The True Cost of Data Breaches

For

ICT 4605 Information Systems Security Principles

Master of Science

Information and Communications Technology

Kristy McNulty

University of Denver University College

July 9, 2018

Faculty: Gary Reeves, CISSP

Director: Thomas Tierney, PhD

Dean: Michael J. McGuire, MLS

Executive Summary

Although costs of data breaches have dropped slightly in the last year, data breaches cost companies massive amounts in both quantitative and qualitative ways that leave a negative footprint on businesses. The purpose of this study is to examine the costs of these data breaches to the companies that they affect, both quantitatively and qualitatively. The results showed that even though the cost of data breaches has decreased by 10% in the past year, they still cost an average of $3.62 million for each incident (Ponemon Institute 2017), and can cost vastly more in particularly malicious cases, such as the Target breach of 2013 (McCoy 2017). Results also demonstrated that the cost of data breaches can vary widely by country and industry, the United States being particularly expensive (Messmer 2012) and the healthcare industry losing billions per year (Anonymous 2012). Data breaches also cost more than just money and can result in a multitude of other significant losses, such as customer trust and brand reliability (Information Management Journal 2016). It has even been shown that the media can have an impact on how people view and treat major data breaches (Reitberger and Wetzel 2017). It is recommended that companies closely examine the cost of data breaches and implement security measures to prevent them as much as possible.

Table of Contents

Introduction

Data breaches have been around as long as humanity and sensitive information have existed. Data breaches in earlier decades were as simple as unauthorized entities thumbing through physical paper files on patients or clients, rather than the modern-day massive data breaches that involve millions of people. It has only been in recent decades, with the emergence of the world wide web and cloud computing, that data breaches have gained international attention and created such a colossal impact. One of the most famous data breaches in recent history involved the global chain store Target, resulting in a $18.5 million lawsuit after affecting 41 million shoppers' credit cards in 2013 (McCoy 2017). Other famous data breaches include Yahoo, the biggest of the millennium that affected 3 billion email accounts in 2013 (USA Today 2017), and the most recent Equifax data breach of 2017 that affected 143 million consumers (Bernard et. al 2017).

Although the cost of data breaches has dropped slightly in the last year, data breaches still cost companies massive amounts in both quantitative and qualitative ways. It is important to study the cost of such data breaches so that both inexperienced and veteran companies can be aware of the true impact that a data breach can have on their businesses. It is imperative for these businesses to conduct cost-benefit analyses for incorporating better security measures in exchange for protection against data breaches. While this study does not cover the methodology to implementing such security systems, it does illustrate the magnitude of even a single data breach and outlines the importance of defending against them.

The Quantitative Cost of Data Breaches

While data breaches have a multitude of effects on targeted businesses, one of the most significant is the financial cost to the company that can be measured in numbers, or the quantitative costs. There are other types of costs that are less concrete and more difficult to attach numerical values to, which are referred to as qualitative costs. The first section of this paper covers quantitative costs and examines how much these breaches cost businesses financially and where these costs come from.

Average Financial Costs and Trends

The Ponemon Institute, an independent research institution based in Michigan, released a study in 2017 covering the costs and impacts of data breaches, called the *2017 Cost of Data Breach Study: Global Overview*. This study showed that the "average total cost of data breaches for the 419 companies participating" was $3.62 million, down from $4 million the previous year (Ponemon Institute 2017). The average cost for each individual stolen or lost record that contained confidential information was $141, which is also a significant reduction from the year before, which was $158 per record (Ponemon Institute 2017). Combining these two reductions in cost, businesses saw an average 10 percent lowered cost, with an 11.4 percent decrease in per capita cost specifically (Ponemon Institute 2017). Despite a decrease in the overall costs of data breaches, businesses in this study experienced larger breaches, the average size increasing about 1.8 percent from the previous year (Ponemon Institute 2017). These costs accrue from a variety of sources, including the number of records lost or stolen, how long it takes to identify the breach, the detection and escalation of the incident, the cost to notify victims, and whether

there was a clear malicious attacker or it resulted from a system glitch and/or negligence from the company.

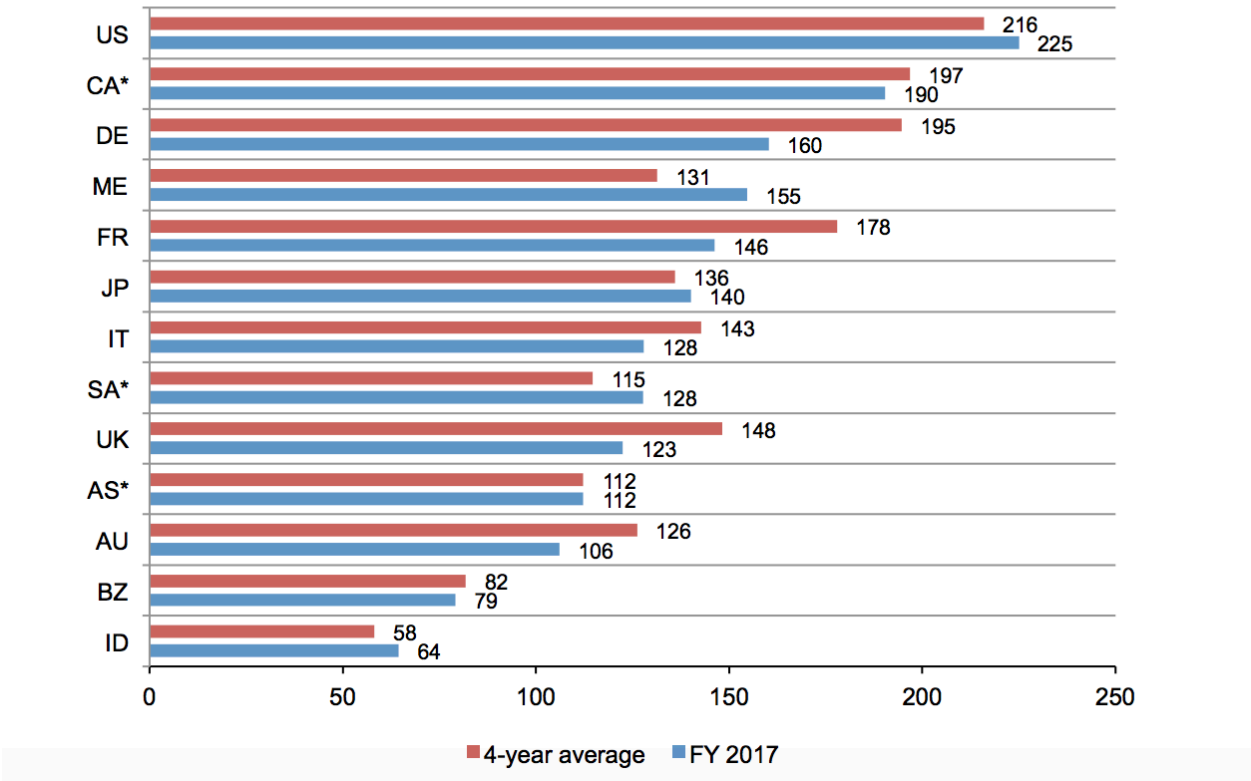
This study also outlined other important implications in relation to the cost of data breaches. For instance, the more records that were lost, the higher the cost of the incident was, and the average cost ranged from "$1.9 million for incidents with less than 10,000 compromised records to $6.3 million for incidents with more than 50,000 compromised records" (Ponemon Institute 2017). Another discovered trend included that faster identification and containment of data breaches led to lower costs, with a mean time to identify (MTTI) of 191 days, and a mean time to contain (MTTC) of 66 days (Ponemon Institute 2017). Some other intriguing statistics relate to malicious attacks versus accidental breaches. Malicious insiders and hackers caused the most data breaches and were the most expensive to mitigate, with 47 percent of breaches caused by malicious or criminal attacks, and an average cost of $156 per record to resolve them, in contrast to the $128 average cost per record for human error and/or negligence (Ponemon Institute 2017). Additionally, it was found that incident response teams and extensive encryption reduced costs. Incident response (IR) teams reduced costs by "as much as $19 per compromised record," and extensive encryption "reduced cost by $16 per capita" (Ponemon Institute 2017). Combining these methods averages at $35 saved per record, and for even a lower-scale attack of 10,000 compromised records, companies could save an upwards of $350,000.

Costs Across the Globe

The cost of data breaches is not uniform across the globe and shouldn't be treated as so in research and mitigation efforts when examining the impact and financial cost of these

incidents. The issue of data breaches in a global context is examined further in a 2012 study published in *Network World*. At an average $225 per capita, data breaches were the most expensive in the United States (as shown in Figure 1).

Figure 1. The 2017 per capita cost of data breach compared to the four-year average
Grand averages for FY2017=$141, FY2016=$158, FY2015=$154, FY2014=$145
*Historical data are not available for all years
Measured in US$



This particularly high cost may be due to specific U.S. laws that require disclosure of data breaches to the public, laws that cost the U.S. an average of $0.69 million per organization (Messmer 2012). In contrast, the nation with the lowest cost per capita was India at $64 per capita, and Brazil had the lowest average total organizational cost at $1.52 million (Messmer 2012). Comparisons of this year's costs to the four-year average revealed that trends in these costs also vary by country. Germany had the largest decrease in the total average cost (-$0.91

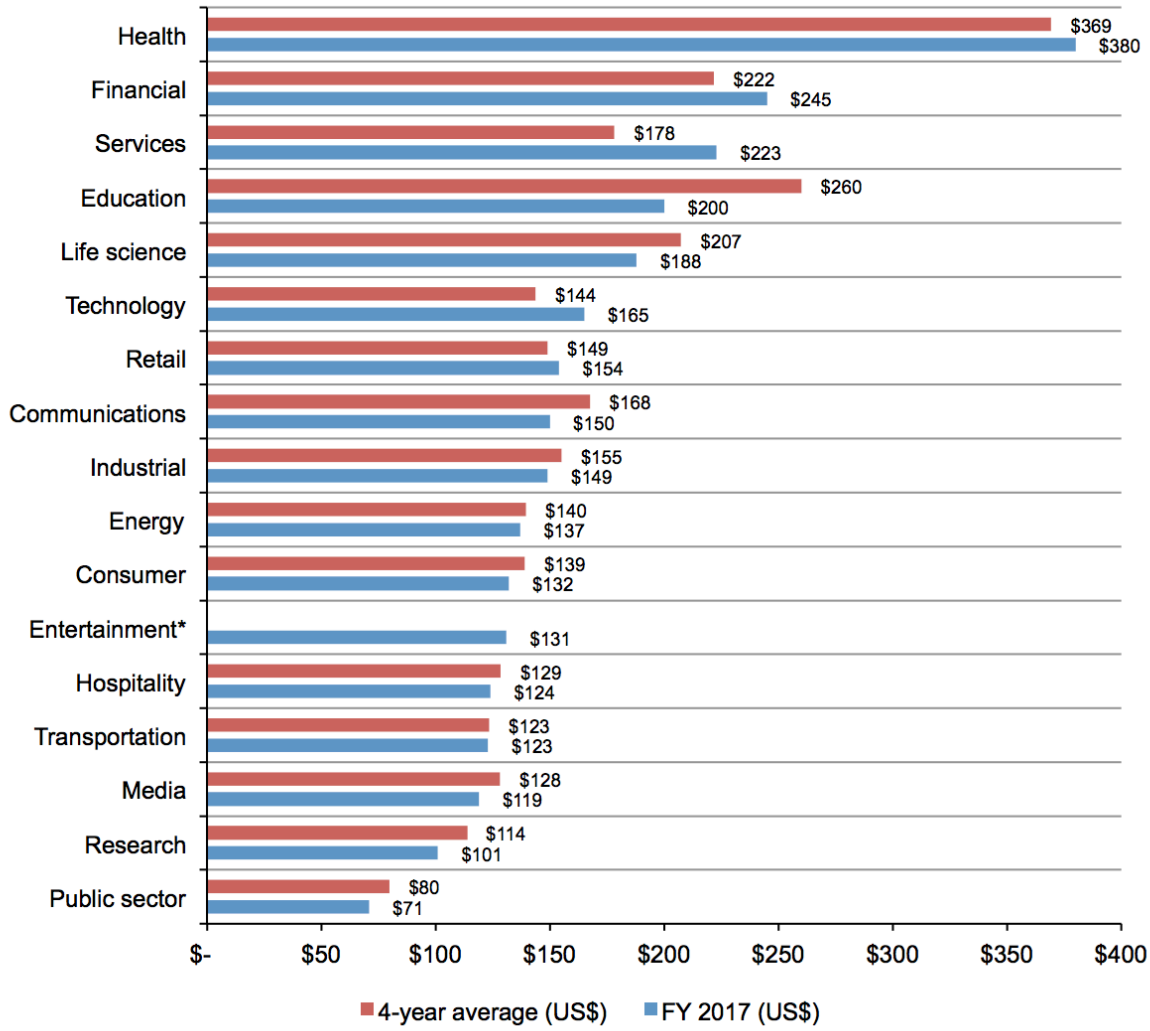
million), followed by France (-$0.68 million), Australia (-$0.48 million), and the United Kingdom (-$0.45 million) (Messmer 2012). The biggest increases in these costs included the Middle East (+$0.83 million), the United States (+$0.66 million), and finally Japan (+$0.52 million) (Messmer 2012).

There was also an assortment of varied trends and predictions across countries as well. Companies in India, South Africa, and Brazil were most likely to undergo a breach involving 10,000 or more records over a period of 24 months, with South Africa having the highest probability at 42 percent (Messmer 2012). Canada had the lowest probability of experiencing a data breach at 14.5 percent (Messmer 2012). The research also showed that some countries are more likely to experience data breaches than other countries. South Africa and India had the highest probability of experiencing a data breach, while Germany and Canada had the lowest probability of experiencing a data breach (Messmer 2012). It is interesting to note that even though Canada had one of the lowest probabilities of experiencing a data breach, they also had the third-highest cost per incident. This is most likely due to Canada losing more money per record on average than the other nations examined in this study at $81 per record (Messmer 2012). The research showed one final interesting trend in the rate of attacks due to malicious hackers versus human error. 59 percent of attacks that occurred in the Middle East and 52 percent in the United States were carried out by malicious hackers, while Italy and South Africa only had 40 percent carried out by attackers (Messmer 2012). Italy contained the highest percent due to human error at 36 percent, while Germany and India had the highest rates due to system glitches, sitting at 34 and 33 percent, respectively (Messmer 2012). These trends and statistics in the Messmer study display the stark differences and unique challenges

that countries face individually in the face of data breaches, and teaches that not every country experiences or responds to these incidents in the same way.

Costs Across Industries

Data breaches not only vary by country or region, but also by industry. This is apparent in a 2012 study published in the International Journal of Micrographics and Optical Technology, which compared the cost of data breaches between differing industries in the United States. There has been an especially daunting effect of data breaches on the healthcare industry, with data breaches being up 32% and costing the healthcare industry a staggering $6.5 billion (International Journal of Micrographics and Optical Technology 2012). It appeared that deeply regulated industries such as healthcare, education, and finance held the highest number in per-capita losses over a four year average, per-capita referring to the loss for each individual record. Healthcare led at $369 lost per capita, education lost $260 per capita, and finance lost $222 per capita, all significantly higher than the average lost per capita of $141, as seen in Figure 2 (International Journal of Micrographics and Optical Technology 2012). It is also interesting that although education had one of the highest costs per capita, the industry also had the most significant decrease over a four year span, with costs decreasing at a rate of $60 per record (International Journal of Micrographics and Optical Technology 2012). The life science and communication industries also saw a significant decrease in costs per record at $18 and $19 per capita, respectively. And finally, the industries that experienced the largest increases in costs per capita were services (+$45 per record), finance (+23 per record), technology (+$21 per record), and health (+$11 per record) (International Journal of Micrographics and Optical Technology 2012).



The Qualitative Cost of Data Breaches

Data Breaches Cost More Than Money

Data breaches don't just cost companies money, and can cause a huge loss in qualitative losses as well. Some of these qualitative losses can indirectly lead to further financial losses, along with tainting the company brand and image. Some of these qualitative costs are outlined in a study published in the *Information Management Journal,* part of the Nov/Dec 2016 volume. The study includes a total of fourteen impact factors after a cyberattack, including "seven that

may not be readily apparent" (Information Management Journal 2016). One of the factors outlined in the study is the cost of business disruption during and after a data breach. For example, a company can suffer financially if they have to shut down their website or pause other business operations, which can lead to losing "current and possibly future business when customers move to a competitor" (Information Management Journal 2016). This loses revenue for the company they would have otherwise made, and also unintentionally drives customers to competitors that could be viewed as more reliable. Another significant qualitative cost to companies after a data breach, related to business disruption, is lost customer relationships. After a business undergoes a data breach, there is a chance that some customers will not want to continue using that company's services or purchasing their goods. According to the hypothetical analysis performed in this study, "customer attrition rate increases 30% after a cyber incident and doesn't return to normal for three years" (Information Management Journal 2016). This means that out of every 100 customers, 30 were leaving after a company underwent a data breach, and the regular rate of attrition (also known as churn rate) pre-incident does not normalize again post-incident for another three years. And lastly, one of the most important factors discussed in this study is the loss of intellectual property, which can have devastating effects. Loss of intellectual property can include anything relating to valuable information the company has attained, such as designs, blueprints, research, ideas, outlines, and any other trade secrets. According to Emily Mossburg, a test reporter in this study, loss of intellectual property "that you've been working on for months or years" and is then "brought to market by another organization faster and cheaper than you can do it, that impact can be reverberating for decades" (Information Management Journal 2016).

Effects of the Media on Qualitative Costs

The methods the media uses to report data breaches can also affect the qualitative costs of major data breaches, such as the infamous Target data breach in 2013 that cost the company $18.5 million and tens of thousands of customers (McCoy 2017). It has been shown that data breaches can change how consumers view affected companie, according to the *2017* IEEE 38th Sarnoff symposium that was authored by Gunther Reitberger and Susanne Wetzel. The results of this symposium were concise, but clear. The authors presented research that showed that consumers were much more likely to be aware of major data breaches the more media they consumed, and were also much more likely to leave companies that were affected by such data breaches and have a negative perception of the companies (Reitberger & Wetzel 2017). Consumers that were not as involved in media coverage or generally less updated on current events were not as affected by data breaches, with 80% of those consumers claiming that they would still use the affected company's services and/or goods, despite a major data breach (Reitberger & Wetzel 2017). These customers' perceptions of the respective companies were also not as negatively impacted. In summary, customers that consumed more media were more negatively impacted and less likely to continue business transactions with the affected companies, while customers that did not consume as much media were not impacted and generally more apathetic towards the affected companies. It is an interesting illustration of the extent that media coverage can affect consumers' attitudes towards businesses that have been hit by a data breach.

Conclusion

Data breaches have existed for many years, long before even the emergence of the internet and the digital age. The cost and impact of these data breaches is important to study so business owners can be aware of potential losses if preventative measures are not taken. In this study, although the cost of data breaches has declined by 10% since 2016 (Ponemon Institute 2017), it was found that data breaches cost an average of $3.86 million per occurrence (Ponemon Institute 2017), though there are certainly outliers including the Yahoo and Target breaches. Data breaches can also vary by country and industry, the United States possessing some of the most expensive data breaches (Messmer 2012), and the healthcare industry maintaining the most frequent numbers of data breaches and largest monetary value lost (Anonymous 2012). Additionally, data breaches have other outlying effects that are not just financial, such as loss of customer trust and loss of a trustworthy brand, which has potential to be further exacerbated by media reports (Reitberger and Wetzel 2017). These costs are important for any business to consider when administering security measures into their networks and IT systems, be they budding startups or seasoned corporations.

References

Anonymous. 2012. “Data Breaches Cost the Healthcare Industry an Estimated $6.5 billion.” *International Journal of Micrographics and Optical Technology,* vol. 29 (June): 3-4.

Bernard, Tara, Tiffany Hsu, Nicole Perlroth, and Ron Lieber. 2017. “Equifax Says Cyberattack May Have Affected 143 Million in the U.S..” *The New York Times*. September 7. Accessed July 10, 2018. https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

Information Management Journal. 2016. “Data Breaches Cost More Than Money.” *Information Management Journal,* vol. 50 (November): 7-8.

Iram, Rotem. 2017. “How to Curb the Costs of a Data Breach.” *CFO Publishing LLC,* vol. 3 (September): 14-17.

McCoy, Kevin. 2017. “Target to pay $18.5M for data breach that affected 41 million consumers.” *USA Today*. May 23. Accessed July 11, 2018. https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/.

Messmer, Ellen. 2012. “Data breaches in the U.S. cost more than in Australia, France, Germany, and the United Kingdom.” *Network World* (April): 1-2.

Ponemon Institute. 2017. “2017 Cost of Data Breach Study.” *Ponemon Institute*. June 1. Accessed July 10, 2018. https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf.

Reitberger, Gunther and Susanne Wetzel. 2017. “Investigating the Impact of Media Coverage on Data Breach Fatigue.” *2017 IEEE 38th Sarnoff Symposium* (September).

USA Today. 2017. “Yahoo Data Breach, Internet's Biggest, Still A Mystery.” *USA Today*. November 8. Accessed July 10, 2018. https://www.usatoday.com/story/tech/news/2017/11/08/marissa-mayer-says-yahoo-still-doesnt-know-who-behind-webs-biggest-breach/844716001/.