). A third of Spanish citizens choose to interact and purchase from brands that "demonstrate" values. Likewise, 58% of respondents would be willing to pay more or choose a brand which demonstrates ethical behaviour and almost 60% prefer a brand that respects the environment, cares about social aspects or that takes care of its workforce (Haz, 2018). Other important values identified by Haz (2018) as purchase determinants are honesty, coherency, trustworthiness, and transparency with 80% of Spanish consumers signalling this to be fact. Therefore, for a business to seem favourable in the eyes of the Spanish population, it should ensure it demonstrates these four values while recognizing how the price of its product or service influences purchasing habits. The company should ensure it aligns its values with its statements and actions, recognizes its mistakes when necessary, and helps consumers to feel proud of their purchase. Targeting these values and behaviours in the management of a data breach will strengthen the brand reputation and specifically target the Spanish subset of their consumers.

Chapter 6: Proposed Solution

Chapter 6.1 Stages Of A Data Breach

For the purpose of this chapter, we will identify and label the different phases of data breach management in order to clearly apply each stage of the data breach management strategy at the most suitable point.

Brombacher (2019) identifies 5 stages of a data breach:

1. The alert
2. Data Leakage
3. Remediation
4. Aftermath
5. Pre-caution

This chapter will elaborate and further these stages to include reference to the developments in the business environment and specifically apply it to Spain.

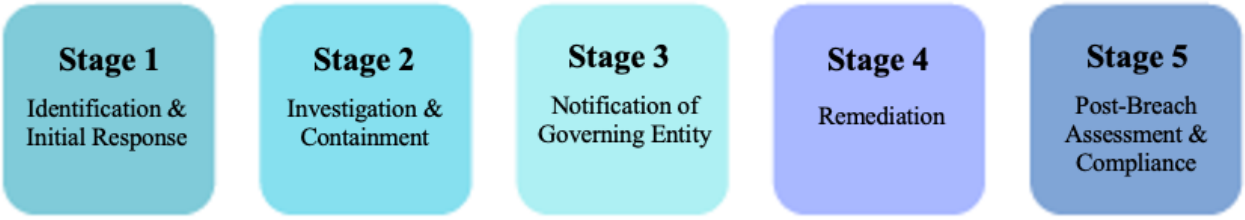

Diagram 1

Stage 1 will begin the moment a data breach has been identified and it will include the initial response strategy. The company should "be alert from the very first moment [it] experiences any problem with [its] IT infrastructure" (Brombacher, 2019). Following the discovery, the company must first confirm the potential data breach, then complete a preliminary assessment to gather information regarding the incident, assessing the potential impact and understanding the scope of the data breach. A response team will be formed, who will be responsible for analysing and responding to this incident. The team will typically include representatives from an array of departments as the data breach will affect the functions in different ways. Most importantly, the incident response team will include members from the IT, legal, public relations, marketing, and finance departments. The company should consider contracting a

cybersecurity expert and consultant if their staff is not sufficiently equipped for this type of incident.

Stage 2 refers to the investigation and containment of a data breach. It is during this phase that the primary and direct impact becomes known; if the data breach is a cyberattack, the hacker will make contact, extract data and/ or stop business operations (Brombacher, 2019). By this point, the company will only have a preliminary understanding of the incident, therefore a detailed and thorough investigation must be completed so the company has all the necessary information to continue. Next, the company will be able to initiate the containment protocol by taking immediate steps to stop the breach if it is still in process, prevent further unauthorized access to sensitive information, and mitigate ongoing damage. Both the investigation and containment processes will take considerable time; however, *Stage 3* must also be initiated in the first 72 hours following a data breach according to the AEPD. In Stage 3, the company must notify the governing body of the data breach and a communication plan must be developed. The communication plan must include a proposed strategy to communicate with all stakeholders: individuals affected by the data breach, employees, shareholders, and the public. This differs from Brombacher's (2019) theory of stages of a data breach; remediation will form Stage 4 so there is a dedicated phase that ensures compliance with Spain's data protection laws and regulations.

Stage 4 is arguably the most significant phase; it refers to the remediation of all impacts of a data breach with all stakeholders and the business itself. It also includes the recovery and restoration of data loss to ensure the business can continue operations. At this point, the business must secure its systems by implementing the lessons learned from the incident. It should no longer be possible for the company to be a victim of a data breach in the same method and all data protection strategies should be strengthened.

The final stage of a data breach is *Stage 5*, which incorporates the post-breach assessment and compliance. It includes aspects of both stages: the Aftermath and Pre-caution as outlined by Brombacher (2019). The post-breach assessment is a thorough and detailed analysis of the data breach in question, its impact on the business functions and overall business success, and the effectiveness of the data breach response. This report will prepare the business for any

future data breaches and similar incidents by identifying any opportunities for improvement in its response. The data protection authorities will have their own investigation for which the business must provide all information regarding the data breach and comply with any requests. Other legal responsibilities may include reporting to insurance providers, if necessary, and the full legal support and compliance if any further legal action is taken. Similarly to Stage 4, the business has a final opportunity to implement data protection strategies and additional security measures to address changes in the business and environment.

Chapter 6.2 Effective Response Strategy

The proposed methodology will state the best management strategies to respond to a data breach that specifically aims to protect the business' reputation and relationship with consumers. Therefore, we will first assume the notification of data protection agencies and the compliance of all legal obligations: providing all the necessary information with full cooperation and that all reports are completed within the given time frame. The following advice is additional to the recommendations proposed in Chapter 4 and Chapter 5 and the points can be applied at different stages of a data breach, Chapter 6.1. The following strategies will exceed the standard recommendations of governing bodies and are specific to the goal of preserving the relationship with Spanish consumers:

1. Clear, uncomplicated, and sincere notification to impacted individuals

The initial communication to impacted individuals should be clear, uncomplicated, and sincere. The company should be transparent with all information known at that time, the data in question, the implications this could have for the individual, and the immediate steps the business will take to remediate this. Contact information should be provided so consumers have easy access to further support and guidance if necessary. The correspondence should be addressed to every consumer directly by name acknowledging the impact and inconvenience caused, and express sincere regret for any harm suffered. Equally, it is important for the business to remain professional and in control of the situation, so consumers feel reassured. The business will make the first contact under Stage 3.

2. Dedicated and specific customer support and assistance

Establish dedicated support channels, such as a helpline or email address, to handle inquiries, concerns, and assistance requests from affected individuals and customers specific to the data breach in question. Businesses should provide timely responses to customer inquiries, offering empathetic and tailored support to alleviate concerns and demonstrate commitment to resolving any issues derived from the incident. It is essential that companies use this time to rebuild trust, if it is unable to provide timely responses then they should clearly outline a time frame in which they can respond and actualise it. The customer support line should be established during Stage 3 once consumers have been notified of the data breach and hence will need assistance; it should be accessible until Stage 5.

3. Retaining customers through compensatory measures

For long-term success, it is important to retain consumers and to ensure their satisfaction with the response to the data breach; dissatisfaction can lead to consumers forming a legal party and taking further legal action against the company. Consider offering appropriate compensation or remedial actions to affected individuals, in compliance with legal requirements. Remedial actions may include credit monitoring services, identity theft protection, etc. The compensatory measures should align with the scale of negative impact according to each individual; the more significant the individual harm, the greater the compensation. Under the GDPR, companies are required to take appropriate measures to address and mitigate the negative effects of a data breach. This may include providing compensation to affected individuals for any financial losses, emotional distress, or reputational harm they may have suffered as a result of the breach (Voigt & Von Dem Bussche, 2017). In Spain, the LOPDGDD (2018) further supplements the GDPR and establishes specific provisions regarding compensation for individuals affected by data breaches. It outlines the conditions and procedures for seeking compensation and allows affected individuals to initiate legal actions against companies to claim damages resulting from data breaches.

4. Re-assuring consumers with enhanced security measures and risk mitigation

First, complete an internal assessment to identify any remaining vulnerabilities and a third-party assessment by a cybersecurity consultant to verify the company's security infrastructure. As further risk prevention, deploy additional security controls and measures, such as encryption and employee training programs, to mitigate the risk of future breaches and instil confidence in consumers. Regularly communicate updates regarding improved security to consumers to demonstrate that consumers should feel safe and still trust the business with their data going forward. Show a genuine commitment to data protection and security by investing in robust security measures, adopting privacy-enhancing technologies, and promoting a culture of security awareness within the organization. Similarly, the organisation should provide transparent updates in data handling through clear communication on the collection, usage, and protection of the data in question.

5. Prevent consumers from dealing with higher prices due to higher costs

It is common for businesses to increase the price of products and services due to increasing cost per unit to protect the profit margin. Santander Trade (n.d.) reported that the Spanish population is hypersensitive to price fluctuations, therefore by maintaining low prices in the aftermath of a data breach, the business is not giving the consumer another reason to change suppliers. If it is not sustainable for the business to absorb these costs, make an effort to maintain the lowest price possible.

6. Rebuilding rapport with consumers through marketing

The most effective way to build rapport includes the identification of common ground, authenticity, and using humour appropriately. All promotional activity is an opportunity to build and strengthen the connection with consumers. Humour can help to create a "relaxed and friendly atmosphere" whereby the consumers feel more relaxed and connected to the brand (Bagley, 2023). This strategy can be applied in Stage 5, in the distant aftermath of the data breach once consumers' needs have been responded to and settled adequately. To be specific to Spanish consumers, promotional activities should reflect the values held highest by consumers in Spain: honesty, coherency, trustworthiness, and transparency (Haz, 2018).

7. Privacy Education and Empowerment

As well as educating employees to reduce the possibility of data breaches, the education of consumers on privacy and security is important to enhance consumer protection. The education of consumers will also act as an additional service that focuses on consumer well-being; the display of the organisations' commitment to consumer privacy will help to rebuild trust and improve the consumers' perception of the company. Companies can achieve this by providing resources like educational materials, and tips on personal cybersecurity to empower consumers to protect themselves online.

8. Control the digital narrative

Control of the digital narrative will allow a company to manage their reputation through the mitigation of speculations and rumours. The company can actively shape the perception of the incident and its response, minimizing reputational damage and restoring confidence in its brand. However, it will be a difficult task and it is unrealistic to expect complete control of the narrative as external media reports may be published. The company should focus on public

relation management to present the image of a united team in control of the incident. The digital narrative may also refer to the maintenance of a well-upheld account on their social media platforms. Consumers may reach out with concerns in a public forum using comments on the company's social media accounts, this is another reason why it is essential for a company to create a specific customer support line to mitigate consumers sharing any negative feedback in an open forum. In the absence of official information, speculation and rumours can spread quickly following a data breach. In 2016, Pew Research Centre reported that 23% of U.S. adults have shared fake news (Ordway, 2021). By taking control of the narrative, a company can combat misinformation, clarify misconceptions, and provide factual updates. This helps prevent the spread of false or exaggerated information that could further damage the company's reputation.

9. Corporate Social Responsibility

The most obvious method of improving a corporate image is through engagement in corporate social responsibility (CSR) initiatives. Corporate social responsibility refers to a model whereby companies demonstrate an effort to improve society and the environment which can be achieved through outreach programs and charitable donations, for example. Invest in initiatives that align with Spanish consumers' values, such as supporting local communities, environmental sustainability, or social causes. Demonstrating a commitment to society beyond profit can positively impact reputation. CSR has been widely investigated by scholars and proven to reap numerous rewards for a business, the most relevant include improved relations with stakeholders, customer loyalty, risk mitigation, avoidance of legal actions and building of a brand image (KsiężaK, 2016).

These 9 additional steps will make a further effort to make reparations to consumers for the damage as a result of the data breach. It will assist in the rebuilding of a relationship and improve the likelihood of continued activity with the company in question and brand loyalty.

Chapter 7: Case Study Analysis

7.1 Iberdrola

The Iberdrola Group is a global leader in renewable energy; its goal is to combat climate change with an energy transition to a low-carbon economy and offer a sustainable and competitive business model, creating value for society (Iberdrola, 2023). The company has been operating for 170 years, and in 2022 registered over 40,000 employees who supply energy to over 100 million people internationally. It is a Spanish multinational corporation whose headquarters are located in Bilbao, Spain.

On the 15th of March 2022, Iberdrola faced a cyberattack which corrupted the data of 1.3 million clients (Sáiz-Pardo, 2022). The data accessed was personally identifiable, it included addresses and contact information, however, the police stated that the cyber attackers did not access "sensitive" information like financial details. According to Iberdrola, the data breach was resolved within the day, nonetheless, and the following day they encountered more attacks which were unsuccessful. Although there are speculations that the cyber attack is related to the Ukraine-Russia war as retaliation to sanctions imposed on the country, it is yet to be confirmed; Spain's National Cryptology Centre (CCN) is working to ascertain the origin of the Iberdrola cyber-attack (Behr, 2022). On March 29th, the Spanish Government instituted a new "National Cybersecurity Plan" as an emergency measure in response to the war in Ukraine arising a greater risk of cyber-attacks for "geostrategic reasons" (Kemp, 2022). The purpose is to fortify the protection of SMEs and public institutions and the approval through a Royal Decree-law of specific cybersecurity regulations for the 5G network, thus relating to the business of Iberdrola. This attack was one of many; other entities like the Spanish parliament and the Cercanías local rail service in Madrid were simultaneously affected by cyberattacks. Iberdrola had the advantage of being prewarned by US officials about the potential of an attack; how did Iberdrola use the extra time to prepare themselves against the anticipated cyberattack?

The Iberdrola case study is untypical as the step mentioned in Chapter 6 as Stage 1 began before the cyber-attack was received by the business. The warning from the US aided Iberdrola which is confirmed by sources from the company itself: "the cyber attack has been limited" and "appropriate measures were established, and the leaking and theft of critical information has been avoided" (Murcia Today, 2022). Iberdrola notified the relevant governing boards of

the data breach within 72 hours as required by law (Stage 3). Following the data breach, Iberdrola contacted affected customers with a warning and advice. It advised consumers to be vigilant as scammers may attempt to use the information as part of phishing attempts and continued "If you have received the statement issued by the company, you must be vigilant and regularly monitor what information circulates on the Internet to detect if your private data is being used without your consent" (Behr, 2022). The company provided specific methods to potentially identify whether their information and private data were being used without their consent and the steps to take if that was the case, "If after conducting an internet search of your personal information you find any data that you do not like or that is being offered without your consent, exercise your rights. The Spanish Agency for Data Protection provides you with the guidelines on how to do it." (Kemp, 2022). Iberdrola experienced a decline in share price in the days following the publicization of the data breach. On the 14th of March 2022, the day before the cyber-attack, the share price was €9,860, and it begins to gradually fall to €9,484 on the 23rd of March 2022, it starts to increase at an inconsistent and gradual rate (Corporativa, 2023). However, the most significant change during the time of the data breach is the volume of shares commercialized which drops from 23,915,871 shares on March 15th 2022, the day of the data breach before the public is made aware, to 13,993,129 shares on the 17th of March 2022, just two days following the data breach. Despite these statistics, Iberdrola achieved a total revenue of €53.9bn in 2022, a 28% increase compared to 2021.

The analysis of Iberdrola's response reveals a mix of effective and ineffective responses. Their notification of the incident to the affected customers (Stage 1) is timely, easy to understand, and includes instructions if your data is being misused with the relevant contact details. It is a good example of transparent communication and helpful guidance as outlined in point 1 of the effective response strategy above. It also included information on how consumers should protect their data following the advice of the INCIBE (Kemp, 2022), extraneous to the data breach, so that they can maintain sufficient cyber security going forward which can be considered a part of remediation, Stage 4. Another positive strategy adopted by Iberdrola is the reassurance of consumers with enhanced security measures and risk mitigation. Iberdrola was able to repair the vulnerability within 24 hours and fight even greater cyber-attacks successfully the next day. Iberdrola holds a "Cybersecurity vulnerabilities mailbox" which can be used to bring attention to any vulnerabilities identified within the digital system to be

resolved. The purpose of the mailbox is to mitigate any further incidents as Iberdrola is "committed to strengthening the security of our systems and the protection of our assets" (Corporativa, 2023). However, Iberdrola could have improved its management of the data breach with a more personal approach by offering a dedicated and specific customer support line in order to have direct communication with the impacted consumers, instead of solely referring them to other data protection entities. This could have bettered Iberdrola's reputation while repairing the relationship with those affected.

From the published reports, Iberdrola did not offer compensation to victims of the data breach during Stage 4, a significant factor in the rebuilding of relationships as consumers want to have trust in their service providers. However, as the degree of compensation should be directly proportional to the level of harm done to the consumer, it can be argued that compensation was not necessary in this instance as no sensitive data was breached nor stolen so the damage to consumers is minimal. Similarly, as there was little financial damage to the company itself, the costs of services did not fluctuate [point 5]. Also, the low scale of the data breach meant there was little conversation online regarding the incident, few reports published by media, hence a lesser impact on its image and no requirement for control of the digital narrative. The remaining additional suggestions outlined by the proposed methodology include the rebuilding of rapport using marketing promotions and investment into its CSR. The investment into marketing campaigns will often prove worthwhile, it can refocus the community on the core values and purpose of the company while strengthening rapport with consumers. It would have been a great option for Iberdrola to reconnect with consumers. Likewise, Iberdrola did not invest in CSR initiatives (Iberdrola España News, 2022) when it is probable to greatly enhance their reputation. It is an effective strategy in the redirecting of narrative to focus on positive actions of the business rather than negative headlines.

Overall, the extra time due to the prewarning of US officials allowed Iberdrola to sufficiently prepare for the attack and mitigate the risks. Therefore, the incident required a less extreme response and so the reputation faced less harm and Iberdrola was able to maintain its rapport with the consumers involved. The company's response was adequate but could have been improved using suggestions from the proposed methodology in Chapter 6, namely a dedicated customer support line and marketing activity to enhance the rapport with the company and its consumer base.

7.2 CaixaBank

CaixaBank is a prominent financial institution with the headquarters in Valencia, Spain. The bank was founded in 2011, it operates as a subsidiary of CriteriaCaixa, a leading financial group. With an extensive presence in Spain, 4,663 offices within Spain and Portugal (CaixaBank Sobre Nosotros, 2023), CaixaBank has established itself as "the leading financial group in Spain" (CaixaBank, 2023). It operates through a network of branches and digital channels, catering to 20.1 million customers internationally and supported by 44,654 employees (CaixaBank Sobre Nosotros, 2023). The bank manages a significant amount of assets, and has a wide range of financial products and services. Committed to innovation and customer-centricity, CaixaBank plays a vital role in the Spanish banking sector, supporting economic growth and financial stability. In the first quarter of 2023, CaixaBank reported a 21.2% increase in net profit from the same period in the previous year amounting to €855 million (CaixaBank, 2023).

CaixaBank's data breach is record-breaking as it was the subject of the largest sanction ever imposed by the APED against a company for violating GDPR; the sanctions totalled €6 million across two fines (Aguiar, 2021). The unfolding of the CaixaBank data breach began in January 2018 due to the reports of a singular user who recognised the institution's notification for compulsory acceptance of new terms and conditions as problematic. Aguiar (2021) accounts that the AEPD heard that the terms and conditions detailed CaixaBank's consideration to transfer the data of its customers to *all* the companies of the "la Caixa" banking group, including BPI, VidaCaixa, CaixaBank Asset Management and MicroBank (CaixaBank Sobre Nosotros, 2023). The implication is that it would require the consumer to actively withdraw their participation of data from every member of la Caixa one by one in order to cease the processing of the individual's data by each of the named companies. This requirement was considered to be "disproportionate" by the claimant and, most importantly, the AEPD as "the transfer is accepted in a single act" (Aguiar, 2021). Two years following the initial complaint, the AEPD confirmed that articles 13 and 14 of the GDPR were violated by CaixaBank as well as article 6 to a "very severe" extent (AEPD, 2021, p.31). The misconduct was summarised by the AEPD as the failure to meet the requirements "for the provision of valid consent" due to "deficiencies in the processes enabled" and that there was an "illicit transfer of personal data to group companies" (Aguiar, 2021). The customer complaint in 2018 resulted in one part of the fine, €4 million, while €2 million can be accredited to a second complaint in 2019 by

the Federación de Asociaciones de Consumidores y Usuarios de Andalucía (FACUA), a non-profit organisation dedicated to the defence of consumer rights (FACUA [FACUA.org], 2021). CaixaBank's data processing operations were also required to ensure compliance with GDPR within 6 months following the sanctions (AEPD, 2021).

Despite the record-breaking fine, CaixaBank's data breach management strategy was limited with few publications addressing the subject. However, CaixaBank participated in multiple well-timed strategic alliances in 2021 following the AEPD's publication of sanctions. In November 2021, CaixaBank partook in a technological and commercial integration with Bankia which was reported in the media to "make history in the Spanish banking system" (Mercader, 2021). In the lead-up to this integration, multiple awareness campaigns, including regular newsletters, were published to both staff and consumers to warn about "the most frequent frauds and scams and the measures they must take to avoid being victims of deception" (Mercader, 2021). Similarly, in October, CaixaBank capitalized on 'cybersecurity awareness month' in an attempt to reinforce a culture of prevention internally (Mercader, 2021). Another transformative and reputation-enhancing activity is CaixaBank's partnership in the EU-SEC (European Security Certification Framework) cybersecurity research project which was funded by the European Union within the Horizon 2020 program (Alconada, 2020). CaixaBank is renowned for its cybersecurity ecosystem, an infrastructure crafted with the aim of protecting its digital assets from cyber threats. It also has a group, CiberSOC, which specializes in responses to computer security incidents and a centre that coordinates the integral security of La Caixa Group; CiberSOC operates 24 hours a day. This team is "one of the most specialized in the sector in Europe" (Alconada, 2020). Another method of data breach management is the mitigation of future risks: CaixaBank is continuously developing safety awareness and awareness programs for all employees which are adapted to each level to maintain a constant level of alert to possible threats that may affect either customers or the bank itself (*Cómo Protegerse De Los Ciberataques*, 2017).

CaixaBank is lacking a targeted response to the data breach of 2018. Despite strategies like strategic alliances and a specialised cybersecurity team which are likely significant factors in the strength of the reputation of its cybersecurity ecosystem, CaixaBank would have benefited from addressing this data breach in a transparent and holistic way. For example, through open communication with the public, either in a press release or across one of its social media

accounts. It is unclear whether the bank notified individuals of their unlawfully transferred data, however in Stage 1, the identification and initial response, the entity should have prioritised transparency with consumers, especially as "trust" is a core value of the business (CaixaBank, 2023). A clear, uncomplicated, and sincere notification to the affected individuals, as recommended by point 1, would initiate the remediation process by taking accountability and being transparent. Despite numerous articles published by CaixaBank about cybersecurity and data breaches, there seems to be no mention of the 2018 GDPR data breach. During stage 1 is the most appropriate time for the creation of a dedicated and specific customer contact line to deal with any queries and concerns. Although CaixaBank did not introduce a line specific to this GDPR violation, the institution has a webpage titled "Data Protection: Exercise of Rights", where consumers can simply and quickly fill in a form to exercise their rights, for example, the right to access personal data stored (CaixaBank, 2023). A specific outreach option for the data breach would increase the ease of communication for consumers, likely enhancing the consumer experience of a negative topic.

Stage 2 encompasses the investigation of the data breach, however, as CaixaBank is aware of its role in the unlawful storage of consumers' data, this is not necessary. Similarly, the act of containment is not relevant to this case study. The notification of governing bodies was completed by an external individual who reported the bank's unlawful behaviour. Stage 3 also refers to the compliance of said governing bodies with the correct and full management of records pertaining to the case. CaixaBank did not uphold this requirement and so was subject to a further €2 million sanction as previously addressed. It is an essential requirement for businesses, not only to avoid the risk of further financial reprimands but also to maintain the reputation of the brand. This exacerbates the risk of negative media reports, increasing the difficulty of presenting a positive digital narrative. There are limited articles and negative publicity regarding this incident, this can be attributed to a lack of published accounts or successful control of the digital narrative. It is not possible to identify which option.

Remediation is usually essential in cases of data breaches, however, there was only a singular claimant in the CaixaBank case study; the company's behaviour affected a large, unknown quantity of consumers, possibly all Spanish consumers. Therefore, Stage 4 and the distribution of compensatory measures are not as feasible as if a limited portion of consumers were affected by the incident. Alternatively, as a compensatory offer, the company could consider a

reduction in services for a temporary period of time, or it could send a small token of appreciation to consumers. Data was unlawfully transferred between La Caixa, however, the data was not lost to unknown parties and is not at risk of being stolen. Therefore, the consequences to the consumer are relatively limited, they are not at risk of fraud or identity theft, hence, the compensation does not need to be significant to align with the level of harm done to the individual. Another opportunity to repair relationships with consumers and rebuild reputation is through CSR practices. CaixaBank has successfully crafted a positive brand reputation associated with cybersecurity, investment into CSR practices presents a positive social image to consumers and removes the focus from the incident. In 2021, CaixaBank signed the Collective Commitment to Financial Health and Inclusion to promote better financial health and inclusion within society and achieved status as the leader in social bonds in Western Europe amongst other social outreach programs (CaixaBank Sustainability Report, 2021). The bank now successfully contributes to consumer privacy education and empowerment by sharing information and advice regularly (Mercader, 2021).

Finally, the institution could improve its 2018 data breach management strategy in Stage 5 with the implementation of point 4, the reassurance of consumers with enhanced security measures and risk mitigation. CaixaBank has surpassed expectations in terms of the standard of cybersecurity with its specialized CiberSOC support system; so consumers can feel assured of this effort into data protection. It is important to convey this information clearly. Communication can be conducted through corporate press releases, notifications through the application or direct email. Direct email allows for personal identification which further facilitates the rebuilding of rapport with consumers as discussed in Chapter 6. To conclude, CaixaBank has excelled with aspects of data breach management, specifically the fortifying of cybersecurity to mitigate future risks and the education of consumer privacy. However, in order to achieve the greatest benefit from the strategy, CaixaBank must improve its communication with consumers to be transparent and informative of new measures.

7.3 Hotel Meliá

Hotel Meliá is a distinguished global hotel chain which is a leader in the hospitality industry. The company, founded in 1956, is headquartered in Palma de Mallorca, Spain, although Meliá boasts an extensive international presence with over 390 hotels in more than 40 countries worldwide (MELIA HOTELS INTERNATIONAL SA, 2023). In its home country of Spain, Hotel Meliá operates an impressive portfolio of over 100 hotels, strategically positioned in prime locations across the country. With a commitment to luxury, innovation, and exceptional service, Hotel Meliá offers an unparalleled guest experience, catering to a diverse range of travellers. Its dedication to excellence is reflected in its substantial guest capacity, accommodating over 7 million guests annually. With its unwavering pursuit of hospitality excellence, Meliá Hotels International is "unique among the 20 largest international hotel groups" especially with its "Spanish warmth and passion" differentiates the brand (Meliá Hotels International, 2023). In 2022, Meliá Hotels International turned over €110,693,000 net profit, a significant increase in comparison to the negative net profit in 2021(MELIA HOTELS INTERNATIONAL SA, 2023).

On Monday October 4th of 2021, Hotel Meliá suffered a suspected ransomware attack in the early hours which activated the response protocols and containment work (INCIBE, 2021). A news article reported that the cyberattack "restricts access and requests a 'rescue' to enter the system" in order to restore access and data (20minutos, 2021). The cyberattackers disassembled parts of the entity's internal network and some web-based servers, including its reservation system and public websites; the breach predominantly affected Meliá's Spain-based operations (Cybersecurity Help, 2021). For example, the Meliá Barcelona Sky Hotel became inaccessible to users as a result of the cyberattack, the page read "*Oops! Sorry, this page does not exist"* (Recacha, 2021). Despite the ransomware cyberattack, no party publicly took credit for the attack and the data in question did not appear on the dark web (Stankard, 2021). However, the hotel group was contacted privately for payment under extortion in return for the key that would unlock the encrypted systems; the Meliá group refused to negotiate with the terrorists (Ortín, 2022). The effects of the ransomware attack as customers were unable to access their rooms with the digital key card and staff were unable to access any online servers and worked with pen and paper, a significant impact on operations. This breach was categorized as "the largest cyberattack suffered by the Meliá group" in its history (Ortín, 2022). The data breach had such a significant impact on the hotel group due to the time of

occurrence; in 2020, Meliá recorded a loss of €426 million due to the Covid pandemic, hence this was a “crucial time” for the corporation (Ortín, 2020).

The hotel group immediately notified the relevant authorities within 24 hours and contracted Telefónica Tech's cybersecurity services as a specialist consultant on the matter (Europa Press [epturismo], 2021). Telefónica formed part of the “Crisis Committee” whose aim is the continuation of business services (Europa Press [epturismo], 2021). The committee consisted of at least 60 members across Meliá and Telefónica (Ortín, 2022). The Meliá group also made a public statement announcing its activation of response protocols and business continuity plans to remediate the incident; the public were regularly updated with relevant news (Stankard, 2021). The hotel chain stated they had prepared for this incident as they had been integrating their data to the Cloud services since 2017, therefore once the incident response plan was initiated, the basic services were recovered “in a large part of hotels in a matter of hours, and 100% in a few days” (Ortín, 2022). Hotel Meliá informed in its 2021 annual financial report that the most critically important issue in its Materiality Analysis is cybersecurity (Meliá, 2021). The Meliá group stated, "We learned many lessons about the strengths and weaknesses of our systems that have allowed us to continue working on strengthening them," (Ortín, 2022). The company have taken the 2020 data breach and reframed it as an opportunity to reassess its systems to mitigate future risks, the Meliá group have a greater understanding of the importance of cybersecurity and, most importantly, has modernized and reinforced its computer defense systems (Ortín, 2022).

The Meliá group is a prime example of data breach management with a consumer-centric focus, it was transparent, informative, and proactive. In Stage 1, the entity responded immediately once the cyberattack presented itself, within 24 hours the governing bodies (Stage 3) and Crisis Committee had been notified and initiated action. The hotel group also published a clear and uncomplicated announcement to the public, through its social media account, clearly stating the current events and the steps which are being taken to remediate the incident. Also, the company have been sincere in their communications, putting the consumer at the forefront; Recacha (2021) reported that Meliá “has regretted the inconvenience caused to its customers and collaborators and is working to mitigate the impact on its operations and return to providing its services normally as soon as possible”. This cyberattack did not involve the

exfiltration of consumer data and, although the introduction of a dedicated and specific customer support line may have still proven advantageous, it is not an essential step when considering the context. Each entity of the hotel group has a direct contact line which is constantly accessible due to the nature of the hospitality industry. The immediate intervention of Telefónica in Stage 2 facilitated the quick return of operations. At all stages of the data breach management strategy, the hotel group have been proactive and quick to respond which will improve how consumers perceive the company in the aftermath of the data breach.

Analysis of the data breach management strategy at Stage 4 reveals some of the techniques identified in the proposed methodology of Chapter 5, most notably the reassurance of consumers with enhanced security measures and risk mitigation. The institution exemplified the way companies should use incidents like this as an opportunity to test for other vulnerabilities to mitigate risks of future reoccurrences. Consumers are more likely to feel comfortable to continue utilizing the services of the Meliá group. As recognised above, consumer data was not exfiltrated and so the extent of harm to consumers would have been a potentially less enjoyable or mildly inconvenient experience in its establishments due to a lack of functioning operations. Therefore, compensatory measures may be deemed unnecessary; consumers would have had the opportunity to complain during their interaction with the hotel group and remediation may have been addressed at this time in person as is typical for the hospitality industry. The Meliá group were not financially harmed as a result of the data breach (excluding the costs incurred with the data breach management strategies), it did not pay the cost of extortion or was liable for sanctions. Therefore, there were no higher fees to consumers in order to account for the increased costs. The hospitality industry allows for personal relationships built with consumers, allowing for strong rapport. Meliá strives for excellence in terms of customer care (Meliá Hotels International, 2023) and so has a prime opportunity to reassure consumers and rebuild the relationship.

Another key method is the investment in CSR, an act that Meliá has actualized over the last 60 years, “[the company] aim to contribute to the common good through strong social commitments and corporate values rooted in more than 60 years of history" (Meliá Hotels International, 2023). It states that “Corporate Responsibility is the backbone of our business strategy” (Meliá Hotels International, 2023), this will refocus the reputation to the positive

actions of the company. The final suggestion from the proposed methodology to be applied in Stage 4 is the privacy education and empowerment of consumers, an action that Meliá could have improved. There are no reports of contact between the hotel group and consumers with the purpose of sharing information, advice, and warnings about personal cybersecurity. It is an important step in the building of relationships and the enhancement of reputation. Finally, in Stage 5 titled the post-breach assessment and compliance, the ongoing control of the digital narrative is important in ensuring the brand connotes positivity. Stankard (2021) states that "a disrupting ransomware attack on a prominent hotel chain would garner major headlines", but by coincidence on the same date Facebook, Instagram and Whatsapp experienced a greater cybersecurity incident. Therefore, Meliá were able to avoid the negative media reports and so did not require control of the digital narrative. However, it is important to note that if media reports were published regarding the Meliá group, control of the digital narrative would have been the most effective approach.

Chapter 8: Discussion

The results from the three case studies revealed that all companies fulfilled points 4 and 9 from the proposed methodology in Chapter 6.2. These points respectively refer to the reassurance of consumers with enhanced security measures and risk mitigation, and investment into corporate social responsibility practices. All three companies have partaken in CSR throughout its history and although it will refocus the reputation on the positive activities of the institution, we cannot definitively state that the CSR practices were data breach management strategies without confirmation from the companies themselves. Therefore, in terms of data breach management strategies, we can confirm that the companies most value enhanced security measures in order to mitigate future reoccurrences and reassure consumers of their capabilities. However, none of the three case studies employed points 2, 3 and 6 which are a specific customer support line, compensatory measures, and the rebuilding of rapport through promotional activities, respectively. The drawbacks of offering compensatory measures could relate to the financial costs, and potentially legal reprimands as it could be considered an 'act of culpability'. Similarly, marketing campaigns can be costly and especially in the cases where companies are already liable for sanctions, it may not be financially feasible. A specific, dedicated customer care line is a low-cost option which is consumer-focused and prioritises ease and access to information. These suggestions should only be used when a company is in the position to afford the strategy and it is expected to be applicable to the context of that data breach.

The case studies Iberdrola and CaixaBank both lacked interaction with consumers on a personal level which may have affected their credibility and rapport, it is an opportunity to improve in the future. Both parties seemed to have pushed for a narrative of improved cyber security and education on the subject while avoiding personal interaction with the individuals affected potentially to avoid too much publicity on the issue which may have negatively impacted their image and rapport with consumers in the long term. Another common theme between all three cases is that the issues were reprimanded relatively quickly, either to resume operations or to improve reputation; therefore, the speed at which the data breach is resolved is a key factor in its success post-data breach.

Limitations of the case study analysis must be considered; the case studies can only consider published external sources. The MNCs in question may have fulfilled other stages of data breach management internally and without such reporting, those actions cannot be discussed or analysed. Future research endeavours could address these limitations by conducting in-depth interviews with key stakeholders and expanding the scope to encompass a broader range of industries and regions. A second limitation is the difficulty of comparing and analysing case studies of companies in different industries with different types of data breaches. Data breaches present in many forms, the context of the data breach is decisive in the selection of data breach management strategy. For example, in the case of CaixaBank, numerous points from the proposed data breach management strategy were inapplicable due to the context of the case study. The proposed methodology does not all need to be applied together, rather it is a list of options from which companies can choose to safeguard reputation and rebuild the relationship with consumers, dependent on its situation.

Chapter 9: Conclusion

The primary objective of this dissertation is the investigation of the optimal response of MNCs to data breaches, with a specific focus on safeguarding their reputation and cultivating positive relationships with Spanish consumers. By conducting an extensive analysis of three case studies -Iberdrola, CaixaBank and Hotel Meliá- and examining the legal and regulatory landscape, this research has provided valuable insights into the key considerations and best practices associated with effective data breach management.

The findings of this study highlight the critical importance of prompt and transparent communication with both the public and individuals affected as a pivotal factor in mitigating the reputational damage arising from data breaches. The examination of case studies critically demonstrates the effectiveness of immediate and open communication, coupled with a proactive approach to addressing customer concerns. Furthermore, the analysis of Spain's legal and regulatory framework illuminates the significance of adhering to data protection laws and promptly reporting breaches to the relevant authorities in order to avoid subjection to large financial sanctions, like in the case of CaixaBank. The case study analysis revealed that for a company to positively stand out, it should consider the implementation of points 2, 4 and 9 which Iberdrola, CaixaBank and Hotel Meliá did not employ following their respective data breaches. Therefore, it will show an even greater commitment to the prioritisation of consumer satisfaction. It is fundamental that the context of the data breach is evaluated in order to choose and apply the most relevant points from the list of proposed methodology to the situation.

This research makes a noteworthy contribution to the field of data breach management by offering a comprehensive analysis of the reputational damage resulting from such incidents. The identification of key factors and measures influencing reputational harm enables MNCs to gain a deeper understanding of the underlying dynamics and make informed decisions regarding their response strategies. Moreover, the proposed solution framework provides practical guidance to MNCs operating in Spain, empowering them to fortify their data breach management practices and minimize adverse repercussions on their reputation and relationship with consumers. The implications of this research extend beyond theoretical insights, providing tangible benefits for MNCs operating in Spain. First and foremost, it is essential for organizations to establish robust data breach response plans, like the ‘Crisis Committee’ of Hotel Meliá, that prioritize effective communication, comprehensive customer support, and

compliance with legal requirements. By adopting these measures, MNCs can not only safeguard their reputation but also cultivate trust and maintain favourable relationships with Spanish consumers.

In essence, this research substantially contributes to the existing foundation of knowledge and provides invaluable insights for organizations, policymakers, and researchers engaged in the field of data breach management.

References

6 Potential Long-Term Impacts of a Data Breach. (2021, November 5). Security Intelligence. https://securityintelligence.com/articles/long-term-impacts-security-breach/

AEPD. (2021). Resolución de Procedimiento Sancionador. In *AEPD* (PS/00477/2019). Agencia Española Protección de Datos. https://www.aepd.es/es/documento/ps-00477-2019.pdf

AEPD. (2021b). Guidelines on Personal Data Breach Notification. In *Agencia Española Protección De Datos*. https://www.aepd.es/es/documento/guidelines-personal-data-breach.pdf

Aguiar, A. R. (2021, January 22). New record: the Spanish Data Protection Agency fines CaixaBank 6 million euros for violating GDPR. *Business Insider*. https://www.businessinsider.com/httpswwwbusinessinsiderescaixabank-multada-6-millones-euros-vulnerar-rgpd-790971?op=1

Bagley (2023, March 24). *Building Rapport in Sales and Marketing*. Lead Forensics. https://www.leadforensics.com/blog/building-rapport-in-sales-and-marketing/#:~:text=To%20build%20rapport%2C%20it%20is,increased%20sales%20and%20customer%20loyalty.

Behr, M. (2022, December 18). Scottish Power Parent Company Iberdrola Hit by Cyber-attack. *DIGIT*. https://www.digit.fyi/iberdrola-cyberattack-scottish-power/

Boehm, J., M. Kaplan, J., Merrath, P., Poppensieker, T., & Stähle, T. (2020). Enhanced cyberrisk reporting Opening doors to risk based cybersecurity. *Risk & Resilience*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/enhanced-cyberrisk-reporting-opening-doors-to-risk-based-cybersecurity

Brombacher, F. (2019, February 15). The 5 Data Breach Stages | Crashtest Security. *Crashtest Security*. https://crashtest-security.com/data-breach-stages/

Burden, K. (2019). EU update. *Computer Law & Security Review*, *35*(1), 103–111. https://doi.org/10.1016/j.clsr.2018.12.007

CaixaBank. (2023, May 5). *CaixaBank reports a net profit of €855 million up to March (+21.1%) and maintains its balance sheet strength with NPLs at all-time lows* [Press release]. https://www.caixabank.com/comunicacion/noticia/caixabank-reports-a-net-profit-of--855-million-up-to-march--21-1--and-maintains-its-balance-sheet-strength-with-npls-at-all-time-lows_en.html?id=44021&loce=NA-SITE-ResultadosPrimerTrimestre2023-1-terrat-NA-DivClassHmSlideTitleH2CaixabankReportsNetProfitOf855MillionUpToMarch211AndMaintainsItsBalanceSheetStrengthWithNplsAtAllTimeLowsH2Div-NA#tercertrimestre

Chin, K. (2023, March 2). *What Should Companies Do After a Data Breach? | UpGuard*. https://www.upguard.com/blog/what-should-companies-do-after-a-data-breach

Cómo protegerse de los ciberataques. (2017, May 25). El Blog De CaixaBank. https://blog.caixabank.es/blogcaixabank/ciberataques-una-amenaza-constante-como-protegernos/

Corporativa, I. (2023). *Cibersecurity vulnerabilities mailbox - Iberdrola*. https://www.iberdrola.com/contact/responsible-disclosure-vulnerabilities

Corporativa, I. (2023). *Iberdrola shares - Today's share price - Iberdrola*. Iberdrola. https://www.iberdrola.com/shareholders-investors/share/price

Cyberattack hits Meliá, one of the largest hotel chains in the world. (n.d.). https://therecord.media/cyberattack-hits-melia-one-of-the-largest-hotel-chains-in-the-world

Cybersecurity Help. (2021, October 14). Cyberattack cripples one of the world's largest hotel chains. *CybersecurityHelp*. https://www.cybersecurity-help.cz/blog/2365.html

De Gregorio, G. (2022). The Transnational Dimension of Data Protection. *The Italian Review of International and Comparative Law*, *1*(2), 335–359. https://doi.org/10.1163/27725650-01020006

Deloitte, & Ryan, O. (n.d.). Changing the game in cyber risk. *Deloitte*. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-gra-Changingthegameoncyberrisk.pdf

Digistor. (n.d.). *What Happens to a Company's Reputation After a Data Breach? | DIGISTOR*. https://digistor.com/what-happens-to-a-companys-reputation-after-a-data-breach/

Drinkwater, D. (2016, January 7). *Does a data breach really affect your firm's reputation?* CSO Online. https://www.csoonline.com/article/3019283/does-a-data-breach-really-affect-your-firm-s-reputation.html

Europe, C. O., & Rights, E. U. a. F. F. (2018). *Handbook on European data protection law: 2018 Edition*. Council of Europe.

Efe. (2021, October 4). Los servidores de varios hoteles Melià sufren un ataque cibernético. *www.20minutos.es - Últimas Noticias*. https://www.20minutos.es/noticia/4844225/0/los-servidores-de-varios-hoteles-melia-han-caido-por-un-ataque-cibernetico/

Europa Press [epturismo]. (2021, October 4). Meliá sufre un ciberataque que afecta a varios hoteles del grupo. *europapress.es*. https://www.europapress.es/turismo/hoteles/noticia-melia-sufre-ciberataque-afecta-varios-hoteles-grupo-20211004201209.html

FACUA [FACUA.org]. (2021). The Spanish Data Protection Agency fines Caixabank 6 million euros following complaints from FACUA and a customer of the bank. *FACUA.org*. https://www.facua.org/es/noticia_int.php?Id=16364&idioma=1

Fie, S. (2023, January 13). *What Happens to a Customer After a Data Breach? - Security Boulevard*. Security Boulevard. https://securityboulevard.com/2023/01/what-happens-to-a-customer-after-a-data-breach/

Forbes & IBM. (n.d.). Fallout: The Reputational Impact of IT Risk. In *Forbes Insights* (212.366.8890). Forbes Media. https://images.forbes.com/forbesinsights/StudyPDFs/IBM_Reputational_IT_Risk_REPORT.pdf

Gracias, T. (2022). What’s the True Cost of a Ransomware Attack? 2022. *CloudAlly*. https://www.cloudally.com/blog/cost-of-ransomware-attack-2022/

Haz. (2018). El 80% de españoles busca marcas con valores más allá de la calidad o el precio. *Revista Haz*. https://hazrevista.org/rsc/2018/01/el-80-de-espanoles-busca-marcas-con-valores-mas-alla-de-la-calidad-o-el-precio/#:~:text=precio%20%2D%20Revista%20Haz-,El%2080%25%20de%20espa%C3%B1oles%20busca%20marcas%20con%20valores%20m%C3%A1s%20all%C3%A1,que%20condicionan%20en%20la%20compra.

How reputational damage from a data breach affects consumer perception. (n.d.). Imprivata. https://www.imprivata.com/blog/reputation-risks-how-cyberattacks-affect-consumer-perception

IBM. (n.d.). Cost of a Data Breach Report 2022. In *IBM Security* (1.800.887.3118). https://www.ibm.com/downloads/cas/3R8N1DZJ

INCIBE. (2021, October 4). *Several Meliá Group hotel servers suffer a cyber attack* [Press release]. https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/several-melia-group-hotel-servers-suffer-cyber-attack

Insitituo Nacional de Ciberseguridad [incibe.es]. (2023). *Balance de Ciberseguridad 2022*. https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2022_incibe.pdf

Instituto Nacional de Ciberseguridad [incibe.es]. (n.d.). Balance de Ciberseguridad 2021. *incibe.es*. https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2021_incibe.pdf

Interactive portfolio - Official Meliá corporate website. (n.d.). https://www.meliahotelsinternational.com/en/our-company/melia-in-the-world/portfolio

Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: a technological perspective and review. *Journal of Big Data*, *3*(1). https://doi.org/10.1186/s40537-016-0059-y

Josh.Breaker-Rolfe. (2022). Spanish energy giant hit by data breach. *IT Security Guru*. https://www.itsecurityguru.org/2022/04/04/spanish-energy-giant-hit-by-data-breach/

Kemp, L. (2022, March 31). Personal data of 1.3 million Iberdrola customers stolen in cyberattack. *Euro Weekly News*. https://euroweeklynews.com/2022/03/31/iberdrola-cyberattack/

Kondruss, B. (2023a). Major cyber attacks Spain, 4th quarter 2021. *KonBriefing Research*. https://konbriefing.com/en-topics/cyber-attacks-2021-cny-spain-q4.html

Kondruss, B. (2023b). Cyber attacks Spain in 2022. *KonBriefing Research*. https://konbriefing.com/en-topics/cyber-attacks-2022-cny-spain.html

KsiężaK, P. (1995). View of The Benefits from CSR for a Company and Society. *Journalof CorPorate resPonsibilityand leadershiP*, *3*(4). https://apcz.umk.pl/JCRL/article/view/JCRL.2016.023/12526

LOPDGDD. (2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. In *LEGISLACIÓN CONSOLIDADA* (BOE-A-2018-16673). https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

MELIA HOTELS INTERNATIONAL SA. (2022). *MELIA HOTELS INTERNATIONAL SA* (No. ES0176252718). https://produkte.erstegroup.com/modules/res/PdfRenderer.php?f=ES0176252718-2023-01-24.pdf&u=%2Fmodules%2Fres%2Fcompany_profile%2Fdownload.php%3FLANG%3Den%26MARKET%3Dat%26ISIN%3DES0176252718

Muha, M. (2020, March 10). *Calculating the severity of a data breach*. https://www.mikemuha.com/2020/03/calculating-severity-of-data-breach.html

Muñoz, R., País, E., Muñoz, R., & País, E. (2017, May 15). Major Spanish firms among victims of massive global cyber attack. *EL PAÍS English*. https://english.elpais.com/elpais/2017/05/12/inenglish/1494588595_636306.html

News team. (2022, October 3). *Long-Term Impacts A Data Breach Can Have on Your Business - Cyber Defense Magazine*. Cyber Defense Magazine. https://www.cyberdefensemagazine.com/long-term-impacts/

O'Driscoll, A. (2022). Spain cyber security and cyber crime statistics (2020-2022). *Comparitech*. https://www.comparitech.com/blog/information-security/spain-cyber-security-statistics/

O'Driscoll, A., & O'Driscoll, A. (2022). Spain cyber security and cyber crime statistics (2020-2022). *Comparitech*. https://www.comparitech.com/blog/information-security/spain-cyber-security-statistics/

Ordway, D. (2021, February 15). *Fake news and the spread of misinformation: A research roundup*. The Journalist's Resource. https://journalistsresource.org/politics-and-government/fake-news-conspiracy-theories-journalism-research/

Ortín, A. (2022, October 8). Meliá, un año del peor ciberataque de su historia: «Estamos siendo atacados, cortamos comunicaciones». *okdiario.com*. https://okdiario.com/economia/melia-ano-del-peor-ciberataque-historia-estamos-siendo-atacados-cortamos-comunicaciones-9785264

Ponemon Institute. (2014). The Aftermath of a Data Breach: Consumer Sentiment. In *Ponemon Institute Research Report*. https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf

PricewaterhouseCoopers. (n.d.). *Trust, risk, and opportunity: overseeing a comprehensive data and privacy strategy*. PwC. https://www.pwc.com/us/en/services/governance-insights-center/library/overseeing-data-privacy-strategy.html

PwC. (n.d.). *Building trust with persistent third-party risk management*. https://riskproducts.pwc.com/resources/building-trust-with-persistent-third-party-risk-management

Ransomware Brings Down Large International Hotel Chain. (n.d.). TitanHQ. https://www.titanhq.com/blog/ransomware-brings-down-large-international-hotel-chain/

Reaching the Spanish consumer - Santandertrade.com. (n.d.). https://santandertrade.com/en/portal/analyse-markets/spain/reaching-the-consumers

Recacha, V. (2021, October 4). Un ciberataque a Meliá deja sin web a varios de sus hoteles. *Crónica Global*. https://cronicaglobal.elespanol.com/business/20211005/un-ciberataque-melia-deja-sin-varios-hoteles/617188373_0.html

Spain - Data Protection Overview. (2022, December 19). DataGuidance. https://www.dataguidance.com/notes/spain-data-protection-overview

Statista. (2022, July 21). *Number of cybercrime victimizations Spain 2011-2019*. https://www.statista.com/statistics/1173320/cybercrime-number-of-victimizations-spain/

Topic: Remote work in Spain. (2023, March 22). Statista. https://www.statista.com/topics/7673/remote-work-in-spain/#topicOverview

Tus datos, en constante peligro: cada día se producen más de cuatro brechas de seguridad en España. (2022, January 28). *20minutos*. https://www.20minutos.es/tecnologia/ciberseguridad/tus-datos-en-constante-peligro-cada-dia-se-producen-mas-de-cuatro-brechas-de-seguridad-en-espana-4948062/

TRADING ECONOMICS. (2023). *Spain Unemployment Rate - 2023 Data - 2024 Forecast - 1976-2022 Historical - Calendar*. https://tradingeconomics.com/spain/unemployment-rate

Voigt, P., & Von Dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). In *Springer eBooks*. https://doi.org/10.1007/978-3-319-57959-7

Appendices

List of Abbreviations

AEDP	Agencia Española de Protección de Datos [Spanish Data Protection Agency]
CCN	Centro Criptológico Nacional [National Cryptology Centre of Spain]
CSR	Corporate Social Responsibility
ENISA	European Union Agency for Cybersecurity
EU	European Union
EU-SEC	European Security Certification Framework
FACUA	Federación de Asociaciones de Consumidores y Usuarios de Andalucía [Federation of Consumer and User Associations of Andalusia]
GDPR	General Data Protection Regulation
INCIBE	Insitituo Nacional de Ciberseguridad [National Institute of Cybersecurity]
IS	Information System
LOPD	Ley Orgánica de Protección de Datos Organic Law on Data Protection
LOPDGDD	Ley Orgánica de Protección de Datos [Organic Law on Data Protection and Digital Rights Guarantee]
MNC	Multinational Corporation
PII	Personally Identifiable Information