https://doi.org/10.48009/3_iis_2019_165-174

Issues in Information Systems
Volume 20, Issue 3, pp. 165-174, 2019

STRATEGIC MARKETING AND CYBERSECURITY: THE CASE OF DATA BREACHES

George Kirk, Southern University and A&M College, george_kirk@subr.edu
Jose Noguera, Southern University and A&M College, jose_noguera@subr.edu

ABSTRACT

Data breaches can have a negative effect on the market value of the breached firm. Numerous studies examining the impact of a data breach on the market value of the firm have suggested that market value impact is moderated by a firm's reputation and customer attributions as to who is to blame for the data breach. While market value is essential, the ability of a firm to recover from a data breach is primarily influenced by the reaction of the firm's customers. This research proposes a model comprised of proactive marketing activities based on the SERVQUAL model that a firm can undertake before a data breach to increase firm reputation, firm trust and subsequently brand equity and brand loyalty that has the potential to increase the likelihood of positive attributions should a data breach occur. The model also offers strategic marketing activities that can be undertaken after a data breach to speed a firm's recovery.

Keywords: Marketing, Cybersecurity, SERVQUAL Model, Brand Equity, Brand Loyalty, Data Breach, Attribution Theory

INTRODUCTION

Marketing is a vital business function that is often underutilized when a firm suffers a data breach. Data breaches are impacting a wide variety of companies across a wide range of industries, states, nations, and individuals (Udo, Bagchi and Kirs, 2018). Much focus has been given on how to protect data held by an organization and how to best proceed once a data breach has occurred. Extent research usually focuses on recovery efforts, liability issues and legally protecting the affected company and somewhat less on the consumer or client victims of the data breach. Traditional post data breach actions often leave effected customers slightly cold and perhaps offended. As such, the company affected by a data breach may be doing more damage in terms of their relationship with their customers or clients. Given that market value is driven in part by the success of the firm and their products or services, several authors have suggested that marketing take a more active and prominent role both pre-data breach and post-data breach should a data breach occur.

The American Marketing Association (AMA) ,defines marketing as "the activity, set of institutions, and processes for creating, communicating, delivering, and exchanging offerings that have value for customers, clients, partners, and society at large" (https://www.ama.org/the-definition-of-marketing/). As indicated by definition, a significant activity of marketing is communication with and creating value for firms. Despite the importance of marketing, frequently marketing is not involved when data breaches occur. This paper will provide an overview of the marketing elements associated with an organization and how they interact with a data breach should one occur. In addition, we propose a framework for examining service marketing under a data breach event based on the SERVQUAL model.

THE IMPACT OF DATA BREACHES

Data breaches are costly both in terms of market value and in terms of the future of the business venture that has been breached. The financial impact of a data breach includes both immediate impacts as well as longer-term impacts, each of which may impede a firm's ability to recover from a data breach. Direct financial impact includes the costs of the breach—customer/client restitution, payment service restitution, credit monitoring for customers impacted by the breach, legal liabilities and shareholder reaction, e.g., shareholders selling stock and lowering the market value of the firm. Longer-term impacts refer to the effects of the breach on damage to corporate image/reputation, damage to the brand, loss of trust, potential loss of customers loss of brand trust and loss of brand loyalty to name but a few. As

such, Longer-term impact is harder to assess due to the intangible nature of the concepts involved. The next section of this paper will explore the direct financial and market impacts of a data breach.

Financial Impacts

By far, the financial impact of data breaches is the most studied impact associated with data breaches. Most of these studies have focused on the market value of the firm. Market value refers to the amount of money one is willing to pay for a given asset. Often, when a data breach occurs, investors fear that the company may suffer financial losses and some shareholders may react by selling their shares of stock. Cumulatively, such actions may lower the price of the stock, thus decreasing the market value of the firm. Numerous authors have examined factors that can moderate or mediate the effect of a data breach on market value. Gwebu, Wang, and Wang (2018) examined the role of corporate reputation on data breach recovery. Gwebu, et. al., found that companies that enjoyed higher levels of corporate reputation tend to recover better after a data breach has occurred than did companies with lesser corporate reputation and image Rasoulian, Grégoire, Legoux and Sénécal (2017) examined the impact of a data breach recovery strategies on shareholder's idiosyncratic risk—unsystematic risk associated with a particular stock. Of three common recovery strategies that they examined—apology, compensation and information system improvement, the apology had a negative impact on idiosyncratic risk while compensation and information system improvement yielded better results. There are measures that firms can take to help to speed recovery. In an examination of the Sony PlayStation breach, Goode, Hoehle, Hartmut, Venkatesh, and Brown (2017), also found that compensation can be a viable means to speed recovery from a data breach if customer expectations regarding compensation are met. The authors also found that not meeting customers compensation expectations can have a negative effect on customer repurchase intentions.

Market value can be negatively impacted even when a firm has not suffered a data breach. Kashmiri, Nicol, and Hsu (2017), found that in the retailer environment after a data breach has occurred, other non-breached retail firms feel adverse effects. Martin, Borah, and Palmatier (2017) also found evidence of what they called a spillover effect in which a data breach on one firm negatively impacted other firms. For the most part, their discussion of corporate reputation was limited to the perspective of the shareholders of the company and did not consider customer or client perceptions of the company pre or post data breach. While market value is essential, it is by no means the only financial impact created by lapses in cybersecurity. If a firm is to recover from a data breach, it is vital the consumers continue to do business with the firm.

Data breaches can have dramatic negative impacts on a firm's market value. The key question is, do breached firms have the ability to recover from a reduction in market value? Market value is impacted by many factors including but not limited to financial performance—profitability, market share, competitive position and demand for the firm's products to name but a few. A firms ability to recover from a data breach is strongly influenced by the firm's ability to recover their financial performance, and the firm's marketing function mostly affects it.

Marketing Impacts

For the most part, data breach recovery research has focused on shareholder reaction (Janakiraman, Lim and Rishika, 2018). Consumer/customer/client reaction can also play a significant role in breach recovery; indeed, in the long-term viability of a firm. Data breaches can also cause financial harm to the marketing aspects of the firm.

The concept of a brand is a vital factor in the success of any company or organization. A brand uniquely identifies a business and as such customers know what to buy and just as importantly what not to buy. Companies work very carefully and invest considerable financial resources in establishing, maintaining and protecting their brand.

Selines (1998) defines brand reputation as the customers' perception of the quality associated with the brand. Thus, brands that consumers perceive as being of higher quality enjoy higher levels of brand reputation. Sengupta, Balaji, and Krishnan (2015) found that brand reputation moderates both consumer coping strategies and behavioral intentions—firms that enjoy higher levels of brand reputation among their customers enjoyed higher levels of behavioral intentions than did firms that suffered from lower levels of brand reputation.

Brand loyalty refers to the degree to which consumers form a preference for a brand and tend to use that brand exclusively for a given usage situation. Choong, Hutton, Richardson, and Rinaldo (2017) found that data breaches can cause a loss of trust, which in turn could harm brand loyalty. Wang and Park (2017) Wang and Johnson (2018)

suggest that effective communication with stakeholders is an integral part of a successful recovery. Frequently, however, it may take a breached firm a great deal of time to discover the breach and subsequently publicly announce that a data breach has occurred. The time between when the data breach occurred and was discovered by the breached company may cause customers to lose confidence in the brand. Once discovered, then the preparation of the announcement may take time. Ford, White, and White (2015) and Green and Martin (2016) discussed legal concerns regarding breach announcements, which vary by state. Generally, as with most legal affairs, the notification may seem cold and impersonal. It may also be the case that by the time a data breach is announced, a firm's customers may have already suffered ill effects from the data breach. In some cases, customers may be informed of the breach by a third party such as LifeLock, which could further erode customer trust and effect patronage decisions. Even if brand loyalty is retained, breached firms may suffer from a loss of patronage. Choong, Hutton, Richardson, and Rinaldo (2017) found that during the downtime created by a data breach, some customers may switch to a competitive product—creating a loss of business in the short term and perhaps a loss of customers who prefer the switched to brand over the original brand n the long-term.

Once a data breach has occurred, some customers or clients may be reluctant to do business with the breached firm. This reduction in business could be temporary or could be long-term. Janakiraman, Lim, and Rishika (2018) found that once a data breach had been announced, the breached firm suffered a reduction in consumer spending. Janakiraman, et al. (2018) also found that in the case of multichannel retailers, i.e., retailer firms that have two or more channels of distribution—e.g., brick-and-mortar and online—consumers may switch their patronage to the non-breached version of the business. While consumer's migrating to the firm's other channel helps multichannel retailers to maintain revenues, it can have a lasting impact on the breached channel of distribution. In the case of brick-and-mortar retailers, a loss of customers at the fixed location, even if the same customer continues to do business with the online version of the firm can result in difficulty with the firm covering the fixed overhead and may result in severe damage to the viability of that aspect of the business.

Taken together, the various impacts discussed above can have a devastating effect on brand equity. According to the AMA, Brand equity "is strategically crucial, but famously difficult to quantify. Many experts have developed tools to analyze this asset, but there is no universally accepted way to measure it. (https://marketing-dictionary.org/b/brand-equity/). Aaker (1991) developed the brand equity model. Aaker's model is comprised of brand loyalty, brand awareness, perceived quality and brand associations. Lai, Chiu, Yang, and Pai (2010) examined brand loyalty, perceived brand quality, brand awareness, brand satisfaction, corporate reputation and brand performance as key components of brand equity. Data breaches represent a significant threat to each if not all of the components of brand equity. Choong, Hutton, Richardson, and Rinaldo (2017) found that data breaches can cause a myriad of adverse effects related to marketing, namely loss of customers, loss of customer trust, loss of reputation for the breached firm, increased perception of risk and a reduction in brand equity.

While few, if any studies have examined the impact of data breaches on marketing variables, several other streams of research relating to product-harm and service failure, have examined how failures of these natures impact various marketing elements. In a meaningful sense, a data breach can be viewed as both product-harm and service failure. Bougoure, Russell-Bennett, Fazal-E-Hasan, and Mortimer (2016), found that how a service failure was handled impacted customer perceptions of brand credibility. In the case of a data breach, how the breach is dealt with will likely also influence customer perceptions of the brand credibility and potentially the customer's intention to do business with the breached company in the future. Brand trust is another factor that could be adversely impacted by a data breach. Brand trust is a critical factor in brand success. A data breach may cause customers to lose trust in a brand. This could be made worse by delays in announcing the data breach or if the consumer is notified by another means other than the company providing notification of the breach.

Product-harm research focuses on the damage done when a product causes harm to customers. Although not a faulty product, a data breach presents a significant form of product-harm. Product-harm research has shown that brand equity can be damaged by product-harm (Dawar and Pillutla 2000; Klein and Dawar 2004; Van Heerde, Helsen, and Dekimpe 2007). One consequence of damage to brand equity is a loss in purchase intention. Xie and Keh (2016), suggest that when product-harm occurs, retaining brand patronage is a major priority.

In an examination of self-service innovation failures, Liao and Cheng (2013) found that brands that enjoy higher levels of brand equity suffered less adverse effects of a service failure than do brands that have lower levels of brand equity. Liao et al., also found that brands with higher brand equity suffered worse than lower equity brands if customers attributed the failure to company factors. Whom customers blame for product failure or, a data breach can play a significant role.
In a study of service failure and repatronage decisions in the hospitality industry, Agarwal, Mehrotra, and Barger (2016) found that personality influenced the likelihood that customers would continue conduct business with a firm after a service failure. They identified four personality types including indifferent and self-critical, mixed-up, empathetic and intolerant. Customers that were high on empathy and low on intolerance were likely to continue patronage as they were less likely to place blame on the firm.

Many studies of data breaches and product/service failure include Attribution Theory (Heider, 1958) in their discussions. Attribution Theory examines how people assign a cause for events or circumstances (Fiske and Taylor, 1991). In the case of a data breach affected consumers may try to make attributions as to who is at fault for the data breach. If consumers feel that the company has been diligent in protecting their information and has been proactive in data protection, they may not blame the breached company for the data breach. On the other hand, if consumers do not feel that a company has proactively protected their data, then consumers may blame the company for the data breach. The attributions that customers make post-breach are very important. Also important are steps that can be taken in advance of a data breach to help to increase the likelihood that customers do not view the breached company as being at fault for the data breach. These activities fall into the wheelhouse of marketing.

THE ROLE OF MARKETING AND CYBERSECURITY

Whitler and Farris (2017) suggest that data breaches can have a dramatic impact on brand image and as such, marketing personnel need to be involved in both protecting companies consumer data before a data breach occurs and after a data breach should one occur. They argue that often corporations that have suffered a data breach focus more on liability issues and less on the impact of the breach has on the level of consumer trust with the brand. Damage to consumer trust can have a marked impact on consumer's willingness to do business with the company in the future which may result in long-term damage to a business's future. Frequently, company's delay announcing that a data breach has occurred potentially leading to even more significant damage to the brand. Research indicates that pre-breach corporate image and reputation can play a vital role one a data breach has occurred.

Lucas, Laurence, and DiSanti (2016), and Tynan (2015) suggest that a firm's cybersecurity can be used as an effective marketing tool—by leveraging the online security measures used by the firm to build consumer trust. Lucas et al., and Tynan suggest that firms should communicate with their customers when they have updated security systems as well as other measures such as partnering with well-known security systems and the like.

Frequent contact with customers regarding security measures represents an excellent way to help to build consumer confidence and trust in the firm. This confidence and trust can prove useful should a data breach occur. Customers impacted by the breach may feel that the company has done all that they could have done to prevent the breach. Likewise, retail-based companies can provide monthly activity statements—regardless if customers had made purchases in that month—this could help customers to feel that they are working with the retailer to protect their accounts. Many websites notify consumers when unusual log-in activity has occurred, monthly account activity reports are an extension of this. These reports can allow customers to check their activity and spot any unusual activity on their account. These reports may also be a means of providing early or earlier discovery of data breaches.

Theoretical Framework

Service quality is an important tool in the marketing arsenal. Quality of customer service effects many consumer decisions and the components of customer service may guide how a firm can undertake proactive measures to help the firm recover after a data breach. By far, the most used scale to assess customer service is SERVQUAL. Designed as a method to measure service quality, the SERVQUAL model (Parasuraman, Zeithaml, and Berry, 1985, Parasuraman, Zeithaml, and Berry, 1988, Parasuraman, Berry and Zeithaml, 1991) is comprised of reliability, assurance, responsiveness, empathy, and tangible variables. Figure 1 presents a diagram of the SERVQUAL Model.

The SERVQUAL model may provide insights on how a firm's marketing efforts can help to optimize various marketing functions that may help shape customer attributions of blame before a data breach occurs and can also provide guidance after a data breach occurs. Figure 1 presents a diagram of the SERVQUAL Model.

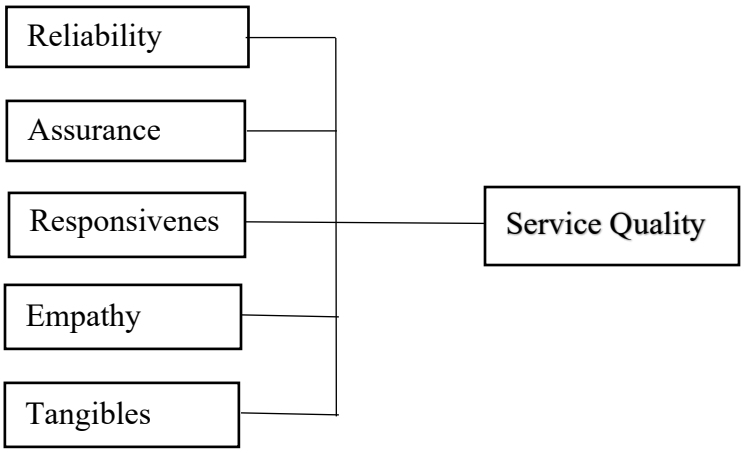

Figure 1 The SERVQUAL Model

Reliability refers to the ability to perform a given service dependably and accurately. In the context of preparation for a data breach, reliability refers to consumer perceptions of the reputation of the firm. It is vital that firms' seek to establish and maintain high levels of reliability—timely delivery of the product or service, mechanisms for handling and resolving customer complaints and issues and post-transaction follow-ups. Such actions can help to build the firm's reputation from the customer perspective. Before a data breach, firms should seek to maximize their customer service; this can help a company establish or maintain a higher level of corporate reputation.

Proposition 1: Firms that are perceived as being highly reliable will have a higher level of firm reputation than do firms with lower levels of reliability.

Assurance refers to the level of trust and confidence that customers place in the firm. Like reliability, the actions of the firm speak volumes about the firm. It is often said trust is difficult to earn but easy to lose. Toward this end, firms should publicize efforts made to maintain customer data security as well as notify customers when data security measures have been updated. Sharing data security measures with customers or potential customers can help to ease customers' minds about doing business with the firm. Well publicized proactive security measures may also provide a firm with a competitive advantage over competitive in that customers may choose to patronize the firm that offers higher levels of perceived security. The firm should also publicize corporate efforts regarding corporate social responsibility. Post-breach, firms should communicate the status of the breach and information regarding the breach with their customers. Even if the firm is not a victim of a data breach anytime a data breach occurs, a firm should re-notify their customers as to the security measures that the firm maintains.

Proposition 2: Firms that are perceived as having higher levels of assurance will enjoy higher levels of trust than do firms perceived as offering lower levels of assurance.

Responsiveness refers to a firm's willingness to engage with its customers. Firms can seek to increase and maintain their level of responsiveness—how quickly customer complaints or concerns are addressed, the quality of the firm's response to customer issues and how customer complaints are resolved. Before a data breach companies should undertake proactive communications with their customers regarding the value that the company places on the business relationship with the customer. Should a data breach occur, swift notification of the breach should be made. Frequently, customers and other entities effect by a data breach find out via a third party, customers and other entities may feel that the breached firm is more interested in protecting themselves than they are in protecting their customers. Announcements of a data breach should include as much detail as possible as well as proactive steps that the customer can take to further protect themselves from further damage including offering free credit monitoring services.

Proposition 3: Firms that are perceived as more responsive will enjoy higher levels of trust and reputation than do less responsive firms.

Empathy refers to the ability to adopt the psychological point of view of others (Davis, 1983). Generally, empathy is manifest in one's interaction with others. If customers perceive that a firm cares about them, this can go a long way toward developing positive feelings toward the firm. Customer concern can be demonstrated in multiple ways—how the firm deals with complaints, using customer satisfaction surveys, and providing follow-up when customers complain are just a few ways that companies can demonstrate empathy. Should a data breach occur, it is important that the breached firm demonstrate concern for their customers. It is common for breach companies to offer credit protection services to their customers, but companies can do more. Becoming the victim of a data breach is a shocking experience and many customers may feel freighted and nervous. Counselors can help to ease breached customers minds and can also reinforce the belief that the breached company is also worried about their (the customers) welfare. At this point, it is very important that the breached company begin to rebuild customer trust as well as reduce the risk associated with a continued business with the firm. The continuing patronage of existing customers as well as the ability to attract new customers are vital to the ongoing success of the firm.

Proposition 4: Firms that are perceived as having more empathy will enjoy higher levels of reputation than do firms that are perceived as having lower levels of empathy.

Proposition 5: When customers perceive that a firm has empathy toward them, customers will reciprocate with increased levels of empathy toward the firm.

Tangibles refer to observable aspects of a business. In the context of this research, tangibles refer to items such as the website, responses to complaints or queries and the like. For the context of this research, tangibles include anything that the company can do to demonstrate the above factors. Tangibles moderate the relationship between the other SERVQUAL constructs and firm reputation and trust.

Proposition 6: Firms that display higher levels of tangibles—visibility and engagement with customers will enjoy higher levels of firm reputation and firm trust than do firms that display lower levels of tangibles.

If customers perceive a firm has reputable, then it is likely that this will lead to higher levels of brand equity.

Proposition 7: Higher levels of a firm's reputation will lead to higher levels of brand equity.

If customers have a higher level of trust in a firm, then it is likely that brand loyalty will increase.

Proposition 8: Higher levels of trust will lead to higher levels of brand loyalty.

When consumers view a brand as being of high quality, it is likely that in the event of a data breach they will have more favorable attributions regarding the data breach—i.e., less likely to place the blame for the breach on the firm.

Proposition 9: Higher levels of brand equity will lead to more positive attributions in the event of a data breach.

When consumers are brand loyal, they have decided to repeat the purchase of the brand. In the event of a data breach, it is likely that they will desire to stay with the same business brand.

Proposition 10: Higher levels of brand loyalty will lead to more positive attributions in the event of a data breach.

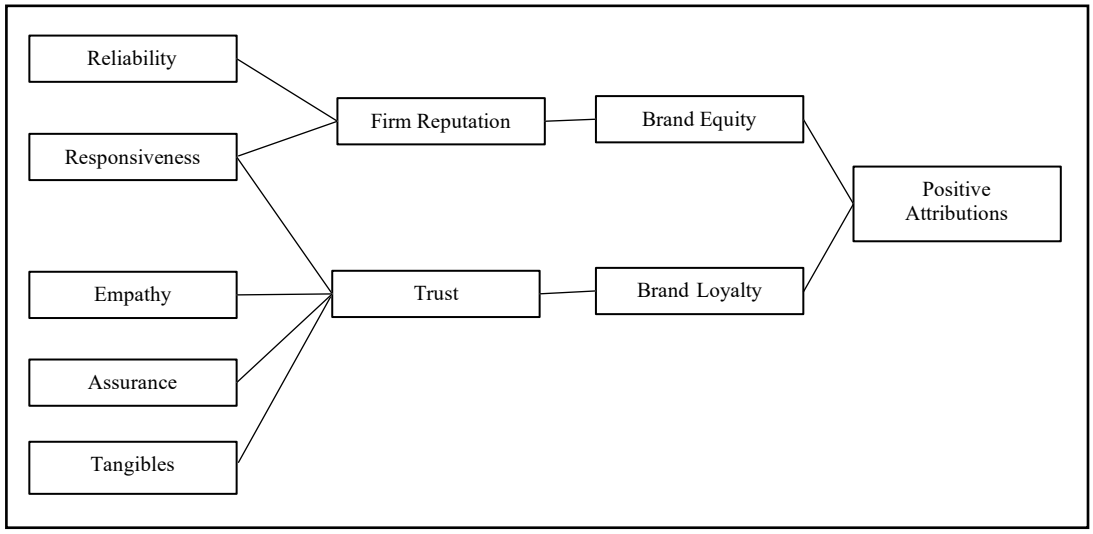

Figure 2. Proposed Theoretical Model

PROPOSED METHODOLOGY

A scenario-based experimental design will be used. Scenarios will be developed that describe the exploits of three companies. Table 1 presents the information for each of the companies that will be provided to the experimental subjects. A modified version of the SERVQUAL survey instrument will be used to assess respondent perceptions of each of the SERVQUAL variables. Based upon the provided information subjects will be asked to indicate their perceptions of the firm's reputation, the level of trust that they place in the company and whether or not they would likely continue to conduct business with the firm in question. In addition, the survey instrument include questions regarding the attribution they make regarding the data breach. Data will be analyzed using Factor analysis to establish construct validity and Scale reliability analysis will be assessed by calculating coefficient, Cronbach (Cronbach, 1951), and structural equation modeling.

Table 1. Scenarios

High Customer Service Level	Medium Customer Service Level	Low Customer Service Level
• Bi-annual updates of cybersecurity policy • Examples of outstanding customer service • Excellent reviews • An actual disguised data breach announcement (common to all packages) • Proactive response statement	• Annual updates of cybersecurity policy • Examples of mediocre customer service • Medium reviews • An actual disguised data breach announcement (common to all packages) • Generic response statement	• A cybersecurity policy that is three years old • Examples of poor customer service • Poor reviews • An actual disguised data breach announcement (common to all packages) • No response statement

CONCLUSION

Data breaches represent an immediate threat to the market value of a firm. Equally important, a data breach may cause long-term harm to a firm's customer base and subsequently, a firm's ability to recover from a data breach. Recovery is dependent on customers; both existing and new. It is vital that customers continue to do business with the firm post-

breach. The SERVQUAL Model presents a framework for developing an aggressive marketing program designed to lead to positive or at least not negative attributions regarding fault for the data breach should a data breach occur. It is essential that the marketing function takes a proactive role regarding cybersecurity both pre-breach to help to establish higher levels of a firm reputation and trust to, in turn, increase the firm's levels of brand equity and brand loyalty and post-breach to help to speed recovery efforts.

REFERENCES

Aaker, D. A. (1991). *Managing Brand Equity.* New York: The Free Press, 206.

Agarwal, Reeti, Mehrotra, Ankit and Barger, Victor (2016). Personality traits and repatronage intentions after a service failure. *Journal of Consumer Satisfaction, Dissatisfaction & Complaining Behavior*, *29*, 31-51.

Bougoure, Ursula Sigrid, Russell-Bennett, Rebekah, Fazal-E-Hasan, Syed and Mortimer, Gary (2016). The impact of service failure on brand credibility. *Journal of Retailing and Consumer Services, 31*, 62-71.

Choong, Peggy, Hutton, Ed, Richardson, Paul S. and Rinaldo, Vincent (2017). Protecting the brand: evaluating the cost of a security breach from a marketer's perspective. *American Journal of Management, 11*(1), 59-68.

Cronbach, L. J. (1951). Coefficient Alpha and the Internal Consistency of Tests. *Psychometrika, 16*, 297-334.

Davis, M. H. (1983). Measuring individual differences in empathy: Evidence for a multidimensional approach. *Journal of Personality and Social Psychology*, *44*, 113-126.

Dawar, N., & Pillutla, M. M. (2000). Impact of product-harm crises on brand equity: The moderating role of consumer expectations. *Journal of Marketing Research*, *37*(2), 215–26.

Fiske, S. T., & Taylor, S. E. (1991). *Social cognition.* New York, NY: McGraw-Hill.

Ford, J. C., White, B. J., and White, K. M. (2015). After the data breach: Notification laws and more. *Issues in Information Systems, 16*(IV), 86-94.

Goode, S., Hoehle, H., Venkatesh, V. & Brown, S. A. (2017). User compensation as a data breach recovery action: an investigation of the Sony PlayStation network breach. *MIS Quarterly, 41*(3), 703-A16.

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.

Green, D. T., & Martin, N. L. (2016). Attributes of data breach notification laws in the United States. *Issues in Information Systems*, 17(I), 107-118.

Heider, F. (1958). *The Psychology of Interpersonal Relations*. Hillsdale, New Jersey: Lawrence Erlbaum Associates, Publishers.

https://marketing-dictionary.org/b/brand-equity/.

https://www.ama.org/the-definition-of-marketing/.

Janakiraman, Ramkumar, Lim, Joon Ho, Rishika, Rishika (2018). The effect of a data breach announcement on customer behavior: evidence from a multichannel retailer. *Journal of Marketing*, 82(2), 85-105.

Kashmiri, S., Nicol, C. & Hsu, L. (2017). Birds of a feather: intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science*, 45(2), 208-228.

Klein, J., & Niraj D. (2004). Corporate social responsibility and consumers' attributions and brand evaluations in a product-harm crisis. *International Journal of Research in Marketing*. 21(3), 203–217.

Lai, Chi-Shiun, Chiu, Chih-Jen, Yang, Chin-Fang & Pai, Da-Chang (2010). The effects of corporate social responsibility on brand performance: The mediating effect of industrial brand equity and corporate reputation. *Journal of Business Ethics*, 95(3), 457-469.

Liao, S. & Cheng, C. C. (2013). Consumer evaluation of self-service innovation failure: the effect of brand equity and attribution. *Service Industries Journal*. 33(5), 467-485.

Lucas, J., Minsky, L., & DiSanti, B. (2016). Good cybersecurity can be good marketing. *Harvard Business Review Digital Articles*, *9*(23), 2-4.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, *81*(1), 36-58.

Parasuraman, A., Zeithaml, V. & Berry, L. (1985). A conceptual model of service quality and itsimplications for future research, *Journal of Marketing* (Fall), 41-50.

Parasuraman, A., Zeithaml, V. A. & Berry, L. (1988). SERVQUAL: A multiple-item scale for measuring consumer perceptions of service quality. *Journal of Retailing*, *64*(1), 12-40.

Parasuraman, A., Berry, L. L & Zeithaml, V. A. (1991). Refinement and reassessment of the SERVQUAL scale. *Journal of Retailing, 67*(4), 420-450.

Rasoulian, S., Grégoire, Y., Legoux, R. & Sénécal, S. (2017). Service crisis recovery and firm performance: insights from information breach announcements. *Journal of the Academy of Marketing Science*, 45(6), 789-806.

Selnes, F. (1998). Antecedents and consequences of trust and satisfaction in buyer-seller Relationships. *European Journal of Marketing*, 32(3/4), 305–322.

Sengupta, Aditi Sarkar, Balaji, M.S., & Krishnan Balaji C., (2015). How customers cope with service failure? A study of brand reputation and customer satisfaction. *Journal of Business Research* 68(2015), 665–674.

Tynan, K. (2015). Good marketing can help banks survive a cybersecurity backlash. *American Banker*, *180*(6), 1.

Udo, G., Bagchi, K. & Kirs, P. (2018). Analysis of the growth of security breaches: A multi-growth model approach. *Issues in Information Systems*, *19*(4), 176-186.

Van Heerde, H., Helsen, K. & Dekimpe, M. G. (2007). The impact of a product-harm crisis on marketing effectiveness. *Marketing Science*, 26(2), 230–245.

Wang, P. & Johnson, Ch. (2018), Cybersecurity incident handling: A case study of the Equifax data breach. *Issues in Information Systems*, *19*(3), 150-159.

Wang, P. & Park, S.-A. (2017). Communication in cybersecurity: A public communication model for business data breach incident handling. *Issues in Information Systems*, *18*(2), 136-147.

Whitler, K. A., & Farris, P. W. (2017). The impact of cyber attacks on brand image: Why proactivemarketing expertise is needed for managing data breaches. *Journal of Advertising Research*, 57(1), 3-9.

Xie, Yi, Keh, Hean Tat (2016). Taming the blame game: Using promotion programs to counter product-harm crises. *Journal of Advertising*, *45*(2) 211-226.