Global Information Assurance Certification Paper

Data Breach Impact Estimation

GIAC (GSNA) Gold Certification

Author: Paul Hershberger, pjhersh13@gmail.com
Advisor: Stephen Northcutt
Accepted: 12/10/16
(Date your final draft is accepted by your advisor)

Abstract

Internal and External auditors spend a significant amount of time planning their audit processes to align their efforts with the needs of the audited organization. The initial phase of that audit cycle is the risk assessment. Establishing a firm understanding of the likelihood and impact of risk guides the audit function and aligns its work with the risks the organization faces. The challenge many auditors and security professionals face is effectively quantifying the potential impact of a data breach to their organization. This paper compares the data breach cost research of the Ponemon Institute and the RAND Corporation, comparing the models against breach costs reported by publicly traded companies by the Securities and Exchange Commission (SEC) reporting requirements. The comparisons will show that the RAND Corporation's approach provides organizations with a more accurate and flexible model to estimate the potential cost of data breaches as they relate to the direct cost of investigating and remediating a breach and the indirect financial impact associated with regulatory and legal action of a data breach. Additionally, the comparison indicates that data breach-related impacts to revenue and stock valuation are only realized in the short-term.

1. Introduction

Audit teams strive to assess the effectiveness of controls to help organizations align their resources to effectively manage risks to limit potential negative impacts. The National Institute of Standards and Technology (NIST), Special Publication 800-30Rev1, defines the purpose of a risk assessment as:

> The purpose of the risk assessment component is to identify: (i) threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation; (ii) vulnerabilities internal and external to organizations; (iii) the harm (i.e., adverse impact) that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring) (NIST, 2012)

When assessing risks faced by an organization, auditors use the combination of the probability of an event in conjunction with the potential impact to the organization to communicate the appropriate level of exposure to that risk. A data breach is one type of risk event for which auditors routinely try to measure exposure. With heightened awareness of data breaches, auditors are increasingly turning to researchers to identify models for estimating the potential impact of a data breach to corporations. This paper focuses on two data breach cost estimation models, the Ponemon model, and the RAND model. Direct and indirect costs associated with recent retail industry data breaches will be used to compare the estimates generated by the models to the actual costs reported by those breached organizations. The purpose of this analysis is to determine the effectiveness of each model to better equip auditors to assess the risk of a data breach. Using an effective model enables auditors to relay a more accurate risk assessment to senior management. In turn, a more accurate risk assessment enables management to allocate resources proportionally based on the potential impact of the threat versus fear and uncertainty.

Paul Hershberger, pjhersh13@gmail.com

2. The Ponemon Institute

Founded in 2002 by Larry Ponemon, the Ponemon Institute is a research organization focusing on privacy, data protection, and information security policy (The Ponemon Institute, 2016). Since 2005, the Ponemon Institute has published their annual Cost of Data Breach Study which focuses on measuring the cost of data breaches and providing organizations with a means by which they can measure the potential impact of a data breach to the organization. In preparation for the annual report, the Ponemon Institute researchers conduct interviews with key individuals from organizations that have experienced a data breach, who have firsthand knowledge of the costs associated with external resources for investigating and remediating the breach, as well as indirect costs such as internal investigation, remediation effort, and loss of customer (Ponemon Institute, 2016). In preparing the 2016 report, more than 1500 interviews were conducted with representatives from 383 participating organizations. The data breaches covered by the research for the 2016 report ranged from 3,000 to just over 101,500 individual records compromised. In the 2016 report, the Ponemon Institute states that they limit their research to exclude breaches over approximately 100,000 records because larger breaches "are not typical of the breaches most organizations experience" (Ponemon Institute, p. 4). The Ponemon research focuses on determining the cost of a data breach by the number of individual records compromised in the breach. For 2016, their research concluded that the global average cost of a data breach is $158 per record compromised (The Ponemon Institute, p. 1). The cost per record differs by country with the US having the highest cost per record of $221. The report goes on to conclude that US organizations paid the highest cost of $3.97 per record in the form of abnormal customer turnover, increased customer acquisition cost, reputation loss, and diminished goodwill (The Ponemon Institute, p. 3).

News reports, as well as security product marketing materials often reference the Ponemon report as a measure of potential data breach exposure. These references drive wide adoption of the findings as a means of measuring the potential impact of a data breach to an organization, despite the limitations

described in the report. The adoption, despite the published limitations, drives the use of the Ponemon model to estimate the potential impact of data breaches of all sizes. The use of the single cost- per -record lost seems reasonable and has filled a void in the discussion around estimating breach-related risks and the Ponemon research has become the default standard of measure.

3. RAND Corporation Research

The Oxford University Press recently published a research paper by the RAND Corporation's Sasha Romanosky in *The Journal of Cybersecurity*. The research examined data associated with more than 12,000 cyber events including data breaches, security incidents, privacy violations and phishing attacks spanning a ten-year period (Romanosky, 2016). The data used in this research is from a third-party organization, Advisen. Advisen is a New York-based company that focuses on serving the risk and insurance communities with information analytics, news, and research (Advisen, 2016). The significance of using the Advisen data as a source for Romanosky's research ties back to the design and intended use of the dataset. Advisen maintains the cyber database and makes it available to their clients "for underwriting and actuarial analysis to inform decisions related to underwriting and pricing cyber risk" (Advisen, n.d., p. 10). Advisen leverages a team of 13 full-time professionals who collect information from a variety of sources including public records, court documents and information obtained through Freedom of Information Act requests. In his research, Romanosky condensed the 11 types of cyber events contained in the Advisen dataset into four categories: data breach, security incident, privacy violation and phishing/skimming. For this paper, the focus will primarily be on the category defined as, "The unintentional disclosure of personally identifiable information (PII) stemming from loss or theft of digital or printed information" (Romanosky, p. 3). Through regression modeling, Romanosky's research draws a correlation between the annual revenue of an organization and the cost of a data breach suffered by that organization. The research concludes that data breaches have cost companies 0.4% of their annual

revenue. Subsequently, based on past data breaches, companies can estimate the potential cost of a data breach as 0.4% of their annual revenue.

4. Data Breaches by the Numbers

Analysis of a data export from the Privacy Rights Clearinghouse, a non-profit consumer education and advocacy organization (Privacy Rights Clearing House, 2016), provides a general understand of the demographics of data breached over time. The dataset downloaded contained information covering 5,143 data breaches from January 2005 to October 2016. Although the number of breaches is often cited as continuing to climb over time, the dataset shows more erratic trending with consistency seen only over short periods of time, between two and three years.

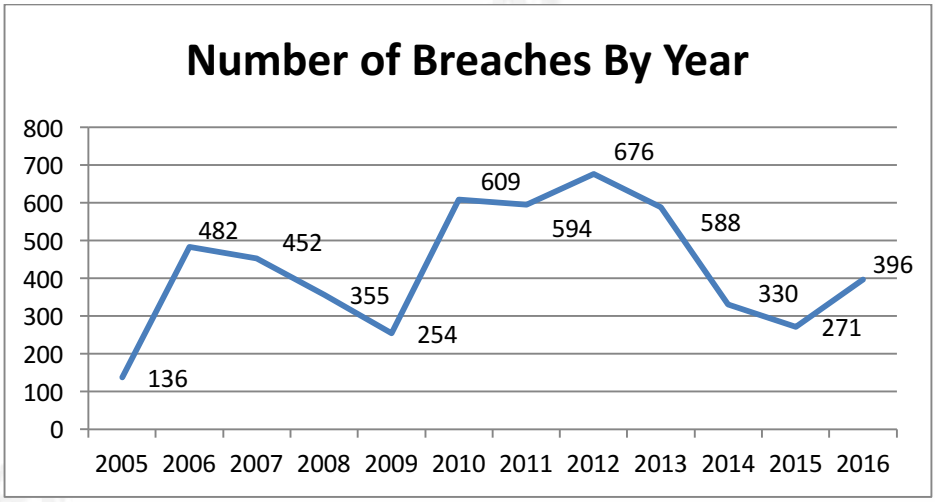


Figure 1: (Privacy Rights Clearinghouse)

Within the dataset, 1,834 breaches reflected an "Unknown" number of records breached, while 3,309 identified the numbers of records breached. Further analysis will focus on the 3,309 breaches, which contained record counts. It is important to note that breaches reporting zero records breached remain in this dataset. As seen in Figure 2, when limited to those breaches with recorded losses, the year-by-year trend remains relatively unchanged:

Paul Hershberger, pjhersh13@gmail.com

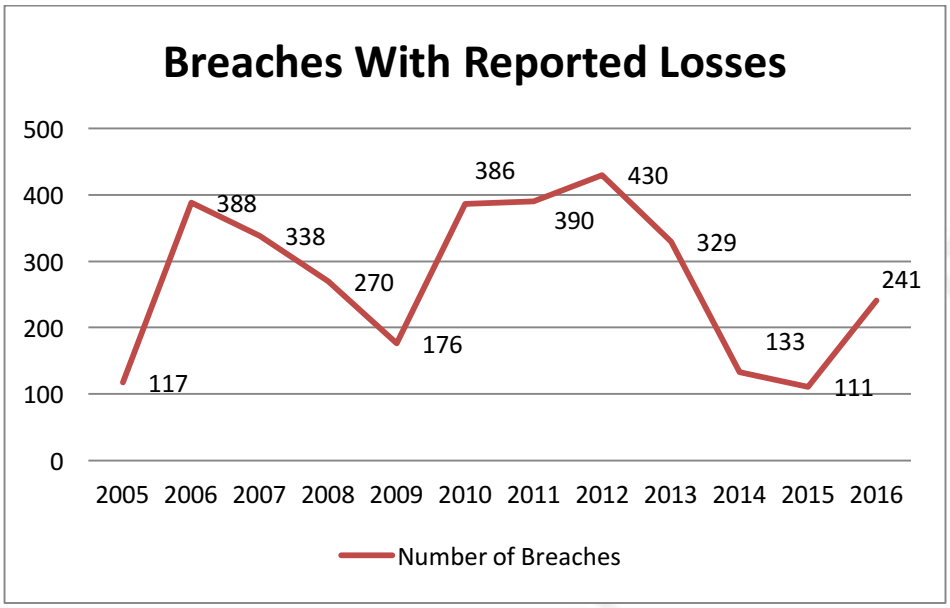


Figure 2 : (Privacy Rights Clearinghouse)

Examining the dataset further, the simple average of records breached by year shows that across the dataset, the average records lost remained below 2 million until 2014, commonly referred to as the "year of the mega breach." The mega breach moniker is further substantiated when comparing Figures 2 and 3, noting the significant drop in the number of breaches, yet a significant spike in the number of records breached.

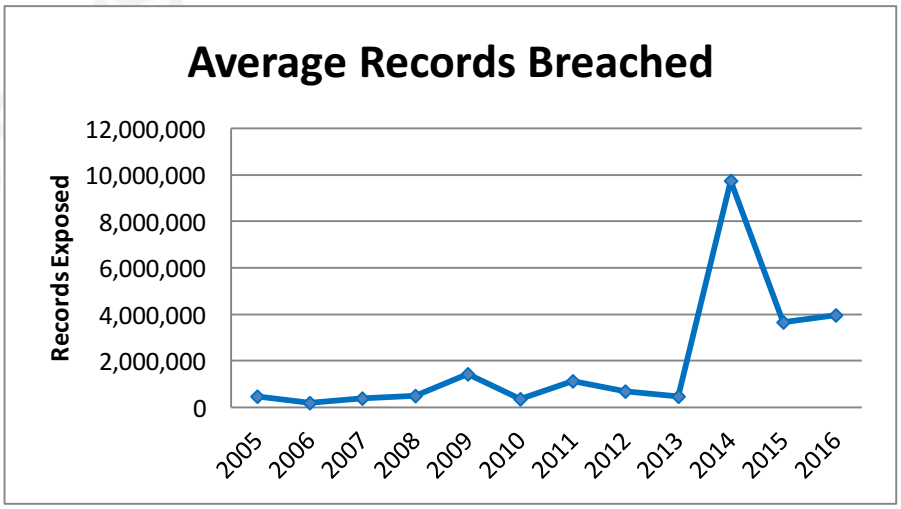


Figure 3: (Privacy Rights Clearinghouse)

Paul Hershberger, pjhersh13@gmail.com

It is important to note that the dataset used for this analysis included the 2014 data breach related to the central Russian hacking group in which over 1 billion user names and passwords were stolen over time. If that single event is removed from the data, the trend changes significantly and creates a more natural upward trend in records breached from 2013 to October 2016, as seen in Figure 4:

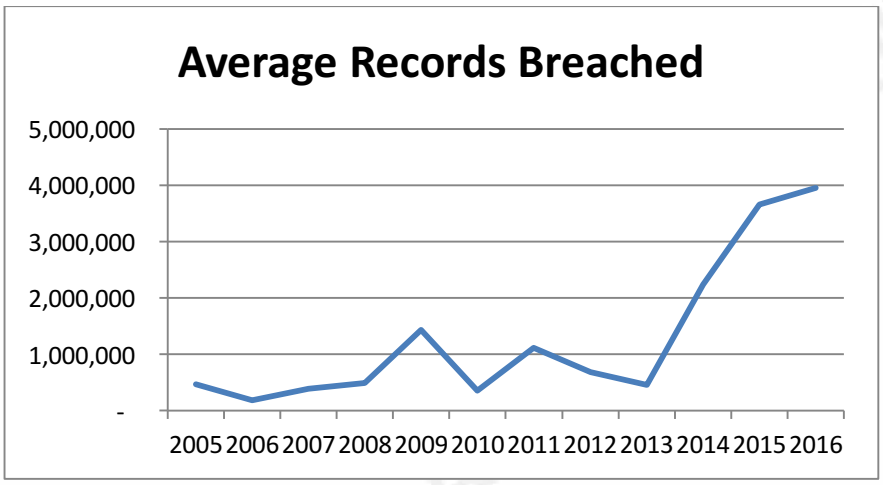


Figure 4: (Privacy Rights Clearinghouse)

Likewise, Figure 5 shows the sum of records breached by year. With the single Russian hack removed, the data shows a sharp upward trend from 2013 to 2016.

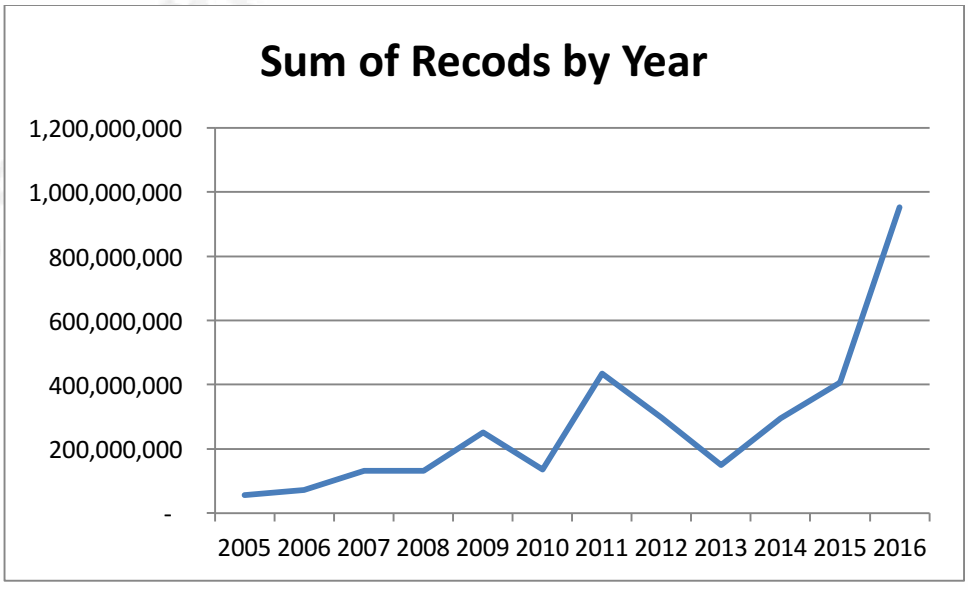
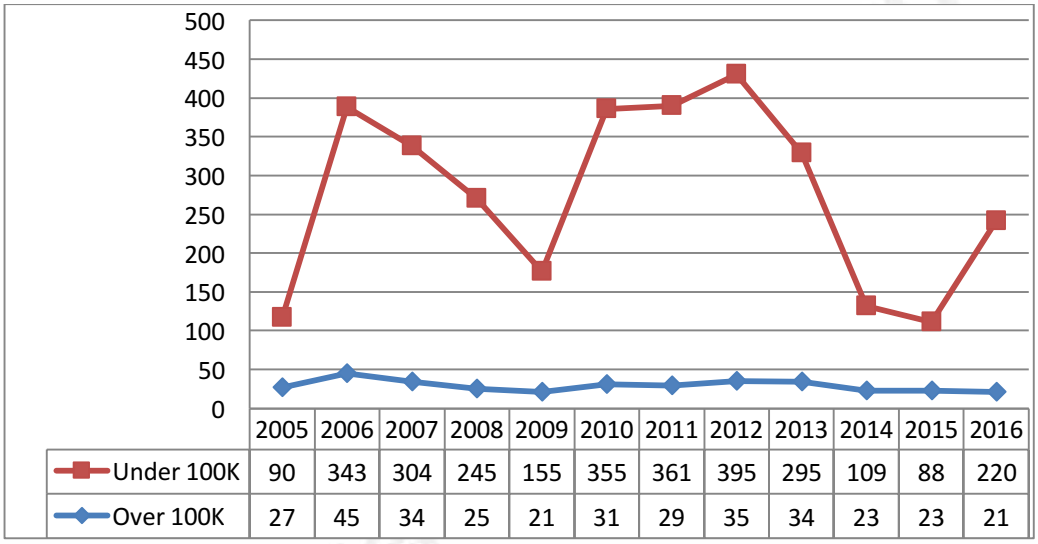


Figure 5: (Privacy Rights Clearinghouse)

Paul Hershberger, pjhersh13@gmail.com

Another important aspect of the dataset is the relative size of breaches. To understand the relative size of breaches within the dataset, the Ponemon threshold of 100,000 records breached is used as a divider. As seen in Figure 6, the dataset shows a significant difference in the count of breaches that exposed less than 100,000 records, versus those exposing more than that:



	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Under 100K	90	343	304	245	155	355	361	395	295	109	88	220
Over 100K	27	45	34	25	21	31	29	35	34	23	23	21

Figure 6: (Privacy Rights Clearinghouse)

With over 4 billion records exposed over more than 11 years, the risk of a data breach is one that organizations need to prepare for. When trying to manage the risk of a data breach, organizations try to place a monetary value on their potential exposure. The accuracy of the estimation continues to be limited due to the limited amount of data available to cover the wide range of data breaches across industries.

5. Testing the Models

The cost of a data breach is often discussed in the context of direct and indirect cost. These terms often take on different meanings depending on the context of the discussion. For the purpose of this paper, the direct cost will be discussed as encompassing the entirety of direct expense related to the breach. Direct cost includes both internal and external costs for the investigation, analysis

and remediation of the breach as well as the cost associated with external requirements such as credit monitoring, regulatory fines, and all cost associated with the litigation and settlement of all legal proceedings resulting from the breach. Indirect costs include factors such as lost revenue because of customer turnover and reduction in stock value. To ensure consistency in the information available, the analysis will focus on publicly traded companies only.

5.1. Direct Costs

The collection of direct costs associated with data breaches will originate primarily from Securities and Exchange Commission (SEC) reports filed by the company experiencing a breach. To provide consistency in use of the two models tested, the Ponemon cost per record will be used as published for the year in which the breach was announced. In leveraging the RAND model, total revenue for the breached company will be the total annual revenue as reported for the year in which the breach occurred. The Annual Revenue will be as filed in the company's respective SEC Form 10-K Annual Report under Section 13 or 15(d) of the Security Exchange Act of 1934. For this analysis, the number of records exposed in the breach is as reported in the Privacy Rights Clearinghouse dataset.

5.1.1. Target Corporation 2013 Breach

In late 2013, Target Corporation (Target) was the victim of a cyber-security attack in which approximately 70 million records were stolen by the attacker(s). As reported in their SEC Form 10-k for their fiscal year ending February 1, 2014, Target had an annual revenue of $72,596 million. At the time of the Target breach, the Ponemon Institute report concluded the cost of a data breach on average for a US-based company to be $201 per record compromised, further defined as $105 per record breached for retail companies worldwide (Ponemon Institute, 2014). Leveraging the US cost and the global retail cost measure provided by the Ponemon research, Target should have expected to incur between $7 and $14 billion. The Ponemon model would have represented costs between 10% and 19% of annual revenue. Conversely, if the RAND model is taken into consideration, Target should

have expected to incur approximately $290 million or roughly $4.15 per record breached of the 0.4% of the annual revenue.

In their SEC Form 10-K for the Fiscal Year ending January 30, 2016, Target summarized their cumulative expenses recorded as a result of the 2013 data breach to be $291 million (Target Corporation, 2016). The reported costs represent 0.4% of Target's annual revenue in the year in which the breach occurred, or just $4.16 per record breached. The cost per record realized by Target was $197 less than the US based company average and $101 less than the global retail company average as defined by the Ponemon model. The deviation from the Ponemon average costs aligns with the assertion that their cost per record is not applicable to "mega breaches". The reported costs represented a percentage of annual revenue consistent with the RAND model, indicating the model can apply to "mega breaches".

5.1.2. Home Depot 2014 Breach

In September 2014, Home Depot confirmed reports of a data breach across stores in the US and Canada in which approximately 56 million records were stolen by attackers. As reported in their SEC Form 10-K for their fiscal year ending February 1, 2015, Home Depot reported an annual revenue of $83,176 million (Home Depot Inc., 2015). At the time of the Home Depot breach, the Ponemon Institute research recorded the cost of a data breach on average for a US based company to be $217 per record compromised, further defined as $165 per record breached for retail companies worldwide. Leveraging the US cost and the global retail cost measure provided by the Ponemon research, Home Depot should have expected to incur between $9 and $12 billion in cost. The Ponemon model would have represented costs between 11% and 15% of annual revenue. Conversely, if we take into consideration, the RAND model of 0.4% of annual revenue, Home Depot should have expected to incur approximately $333 million or approximately $5.94 per record breached.

In their SEC Form 10-K for the fiscal year ending January 31, 2016, Home Depot summarized their cumulative expenses recorded because of the 2014 data breach to be $261 million (Home Depot, 2016). The reported costs represent 0.31% of annual Home Depot revenue in the year in which the breach occurred, or just $4.66 per record

breached. The cost per record realized by Home Depot was $212 less than the US based company average and $160 less than the global retail company average as defined by the Ponemon model. The deviation from the Ponemon average costs aligns with the assertion that their cost per record is not applicable to "mega breaches". The reported costs represented a percentage of annual revenue 0.09% less than the RAND model would estimate, indicating the model can apply to "mega breaches".

5.1.3. Neiman Marcus 2014 Breach

In January of 2014, Neiman Marcus confirmed that they had suffered a data breach in which approximately 1million records were stolen by the attacker(s). According to their SEC Form 10-K for their fiscal year ending August 2, 2014, Neiman Marcus reported an annual revenue of $4,839 million (Neiman Marcus, 2014). At the time of the Neiman Marcus breach, the Ponemon Institute research recorded the cost of a data breach for a US based company to be on average $217 per record compromised, further defined as $165 per record breached for retail companies worldwide. Applying those cost measures to the breach, Neiman Marcus should have expected to incur between $165 and $217 million of cost related to the breach. The Ponemon model would have represented costs between 3% and 4% of annual revenue respectively. Conversely, if we take into consideration the RAND model and estimate based on 0.4% of annual revenue, the cost is estimated at $19.4 million or $19.36 per record compromised.

In their SEC Form 10-K for the years ending August 3, 2014, August 1, 2015 and July 30, 2016, Neiman Marcus reported expenses associated with the data breach to be $12.6 million, $4.1 million and $1 million, respectively (Neiman Marcus, 2014, 2015, 2016). The individual reports show a cumulative total of $17.7 million in direct costs associated with the 2014 breach. The reported costs represent 0.37% of Neiman Marcus' annual revenue at the time of the breach or a cost of $17.70 per record exposed. The cost per record realized by Neiman Marcus was $212 less than the US based company average and $160 less than the global retail company average as defined by the Ponemon model. The deviation from the Ponemon average costs aligns with the assertion that their cost per record is not applicable to "mega breaches". The deviation from the Ponemon average

costs aligns with the assertion that their cost per record is not applicable to "mega breaches". The reported costs represented a percentage of annual revenue 0.03% less than the RAND model, indicating the model can apply to "mega breaches".

5.1.4. Sally Beauty Supply 2014 and 2015 Breaches

In March of 2014 and May of 2015, Sally Beauty Supply was the victim of two cybersecurity attacks in which some records were exposed (Sally Beauty Holdings Inc., 2014, 2015). According to the Privacy Rights Clearinghouse data, the 2014 breach exposed 25,000 records while the 2015 breach exposed an unknown number of records (Privacy Rights Clearing House, 2016). In comparing the cost models, some assumptions can be made about the nature of the 2015 breach compared to the 2014 breach at Sally Beauty. In their SEC Form 10-Q filed August 4, 2016, Sally Beauty discussed the two security incidents and recorded an accrued liability of $2.9 million and $0.9 million related to loss contingencies associated with the 2014 and 2015 breaches respectively (Sally beauty Holdings Inc., 2016). Using the combined accrual amounts, the 2015 contingency represents approximately 31% of the 2014 contingency. Assuming the contingency correlates directly to some records exposed, the 2015 breach, at 31% of the 2014 breach, represents 7,759 records exposed. Because of the relatively short duration between the two breaches, this analysis will combine the record counts and costs into one breach total representing the 2014 and 2015 breach events in total. Collectively, and based on the assumptions previously outlined, the Sally Beauty breach exposed an estimated 32,759 records. Combining costs reported by Sally Beauty Holdings Inc. in their Fiscal Year 2015 annual report, (Sally Beauty Holdings Inc., 2015) along with the costs reported in their Quarterly report for the period ending 6/30/16, (Sally beauty Holdings Inc., 2016) the total costs of the breaches are reported to be $10.7 million, as shown in Table 1.

	Form 10-K 8/30/15	Form 10-Q 6/30/16	Total
2014 Breach	$ 5.4	$ -	$ 5.4
2015 Breach	$ 2.7	$ 2.6	$ 5.3
Cumulative	$ 8.1	$ 2.6	$ 10.7

Table 1 (Sally Beauty Holdings Inc.)

Using the 2015 annual revenue reported by Sally Beauty Holding, Inc, Sally Beauty Supply recorded an annual revenue of $2,330 million (Sally Beauty Holdings

Inc., 2015). At the time of the 2015 breach, the Ponemon Institute research recorded the cost of a data breach to be on average for a US based company $221 per record breached with a more specific $172 pre-record breached for retail companies worldwide. Applying those cost measures to the breach, Sally Beauty Supply should have expected to incur between $5.6 and $7.2 million of cost related to the breach. The Ponemon model would have represented costs totaling 0.24% and 0.31% of annual revenue. Conversely, considering the RAND model and estimate based on 0.4% of annual revenue, the costs would have been estimated at $9.3 million or $284 per record compromised. The reported cost of the breaches to Sally Beauty Supply was $10.7 million, 0.46% of 2015 annual revenue and $326 per record. The cost per record realized by Sally Beauty Holdings, Inc. was $63 more than the US based company average and $112 more than the global retail company average as defined by the Ponemon model. Although the size of the Sally Beauty breach was within the range in which the Ponemon model applies, the actual costs deviated substantially from what the model would have predicted. The reported costs represented a percentage of annual revenue 0.06% greater than the RAND model, indicating that the RAND model can apply to smaller breaches as well as the "mega breaches" as previously shown.

5.2. Direct Cost Summary

Having reviewed the direct cost associated with the select breaches of organizations in the retail industry against the Ponemon Institute and the RAND Corporation's data breach cost research models, it can be concluded that the RAND model of estimation based on the organization's annual revenue is more consistently aligned with the actual direct costs realized by companies who experience data breaches. Although the Ponemon Institute model shows to be ineffective as a means of estimating large data breaches, the analysts have consistently stated that their estimates should not be used to estimate breaches referred to as "mega breaches" such as the Target and Home Depot breaches. When estimating the potential direct costs to an organization, the RAND model appears to be more effective at scaling with the organization and the size of data breaches. Given the ability to scale, the RAND model appears to be a more effective way of estimating the potential impact of a data breach to an organization.

5.3. Indirect costs

Although direct costs can be easier to estimate and project, the indirect costs associated with customer turnover and investor confidence is another area in which risk assessments should consider the total potential impact on an organization. The Ponemon Institute research discusses abnormal churn, and in the 2016 report, noted an average 2.1% churn rate as a result of a data breach for the retail industry (Ponemon Institute, 2016). The research conducted by Romanosky of the RAND Corporation concluded that 11% of customers are lost due to a data breach (Romanosky, 2016). The loss of customers, (resulting in lost revenue) and investor confidence (resulting in lost market value) are two significant factors that must be considered when estimating the cost of a potential data breach. To evaluate the indirect cost of a data breach, leveraging the previously discussed companies, revenue, same-store sales, and stock price as a means of understanding the indirect impact on the organization will be analyzed.

5.3.1. Target

As shown in Figure 7, in the two years leading to the late 2013 data breach, Target's stock performance trended very close to the Standard and Poor's 500 index fund (S&P 500) as well as their main competitor's, Wal-Mart (WMT) (Google Finance, 2016). In the second half of 2013, leading up to the breach, Target (TGT) began to trend lower than WMT and the S&P 500. Although the stock was remaining consistent with the trend

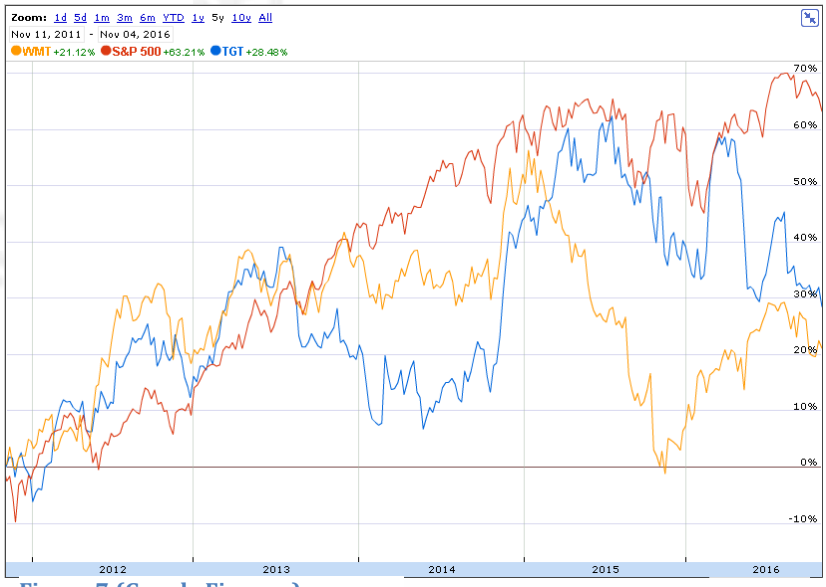


Figure 7 (Google Finance)

of both comparable, TGT began to experience steeper drops and hit lower valleys than both WMT and the S&P 500. Once TGT dropped below WMT and the S&P 500, TGT continued to follow trend lines, however at a lower performance level through the breach announcement and the majority of 2014. Through 2014, TGT and WMT followed a similar trend and deviated more significantly from the S&P 500. In late 2014 and into early 2015, TGT began to diverge from WMT and trend significantly higher, following along with the S&P 500. From 2015 and 2016 to date, TGT has followed the S&P 500 and outperformed WMT as demonstrated in Figure 7:

Looking at stock performance around the time Target confirmed the breach (see Figure 8), TGT initially experienced a slight downward movement, but nothing significant until early January 2014. The most significant drop in TGT price came on January 10, 2014, which corresponds with a press release in which the breach report was updated to cover over 70 million records and their fourth quarter 2013 guidance was revised downward, attributing a projected "meaningfully weaker-than-expected sales since the announcement," (Target Corporation, 2014). The drop was followed by an equally dramatic spike in TGT performance, 11 days later.

Figure 8 (Google Finance)

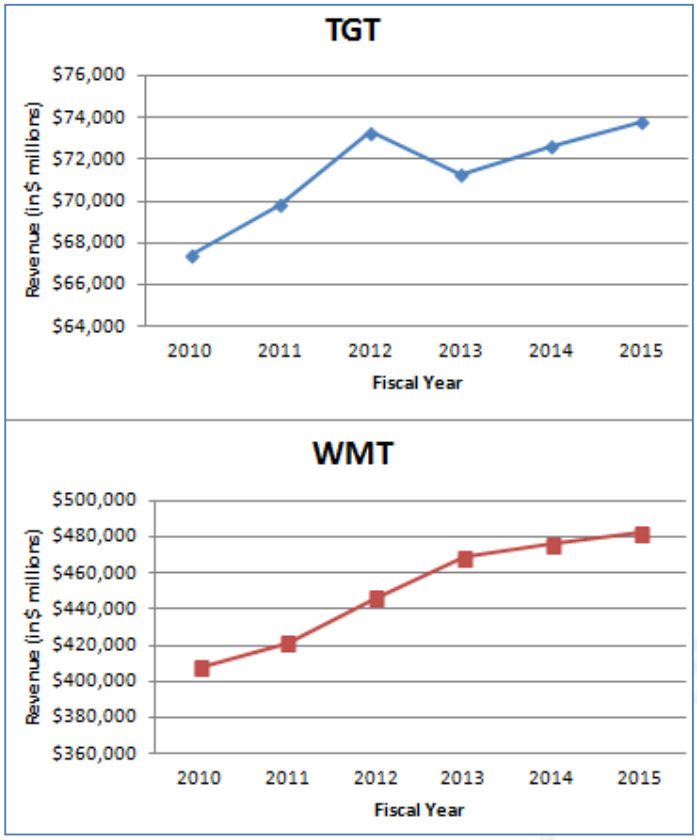


Figure 9 (Google Finance)

As seen in Figure 9, TGT experienced a drop in annual revenue for the year in which the breach occurred and returned to a relatively normal revenue trend from there. In comparison, WMT maintained a steady revenue trend over that same five year period. In their SEC Form 10-K covering the fiscal year 2013 Target stated:

"We believe the Data Breach adversely affected our fourth quarter U.S. Segment sales. Before our December 19, 2013, announcement of the Data Breach, our U.S. Segment fourth quarter comparable sales were positive, followed by meaningfully negative comparable sales results following the announcement. Comparable sales began to recover in January 2014. The collective interaction of year-over-year changes in the retail calendar (*e.g.*, the number of days between Thanksgiving and Christmas), combined with the broad array of competitive, consumer behavioral and weather factors makes any quantification of the precise impact of the Data Breach on sales infeasible" (p. 18).

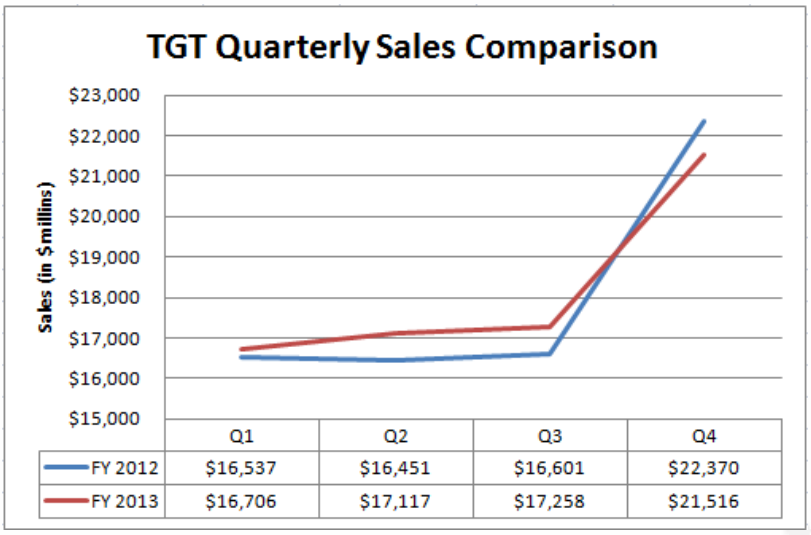


Figure 10 (Target SEC Form 10-K)

As Target indicated, the direct attribution of the decline in sales to the data breach is difficult to prove; however, the timing of the breach was such that Target was at the height of the 2013 holiday season, a significant period important, and for some retailers, crucial to its annual revenue. Regardless, there is an acknowledgment by Target that sales showed a meaningful negative shift after they announced the breach; however, that shift reportedly only lasted a short period. Furthermore, if compare the quarterly sales (see figure 10) for TGT in the fiscal year 2013 as compared to the fiscal year 2012, we see a similar upward trend in Q4.However, the trend is slowed and results were negative in comparison. The 2012 comparison between Q3 and Q4 sales showed an increase of 26%, while the 2013 Q3 to Q4 sales only increased at a 20% rate. If we take into consideration the trend between 2012 and 2013, there was close to a 4% increase in sales starting in Q2 if that trend had remained, the Q4 2013 results should have been approximate $22,435 million, as compared to the reported $21,516 million. As TGT stated, the negative sales trend in Q4 can be attributed to various factors; however, if only 10% of lost sales is attributed to the data breach, then the loss would be approximately $91 million in lost sales alone.

5.3.2. Home Depot

As seen in Figure 11 below, in the years leading up to the 2014 data breach, Home Depot's (HD) stock trended very tightly with their main competitor Lowes (LOW), with both stocks remaining significantly above the performance of the S&P 500 (S&P) (Google, 2016). Late in 2014, HD began to converge with and then began performing below LOW; this trend continued through early 2015 until HD reversed the trend and returned to outperforming LOW, as was the norm before 2014.

Figure 11 (Google Finance)

As seen in Figures 12 and 13, the downward trend in late 2014 began in August with a sustained downward trend through early September, rebounding shortly after the time in which HD confirmed that they had suffered an attack that resulted in a data breach. The HD stock continued to perform generally above LOW, although following a much flatter trend line. With HD maintaining a relatively flat trend line through late 2014 they began to under- perform as compared to LOW in November 2014.

Figure 12 (Google Finance)

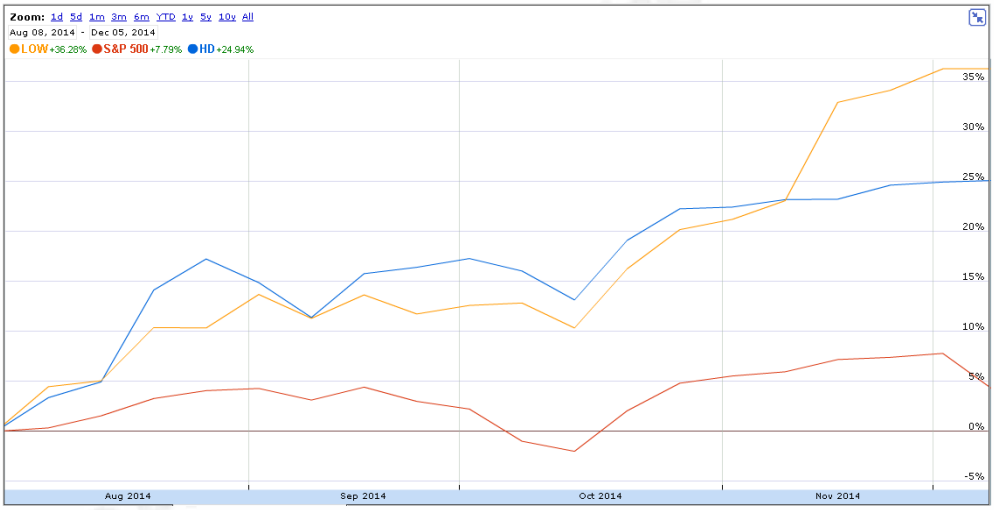


Figure 13 (Google Finance)

As seen in Figure 14 above, HD showed no indication of revenue impact and continued a positive trend in revenue growth year over year, continuing to outperform LOW.

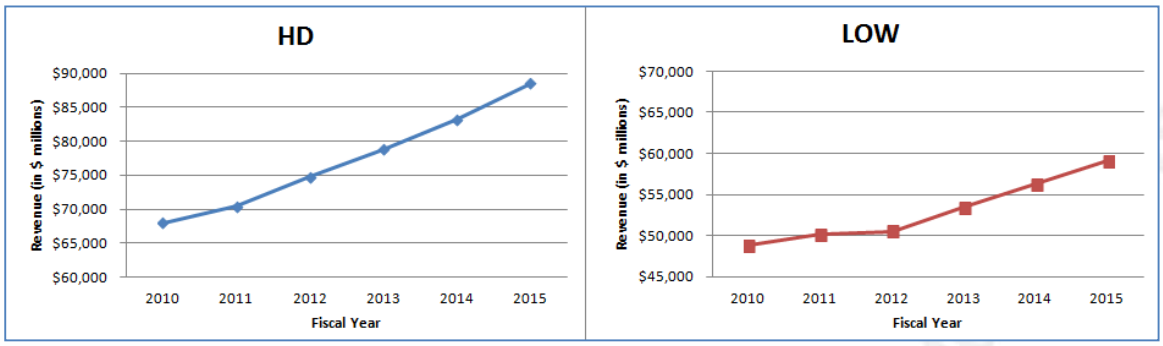


Figure 14(SEC Form 10K)

Although annual revenue continued to sustain an upward trend for HD, as seen in Figure 15, quarterly revenue for their fiscal year 2014 showed a significant shift in Q4 revenue. During the fiscal year, 2014 HD trended consistently with revenue growth quarter over quarter, through the first three-quarters. In the fiscal year 2013, the company's Q4 results demonstrated a 1% growth over Q3. Conversely, in the fiscal year 2014, their results reflected a -10% decline in Q4 as compared to Q3. Had their fiscal year 2014 Q4 revenue followed the fiscal year 2013 trend, HD should have reported the fiscal year 2014 Q4 revenue of $21,417 million, as compared to the actual report of $17,696 million. Although a multitude of factors can impact revenue, if 10% of the impact were related to the data breach, that would still represent approximately $372 million in lost revenue. That estimated lost revenue would be included in the indirect costs associated with the breach and included in the total impact to Home Depot.

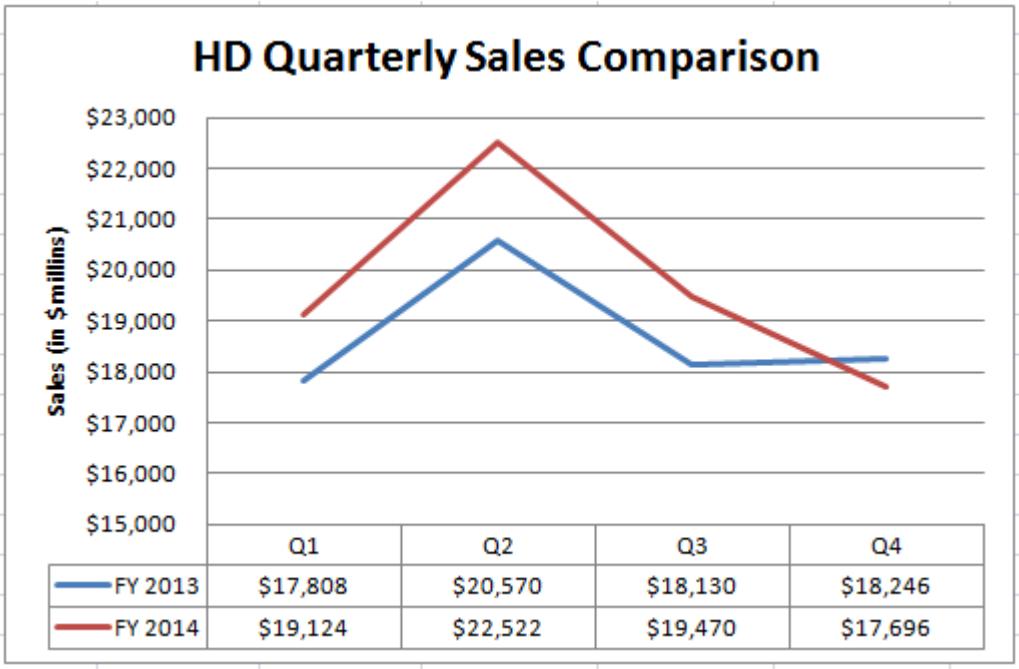


Figure 15 (Home Depot SEC Form 10K)

5.3.3. Neiman Marcus

Neiman Marcus is a wholly owned subsidiary of the Neiman Marcus Group, a private company headquartered in Dallas, Texas that focuses on the luxury retail market (Neiman Marcus Group, 2016). Although Neiman Marcus group files annual reports with the SEC, they are not a publicly traded company and accordingly, there is no stock information to compare. Instead of stock information regarding the company's revenue and trend over time will be provided (Neiman Marcus Group, 2016). As seen in

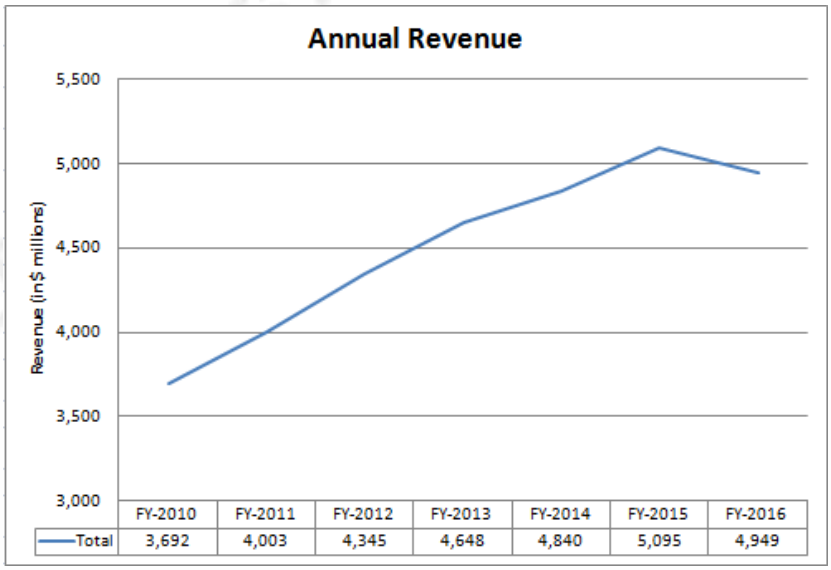


Figure 16 (Neiman Marcus SEC Form 10-K)

Figure 16, Neiman Marcus showed a relatively normal, upward trend in annual revenue over time leading up to and after its 2014 breach, with declining revenue well after the time of the breach.

As seen in Figure 17, Neiman Marcus maintained a consistent trend of quarterly revenue through Q3 of the fiscal year 2014 as compared to 2013. Using the fiscal year 2013 trend Neiman Marcus should have recorded a positive 2% growth in revenue in Q4 2014 as opposed to the -5% or $1,398 million compared to the reported $1,113 million. If we assume 10% of that difference is attributed to the data breach, that represents approximately $29 million in lost revenue.

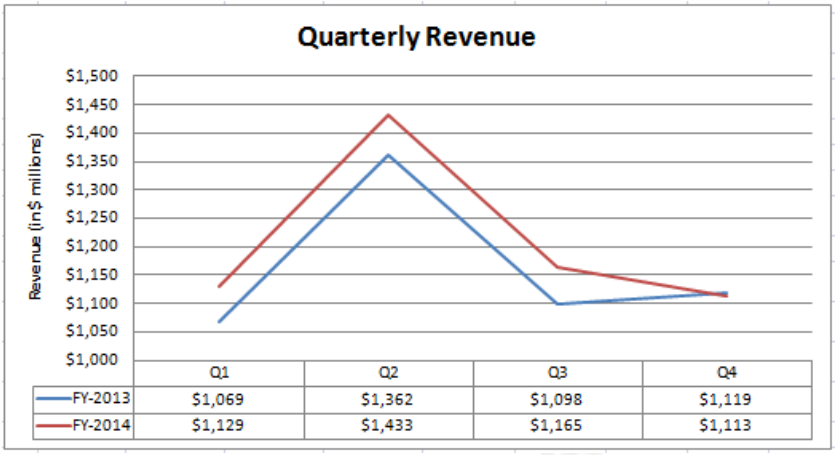


Figure 17(Neiman Marcus SEC Form 10-K)

5.3.4. Sally Beauty Holding, Inc.

As seen in Figure 18, Sally Beauty Holding, Inc.(SBH) trended consistently with the S&P 500, along with their competitor, Ulta Salon, Cosmetics & Fragrance, Inc. (ULTA) with periods of divergence throughout 2013. In mid-2014, SBH continued a relatively flat trend in line with the S&P 500, while ULTA shifted significantly upward.

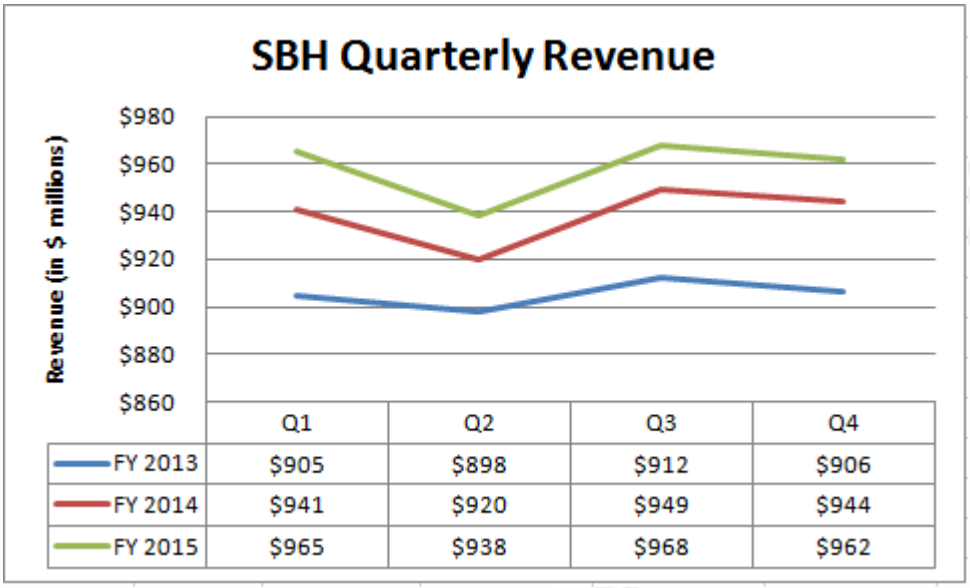
Figure 18 (Google Finance)

Throughout the time of breach notifications by SBH, its stock performed relatively flat with only a small downward deviation from the S&P 500(see figure 19). The deviation noted could not be directly attributed to any specific cause.

Figure 19 (Google Finance)

Because SBH experienced two consecutive breaches covering 2014 and 2015 we will look at the three-year trend of quarterly revenue. The trends are consistent across the - three-year period, with the only significant deviation being the improved performance in

Q4 2015 during which SBH reported a slight increase in revenue, as opposed to the annual trend of a slight decrease in revenue during Q4.



	Q1	Q2	Q3	Q4
FY 2013	$905	$898	$912	$906
FY 2014	$941	$920	$949	$944
FY 2015	$965	$938	$968	$962

Figure 20 (Sally Beauty Holdings Inc. SEC Form 10-K)

5.4. Indirect Cost Summary

Having reviewed the indirect costs associated with the select breaches of organizations in the retail industry, focusing on the stock performance and revenue over time, as well as around the time of the breach, we can conclude there is some impact. However, that impact is not always as significant or transparent as initially thought. With the exception of Sally Beauty Holdings, Inc., each organization showed at least some level of impact on revenue around the time of the breach. The direct attribution of the decline in sales is difficult, however; it can be reasonably inferred that the data breach events had at least an amplifying impact on the cumulative conditions that contributed to the decline in revenue. From the stock performance perspective, although there were signs of increased volatility in two of the three publicly traded companies, the timing of the negative stock performance may be more directly correlated to the impact on revenue than any other factor. In the case of Sally Beauty Holding, Inc., there was no significant deviation in revenue and, likewise, little deviation in stock performance over time. It's important to note that, although there was an indication of significant indirect costs in the

form of lost revenue on a quarterly basis, the trend was isolated and, in general, had very little impact on annual revenue trends over time.

6. Conclusion

A key element of risk management is the ability to effectively estimate the potential impact of risk to the organization; the risk of a data breach being one of those risks that retailers have come to focus on heavily in recent years. With few options available to auditors to estimate that risk, the Ponemon Institute annual report on the cost of a data breach often becomes the default measure of a data breach. Although the Ponemon Institute's research provides a significant amount of value to the community, the scope and clearly defined limitations of the research can lead to misstatements in the actual risk to the organization. Sasha Romanosky of the RAND Corporation recently published research that provides auditors another option for estimating those costs. Unlike the Ponemon model, the RAND model shows to be more effective for scaling across a wide range of data breach sizes. As seen in Table 2, combining the two costs associated with the potential impact of a data breach resulted in a range between 0.4% and 0.9% of annual revenue.

	Direct Cost	Indirect Cost	Total	% of Revenue
Target	$ 291,000,000	$ 91,000,000	$ 382,000,000	0.53%
Home Depot	$ 261,000,000	$ 372,000,000	$ 633,000,000	0.76%
Neiman Marcus	$ 17,700,000	$ 29,000,000	$ 46,700,000	0.97%
Sally Beauty Holding Inc.	$ 10,700,000	$ -	$ 10,700,000	0.46%

Table 2 (Cost Analysis Summary)

Effectively estimating the potential impact of a data breach is important to ensure auditors and executive management focus on managing risk to the organization based on potential impact to the organization. The RAND model provides an approach to impact estimation that is more effective than the Ponemon model in estimating potential impact of breaches of different sizes. The potential advantage of the RAND model is the correlation between the size of the organization, as it relates to annual revenue, to the potential cost of a breach. As indicated by this research, the limitations defined in the Ponemon research can artificially elevate the monetary implications of a data breach.

Paul Hershberger, pjhersh13@gmail.com

However, the RAND model appears to be more effective in estimating the potential impact of a data breach. The Ponemon model has served as the default standard for data breach cost estimation; however, the defined limitations of the model can provide an inaccurate estimate of risk. The potential inaccuracy of the impact estimation can lead to a misalignment of risk mitigation priorities senior leaders when assessing the various risks corporations face. Auditors face the challenge of estimating the impact of risks they document. The auditor should focus on effective strategies and models to estimate potential impacts to the organization. Through effective risk estimation, auditors can provide leadership an accurate assessment of risk and help align critical resources where they are most effective to the goals of the organization.

References

Advisen. (2016). *About*. Retrieved October 25, 2016, from Advisenltd: http://www.advisenltd.com/about/

Advisen. (n.d.). *Cyber Risk Datra Methodology for Insurance & Risk Analysis.* New York: Advisen.

Google. (2016 йил 3-October). *Google Finance*. Retrieved 2016 йил 3-October from Googel Finance: https://www.google.com/finance?chdnp=1&chdd=1&chds=1&chdv=0&chvs=Linear&chdeh=0&chfdeh=0&chdet=1478361861370&chddm=1173&chls=IntervalBasedLine&cmpto=INDEXSP%3A.INX%3BNYSE%3ALOW&cmptdms=0%3B0&q=NYSE%3AHD&ntsp=1&fct=big&ei=BAMeWLj5CYXcjAG0m424CQ&authuser=0

Google Finance. (2016, November 3). *Google Finance*. Retrieved November 3, 2016, from Google: https://www.google.com/finance?q=NYSE%3ATGT&ei=A7scWICCKcanjAGW4aXoDA

Home Depot. (2016). *United States Security Exchange Commission Form 10-K.* Atlanta: The Home Depot, Inc.

Home Depot Inc. (2015). *United States Security Exchange Commission Form 10-K.* Atlanta: Home Depot.

Neiman Marcus. (2014). *United States Security and Exchange Commission Form 10-K.* Dallas: Neiman Marcus.

Neiman Marcus. (2014). *United States Security and Exchange Commission Form 10-K.* Dallas: Neiman Marcus.

Neiman Marcus. (2015). *United States Security and Exchange Commission Form 10-K.* Dallas: Neiman Marcus.

Neiman Marcus. (2016). *United States Security and Exchange Commission Form 10-K.* Dallas: Neiman Marcus.

Neiman Marcus Group. (2016 йил N.D.). *Investor Relations*. Retrieved 2016 йил 3-November from Neiman Marcus Group: http://phx.corporate-ir.net/phoenix.zhtml?c=118113&p=irol-homeProfile&t=&id=&

Neiman Marcus Group. (2016 йил 2-November). *Investor Relations*. From Neiman Marcus Group: http://phx.corporate-ir.net/phoenix.zhtml?c=118113&p=irol-monthly2014

NIST. (2012, September). Special Publicaiton 800-30 Revision 1. Gaithersburg, Md. Retrieved Octover 21, 2016, from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Ponemon Institute. (2014). *2014 Cost of Data Breach Study: Global Analysis.* Ponemon Institute. Retrieved from https://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf

Ponemon Institute. (2016). *2016 Cost of Data Breach Study: Global Analysis.* The Ponemon Institute.

Paul Hershberger, pjhersh13@gmail.com

Privacy Rights Clearing House. (2016). *Data Breaches*. Retrieved October 20, 2016, from Privacy Rights Clearing House: https://www.privacyrights.org/data-breaches

Romanosky, S. (2016). *Examining the costs and causes of cyber incidents.* RAND Coproration. Oxford University Press. Retrieved October 21, 2016, from http://cybersecurity.oxfordjournals.org/content/early/2016/08/08/cybsec.tyw001

Sally Beauty Holdings Inc. (2014, March 5). *Sally Beauty Holdings Statement.* Retrieved November 3, 2016, from Sally Beauty Holdings, Inc.: http://investor.sallybeautyholdings.com/investor-relations/press-releases/2014/03-05-2014-014510832

Sally Beauty Holdings Inc. (2015, May 4). *Sally Beauty Holdings, Inc. Statement.* Retrieved November 3, 2016, from Sally Beauty Holdings, Inc.: http://investor.sallybeautyholdings.com/investor-relations/press-releases/2015/05-04-2015-014508867

Sally Beauty Holdings Inc. (2015). *United States Securities and Exchange Commission Form 10-K.* Denton: Sally Beauty Holdings, Inc.

Sally beauty Holdings Inc. (2016). *United States Securities and Exchange Commision Form 10-Q.* Denton: Sally Beauty Holdings, Inc.

Target Corporation. (2014 йил 12-January). *Target Bullseye View*. Retrieved 2016 йил 3-November from Target Provides Update on Data Breach and Financial Performance: https://corporate.target.com/press/releases/2014/01/target-provides-update-on-data-breach-and-financia

Target Corporation. (2014). *United States Securities and Exchange Commission Form 10-K.* Minneapolis: Target Corporation.

Target Corporation. (2016). *Uniteed States Security Exchange Commission Form 10-K.* Minneapolis.

The Ponemon Institute. (2016). *About Ponemon*. Retrieved October 21, 2016, from Ponemon Institute: http://www.ponemon.org/about-ponemon

Paul Hershberger, pjhersh13@gmail.com

Last Updated: June 26th, 2017

Upcoming Training

SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS AUD507 (GSNA) @ Canberra 2017	**Canberra, Australia**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**