THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

THE EFFECT OF DATA BREACH: LOSS OF BRAND REPUTATION AND FINANCIAL PENALTIES

Master's Thesis

ŞEREF CAN ÖZKAYA

ISTANBUL, 2020

THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

THE INSTITUTE OF SOCIAL SCIENCES
BUSINESS ADMINISTRATION MASTER PROGRAM

THE EFFECT OF DATA BREACH: LOSS OF BRAND REPUTATION AND FINANCIAL PENALTIES

Master's Thesis

ŞEREF CAN ÖZKAYA

Supervisor: Prof. Dr. Figen Yıldırım

ISTANBUL, 2020

THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

THE INSTITUTE OF SOCIAL SCIENCES
BUSINESS ADMINISTRATION MASTER PROGRAM

Name of the thesis: The Effect of Data Breach: Loss of Brand Reputation and Financial Penalties
Name/Last Name of the Student: Seref Can ÖZKAYA
Date of the Defense of Thesis: 11.03.2020

The thesis has been approved by the Graduate School of Social Sciences.

Dean of Graduate School
Signature

I certify that this thesis meets all the requirements as a thesis for the degree of Master of Business Administration.

Program Coordinator
Signature

This is to certify that we have read this thesis and we find it fully adequate in scope, quality and content, as a thesis for the degree of Master of Business Administration.

Examining Committee Members	Signature
Thesis Supervisor Prof. Dr. Figen YILDIRIM	
Member Prof. Dr. Özgür Çengel	
Member Dr. Öğr. Üyesi Gülberk Salman	

ACKNOWLEDGEMENT

I wish to express my deepest gratitude to my supervisor Figen Yıldırım for her guidance, advice, criticism, encouragements and insight throughout the research.

I would also like to thank to my parents for their great support throughout their life. Without their understanding and continuous support, I could have never been able to aspire for this level of education and complete this study

June, 2020 **Şeref Can Özkaya**

ABSTRACT

THE EFFECTS OF DATA BREACH:
LOSS OF BRAND REPUTATION AND FINANCIAL PENALTIES

Özkaya, Şeref Can

Business Administration Master Program

Thesis Supervisor: Prof. Dr. Figen Yıldırım

June 2020, 63 pages

Social life and professional life becomes digital since information technologies have developed rapidly and become a constant part of life. As a part of this digitalization process, individuals and organizations are linked to the idea of being online and bringing on digital channels their professional and social needs. As digital channels became global markets, channels arose that are unique to the fields of work of almost every sector (social media, finance, communication, etc.). There are social, political and economic benefits to any operation in this globally competitive market. Increased digital activity with technology addiction and an increase in the volume of data collected in the virtual world have posed global concerns related to data leakage and the protection of personal data. It is understood that the national and foreign sanctions in this area are severe, and it is observed that those sanctions affect the individuals and institutions ' respect and financial values. The consequences of data breaches, such as loss of brand credibility, and financial penalties are discussed in this report.

Keywords: Data Breach, Loss of Brand Reputation, Financial Penalties, Personal Data.

ÖZET

VERİ İHLALİNİN ETKİLERİ: MARKA İTİBARININ KAYBI VE MALİ YAPTIRIMLAR

Özkaya, Şeref Can

İşletme Yüksek Lisans Programı

Danışman: Prof. Dr. Figen Yıldırım

Haziran 2020, 63 sayfa

Bilgi teknolojilerinin hızlı gelişimi ve hayatın önemli bir parçası haline gelmesi nedeniyle sosyal ve profesyonel yaşam dijitalleşmektedir. Dijitalleşme sürecinin bir sonucu olarak, bireyler ve tüzel kişiler çevrimiçi olma kavramına bağlanmakta ve profesyonel ve sosyal ihtiyaçlarını dijital platformlara taşımaktadır. Dijital platformların küresel piyasa haline gelmesiyle birlikte, birçok sektörde sosyal medya, finans, iletişim gibi çalışma alanlarına özgü platformlar ortaya çıkmıştır. Küresel olarak etkin olan bu piyasada gerçekleştirilen her bir faaliyetin siyasi ve ekonomik faydaları bulunmaktadır. Teknoloji bağımlılığı ile birlikte artan dijital faaliyetler ve sanal âlemde depolanan verinin artan hacmi veri ihlalleri ile kişisel veri mahremiyeti konularını gündeme getirmiştir. Veri ihlali alanındaki ulusal ve uluslararası yaptırımların oldukça ağır olduğu bilinmekte, söz konusu yaptırımların kişilerin ve kurumların finansal değerlerini etkilediği görülmektedir. Bu çalışmada, veri ihlallerinin marka itibarının kaybı ve mali yaptırımlar gibi etkileri incelenmiştir.

Anahtar Kelimeler: Veri İhlali, Marka İtibar Kaybı, Mali Yaptırımlar, Kişisel Veri.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AMCA	: American Medical Collection Agency
CASB	: Cloud Access Security Broker
DBA	: Data Breach Announcement
DLP	: Data Loss Prevention
EDR	: Endpoint Detection and Response
GDPR	: General Data Protection Regulation
ICO	: Information Commissioner's Office
IP	: Intellectual Property
IS	: Information Systems
IT	: Information Technology
p.	: Page
PII	: Personally Identifying Information
SMEs	: Small and Medium Sized Enterprises

1.INTRODUCTION

1.1 STATEMENT OF THE PROBLEM

In recent years cybercrimes related to data breaches have become common and cases of data breach have been reported by more and more organizations ranging from health and retail to the financial sector. (Abelson and Goldstein 2015). In 2017, one of the three big US credit reporting agencies, Equifax reported a data breach that could potentially impact 143 million consumers ' personal details (Janofsky 2017).

The economic consequences on corporate companies of data breach cases may be surprising. Cyber security problems could cause companies to lose $445 billion and 200,000 jobs annually, according to projections from the Center for Strategic and International Studies (Intel Security-McAfee, 2014). In 2014, the Chief Executive Officer of Target Corporation resigned after a major data breach by the company during the Thanksgiving holiday season 2013, when the personal details of about 100 million consumers was stolen (Trefis Team 2014). Verizon's purchase of Yahoo was delayed, and the sale price eventually decreased due to Yahoo's violation fine (Athavaley and Shepardson 2017).

In the context of a customer's view, data breach involving personal and financial details may be viewed as a violation of the social contract and a service violation that adversely affects the customer-firm relationship or brand credibility (Janakiraman et al 2018).

1.2 PURPOSE OF THE STUDY

Organizations lose when they expose themselves to a data breach in several respects. The financial factors are therefore the most concerning. There are multiple costs associated with a data breach such as compensating impacted consumers, setting up breach mitigation programs, for instance helpdesks for affected customers and supplementary

credit checks; investigating the event that may include hiring a third party, reducing share prices, and loss of brand value.

The expense, on the other hand, is linked to the effect of regulatory sanctions. The forces controlled by the General Data Protection Regulation (GDPR) have made this potentially the largest financial expense of a data breach by far. The GDPR grants supervisory authorities–which is the Information Commissioner's Office (ICO) in the UK–the power to fine non-compliant organizations € 20 million (about £ 17.5 million) or 4 per cent of global annual revenue.

The violated company has also to deal with the damage to its brand image after paying off fines. It can be difficult for the organization to recover the confidence of customers, particularly if the breach was widespread or triggered by major faults in protection. Unless a catastrophic breach happens, the loss of trust will subside over time as people forget the incident and rivals suffer a similar fate (Graham 2019).

The aim of this study is to investigate the impacts of data breach such as loss of brand reputation and imposing to pay financial penalties.

1.3 RESEARCH QUESTIONS

In this study; research questions will be as follows:

a. How do companies discover data leakage?
b. How does data breach effect brand reputation?
c. How do companies improve their system for cyber-attacks?
d. How will data breach shape on trust, penalty and brand reputation in the future?

1.4 SIGNIFICANCE OF THE STUDY

Companies and individuals are using technical advances to enhance lives, sustain business processes and promote interaction between person and machine. The incorporation of technology in business fields presents new opportunities as well as problems such as data privacy and security. Mellado and Rosado (2012) said data protection is a growing issue affecting all sectors of society. Considering the growing reliance of organizations on information systems, data has become a vital business asset.

Google and McAfee predicted about two thousand cyber-attacks every day across the planet, bringing back around £ 300bn a year on the global economy. This situation requires managers of Information Technology (IT) to possess the skills to efficiently protect organizational data. The findings of this study will help IT managers identify employee skills to avoid data breaches. However, the results in this study may enable IT managers to avoid and resolve the gaps in business practice regarding proactive data protection measures and the reduction of data breach risk.

Research shows that breaches have a substantial effect on operational and financial results (Chai et al., 2011), and that publicly traded companies with data breaches also had a detrimental impact on brand credibility. (Zafar et al. 2012). This study might help IT managers to determine best practices to mitigate breaches.

Considering the performance effect of security-related accidents on U.S. companies is about $67.2 billion a year (Gordon et al. 2011), the results of this study could pave the way for IT managers to reduce the cost of protecting company sustainability confidential data. In addition, because 81 percent of all data breach incidents stem from customer data theft (Lai et al. 2012), this study can allow companies with the best protection strategies and policy management tools to protect consumers from data breach costs.

1.5 DEFINITIONS

Data security: "Security of information in repose and transit from unauthorized entry, disclosure and/or intentional or unintentional alteration" (Saidani et al. 2013).

Information security: *"Safeguarding and protecting information and IT systems against vulnerabilities and threats resulting from unauthorized access, alteration or destruction to protect the availability, integrity and confidentiality of a system"* (Fuchs et al. 2011).

Data breach: "The abuse of information, unauthorized access to information and/or IT systems or the failure and theft of such systems as laptops and mobile devices resulting in a breach" (Gordon et al. 2011).

2. LITERATURE REVIEW

In the literature review, data breach cases and researches regarding the scope of data breach are reviewed. Furthermore, the economic impact and the loss of brand reputation of companies due to data leakage is examined.

2.1 SCOPE OF DATA BREACH

Cyber security has occurred a main issue in recent years following many wide-range data breaches. Cyber-attacks were carried out for the purpose of financial gain, but attacks today are largely motivated by state or commercial surveillance. The evolving nature of these attacks has generated tremendous concern on the part of corporate decision-makers and politicians. According to Makridisa and Dea (2018), one of the most troubling components in this environment is the result of many device vulnerabilities and their magnitudes are not established. This situation makes it difficult for specialists and regulators to bind the range of probable outcomes.

Personally Identifying Information (PII) or personal data is defined as "any information relating to an identified or identifiable natural person". Samples of personal data provide important details such as nationality, gender, political thoughts, and health data. Infringement of data stems from unauthorized access to data, leakage of data, data theft and cyber-attacks. Many forms of stealing data are often known to be the manipulation of weaknesses of information technologies. Social engineering attacks are also one of the most significant way of attacks.

An electronically mediated service failure that occurs when sensitive financial, personal, or consumer data exposed to or accessed by external parties is called as data breach. This disclosure may be carried out deliberately, for instance through a hacking incident or due to the actions of a disgruntled employee, or unintentionally, for example a missing laptop and concern for some element of the activities or relationships of an organization, such as clients, partners and internal systems (Johnston et al. 2016; Kwon and Johnson 2015; Lowry et al. 2015 ;Hsu et al. 2015; Johnson 2008).

Because data is usually collected by a firm as it fulfills its customer service offerings, at least some of the data retained by an organization that involve customers of the organization itself. Some researchers used different terminology to describe data breaches, such as breaches of security (Çavusoğlu et al. 2004), breaches of information (Malhotra and Malhotra 2011), and breaches of privacy (Wong et al. 2011). After Culnan and Williams (2009) and others, the word "data breach" has been widely used because it does not understand the quality of the violated data until after the incident has been recognized and evaluated because the company may know that their data has been infringed (Tomaszewski 2006). A data breach can therefore involve breaches of protection, information, and privacy.

Furthermore, external physical attacks towards companies and inside data theft actually occur in contemporary business life. The attackers sometimes share the results of their attacks with the target company so as to earn money, or upload the results in platforms such as social media. Investigations about attacks have demonstrated that cyber attackers cannot be detected for a long time in the systems. In other words, most of companies cannot catch these attacks with their own capabilities (Özkaya 2019).

A new research was conducted for revealing the data breach facts and responses of commercial organizations (1,000 to 5,000 employees) and enterprise organizations (more than 5,000 employees) in Australia, Canada, France, Germany, India, Singapore, the UK, and the US. 700 information technology and security professionals who experienced at least one serious data breach in their careers were interviewed in December 2018. The data breach was very severe in nearly three quarters of those cases, requiring public notification or having a significant financial impact on the company. The professionals were asked about breach and exfiltration details, insider or external threats, and the people, processes, and technologies that was helpful for preventing these breaches. Consistent with previous studies, leakage of PII is the number one concern (PCQUEST 2019, p. 37).

There are various actors who conduct data breaches. Hackers, malware authors, nation states, and activists are samples of external actors. External actors and threats are influential in increasing percentage of data stealing, rising from 57% of breaches in 2015 to 61% in 2018. The most important change over the past three years in this group was an increase in malware-oriented stealing, rising from 23% in 2015 to 29% in 2018. Employees, contractors and other parties with inside access are samples of internal actors. This group has deliberate as well as accidental exfiltration. Employee-oriented attacks account for almost 60 percent of employee accidents. The most notable changes in this category are a four-point rise in accidental breaches (27% to 31%), and a six-point drop in deliberate breaches (30% to 24%).

61 percent of IT professionals record at least one incident of data breach across their careers, according to this study. This figure shows that companies tend to be impacted by data theft. The incidence of these incidents tends to increase, because 61% registered a breach in their current company but only 48% in their former company (PCQUEST 2019, p. 37).

According to the research, stringency of breaches is also increasing. From 2015 to 2018, the percentage of organizations experiencing a serious breach requiring public disclosure or having a negative financial effect on the company has risen from 68% to 73%. In the course of their working lives, interviewees have experienced almost six serious violations each. Moreover, it is revealed that IT or security departments have entangled in just over half of all leakage events, and more than 60% of those take place in Asia-Pacific organizations.

Business operations and production departments are second at 29%, possibly because of their extensive interactions with a wide range of external companies. Sales employees are in third degree, at 26%. Least likely departments to induce leaks are legal (6%), finance (12%) and human resources (15%). Those rates show that these groups are distinguishing the vulnerability of data they use.

Another issue in the scope of data breach is the types of data that insiders can take. According to the research, PII and Intellectual Property (IP) are tied as the data groups with the highest potential effect to 43% of interviewees. Especially, PII is of greater concern in Europe (49%), because of the enforcement of the GDPR. However, in Asia-Pacific countries, IP theft is of greater concern (51%) than PII.

Thanks to significant improvements in fraud detection and prevention methods for credit cards, theft of payment card information has declined to 30%. As to IP theft, direct competitors are considered as the first source of concern (23%), followed by internal employees (19%). This result may be a combined threat depending on job changes and movement of people between companies within the same industry. Generally, companies consider structured data as a higher priority for protection (45%) than unstructured data (39%). According to the survey, structured data is defined as databases related with information such as payment card data and health records. Unstructured data is described as documents related with IP such as formulas, designs, and proprietary knowledge.

Confidential data is being stolen by a wide range of electronic or physical vectors. In general, database leaks and network traffic are the most known vectors. On the other hand, corporate email comes first in North America, while USB drives are the first exfiltration vector in European and Asia-Pacific region. As to the insider threats, email leakage is the most important security hole, followed by risky users and USB drives. All of these could be significantly decreased with additional education on corporate policies and suitable online behavior.

Cloud applications and infrastructure are widely applied; however they do not seem to result in any more data theft than traditional networks and data centers. Around two-thirds (63%) of the breaches experienced by the interviewees happened on traditional networks, and one-third were on cloud infrastructure. Even with the increase in cloud usage from 2015 to 2018, this ratio has remained the same, implying the potentially effective security available for or from cloud providers. However, this does not prevent people from concerning about the cloud. When asked if they had big concerns about Infrastructure-as-a-Service cloud providers, interviewees mentioned Amazon Web Services (AWS) (22%),

Google Cloud (21%), Oracle Cloud (18%), and Microsoft Azure (16%). When presented with a list of cloud applications and services and asked which ones they are most concerned about, respondents listed Microsoft OneDrive as number one, followed by Cisco WebEx and Salesforce (PCQUEST 2019, pp. 38-40).

By means of keeping up with evolving threats, security technology is the first prior tool for about half of organizations worldwide (49%). Enhancing the skills of their people (29%), and changes to business processes (22%) are the others. In 2018, more than half of all organizations bought additional security products, focused on employee security training, and increased the capabilities of their security operations center. Some of organizations hired more security staff, while some preferred to work with a man-aged security service provider. Data Loss Prevention (DLP) and Endpoint Detection and Response (EDR), and Cloud Access Security Broker (CASB) are the classic security technology tools applied to combat data leakage. However, even if these tools are applied in an organization, they are used in a default configuration or in monitor-only mode because of lack of experienced resources to properly configure the tools, and belief that automatically blocking suspicious activities leads to disruption to business activities or production processes.

Although applying and configuring those tools effectively, the main technology-related measure against reducing the risk of data leakage is to integrate various security technologies. Technology integration and employee education are considered to be the top two steps to decrease the risk of data exfiltration. Thus, full deployment and active configuration of basic security technology tools such as CASB, DLP, and EDR is an important step that would be likely to prevent as much as 80% of breaches experienced by interviewees (PCQUEST 2019, p. 41).

2.2 SAMPLES OF DATA BREACH INCIDENTS

A lot of major data leakage incidents occurred in the world. For instance Yahoo's 3 billion dollar account stolen in 2013 is one of those incidents. Another incident is called as "The Cambridge Analytica" scandal. It was found that Cambridge Analytica had unauthorized

access to nearly 87 million people's publicly available data on Facebook, "including gender, location, political views, religious beliefs, private correspondence, web sites and profiles they liked, thus influencing and changing user preferences".

In fact, it was announced in 2019 that Facebook data such as user ratings, likes, user names and more than 540 million Facebook accounts, as well as Amazon's cloud service, were open to the public. Taking into account the effects of Facebook leaks, the number of Facebook users fell in the US by 15 million annually, and in Europe by 3 million. Also Facebook was sentenced to $5 billion in the US and $645,000 in the UK because of the Cambridge Analytica scandal (Özkaya 2019).

Another wide ranging data leakage incident was the Equifax leakage in 2017. The US credit rating agency, Equifax was attacked and its data was leaked. It was found that the reason of the weakness was related to the patch. On the other hand, although revealing the reason of the leakage, it was found that Equifax had not installed any updates for the patch. As a result of this shortcoming, 145 million people's financial data and social identity numbers were seized by cyber-attackers (Özkaya 2019).

This data leak incident was hidden from the public for a while. Equifax's leaked data was shared with the public five months after the leak occurred. As a result of this incident, senior executives had sold their shares, and the CEO resigned. Equifax which was the victim of one of the largest cyber-attacks in US, was sentenced to $700 million for the infiltration of private information of approximately 150 million customers. All these results have shown that the brand reputation of Equifax was damaged.

In 2019, the American Medical Collection Agency (AMCA) announced its clients (Quest Diagnostics, LabCorp, and OPKO Health, which serve 11.9 million, 7.7 million, and 400,000 patients respectively) of a data breach that might expose personal and billing data of its clients. Due to Securities and Exchange Commission filings from Quest Diagnostics, LabCorp, and OPKO Health, an unauthorized user accessed to AMCA's system between August 1, 2018, and March 30, 2019, exposing information which AMCA had collected from various entities. Approximately 20 million patients was

affected, and this situation indicated that the second largest security breach in the healthcare industry was seen (Briefings on HIPAA 2019, p. 5).

Unintentionally or unintentionally exposing vast volumes of confidential organizational data to third parties is considered a "large-scale data breach." This kind of data breach can be detrimental to consumer expectations of a company's customers. Studies show that more than five significant incidents of data breach are recorded each day (Goode et al 2017, p. 704). In the US, as a big problem for firms, the average cost of a data breach reached $6.53 million in 2015. The Sony PlayStation Network was breached in 2011, and this was the largest data breach ever reported at the time (Reynolds 2011), when more than 77 million user accounts ' personal and financial information was exposed (Richmond and Williams 2011). The direct costs of the breach reached $171 million, and Sony's indirect costs were expected to exceed $1 billion arising from brand reputation loss due to adverse exposure to the consumer (Sherr and Wingfield 2011). In fact, other international companies have suffered large-scale data breaches aside from the Sony data breach. For example, a leading Fortune 500 technology company, Adobe, and a major US-based retailer, Target reported that more than 170 million user accounts ' personal and financial data have been compromised. The related costs for both companies were contrasted with those that Sony faced (Williams 2013).

On 22 October 2015, TalkTalk reported a cyber-security leak. It was the latest in a long line of similar events that affected companies including Sony, Ashley Madison, Barclays, Carphone Warehouse and others. After the cyber-attack the credibility of Talk Talk was badly hurt. Talk Talk faced intense criticism for its tactics for handling conflicts and reputations. Other data controllers have been recommended to ensure that they implement rigorous data protection contingencies, prepare their staff for data breach awareness, develop data breach strategies and provide a reliable and efficient communication policy at their disposal when data goes wrong (Alva 2015).

2.3 EFFECTS OF DATA BREACHES

Information technology has increased economic growth across industries, companies, and individuals. As information technology has paved the way for promoting global integration, greater firm-level innovation, increased product efficiency, and lower costs of doing routine businesses, cyber security has drawn back. Many vulnerabilities within infrastructure, logical, and software layers constitute risks for companies and individuals who use and rely on these technologies. On the other hand, there is few empirical research content for grounding sensible cyber security decision-making in the public and private sectors. It is true that there is some evidence of a negative effect of breaches on firm outc omes, however researches have produced uncertain outcomes.

One of the reason for this uncertainty stems from the nature of the heavy-tailed distribution of data breaches such as number of records affected. Other reason is that there is no available related financial and cyber security outcome data for conducting causal result. Nevertheless, many event studies have executed, predicting the influence of data breaches on stock prices (Makridisa and Dea 2018, p. 62). A literature analysis of 45 studies, for example, showed that approximately one quarter of the studies did not find a statistically significant association between instances of breach and stock prices (Spanos 2016).

According to Makridisa and Dea (2018), although the increasing significance of cyber security, little is known about its effects on firm-level investment and other economic results. Part of the challenge stems from the fact that there is no ready-to-use database including both financial firm-level outcomes and cyber security information to predict statistical models or arrange computational models.

2.3.1 Loss of Brand Reputation

A fundamental challenge for breached companies is that impacted consumers always terminate the customer-to-organization relationship, and when a data breach happens, they do not purchase goods or services again. For example, the Ponemon Institute (2013)

reported that more than 40 per cent of customers warned of a data breach were considered to cease their relationship with the organization because of unfulfilled expectations of service quality. Companies regularly inform affected consumers of the breach and provide an apology, perform a breach report, explain what data has been compromised, notify consumer security initiatives and provide a concise overview of what the company is doing to deter future breaches. These announcements are characteristic of recovery initiatives and are also compulsory in some countries (HHS 2013).

In fact, organizations are expected to be eligible to collect, use and protect data from the stakeholders safely. The failure of an organization to prevent these data breaches the interests of the stakeholders (Burgoon 1993). Negative infringements can produce unhealthy emotions such as deception, anxiety, resentment, and mistrust, and have adverse behavioral consequences (Morrison and Robinson 1997). Therefore, investors are required to view a violation as a violation of their standards of good firm conduct and to sell stocks of the violated company. The foreseen costly litigation and adverse public image resulting from the violation of the data could result in further negative reaction from the investors and greater financial losses for the violated company. In the event of a company contracting a data breach, the company is likely to handle different response approaches to mitigate the damage. Some research have revealed that if information on a breach is released on the announcement time, investors typically respond negatively to breach disclosure (Campell et al 2003; Acquisti et al 2006; Cavusoglu et al 2004; Gatzlaff and McCullough 2010; Goel and Shawky 2009).

Companies affected by data breaches are subject to significant financial costs such as litigation costs and legal responsibilities, loss of brand image, consumer loyalty and market share and sales (Sen and Borle 2015). Researches have tried to materialize the financial cost related with data breaches and have generally revealed the negative effects of breaches on shareholder wealth (Campell et al 2003; Acquisti et al 2006; Cavusoglu et al 2004). These results have provoked Information Systems (IS) researchers for developing effective preventive controls, basically around planning and decreasing of security risks (Kwon and Johnson, 2013; Liang et al, 2016). However, it is found that complete security risk prevention is not feasible (Choi et al 2016; Wang et al 2013).

Therefore, implementing effective recovery and damage control strategies in order to protect firm's brand reputation following a breach have reached at an all-time high (Gwebu et al 2018, p. 684).

Data breaches, compared to other corporate problems, pose special obstacles for the IS functioning of an organization. Managing a data breach involves IS experience, which includes detecting control and monitoring vulnerabilities, performing forensic reviews, restoring service and protection, avoiding potential repeated attacks, and determining when and when to interact with senior management, business functions, legal counsel and the role of public relations. When an infringement exposes the flaw in the firm's structure and control, an appropriate forensic examination is also required to determine the key reason for the infringement and minimize the likelihood of repeated incidents (PWC 2011; Deloitte).

Researchers have begun to identify processes in recent IS studies which can help businesses recover efficiently from data breaches. A study found that the market responds less negatively to announcements by companies that reported action-oriented protection risk factors before the infringement (Wang et al 2013). Another research indicates that recovery measures directed at the distributive, procedural and interactional conceptions of justice of customers collectively affect perceived violations and a sense of injustice, which in turn determine post-breach behaviors of customers like word of mouth and the probability of switching (Choi et al 2016). Another study suggests that apology and denial are successful in restoring confidence after breach, especially where the breach can be attributed to factors outside the firm (Bansal and Zahedi 2015). Gwebu et al (2018) explores the risk of corporate credibility and a variety of mitigation techniques as tools for damage management to protect the brand image of an infringing company.

Various breaches of sensitive corporate data have become a threat for a lot of companies in different industries. Critical incidents constitute vulnerability for companies' reputation. In other words, businesses that are subjected to data breach are influenced in different ways by the negative views of customers. Furthermore, the severity of social

media data breach scandals will increase negative impacts on related companies (Confente et al. 2019).

The results of data breaches have shown that, in comparison with the large enterprises, Small and Medium Sized Enterprises (SMEs) are more affected by cyber-attacks. When a SME's data is leaked, competitive companies can take advantage of those data in order to transfer its customers. This situation will cause economic damage and may even result with the bankruptcy of these companies.

As it is understood from samples above, companies confronted with data leakage will exposure to financial losses within case of stock value decrease, loss of incomes, drop in the number of customers, redound in the competition, exposing to financial penalties and expenditure to regain their losses. After disclosure of data leakage, companies' shares lose 5% of their value depending on sector. These losses also vary with the department where the leakage happens. For instance, in case of a data leak in the financial department would likely suffer more than any other department. *"The impact of leaks on brand reputation generally includes the loss of customer trust and loyalty, the decline in the customer-brand relationship, and the emergence of negative media coverage"* (Özkaya 2019).

Özkaya (2019) states that a lot of detailed and unnecessary customer data stored in the company's server is the most important factor that causes data leak. According to him, some companies do not handle and encrypt the information and continue to keep most of those data. That's why, in case of a cyber-attack, many of these data are easily captured by attackers. At this point, the most important thing is to keep the necessary information only and do not hold the useless data.

Özkaya (2019) asserts that data breaches can be eliminated by timely audits for the IT infrastructure. For instance, in the Equifax leak, if the expansion was applied in right time, then the security bug could be stopped until exploitation. So, IT audits should be applied periodically for companies. Also only authorized employees should access to company data. Companies should be obliged to *"allocate resources for security, training, system*

audits and raising the awareness of employees against cyber-attack. Companies should prepare action plans against data leak incidents."

A work performed by Confente et al. (2019) explored the impact of data infrengement on facets of client credibility. This study showed that latent Dirichlet allocation analysis on user-generated content in social media for a sample from 35 firms in nine different industries were exposed to an incident of data leak between the years 2013 and 2016. Incidents divided into three main categories such as data breaches "intentional and internal," "unintentional and internal," and "intentional and external." The research aimed to find out how reputational dynamics changed after the crucial events and to establish the distinctions between forms of data leak.

Results showed that most of the reputational factors tend to become an important after critical incidents. Consumers are now looking at "customer focus" and "corporate efficiency" aspects before critical events, while customers find the "perceived consistency" of a company's product after all three kinds of data breaches. Another fundamental element of reputation, is the "firm as an employer", especially in sense of being without training expenditure in this incidents. According to Confente et al. (2019), findings of the research provided basic insights for academicians and operators to reveal wide-range data breaches impacts and reputational defects after these events.

According to Makridisa and Dea (2018), while there some researches which analyze the tendency of share prices after a cyber-security breach at a company, these researches created contradictory outcomes because of two reasons. Firstly, the sort of data that may be leaked in a breach is not homogenous. For instance, like in the case of Equifax, the release of private consumer records is likely to weaken consumer trust (Berr 2017). However, malware attacks for manufacturing companies is more likely to decrease cash flow rather than consumer trust because of the character of their products and services. Secondly, while many violations occur without firm knowledge, those firms which detect cases might not have a motivation to state the whole dimensions of a breach, likewise in the case of Yahoo (Collins 2017).

Dolezel and McLeod (2019) looked for the connection between data breach features and the number of individuals affected by these breaches. The data were obtained from the Department of Health and Human Services ' infringement monitoring database. The results showed that the form of hacking / IT incident breach and network server breach position were the most significant predictors of the number of people affected; however, when combined, they were not predictive.

In addition, the location of the network server and the form of unauthorized access / disclosure infringement were predictive when combined. Additional analysis of variance found that the company type covered and the presence of business associates were major predictors, while the geographic area of an infringement case was unimportant.

The results of this study showed many associations between the characteristics of healthcare breaches and the number of individuals affected, indicating that more individuals are personally affected by hacking / IT accidents and network server breaches, and that violation of network server location and form of unauthorized access / disclosure violation were predictive in combination.

Janakiraman et al (2018) assessed the effect of a Data Breach Alert (DBA) from a multichannel retailer on customer behavior. They used the retailer's natural experiment and individual customer transaction data to perform a detailed and systematic empirical study of the impact of a DBA on consumer purchasing and the nature of channel migration.

The authors compared the difference in consumer behavior before and after the DBA between a treatment group (customers whose information is infringed) and a control group (customers whose information is not infringed) using the distinction modeling method to explain the effects. They found that following the data breach, the consumers of the company moved from the breach to the unbreached networks of the retailer, resulting in a substantial drop in consumer spending. The results also showed that consumers with higher retailer patronage were more forgiving as the negative effects of the DBA were lower for clients with higher patronage.

The 2014 global reputation risk survey conducted by Deloitte found that physical or cyber protection was one of the top three reputational risk factors among the executives it interviewed. The most prevalent approach to understanding reputation factors is to explore what various stakeholders think and feel about the topic, and to what degree they are concerned about a specific problem cloud, or come to define their own. For example, data breaches may cause some of the most impactful downturns in an organization's sentiment.

The impacts of a data breach on reputation is best analyzed over stakeholders such as media, investors, politicians, regulators, and customers since an organization's reputation is what other people think and feel about that entity. As to the TalkTalk data breach incident, it can be observed that an organization's reputation is highly affected by data breaches. Taking into consideration the media stakeholder, Reuters, The Times and the Financial Times criticized TalkTalk for threatening customer finances, with sources calling the firm as "careless". After a while, national media coverage of the Carphone Warehouse cyber-attack criticized TalkTalk for not helping customers use safer passwords. For investors, TalkTalk shares fell 11% after the October cyber-attack. Politicians, such as Labor MP Keith Vaz told that he would be writing to Talk Talk chairman to ask for a "timeline as to what they did" when the attack was discovered. MPs were reported to launch an enquiry into the cyber-attack on TalkTalk.

For regulators, Information Commissioner was reported to question whether TalkTalk acted fast enough in telling customers about the attack. Former Labor Minister was reported to say that "companies have got to improve their systems and the attack should prompt a debate about whether further regulation is needed because this is probably the biggest threat to our economy". The customers complained about waiting to be compensated by TalkTalk. TalkTalk received negativity on social media for being unable to specify the exact number of customers affected by the cyber-attack. Customers' bank accounts were reported to be targeted by fraudsters after the attack, increasing negativity within the customer stakeholder group. As a result, it can be said that the magnitude of

the reputational risk depends on the amount of stakeholders involved; the longer the risk is involved, the more harmful it is. (Alva 2015).

2.3.2 Financial Penalties

In case of a data breach, companies are fined with financial penalties. GDPR in international field and Data Protection Law in Turkey will be examined within the context of financial penalties.

2.3.2.1 GDPR

As of May 2018, with the entry into application of the GDPR, there is one set of data protection regulations for all companies operating in the EU, wherever they are established. Those companies in the EU are obliged to enforce the data protection regulations in the GDPR, otherwise due to Article 83 of the GDPR they are sentenced with various administrative fines which highly affect their brand reputation. For the first half of 2019, top 5 GDPR fines will be examined by taking into account the scope of fine amount, the extent of impact on the rights of the data subjects, the quality of the data processed and the number of subjects exposed.

The Danish Data Protection Agency has announced the taxi company's first GDPR fine in Denmark–Taxa 4x335. The fine was levied at about € 160,000 or 2.8 per cent of the annual revenue of the company. The fine was imposed as the taxi company did not comply with the GDPR data minimization law, the aim and the restriction on storage and held their customers' personal information longer than required. The data concerned about 9 million people. Despite of their data protection strategy, after two years Taxa removed personal data but kept the telephone numbers of customers for another three years. Their argument was that the telephone numbers in their IT database were an essential part of the information and cannot be removed at the same time as other records.

The Danish Data Protection Agency with the sophistication of Taxa's IT program for such a severe violation, could not support this claim. In addition, attempts at data anonymisation by Taxa failed. Anonymisation was believed to make it difficult for the unauthorized workers to be able to link individuals with their personal data, which was not the case. The Agency decided to announce that organizational IT shortcomings would not constitute a valid reason for any violation of GDPR (Data Privacy Manager, 2019).

The Italian data protection regulator Garante has issued yet another GDPR fine. Garante specifies the lack of privacy and security measures which resulted in a data breach on the Rousseau platform running a website for the Movimento 5 Stelle Italian political party. Garante claimed a violation of Article 32 of the GDPR, and levied a fine of € 50,000. The fine was imposed because few political party websites were run via the data processor– the Rousseau platform and the platform experienced a data breach in 2017 that made Italian data protection authority turn its head in that direction. They established that Rousseau needs to update security measures, notify privacy information and show transparency in the way it processes data (Data Privacy Manager 2019).

The Portuguese supervisory authority has fined a hospital in Centro Hospitalar Barreiro Montijo for GDPR violation. The reason for the fine was due to the non-medical staff using health workers profiles to log in to the hospital computer which exposed all confidential patient data to unauthorized staff. Medical data of all patients were added to the hospital's program. When it was on the list, the staff at the hospital could access each individual medical card, even if they had little to do with the care of the patient and irrespective of their position at the medical. The specific thing they wanted was the hospital supplying username and password. The hospital management has been warned before and has done little to correct their incompetence. Two fines totaling 400,000 euros were released. The first fine was € 300,000 imposed for the failure to limit access to patient data and violation of confidentiality. The second fine was €100,000 because of failing to *"ensure the confidentiality, integrity, availability and permanent resilience of treatment systems and services"* (Data Privacy Manager 2019).

The Polish Data Protection Agency has imposed a first fine of € 220,000 to Bisnode–the provider of digital business, marketing and credit information, for violation of the rights of data subjects under Article 14 of the GDPR. Bisnode did not fulfill its obligations to inform, via personalized notice, all data subjects whose data they were processing. Around 700,000 people were announced by the organization but not all. The personal information collected included names, surnames, contact details and more than 7 million Polish identification numbers (PESEL number). The company published the notice on its business website, but Bisnode clarified that the notification was in compliance with Article 14(5)(b) of the GDPR, which specified that the duty to provide information was not appropriate if it required excessive effort. Their line of defense was that performing their duty would trigger unreasonably high costs in excess of € 7 million, which would slaughter the entire action's intent. On the other hand, it was not judged the same way by the Polish Department. They levied a fine of € 220,000 after taking into account many factors and gave Bisnode three months to inform about 6 million data subjects in order to rectify the situation (Data Privacy Manager 2019).

Owing to lack of clarity and informed consent, the French Data Protection Authority has fined Google with the highest financial penalty, so far € 50 million. Google was charged with not obtaining explicit consent from data subjects and avoiding clarity as to how data was obtained from data subjects and used for ad targeting. Several documents eradicated information, and consents were not specified for each particular purpose. Also an issue was pre-ticked opt-in, it was more like one box to tick them all which is a direct breach of Article 7 of GDPR. Taking into account the fines according to GDPR and Google's revenue, the €50 million fine was not considered as reasonable. However Google was not very happy with fine because this penalty damaged its brand reputation (Data Privacy Manager 2019).

2.3.2.2 Personal Data Protection Law in Turkey

Before Personal Data Protection Law Numbered 6698 entered into force, Turkish Penal Code has been applied for unlawful recording, acquiring and destroying of the personal data. Yet, still there is no penal regulation on unlawful personal data processing. On the

other hand, in addition to penalty of imprisonment, administrative fine is envisaged as a sanction of unlawful data processing for the first time. It is regulated in the Article 18 of the Law that real persons and private law legal entities, which act contrary to various liabilities stated by the Law can be subjected to different penalties. In this framework: "i. If the disclosure requirement is not fulfilled, from 5.000 TL to 100.000 TL, ii. If the obligations regarding data safety is not fulfilled, from 15.000 TL to 1.000.000 TL, iii. If the decisions given by the Committee are not implemented, from 25.000 TL to 1.000.000 TL, iv. If the notice and registration requirement of the Registry of Data Controller is not fulfilled, from 20.000 TL to 1.000.000 TL, shall be paid as an administrative fine" (Arslan and Ekşi 2016, p. 18).

3. METHODOLOGY

The aim of this research is to examine the consequences of breaches of data such as loss of brand reputation and to enforce financial sanctions. In this research there are 7 search questions which are answered with in-depth interview.

3.1 AIM OF RESEARCH

Organizations lose out in several respects when they expose themselves to a data breach. There are several costs associated with a data breach, such as compensating impacted users, setting up breach mitigation programs, such as helpdesks for affected customers and extra credit checks; investigating incidents that may include recruiting a third party, lowering share prices and loss of brand value. The aim of this study is to investigate the effects of data breaches such as loss of brand reputation, and to impose financial penalties.

3.2 RESEARCH QUESTIONS

In this research, the below questions are being researched:

a. What is data breach? What are the degrees of it?
b. When do the entities that have data breach take your consultancy?
c. Can you tell us about the different data leakage cases when you evaluate the sector in which the companies you serve?
d. How did your customer discover data leakage? How did this effect brand reputation? How did they improve their systems for cyber-attacks?
e. What is your opinion on the penalty process? How is the data breach penalty process applied in Turkey?
f. How to prevent data breaches in the future with different measures?
g. How does data breach shape on trust, penalty and brand reputation in the future?

The questions are answered in 4. Findings section.

3.3 RESEARCH DESIGN

3.3.1 Data Collection Methods

In the current research there were two experts who had been consulted. In order to record all the interviews, a recorder was used. Each of the interview lasted between 20 to 30 minutes and the whole data collection process lasted a week. Before each interview the researcher made appointment with each participant. The interviews were in Turkish, which is all the participants' mother tongue; because it was obvious that the participants would express themselves better in their mother tongue and they would feel more comfortable to talk about their opinions and feelings about the issue. After the one-to-one interview process was completed, sound recording was transcribed into word documents.

3.3.2 In-depth Interview description

To research this topic, in-depth interview methodology is practiced. Existing literature had been reviewed long before performing the interviews. The insight gained was used as a basis for open-ended questions to explain the related definition. Relevant theories or related themes were gathered, and for each of them, several questions were created. The questions have been divided into various groups to schedule fluent interviews.

Nevertheless, the order of questions in the interview guide was not strictly obeyed during the interviews. Because of the study's open and semi-structured nature, it seemed more prudent to let the interviewees address the questions in an unconstrained way, listing everything that came into their minds. Several interviewees posed subjects that were scheduled at the beginning for a later part of the interview so it seemed necessary to advance questions on that specific subject. Therefore, the interview guide was used much more as a tool during the interview to facilitate orientation and to ensure all aspects of the study were covered (Patton 2002, p. 342).

The interviewees were from various domains. Following developing the interview guide, a pre-test was performed to test the questions of the interview, the questionnaire and the

method of study. This study resulted in some slight improvements because they appeared overwhelming and too complex, such as an improvement of the questions about Berry's acculturation strategies. Accordingly, the interview guide structure and the question wording have been rethought and updated. In addition, questions concerning martial status, babies, and mother tongue were added to the short questionnaire that supported the interview guide. The questionnaire served to collect the interviewee's background details, such as name, education and occupation. First of all, this was in order not to have to ask certain questions during the interview but also to get to a fast summary of the background of the interview person.

3.3.3 Setting and Participants

The participants Cihan Vehbi Salihoğlu and Furkan Özer are cyber-security responsible with various experience and serving cyber security consultancy to their customers. An interview with each participant was held which was arranged in advance. The participants were carefully chosen in terms of expertise in the area of information security. The contents of the analysis and the interview were told to the participants.

3.3.4 Interviewer Roles

Interviewer, interviewee, and instrument are key criteria of a research interview. Various survey methodology studies have centered on the interviewer's positions within the standard of survey interests (Hanson and Marks 1958). Face to face interviewing becomes very dynamic by returning denials and helping in the process of questioning. Hence, interviewer-assisted surveys tend to have mistakes in the duties of interviewees. The principal duties of the interviewer are to send survey questions to the interviewee and to record responses correctly on the questionnaire, and both of these duties are troublesome.

Interviewer's role is not limited with reading questions to the interviewee, following instructions properly, or recording answers on survey instrument(s) correctly. In general, interviewer's functions are concerned with seeking a sample structure. Then, a table is created that provides information on the contact status between the interviewer and the

sample unit (Kulka and Weeks 1988). After that, cooperation with the sample unit is another important issue which can be established through interaction strategies at the doorstep (Morton-Williams 1993).

Another job for an interviewer is to pick qualified interviewees from the survey unit. Eligible individuals are selected by improved Kish method in 1949 or by birthday methods (Oldendick et al. 1988) to allow an objective selection of eligible individuals. Due to a survey parameters like age and gender in Kish process, everyone who is selectable for the target population is decided. After that, interviewees are chosen from all eligible individuals for the grid-based survey using random selection.

3.3.5 Data Analysis Methods

The data were then analyzed using the process of content analysis. Data thematic analysis was applied to the content analysis. The data analysis process was performed in the form of an in-depth interview, based on the questions. The participants analyzed the answers given to every question in detail and were systematically coded. When coding the answers to the questions relating to the conceptual context used in the literature review (Yıldırım and Şimşek 2013).

The data processing was carried out in conjunction with the method of data collection. After collecting all the data, all of the codes that were made earlier were re-examined. After this analysis of the results, codes were developed in parallel to the interview questions under seven categories of questions. The results of the current study relating to these seven themes were reported.

3.3.6 Reliability and Validity

Some approaches have been proposed in the field in order to ensure reliability and guarantee validity. One of the techniques that has been implemented in this analysis was expert examination. Two experts gave their opinions on it when structuring the data instrument.

3.3.7 Limitations

Limitation identifies potential weaknesses of the study. Because of the low number of eligible specialists in cyber security in Turkey, only two specialists could be chosen for interviews in this study.

3.3.8 Census and Sampling

The in-depth interviews have been performed with Mr. Cihan Vehbi Salihoğlu who is the Cyber Security and Privacy Services Leader at PWC and Mr. Furkan Özer (26) who is worked for STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. as a cyber-security specialist, he establishes his own cyber-security company. Salihoğlu and Özer are responsible for cyber security works in their companies and they serve cyber security consultancy to their customers for several years. To understand the effects of data breaches deeply, some questions have been asked to them.

4. INTERVIEW

In order to perform an interview it is important to understand in depth the characteristics of qualitative process. An interview involves asking people questions and taking answers from them to describe it all in clear means (Marvasti 2004). Interviews are performed orally and one - to-one, in general. (Gass and Selinker 2008). Mostly the questions are open-ended, and the answers to those questions give the researcher an idea of the views, attitudes, information, ideas and feelings of the participants (Patton 2002). Numerous types of interviews exist: single or multiple sessions, organized, unstructured, semi-structured or in depth (Dörnyei 2007). In this study an in-depth interview is used in which the questions are already formulated so that the researcher could direct and guide the process to examine the analysis as deeper during the interview.

4.1 THE DEFINITION OF DATA BREACH AND THE DEGREES OF IT

Mr. Salihoglu said that breach means unauthorized access. Cyber security aims to protect confidentiality, integrity and availability. If one of them crashes, the firm can come up with data breach. The degrees of the data breaches depend on the quality and quantity of the leaked data. Type of data leaked such as personal health data, ID number, shopping habits etc. reflect the quality of the data. According to Health Insurance Portability and Accountability Act, if a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered. Also, these entities which a breach affects fewer than 500 individuals should notify the local press. If the entity is affected by a breach of 5000 individuals, they should notify more than the local press. Finally, if the entity is affected by a breach of 10000 individuals, they must notify the national press. Even in the GDPR, the degree of data breach is described according to

data's type and size. To determine the penalty, the degree of the breach is also an important point.

Mr. Özer mentioned that to identify a data leak, we first need to define the data. Data is the smallest unit produced and operated by individuals and institutions, obtained from various organizations and used in decision making. The value and privacy of this unit may vary according to various axes. For example, the address data should be kept confidential and important to the individual, while the data can be shared openly and relatively low. Data leakage is the deliberate or unconscious transfer of this information belonging to the organization or person outside the organization or outside the access area of the person by different methods. Persons who would normally have access to the data due to the exclusion of the data have access to the data that should remain confidential and have the authority to harm the organization or the person. This increases the attack surface of the institution or person. The degree of data leakage is also directly proportional to the increase in attack level. For example, when a person's TC identity data is leaked, attackers can use this data to perform various malicious administrative actions related to the person, in which case it may have bad consequences for the person. The degree of such a data leak is considered critical. The infiltration of e-mail addresses of a small group of users of an organization is a lower level of data leakage than the entity's information presence.

4.2 THE CONSULTANCY NEED OF ENTITIES AFTER HAVING DATA BREACHES

Mr. Salihoglu mentioned that there are many types of customer behaviors. One of them is a customer who has a low impact of cyber security. After a breach, they want a quick penetration testing service which is an authorized simulated cyber-attack on a system, performed to evaluate the security of the system. This type of customers do not easily say that they have experienced a data breach. The second type of customer directly says that they have a data breach and tell them to do a forensics assessment about the case. They are cooperative and collaborative with consultants to get a quick result. The final type of customers has high level impact of cyber security. They call us when they detect an

anomaly; it is not a breach; it can be any malicious activity or traffic. Customers want us to analyze their network, even if there is a breach or not. In addition, this kind of customers tell if they have data breach or not at the moment. One of their characteristic is, they make forensics, cyber security contracts for a data breach process before a data breach or cyber security incident. For all types of customers, the cyber security budget is important. Even they want to spend less but the effects of breaches are high. After the regulation of personal data protection authority of Turkey, customers started to take much more preventive measures for cyber security incidents in the perspective of technology, human and technology.

Mr. Özer said that 60% of the leakage incidents occur and are shared/sold by attackers, 30% of the leakage incidents occur but the data is not publicly available, and 10% of the leakage incidents ask us for help at the time of the leak. For the first scenario, the attackers leak the data from the institution system 6 months -12 months ago. Since the leak has passed over this time, traces of the attackers can become undetectable. For this reason, we often have difficulties in detecting the technical tactics and procedures used by attackers in detecting IP addresses. Therefore, it is not proactive to prevent damage, but reactive actions are applied to prevent this damage from occurring again. We recommend such organizations to implement similar scenarios in their networks, which cause data leakage. With these periodic exercises, it will increase the maturity of the institution and prevent data leaks.

For the second scenario, the stages of detecting the attacker are easier and faster than the first scenario. Since the traces of the attacker are more evident in the system, we can also learn the methods and aims of the attackers. With this information, we can provide the institution with insight into which channels are used for which purpose. In this way, we can ensure that the organization receives less damage from leakage. However, the risk is still not fully prevented since the data is out of the organization.

For the last scenario, they run to the help of the institution at the time of leakage and firstly allow the leakage and analyze the attacker. Once we have verified all of our attacker hypotheses, we prevent leakage. Such scenarios are scenarios where the organization

receives the least damage since the quality and quantity of the leaked data can be clearly known. As the attacker's characteristics are known, all precautions can be taken for the malicious use of the leaked data. After these procedures, we conduct penetration tests to find the root cause of the leak and to detect and close the weaknesses at that stage.

4.3 THE TYPE OF DATA LEAKAGE CASES DURING EVALUATING DIFFERENT COMPANIES

Mr. Salihoglu said that well known cyber-attacks mainly focus on financial sector especially on banks, because the bank is where money is. Previously, cyber criminal's attacks focus on to get credit card data but nowadays, attackers mostly focus on to get personal data such as credentials since it causes more data and money breach.

Mr. Özer mentioned that financial sector is more important than the retail sector in cyber security circumstances. On the other hand, in energy or telecom sector, the most prevalent breaches are related with vendors. In e-commerce sector, content breach is the coming forward case. Advertisements and products are crawled by attackers.

4.4 THE DISCOVERY OF DATA LEAKAGE, IMPROVEMENT BY CUSTOMER AND THE IMPACT OF DATA LEAKAGE ON BRAND REPUTATION

Mr. Salihoglu mentioned that the entities which are effected from data breach start to improve their respond of system, and increase their budget. They buy and integrate technology products and solutions. To analyze brand reputation due to data breach, there are some accurate points that can specify to all breaches. The points are stock loss, decrease in income, customer loss, and fall back on the competition, penalties, spending to regain reputation, 5% loss of stock at the time of data leakage. They make agreements with identity protection firms. According to customer perspective, data breaches make loss of confidence, loss of belonging, termination of the customer-brand relationship, negative media news, becoming vulnerable for future cyber-attacks, negative impact on brand value like poor customer relationship. As a result of major violations, customers start to share less personal information. In addition, they pay more to service providers

with better data security. Due to these findings, during purchasing products and services, importance of data security become higher for the customer. The critical breach cases probably leads CIO (chief information officer) or CEO (chief executive officer) to resign.

Mr. Özer said that to improve their systems and perspective of cyber security, firms should have policy and strategy on cyber security and cyber risks. These strategies should be related to their general strategy. According to their cyber security strategy, they should have an organizational chart. These organizations consist of cyber security teams such as incident response team, security operations team, blue team and red team. After determining organizations, firms specify the politics and procedures on cyber security and data breach. They should invest on technology to protect their systems and data. To provide sustainability, these processes must be audited. Restrictions are strengthened from audit and implementation. The executive management should have perspective of cyber security and they should support cyber security procedures. According to all these points, even if there is a data breach, the penalties are decreasing because of the maturity of cyber security. They should show that they are prudent trader.

Özer: "The company that we serve, discovered a data leak as a result of an anomaly alarm that night. The event that triggered this alarm was the fact that very large data came out of an IP in the corporate network between 3-4 hours at night. Immediately after the alarm, they began to investigate and take the necessary actions. They detected the IP addresses of the attacker and blocked them from the system and reported the information to the national CERT. Since the organization had its own security team, they called us at the compromise assessment stage. At this stage, we found that only 10% of the total data leaked. The leaked data indicated the membership user name, password, e-mail, and groups that the customers were members of. The organization managed the process transparently and announced the process to the public via e-mail and social media. It also quickly created the necessary infrastructure to change the information of affected users. In this way, the process was managed without effecting the brand reputation of the company.

4.5 THE OPINION ON THE DATA BREACH PENALTY PROCESS AND THE APPLICATION IN TURKEY

Mr. Salihoglu said that 6698 numbered Personal Data Protection Law (PDPL) is a regulation for data breaches and data protection and Personal Data Protection Authority (PDPA) is the authority for data protection in Turkey. PDPL regulates the penalties on data breach. These penalties change due to breach such as publishing on the website of the entity or in money. These penalties are related to the breach's content. However, in Turkish regulations and penalties, metrics are not well specified. For instance, these metrics are cyber security and breach strategy, organization structure for the data privacy and cyber security, processes and policies, technology to prevent cyber-attacks and audit mechanism to follow. These metrics should be considered while detecting the penalty by the authority. Because if the entity takes these prevention methods into consideration, the penalty should be reduced.

Mr. Özer mentioned that the data is divided into two groups due to regulations. They are specially qualified personal data, and general qualified personal data. "Data on people's race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, disguise and dress, association, foundation or union membership, health, sexual life, criminal conviction and security measures and biometric and genetic data" is considered as private personal data and it can be processed only with the express consent of the person concerned. These penalties should cover whether this data is breached or not. In some cases, in the international market, the CEO have to resign due to quality of breach.

4.6 THE PREVENTION OF DATA BREACHES IN THE FUTURE WITH DIFFERENT MEASURES

Mr. Salihoglu mentioned that the holistic approach on cyber security is the first aim. This approach, including, but is not limited to technology. Data breach on achieved data, and when an employee left his computer in a taxi are some examples of data violation. Data breaches, cyber-attacks are real life stories. They should be ready for the data breach day. The entities must recognize these issues and take their measures. Firstly, they should have

a data breach process management policy. Audit and control mechanisms must be specified. In the future, these data breach cases will still be on our life, so entities should be ready for countermeasures. To enable these countermeasures, they need to apply technical assessments. These cyber security technical services are red team, blue team and purple team assessments. Red team assessments include cyber-attack simulations. Blue team assessments consist of cyber crisis simulations and cyber security defense methods. The purple team assessments conjunct these two assessments together.

Mr. Özer said that the entities do not have to solve their cyber security issues by themselves. They may take it as a service. While taking a third party consultancy and service, the quality of the service is important for entities. They should choose qualified cyber security consultancy companies and specialists. They should increase their budget on cyber security and data protection activities. Even, they do not have a problem on data breach; they should have a contract on forensics and breach issues with third party.

4.7 THE CONFIGURATION OF DATA BREACH ON TRUST, PENALTY AND BRAND REPUTATION IN THE FUTURE

Mr. Salihoglu said that when we focus on consumer behaviors, they become connect to internet more and more. Smartphones have become the go-to technology for online shopping. As consumers become more familiar with trusting of digital technology, they would go online for other services, too. People pay their bills and invoices online. Mobile payment services also are gaining widespread acceptance, especially in emerging regions that have leapfrogged past landline-based telephone systems and gone straight to mobile and smartphones. The number of people make mobile payments in stores. However, connected cars are also becoming a part of daily life. In light of this information cyber security is the growing topic of the industry. They have to be ready for cyber-attacks by means of both policy and technology aspects. On the other hand, if the entities do not pay attention to their data and security, their reputation will be negatively affected and due to penalties and customer loss, their finance will be effected. To validate trust on customer, data protection is one of the most valuable part.

Mr. Özer mentioned that it is an undeniable fact that data leakage is a subject that is dealt with more with the formation of legal regulations such as GDPR and PDPL. In order to comply with these regulations, organizations try to increase security and reliability in various ways. The security of the digital infrastructures of the organization and the cyber security awareness of the employees will increase. This will be a more prominent feature in inter-institutional competition, and customers will now turn to organizations that they think better protect their data. In this way, organizations will work more on data security in order to gain the trust of customers and take the lead in competition.

5. FINDINGS

After interviewing with 2 participants 7 research questions regarding data leakage are answered in this section. Data breach is defined and the methods to cope with data leakage which can be used in Turkey and global is found. In addition, future position of cyber security

5.1 THE DEFINITION OF DATA BREACH AND THE DEGREES OF IT

Cyber security aims to protect confidentiality, integrity and availability. If one of them crashes, a firm can come up with data breach which means unauthorized access. Data breach is the deliberate or unconscious transfer of data belonging to the organization or person outside the organization or outside the access area of the person by different methods. The degrees of the data breaches depend on the quality and quantity of the leaked data. Types of data leaked such as personal health data, ID number, shopping habits etc. reflect the quality of the data. Due to the GDPR, the degree of data breach is described according to data's type and size. The degree of data leakage is also directly proportional to the increase in attack level.

5.2 THE CONSULTANCY NEED OF ENTITIES AFTER HAVING DATA BREACHES

Entities' approaches against data breach change due to their behaviors. The first approach reflects the low impact of cyber security. After a breach, they want a quick penetration testing service which is an authorized simulated cyber-attack on a system, performed to evaluate the security of the system. This type of customers do not easily say that they have experienced a data breach. The attackers leak the data from the entity system 6 months -12 months ago. Since the leak has passed over this time, traces of the attackers can become undetectable. For this reason, it is difficult to detect the technical tactics and procedures used by attackers in detecting IP addresses. Therefore, it is not proactive to prevent damage, but reactive actions are applied to prevent this damage from occurring again.

The second approach directly indicates that they have a data breach and tell them to do a forensics assessment about the case. They are cooperative and collaborative with consultants to get a quick result. Since the traces of the attacker are more evident in the system, the methods and aims of the attackers can be learned. With this information, the entity can be provided with insight into which channels are used for which purpose.
The third approach reflects high level impact of cyber security. They ask for consultancy when they detect an anomaly, any malicious activity or traffic; even if it is not a breach. In this stage, the entity can be provided with help at the time of leakage. Once all of attacker hypotheses are verified, leakage can be prevented. The entity receives the least damage since the quality and quantity of the leaked data can be clearly known. As the attacker's characteristics are known, all precautions can be taken for the malicious use of the leaked data. After these procedures, penetration tests are conducted to find the root cause of the leak and to detect and close the weaknesses at that stage.

5.3 THE TYPE OF DATA LEAKAGE CASES DURING EVALUATING DIFFERENT COMPANIES

Well known cyber-attacks mainly focus on financial sector especially on banks. Previously, cyber criminal's attacks focus on to get credit card data but nowadays, attackers mostly focus on to get personal data such as credentials since it causes more data and money breach. Financial sector is more important than the retail sector in cyber security circumstances. On the other hand, in energy or telecom sector, the most prevalent breaches are related with vendors. In e-commerce sector, content breach is the coming forward case. Advertisements and products are crawled by attackers.

5.4 THE DISCOVERY OF DATA LEAKAGE, IMPROVEMENT BY THE CUSTOMER AND THE IMPACT OF DATA REPUTATION

To analyze brand reputation due to data breach, there are some accurate points that can specify to all breaches. The points are stock loss, decrease in income, customer loss, and fall back on the competition, penalties, spending to regain reputation, 5% loss of stock at the time of data leakage. They make agreements with identity protection firms. According

to customer perspective, data breaches make loss of confidence, loss of belonging, termination of the customer-brand relationship, negative media news, becoming vulnerable for future cyber-attacks, negative impact on brand value like poor customer relationship. As a result of major violations, customers start to share less personal information. In addition, they pay more to service providers with better data security. Due to these findings, during purchasing products and services, importance of data security become higher for the customer. The critical breach cases probably leads CIO or CEO to resign.

In case of following some processes, it is possible to manage the data breach crisis without effecting the brand reputation of the company. For instance, if a company discovers a data leak as a result of an anomaly alarm related with very large data came out of an IP in the corporate network between 3-4 hours, the company should immediately begin to investigate and take the necessary actions. In this stage, if the IP addresses of the attacker are detected, these should be blocked from the system and reported to the national CERT. Then the company should assign its own security team, and ask for consultancy at the compromise assessment stage. Thanks to the success of company's transparent process management which includes announcing the process to the public via e-mail and social media, and creating the necessary infrastructure to change the information of affected users, the brand reputation of the company will not be affected.

The entities which are affected from data breach start to improve their respond of system, and increase their budget. They buy and integrate technology products and solutions. To improve their systems and perspective of cyber security, firms should have policy and strategy on cyber security and cyber risks. These strategies should be related to their general strategy. According to their cyber security strategy, they should have an organizational chart. These organizations consist of cyber security teams such as incident response team, security operations team, blue team and red team. After determining organizations, firms specify the politics and procedures on cyber security and data breach. They should invest on technology to protect their systems and data. To provide sustainability, these processes must be audited. Restrictions are strengthened from audit and implementation. The executive management should have perspective of cyber

security and they should support cyber security procedures. According to all these points, even if there is a data breach, the penalties are decreasing because of the maturity of cyber security.

5.5 THE OPINION ON THE DATA BREACH PENALTY PROCESS AND THE APPLICATION IN TURKEY

In Turkish regulations and penalties, metrics are not well specified. For instance, these metrics are cyber security and breach strategy, organization structure for the data privacy and cyber security, processes and policies, technology to prevent cyber-attacks and audit mechanism to follow. These metrics should be considered while detecting the penalty by the authority.

5.6 THE PREVENTION OF DATA BREACHES IN THE FUTURE WITH DIFFERENT MEASURES

The entities should have a data breach process management policy. Audit and control mechanisms must be specified. In the future, data breach cases will still be on our life, so entities should be ready for countermeasures. To enable these countermeasures, they need to apply technical assessments. These cyber security technical services are red team, blue team and purple team assessments. Red team assessments include cyber-attack simulations. Blue team assessments consist of cyber crisis simulations and cyber security defense methods. The purple team assessments conjunct these two assessments together. The entities do not have to solve their cyber security issues by themselves. They may take it as a service. While taking a third party consultancy and service, the quality of the service is important for entities. They should choose qualified cyber security consultancy companies and specialists. They should increase their budget on cyber security and data protection activities. Even, they do not have a problem on data breach; they should have a contract on forensics and breach issues with third party.

5.7 THE CONFIGURATION OF DATA BREACH ON TRUST, PENALTY AND BRAND REPUTATION IN THE FUTURE

Cyber security is the growing topic of the industry. The entities have to be ready for cyber-attacks by means of both policy and technology aspects. On the other hand, if the entities do not pay attention to their data and security, their reputation will be negatively affected and due to penalties and customer loss, their finance will be effected. To validate trust on customer, data protection is one of the most valuable part.

In order to comply with regulations on data protection, organizations should increase security and reliability in various ways. The security of the digital infrastructures of the organization and the cyber security awareness of the employees will increase. This will be a more prominent feature in inter-institutional competition, and customers will now turn to organizations that they think better protect their data. In this way, organizations will work more on data security in order to gain the trust of customers and take the lead in competition.

6. CONCLUSION

Cyber security is the growing topic of the industry. The entities have to be ready for cyber-attacks by means of both policy and technology aspects. On the other hand, if the entities do not pay attention to their data and security, their reputation will be negatively affected and due to penalties and customer loss, their finance will be effected. To validate trust on customer, data protection is one of the most valuable part.

Entities generally reflect different approaches when a data breach incident occurs. Entities who are afraid of losing brand reputation do not easily indicate that they have experienced a data breach. For this reason, it is difficult to detect the technical tactics and procedures used by attackers. It is evaluated that it is vital for breached companies to timely admit the data breach incidents.

Data breach incidents have some effects for companies such as loss of brand reputation and financial penalties. Stock loss, decrease in income, customer loss, and fall back on the competition, financial penalties, and spending to regain reputation are the main results of data breaches which directly affect the brand reputation of a breached company. Due to customer perspective, data breaches make loss of confidence, loss of belonging, termination of the customer-brand relationship, negative media news, becoming vulnerable for future cyber-attacks, negative impact on brand value like poor customer relationship. As a result of major violations, customers start to share less personal information. In addition, they pay more to service providers with better data security. Due to these findings, during purchasing products and services, importance of data security become higher for the customer.

However, in case of following some processes, it is evaluated that it is possible to manage the data breach crisis without damaging the brand reputation of the company. That's why, the entities should have a data breach process management policy, and audit and control mechanisms must be specified. It is evaluated that if a company discovers a data leak, the company should immediately begin to investigate and take the necessary actions

including blocking the detected attackers and reporting them to the national CERT. Then the company should assign its own security team, and ask for consultancy at the compromise assessment stage. Thanks to the success of company's transparent process management which includes announcing the process to the public via e-mail and social media, and creating the necessary infrastructure to change the information of affected users, it is believed that the brand reputation of the company will not be affected. By virtue of following a transparent management against data breaches, the traces of the attackers would be more evident in the system, and the methods and aims of the attackers can be learned easily. Furthermore, as the attacker's characteristics are known, all precautions can be taken for the malicious use of the leaked data.

On the other hand, it is a known fact that cyber-attacks generally focus on financial sector especially on banks. Previously, cyber criminal's attacks focus on to get credit card data but nowadays, attackers mostly focus on to get personal data such as credentials since it causes more data and money breach. So the importance of financial sector is higher than other sectors in cyber security aspect. Therefore it is assessed that financial entities should establish more sensitive processes for crisis management of data breach incidents.

The companies which are affected from data breach should start with improving their respond of system, and increasing their budget for cyber security. To improve their systems and perspective of cyber security, companies should have policy and strategy on cyber security and cyber risks. Also it should be added that these strategies should be related to their general strategy. According to their cyber security strategy, they should have an organizational chart. These organizations consist of cyber security teams such as incident response team, security operations team, blue team and red team. After determining organizations, firms specify the politics and procedures on cyber security and data breach. They should invest on technology to protect their systems and data. To provide sustainability, these processes must be audited. The executive management should have perspective of cyber security and they should support cyber security procedures. By taking into consideration all these points, even if a data breach incident occurs, the financial penalties for such incidents would not be so high.

As to financial penalties, it is assessed that metrics for issuing penalties against data breach incidents are clear enough in Turkish legislation. However, considering the decisions of Personal Data Protection Committee, it is evaluated that these metrics are not sufficiently regarded in its decisions related with financial penalties on data breach incidents.

As a result of discussion of findings for research questions, it is concluded that the research question of *"Data breach incidents have some effects for companies such as loss of brand reputation and financial penalties. However, those companies' brand reputation may not be affected through transparent process management against data breach incidents."* has been verified. As World becomes globalized and digitalized, companies have to invest in cybersecurity technologies. In future researches, the long term impact of data breach on companies could be researched.

REFERENCES

Books

Dörnyei, Z. (2007). *Research methods in applied linguistics: quantitative, qualitative, and mixed methodologies.* New York: Oxford University Press.

Gass, S., & Selinker, L. (2008). *Second language acquisition: an introductory course.* New York: Routledge/Taylor and Francis Group.

Marvasti, A. B. (2004). *Qualitative research in sociology.* U.K.: SAGE Publications.

Morton-Williams, J. (1993). *Interviewer approaches.* Aldershot: Dartmouth.

Patton. M. Q. (2002). *Qualitative research and evaluation methods* (3rd edition). Thousand Oaks, CA: Sage Publications.

Yıldırım, A., & Şimşek, H. (2013). *Sosyal bilimlerde nitel araştırma yöntemleri.* Ankara: Seçkin Yayıncılık.

Periodicals

Alva (2015, October 31). TalkTalk case study: reputational risk of cyber security attacks. *Predictive analytics, Reputation management, Technology, Media and Telco,* Retrieved January 29, 2020, from https://www.alva-group.com/blog/the-reputational-risk-of-cyber-attacks-talktalk-case-study/ [accessed on 29.01.2020].

Arslan, Z., & Ekşi, A. A. (Winter 2016). The assessment of the Personal Data Protection Law numbered 6698. *Articletter GSI,* 7-24.

Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems*, 71, 62–77.

Burgoon, J. K. (1993). Interpersonal expectations, expectancy violations, and emotional communication. *Journal of Language and Social Psychology*, 12, 1–2, 30–48.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, 11, 431–448.

Çavusoğlu, H., Mishra, B., & Raghunathan, S. (Fall 2004). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce*, 9(1), 69–104.

Chai, S., Kim, M., & Rao, R. H. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems,* 50, 651-661.

Choi, B.C., Kim, S. S., & Jiang, Z. (2016). Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems*, 33(3), 904–933.

Confente, I., Siciliano, G., Gaudenzi, B., & Eickhoff, M. (August 2019). Effects of data breaches from user-generated content: A corporate reputation analysis. *European Management Journal*, 37(4), 492-504.

Culnan, M. J., & Williams, C. C. 2009. How ethics can enhance organizational privacy: Lessons from the choice point and TJX data breaches. *MIS Quarterly,* 33(4), 673-687.

Dolezel, D., & McLeod, A. (Summer 2019). Cyber-analytics: Identifying discriminants of data breaches. *Perspectives in Health Information Management*, 1-17.

Fuchs, L., Pernul, G., & Sandhu, R. (2011). Roles in information security – A survey and classification of the research area. *Computers & Security*, 30, 748-769.

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, 13(1), 61–83.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information and Management*, 46(7), 404–410.

Goode, S, Hoehle, H, Venkatesh, V., & Brown, S. A. (September 2017). User compensation as a data breach recovery action: An investigation of the Sony Playstation Network breach. *MIS Quarterly*, 41(3), 703-727.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 19, 33–56.

Gwebu, K. L., Wang, J. & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, 35(2), 683–714.

Hanson, R. H. & Marks, E. S. (1958). Influence of the interviewer on the accuracy of survey results. *Journal of American Statistical Association*, 53(283), 635-655.

Hsu, J. S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, 26(2), 282-300.

Janakiraman, R., Lim, J. H., & Rishika, R., (March 2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, 82, 85–105.

Johnson, M. E. (2008). Information risk of inadvertent disclosure: An analysis of file-sharing risk in the financial supply chain. *Journal of Management Information Systems,* 25(2), 97-123.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems,* 25(3), 231-251.

Kulka, R. A. & Weeks, M. F. (1988). Toward the development of optimal calling protocols for telephone surveys: a conditional probabilities approach. *Journal of Official Statistics*, 4(4), 319-332.

Kwon, J., & Johnson, M. E. (2013). Health-care security strategies for data protection and regulatory compliance. *Journal of Management Information Systems*, 30(2), 41–66.

Kwon, J., & Johnson, M. E. (2015). Protecting patient data-the economic perspective of healthcare security. *IEEE Security and Privacy,* 13(5), 90-95.

Lai, F., Li, D., & Hsieh, C. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, 52, 353–363.

Liang, N., Biros, D. P., & Luse, A. (2016). An empirical validation of malicious insider characteristics. *Journal of Management Information Systems*, 33(2), 361–392.

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organizational information security policies: an empirical study of the influence of counterfactual reasoning and organizational trust. *Information Systems Journal,* 25(3), 193-273.

Makridisa, C., & Dea, B. (2018). Measuring the economic effects of data breaches on firm outcomes: Challenges and opportunities. J*ournal of Economic and Social Measurement,* 43, 59–83.

Malhotra, A., & Malhotra, C. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research*, 14(1), 44-59.

Mellado, D., & Rosado, G. D. (2012). An overview of current information systems security challenges and innovations. *Journal of Universal Computer Science*, 18, 1598-1607.

Morrison, E. W., & Robinson, S. L. (1997). When employees feel betrayed: A model of how psychological contract violation develops. *Academy of Management Review,* 22(1), 226–256.

Oldendick, R. W., Bishop, G. F., Sorenson, S. B. & Tuchfarber, A. J. (1988). A comparison of the Kish and last birthday methods of respondent selection in telephone surveys. *Journal of Official Statistics*, 4(4), 307-318.

Saidani, M., Shibani, A., & Alawadi, K. (2013). Managing data security in the United Arab Emirates. *Prime Research on Education*, 3, 458- 464.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, 32(2), 314–341.

Spanos G., & Angelis L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, 58, 216-229.

Tomaszewski, J. P. (2006). Are you sure you had a privacy incident. *IEEE Security and Privacy*, 4(6), 64-66.

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, 24(2), 201–218.

Williams, L. C. (2013, December 31). The 9 biggest privacy and security breaches that rocked 2013. *Thinkprocess*.

Wong, R. C.-W., Fu, A. W.-C., Wang, K., Yu, P. S., & Pei, J. (2011). Can the utility of anonymized data be used for privacy breaches. *ACM Transactions on Knowledge Discovery from Data*, 5(3), 1-24.

Zafar, H., Ko, M., & Osei-Bryson, K. (2012). Financial impact of information security breaches on breached firms and their non-breached competitors. *Information Resources Management Journal*, 25(1), 21-37.

Other Sources

Abelson, R., & Goldstein, M. (2015, February 5). Millions of anthem customers targeted in cyber attack. *The New York Times,* http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html, [accessed on 29.01.2020].

Acquisti, A., Friedman, A., & Telang, R. (2006). *Is there a cost to privacy breaches? An event study.* Paper presented at the Twenty Seventh International Conference on Information Systems Proceedings. Paper 94. Milwaukee, WI, Dec 10 2006–Dec 13 2006.

Athavaley, A., & Shepardson, D. (2017, February 21). Verizon, Yahoo agree to lowered $4.48 billion deal following cyberattacks. *Reuters,* http://www.reuters.com/article/us-yahoo-m-a-verizon-idUSKBN1601EK, [accessed on 29.01.2020].

Berr J. (2017). Equifax breach exposed data for 143 million consumers. *CBS News.*

Briefings on HIPAA (July 2019). Biggest healthcare data breach of 2019 shows health data still highly valuable to cyber attackers.

Collins K. (2017). Yahoo and Equifax just proved that you can never trust the first number announced in the data. *Quartz.*

Data Privacy Manager (2019). Top 5 GDPR fines [first half of 2019]. https://dataprivacymanager.net/top-5-gdpr-fines/, [accessed on 29.01.2020].

Deloitte, D. Cyber crisis management: Readiness, response, and recovery. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf, [accessed on 29.01.2020].

Graham, A. (2019, October 18). The damaging after-effects of a data breach. *IT Governance*, https://www.itgovernance.co.uk/blog/the-damaging-after-effects-of-a-data-breach, [accessed on 29.01.2020].

HHS (2013). Submitting notice of a breach to the secretary. U.S. *Department of Health & Human Services,* http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html, [accessed on 29.01.2020].

Intel Security-McAfee (2014, June 1). Net losses: Estimating the global cost of cybercrime. http://globalinitiative.net/wpcontent/uploads/2017/01/csis-estimating-the-global-cost-ofcybercrime-june-2014.pdf, [accessed on 29.01.2020].

Janofsky, A. (2017, September 15). Equifax breach could cost billions. *The Wall Street Journal*, https://www.wsj.com/articles/equifax-breach-could-cost-billions-1505474692, [accessed on 29.01.2020].

Özkaya, Ş. C. (2019). The effects of a data breach: Loss of brand reputation and financial penalties. *FIC OBSERVATORY.com, Crossroads of reflections on cyber security*, https://observatoire-fic.com/en/the-effects-of-a-data-breach-loss-of-brand-reputation-and-financial-penalties-by-seref-can-ozkaya/ [accessed on 29.01.2020].

PCQUEST (May 2019). Data breaches. *PCQuest*, 36-41.

Ponemon Institute (2013). *2013 Cost of data breach: Global analysis. Research Report*, Ponemon Institute.

PWC, P. (2011). Cyber crisis management: A bold approach to a bold and shadowy nemesis. https://www.pwc.com/ca/en/technologyconsulting/security/publications/pwccybersecurity-crisismanagement-2013-05-en.pdf, [accessed on 29.01.2020].

Reynolds, I. (2011, May 6). Sony CEO apologizes for data theft; shares fall 2 pct. *Reuters*.

Richmond, S., & Williams, C. (2011, April 26.). Millions of Internet users hit by massive Sony PlayStation data theft. *The Telegraph*.

Sherr, I., & Wingfield, N. (2011, May 7). Play by play: Sony's struggles on breach. *Wall Street Journal*.

Trefis Team (2014, May 8). Target's CEO steps down following the massive data breach and Canadian debacle. *Forbes*, http://www.forbes.com/sites/greatspeculations/2014/05/08/targetsceo-steps-down-following-the-massive-data-breach-and-canadiandebacle/#28cb80763f56, [accessed on 29.01.2020].

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Özkaya, Şeref Can
Nationality: Turkish (T.C.)
Date and Place of Birth: 10 April 1991, Ankara
Marital Status: Single
Phone: +90 538 311 07 91
email: serefcanozkaya@gmail.com

EDUCATION

Degree	Institution	Year of Graduation
BS	TOBB ETÜ	2014
High School	Ted Ankara Koleji	2009

WORK EXPERIENCE

Year	Place	Enrollment
2017-...	STM A.Ş.	Cyber Security Specialist
2016-2017	Deloitte Turkey	Cyber Security Consultant

FOREIGN LANGUAGES

Advanced English, French

PUBLICATIONS

1. Özkaya, Ş. C. (2019). The effects of a data breach: Loss of brand reputation and financial penalties. FIC OBSERVATORY.com, Crossroads of reflections on cyber security, https://observatoire-fic.com/en/the-effects-of-a-data-breach-loss-of-brand-reputation-and-financial-penalties-by-seref-can-ozkaya/

HOBBIES

Running, Travelling