Protecting the Brand: Evaluating the Cost of Security Breach from a Marketer's Perspective

Peggy Choong
Niagara University

Ed Hutton
Niagara University

Paul S. Richardson
Niagara University

Vincent Rinaldo
Niagara University

Cyberattacks have increased over the years both at the individual and firm level. Yet, the organizational budgets directed toward information security remains low. One reason is that the ramifications of information breach, such as increased consumer perception of risk and brand equity erosion remain, to the senior executives and board of directors in organizations, almost invisible. The second reason is that managers are required to justify budgets. The cost of system breach is often difficult to quantify. There are direct and enduring costs of information breach. As such, it has implications that impact not just the downtime during a data breach but loss of customers, trust, loyalty and brand equity, all of great concern to marketing managers. This paper analyzes the impact of a breach announcement on the market valuation of the company. Such an analysis using the event study methodology provides a clear indication of how the market reacts to the firm's breach in information. The results of the study indicate that the market punishes the firm with a small but significant negative abnormal return on the announcement of the breach, and this trend persists. This result, together with the indirect or enduring costs related to brand erosion, provides a good justification to senior executives for protecting the integrity of information, and by so doing, protecting the equity of the brand.

INTRODUCTION

Over the last three decades, the rapid development of the internet and its associated innovative devices have enabled businesses of all sizes to engage effectively in the global market. In 2014, about two million people purchased on the internet, spending a total of more than $300 billion (Enright, 2015). In addition, consumers have begun to routinely engage in banking on the internet as well as submitting insurance claims and filing tax returns online. Health records, personal information, social security

numbers, bank accounts and all aspects of an individual's purchasing behavior are transmitted online and stored online.

Marketers have welcomed this abundant data and have been stridently working to leverage these valuable consumer information as part of their strategic marketing practice. This is useful information that can be analyzed to expand a firm's customer base, serve its customers better through customized offerings, target consumers with more accurate communication and increase the firm's loyalty base and brand equity. However, this cloud of rich data and the sensitive personal information that consumers inadvertently leave behind have become the target of unscrupulous, financially driven criminal elements (Richardson, 2012).

In 2014, 47% of Americans were personally affected by cybercrime. Very importantly, at the organizational level, 43% of companies in 2013 reported that their data system had been breached. More recent highly publicized cases such as Target, Home Depot and JP Morgan Chase and Company, have highlighted the inability of the IT system in many organizations to properly protect the personal information of their customers (Ponemo Institute, 2015a).

The continued escalation of malicious cyberattacks have finally forced some organizations to place information security at the forefront of their IT management (Yayla & Hu, 2011). While increasing their budgets directed towards information security is a step in the right direction, the total IT budget directed toward information security management remains low. In 2014 it was less than 6% of the total IT budget (Filkins, 2016). This is not inconceivable. One of the reasons for this low expenditure is that the ramifications of information breach, such as an increase in perceived risk and equity erosion remain almost invisible to the senior executives and board of directors in organizations (Richardson, 2012). The second reason is that managers are required to justify budgets. The cost of system breach is often difficult to quantify. There are direct and indirect costs of information breach (Mercuri, 2003). As such, it has implications that impact not just the downtime during a data breach but loss of customers, trust, loyalty and brand equity, all of great concern to marketing managers. Hence, the security quality of an organization is a marketing manager's problem, too important to be relegated solely to the IT experts in organizations.

The purpose of this paper is to analyze the cost of information breach in organizations and their implications for marketers. An event study methodology is adopted to study the impact of the announcement of a breach of data on the company's valuation. It is by understanding the cost of breach that we may be able to provide good justification for protecting the integrity of information and by so doing protecting the equity of a company's brand.

LITERATURE REVIEW

The internet and its related mobile and innovative devices have opened markets and opportunities for businesses large and small. Businesses and enterprising entrepreneurs are now able to reach consumers in different parts of the world with a more diverse set of market offerings. There is a rich body of marketing literature that examines consumer behavior in e-commerce (Goldsmith, 2002; Kau, Tang & Ghose, 2003; Finn, Wang & Tema, 2009; Gounaris, Dimitriadis & Stathakopoulos, 2010; Smith, 2012), effectiveness of specific website characteristics as well as their impact on consumer loyalty, perceived risk and intentions (Hofacker & Murphy, 2000; Danaher, Mullarkey & Essegaier, 2006; Youn & Lee; Rowley, 2008; Jaiwal, Niraj & Venugopol, 2010; Schumann, 2014) and third-party endorsement on brand reputation and trust (Nienaber, Hofeditz & Searle, 2014).

However, there has been little focus in the marketing literature on information security breach and its impact on the consumers. In this area, a stream of marketing literature have examined the factors impeding consumer adoption of web services. Findings have identified perceived security as a key factor that prevents consumers from purchasing online. Adoption is contingent on the consumers' perception of the safety of their personal information on the internet. Consumers who perceive that the internet is not safe, tend to limit their exposure to online activities (Delafrooz, Paim & Khatibi, 2011). This is exacerbated by consumers' fear that their personal information such as home address and credit

information may be compromised or misused by web companies (Miyazaki and Fernandez, 2001; Suki and Suki, 2007). Other studies in this area have attempted to identify sources of security threats and processes to undertake when a breach occurs. While external hackers and fraudsters remain the major threat, these studies have found that employees of firms are one of the key perpetrators of serious breaches in security sometimes by negligence through loss of storage devices containing customer information or by criminal action through the theft of information (Gregory, 2008; Canhoto, 2009). Oates (2001) in examining the causes of security breaches conclude that while it is important for firms to provide proper internal measures to safeguard customer information, the problem will continue to persist and escalate unless there are external processes to identify and prevent fraudsters. The problem of security breach can only be resolved when private, public and international entities share information and work together (Oates, 2001; Gregory, 2008).

The impact of security breach on consumer intentions have been further studied by Berezina, Cobanoglu, Miller and Kwansa (2012). They examined the impact of information security breach in the hospitality industry using a case scenario method and found that information breach had a significant negative impact on perceived service quality, consumer satisfaction and repurchase. Miyazaki and Fernandez (2000) examined the impact of retailer online practices pertaining to consumer privacy and security. Examining seventeen product categories, they evaluated the impact of these online disclosures on perceived risk and purchase intention. They found that privacy disclosures is positively related to the likelihood of purchase. Studies that examine the impact of perceived online security by consumers find that perceived risk have a negative impact on loyalty and purchase behaviors. (Youn & Lee, 2009; D'Alessandro, Girardi & Tiangsoongnern, 2012). Smith, Smith and Smith (2011) examined the impact of cybercrime on shareholder value using a case approach. They examined 10 publicly traded companies affected by cybercrime. Stock prices of the ten companies were presented for three days before and after the date of the news story reported in the media. Using a matched pair t-test they attempted to show the difference in stock price between the company and the S&P 500. While this is one of the first attempts in the marketing literature to examine the impact of a breach on the company stock price, the sample size is very small and the methodology employed is seriously flawed. The accepted method of evaluating the impact of news announcement on the valuation of a firm is by using the event study methodology as will be discussed in the next section.

DATA AND METHODOLOGY

The security breach notification act requires that companies that have experienced a security breach report the incident and notify the victims and other parties (Bergsieker, Cunningham & Young, 2015; National Conference of State Legislature, 2016). California was the first state to enact the data breach security act in 2002. However, several major breaches in 2005 triggered significant legislative changes. Prior to 2005, information breach tended to be relatively small, affecting few individuals. However, in February 2005, CrossPoint reported that they sold 145,000 customer data to criminals. In that same month Bank of America lost 1.2 million customer records, and in June, CardSystem had the information of 40 million of its card subscribers compromised. Important legislative changes ensued which included the notification of risk to personal data act and the personal data privacy and security acts of 2005 (Sutton, 2006). The data chosen for this study is from 2005-09, a period of importance.

To identify companies for this study, the national database was searched. In the event study methodology, it is essential that the firms be publicly listed companies and that the announcement date in the public forum be clearly identified. As such, companies that were not publicly listed were deleted. Using LEXIS/NEXIS, each company was subjected to a thorough search in the Wall Street Journal, New York Times and other news outlets for the first announcement of such a breach. This is captured as the announcement date of the event, which is defined as the date the breach was publicly made known. The sample indicated a total of 166 disclosures involving companies whose stocks trades in public markets. Eighteen firms were deleted because of anomalies such as mergers, bankruptcy or stock market delisting. For each of the firms, the CUSIP number was obtained. The CUSIP is a unique numerical identifier to a

publicly traded security. The event study methodology is a useful statistical procedure that examines the effect a release of new information has on the stock market returns of the firm. It has been well accepted and employed in the finance and accounting literature. In the marketing discipline, it has been used to examine strategies such as product innovation, change in a company's name, advertising, announcements of green activities and the introduction of e-commerce (Horsky & Swyngedouw, 1987; Mathur & Mathur, 2000; Subramani & Walden, 2001; Choong et. al., 2003; Choong, Filbeck & Tompkins, 2007; Filbeck et. al., 2009). The theory underlying this procedure is the efficient market hypothesis, which states that a firm's stock price is the present value of the stream of future cash flows. This means that, at any point in time, a stock price captures all known information pertaining to the firm's current and future profits. In this way, stock prices reflect the true value of the firm because they reflect the discounted value of future earnings as well as all relevant information known in the market. New information that will impact the firm's current and future profitability will result in a change in security price. The purpose of this methodology is to determine whether the announcement of some upcoming event produces a significant stock price reaction around the time of the announcement. For example, the announcement of new information in the form of the company's security breach constitutes new signals. This signal will impact its stock price depending upon the market's valuation of how this breach will affect present and future earnings of the company. To conduct such tests, daily stock returns are measured around the announcement or event date and are compared with the expected return. The change in the price of the stock, or abnormal returns, after the event reflects the unbiased market valuation of the economic value of the event. This methodology provides a unique opportunity to evaluate the financial effect of a corporate strategy or an event. By examining a sample of firms over a period of years, it is possible to evaluate the overall market valuation of a particular business strategy.

The hypothesis in this paper is tested using the standard event study methodology (see e.g., Brown & Warner, 1985). The expected return is generally based on the capital asset pricing model or some other suitable market based return generating mechanism. Following Choong, Filbeck, Tompkins and Ashman (2003), the market model is specified as:

$$R_{j,t} = \alpha_j + \beta_j R_{mt} + u_{jt}, j = 1, ..., N;\ t = -325, ..., -71, \quad (1)$$

where:

N is the number of issues in the sample,

$R_{j,t}$ is the return on stock j for day t,

$R_{m,t}$ is the return on market proxy m for day t,

$u_{j,t}$ is the random error for stock j for day t normally distributed with $E\lfloor u_{j,t} \rfloor = 0$,

α_j is the estimated intercept term for stock j, and

β_j is the estimated risk coefficient for stock j.

The market model is estimated by using the equally-weighted market returns from the University of Chicago's Center for Research in Security Prices, CRSP files as the market proxy. The prediction errors are calculated for each day in the test period, which begins 50 days before the announcement day and ends 50 days after the announcement day. The prediction error for stock j for day t is defined as:

$$PE_{j,t} = R_{j,t} - (\alpha_j + \beta_j R_{m,t}), j = 1, ..., N;\ t = T_1, T_1 + 1, ..., T_2, \quad (2)$$

such that $E\lfloor PE_j \rfloor = 0$, i.e., the prediction error is not expected in an efficient market in equilibrium. If $E\lfloor PE_j \rfloor \neq 0$, then we infer that some unanticipated information had come to the market and was used by well-informed individuals.

The cross-sectional average prediction error for day t for a sample of size n is:

$$APE_t = \frac{1}{N}\sum_{j=1}^{N} PE_{j,t}\ , \tag{3}$$

and the cumulative average prediction error is:

$$CAPE_i = \sum_{k=T_1}^{i} APE_k\ . \tag{4}$$

The time-series of CAPEs tells us whether prediction errors would have occurred had investors bought the test portfolio in day T_1 and held until day I, $i = T_1,\ T_1+1\ ,...,\ T_2$. Following Patell (1976), tests of statistical significance are based on standardized prediction errors. The standardized prediction error for stock j in day t, is calculated as:

$$SPE_{j,t} = \frac{PE_{j,t}}{S_{j,t}}, \tag{5}$$

where

$$S_{j,t} = \{\sigma_j^2(1 + \frac{1}{T} + \frac{(R_{m,t} - \overline{R_m})^2}{\sum_{k=1}^{T}(R_{m,k} - \overline{R}_m)^2})\}^{1/2} \tag{6}$$

where:

σ_j^2 is the residual variance from the market model estimation for stock j,
T is the number of days in the period used to estimate the model, and
$\overline{R}_m$ is the mean market return in the estimation period.

The average standardized prediction error for day t is:

$$ASPE_t = \frac{1}{N}\sum_{j=1}^{N} SPE_{j,t}\ . \tag{7}$$

For each day, the Z-statistic is calculated as:

$$Z_t = \sqrt{N} \bullet ASPE_t\ . \tag{8}$$

The limiting distribution of Z_t is the unit normal, under the null hypothesis that the mean normalized, standardized prediction error equals zero. Over the testing period, which begins with T_1 and ends with T_2 the cumulative normalized, average standardized prediction error is then the Z-statistic calculated as:

$$Z_{T_1,T_2} = \sqrt{N} \bullet CASPE_{T_1,T_2}, \tag{9}$$

It has a unit normal limiting distribution under the null hypothesis that the cumulative normalized,

$$CASPE_{T_1,T_2} = \left(\frac{1}{N}\right)\frac{\sum_{t=T_1}^{T_2}\sum_{j=1}^{N} SPE_{j,t}}{\sqrt{T_2 - T_1 + 1}}\ . \tag{10}$$

average standardized prediction error over the period from T_1 through T_2 equals zero.

The hypothesis for the study is:

H_0: The announcement that a firm has a security breach will result in no significant change in the firm's share value.

RESULTS

Table 1 exhibits the abnormal returns beginning five days prior to the actual event date and ending five days after the date. Negative abnormal returns of 0.35% is observed on the date of the security breach announcement. This downward drift is observed in day +1 with negative abnormal returns observed at 0.32%. These results are significant at the p=0.05 level.

TABLE 1
ABNORMAL RETURNS AROUND DATE OF SECURITY BREACH

Day	Abnormal Returns (%)	Z-score
-5	0.13	1.347+
-4	0.13	0.311
-3	0.44	2.409
-2	-0.23	-1.130
-1	0.19	0.881
0	-0.35	-2.059*
+1	-0.32	-2.658**
+2	0.16	1.495+
+3	-0.05	-0.197
+4	0.22	1.331+
+5	-0.02	0.410
+ Significant at the 0.1 level; * Significant at the 0.05 level; ** Significant at the 0.01 level		

Cumulative abnormal return (CAR) is the sum of the average abnormal returns to a point in time. It represents the impact of the event over time.

TABLE 2
CUMULATIVE ABNORMAL RETURNS (%) AROUND DATE OF SECURITY BREACH

Days	Abnormal Returns (%)	Z-score
(-10, -1)	0.73	1.923*
(-1,0)	-0.16	-0.833
(0,0)	-0.36	-2.059*
(-1,+1)	-0.48	-0.214*
(+1,+10)	-0.26	0.062
* Significant at the 0.05 level		

Looking at the cumulative abnormal returns exhibited in Table 2, negative cumulative abnormal returns is observed on (0,0) and (1,+1) of 0.36% and 0.48% respectively. These results are significant at the p=0.05 level. The Null Hypothesis is rejected.

DISCUSSION

Negative abnormal returns of 0.35% on the announcement date and 0.32% on day +1 indicates that the market views the breach of security negatively. This event, the breach in security, has an impact on the firm's profits and future cash flows and hence the negative and significant abnormal returns on shareholder value is identified. Firms that experience and announce a security breach can expect a small but significant decline in their market value. In addition, the cumulative abnormal returns is observed to be negative 0.36% and negative 0.48% on days (0,0) and (-1,+1) respectively. This indicates that the negative and significant decline in valuation persists over time.

While these results represents a good measurement of the market valuation of the cost of breach, marketers need to consider other elements in the cost. The cost of information breach includes both direct and indirect cost. The Ponemo Institute (2015b) includes as direct costs all the activities required to rectify the breach. This includes hiring forensic experts, law firms and offering the victims identity theft protection. Included as well are the loss of productivity within the organization as personnel are mobilized to address the crisis. Obviously, the direct costs include the sizeable expenditure for software and hardware replacement. Indirect costs is more difficult to quantify but tend to have a more lasting and critical impact on the organization and are more aptly referred to as enduring costs. The following are the key enduring costs:

Loss of Customers

During the downtime resulting from a breach, customers are lost and sometimes denied service. This provides them with the opportunity to seek alternative brands. Switching erodes an organization's customer and loyalty base.

Loss of Customer Trust

One of the more serious problems in information breach is the impact on customer loyalty. The nature of the e-commerce environment is that it enlarges the marketer's opportunity to engage in "temporary relationships with a large number of potential transaction partners," but it is often devoid of the rich face-to-face interaction that relationship marketing requires (Lee & Lee, 2012, p376). As such, trust in the transaction partner becomes an important and tenuous attribute that is closely linked to consumer perception of security. A data breach will result in a decrease in trust, a critical factor in foster a successful, long-term relationship (Chen, 2006; Chen & Dibb, 2010; Choi & Nazareth, 2014). Longitudinal study indicated that trust has a positive impact on purchase decision and long-term loyalty (Kim, Ferrin & Rao, 2009).

Erosion of Reputation

Vendor reputation captures past performance of the brand as well as suggests that the vendor's security protects customers' privacy and information (Choi & Nazareth, 2013). It is a factor that directly impacts trust formation both initial trust as well as the on-going maintenance of trust. This is especially important in Asia, the fastest growing e-commerce region in the world (Nienaber, Hofeditz & Searle, 2014).

Increased Perception of Risk

Perception of security rather than the state of security artifacts mainly influences trust and intentions (Challappa & Pavlou, 2002). As such, the public announcement or denouncement of companies experiencing data breach services has a detrimental effect on firms. It increases the perceived risk of consumers and results in consumers exhibiting "retreative" behavior associated with particular firms. The availability of alternative avenues for purchase significantly increases this type of behavior (Lee & Lee, 2012, p375). This will not simply result in a migration of consumers but a decrease in customer acquisition. The FTC nearly twenty years ago in its address to the House Committee highlighted the important fact that consumers "must feel confident that the internet is safe from fraud" if the growth of e-

commerce is to be sustained. This has not changed and it is more important now than ever before (FTC, 1998).

Brand Equity

A firm's relationship with its customers is contingent on the customers' trust in the firm delivering its brand promise as well as its belief that the firm is operating in credible ways that does not compromise or exploit their personal information and records. Data breach erodes this equity.

CONCLUSION

The cost of data breach encompasses both direct and indirect cost. The findings of this study indicate that data breach results in a significant decline in the market valuation of a firm. In other words, investors in the market have a negative view of the data breach and the market punishes the firm's stock price with a negative abnormal return. This should be persuasive to top executives and board of directors of companies who make budget allocation decisions. However, included in the decline in market valuation is the notion the cost of data breach encompasses both direct and indirect costs that endures over time and when viewed in this light would make the neglect of information security systems untenable. The ramifications of information breach is far reaching and impacts brand equity. Firms depend on information security to protect its customers, reputation and brand equity (Ernst & Young 2003, 2008). Thus, marketers need to demonstrate the impact of indirect costs to the organization. The Ponemon Institute has made an attempt at this and found that for 2015, on a global aggregate level, the average cost per lost record is $154 (Ponemon Institute, 2005b). Firms using their internal metrics need to be able to quantify the indirect costs specific to their organization. As such, ensuring the security of information goes beyond the IT experts within the firm. It is a marketer's problem as well.

LIMITATIONS

This study demonstrated that the market punishes companies that experience a security breach and firms experience a significant and negative abnormal return. Future research should be directed toward helping firms quantify the enduring costs of breach. The study focused on a specific 4-year period in time. Investigation into other time periods would also be insightful. Currently, consumers are finding more frequent reports of security breach in the media. An interesting area of research is whether consumers have become desensitized to reports of such infractions and whether the market valuation would reflect this perspective.

REFERENCES

Berezina, K., Cobanoglu, C., Miller, B.L.& Kwansa, F. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Management*, Vol. 24, No. 7.

Bergsieker, R.T., Cunningham, R.H.& Young, L. (2015). The Federal Trade Commission's enforcement of data security standards. *The Colorado Lawyer*, June, 39.

Canhoto, A.I. (2009). Safeguarding customer information: The role of staff. Journal of Consumer Marketing, Vol. 26, No. 7.

Chellappa, R.K. & Pavlou, P.A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, Vol. 15, No. 5/6.

Chen, E. (2006). Identifying significant factors influencing consumer trust in an online travel site. *Information Technology & Tourism*, 8(3).

Chen, J & Dibb, S. (2010). Consumer trust in the online retail context: Exploring the antecedents and consequences. *Psychology and Marketing*, 27(4).

Choi, J.& Nazareth, D.L. (2014). Repairing trust in an e-commerce and security context: an agent-based modeling approach. *Information Management & Computer Security*, Vol. 22, No. 5.

Choong, P., Filbeck, G., Tompkins, D. & Ashman, T. (2003). An event study approach to evaluating the economic returns of advertising in the Super Bowl. *Academy of Marketing Studies Journal*, Vol. 7, No. 1.

Choong, P., Filbeck, G., & Tompkins, D. (2007). Advertising strategy and returns on advertising: A market value approach," *The Business Review*, *Cambridge*, Vol. 8, Num. 2, December.

D'Alessandro, S., Girardi, A. & Tiangsoongnern, L. (2012). Perceived risk and trust as antecedents of online purchasing behavior in the USA gemstone industry. *Asia Pacific Journal of Marketing and Logistics*, 24.3.

Danaher, P., Mullarkey, G.W. Essegaier, S. (2006). Factors affecting website visit duration: A cross-domain analysis. *Journal of Marketing Research*, 43.2.

Enright, A. (2015). U.S. annual e-retail sales surpass $300 billion for the first time. *Internet Retailer*, January 17.

Ernst & Young (2003). *Global Information Security Survey 2003*, London, UL: Ernst & Young L.L.P.

Ernst & Young (2008). *Global Information Security Survey 2008*, London, UL: Ernst & Young L.L.P.

Filbeck, G., Zhao, X., Tompkins, D. & Choong, P, (2009). Share price reactions to advertising announcements and broadcast of media events. *Managerial and Decision Economics*, Vol. 30(4).

Filkins, B. (2016). *A Sans Survey. IT Security Spending Trends*. Retrieved on January 2016 from www.sans.org/reading-room/whitepapers/leadership/security-spending-trends-36697.

Finn, A., Wang, L., Tema, F. (2009). Attribute perceptions, consumer satisfaction and intention to recommend e-service. *Journal of Interactive Marketing*, 23.3.

FTC. (1998). *Fraud could slow growth of electronic commerce: FTC*. Retrieved on January 2016 from www.ftc.gov/news-events/press-release/1998/06/fraud-could-slow-growth-electronic-commerce-ftc

Goldsmith, R.E.(2002). Explaining and predicting intention to purchase over the internet: An exploratory study. *Journal of Marketing Theory and Practice*, 10.2.

Gounaris, S. Dimitriadis, S., & Stathakopoulos, V. (2010). An examination of the effects of service quality and satisfaction on customers' behavioral intentions in e-shopping. *The Journal of Services Marketing*, 24.2.

Gregory, A. (2008). Conserving customer value: Improving data security measures in business. *Database Marketing & Customer Strategy Management*, Vol. 15, Iss. 4.

Horsky, D. & Swyngedouw, P. (1987). Does it pay to change your company's name? A stock market perspective. *Marketing Science*, 6, 32-34.

Hofacker, C.F. & Murphy, J. (2000). Clickable world wide web banner ads and content sites. *Journal of Interactive Marketing*, Vol. 4, No. 1, winter.

Jaiwal, A.K., Niraj, R.& Venugopol, P. (2010). Context-general and context-specific determinants of online satisfaction and loyalty for commerce and content sites. *Journal of Interactive Marketing*, 24.3.

Kau, A.K., Tang, Y. & Ghose, S. (2003). Typology of online shoppers. *The Journal of Consumer Marketing*, 20.2/3.

Kim, D.J., Ferrin, D.L. & Rao, H.R. (2009). Trust and satisfaction, two stepping stones for successful e-commerce relationships: A longitudinal exploration. *Information Systems Research*, Vol. 20, No. 2, 237-257.

Lee M. & Lee J. (2012). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. *Information System Front*, 14: 375-393.

Mathur, L.K. & Mathur, I. (2000). An analysis of the wealth effects of green marketing strategies. *Journal of Business Research*, 50(2), 193-200.

Mercuri, R. (2003). Analyzing security cost. Communications of the ACM, Vol. 46, No. 6, June.

Miyazaki, A. & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing*, Vol., 19, No. 1, spring.

Miyazaki, A. & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *The Journal of Consumer Affairs*, 35.1, summer.
National Conference of State Legislature. (2016) *Security breach notification laws*. Retrieved on January 2016, www.acsl.org/research/telecommunication-and-information-technology/security-breach-notification-laws.
Nienaber, A., Hofeditz, M.& Searle, R. (2014).Do we bank on regulation or reputation? A meta-analysis and meta-regression of organizational trust in the financial services sector. *The International Journal of Bank Marketing,* 32.5.
Ponemo Institute Research Report. (2015a). *2015 Cost of cybercrime study: Global. Benchmark study of global companies.* Ponemo Institute L.L.C., October.
Ponemo Institute Research Report (2015b). *2015 Cost of data breach study: Global Analysis.* Ponemo Institute L.L.C., May.
Richardson, R. (2012). *15th Annual 2010/2011 Computer crime and security survey.* Computer Security Institute, U.S.A.
Rowley, J. (2008). Understanding digital content. *Journal of Marketing Management*, 24.5/6.
Schumann, J.H., von Wagenheim, F. & Groene, N. (2014). Targeted online advertising using reciprocity appeals to increase acceptance among users of free web services. *Journal of Marketing,* 78.1.
Smith, K.T., Smith L.M. & Smith, J.L. (2011). Case studies of cybercrime and their impact on marketing activity and shareholder value. *Academy of Marketing Studies Journal*, Vol. 15, No. 2.
Smith, K.T. (2012). Longitudinal study of digital marketing strategies targeting Millennials. *Journal of Consumer Marketing*, 29.2.
Subramani, M. & Walden, E. (2001). The impact of e-commerce announcements on the market value of firms. *Information Systems Research*, 12(2), 135-154.
Suki, N.M., Suki, N.M. (2007). Online buying innovations: Effects of perceived value, perceived risk and perceived enjoyment. *International Journal of Business and Society*, Vol. 8, No. 2.
Sutton, M.C. (2006). Security breach notifications: State laws, federal proposals, and recommendations. *Journal of Law and Policy*, 2:3.
Yayla, A.A. & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, 26, 60-77.
Youn, S. Lee, M. (2009). The determinants of online security concerns and their influence on e-transactions. *International Journal of Internet Marketing and Advertising*, 5.3.