The Impact of Data Breach on Short-Term Profit Margins

Cretson L. Dalmadge
Winston-Salem State University

This paper addresses the impact of data breaches on the short-term profit margin of breached firms. Data from 2013 to 2018 is used to test the model. The data represents 441 breaches, impacting 166 companies in twelve industries, with 77 percent of the breaches in the retail, technology, healthcare, and financial sectors. The analysis is first conducted with the broad collection of businesses, then repeated for retailers only. Breaches were found to have no adverse effect on profit margins for the broad group of firms. The retailers were negatively affected, but this was not statistically significant.

Keywords: data breaches, profit margin, t-tests, continuity management

INTRODUCTION

Data breaches seem to be occurring with increasing frequency and far more often than reported (Rashid 2017). While the very large breaches, such as those at Target and TJXX, dominate the news and seem to have significant impacts, smaller breaches appear to be constantly occurring and, in many cases, receiving little to no media coverage, often resulting in minimal financial impact.

The 'Breach Level Index' website (https://breachlevelindex.com/) and data repository reported the occurrence of almost ten thousand data breaches between the second quarter of 2013 and the second quarter of 2018. While most of these passed quietly, several of the major ones had extensive coverage in both the leading online technology journals and the mainstream media. This coverage addressed both the extent of the data breaches and their resulting financial impact.

Target suffered one of the most widely covered breaches in November of 2013. The breach was reported to have affected approximately 40 million payment cards and over 100 million data records and was given the maximum rating of level 10 on the breach level index scale. Target incurred $291 million in cumulative expenses relating to the end of 2013 data breach (Quick 2017, Plachkinova and Maurer 2018). The business also suffered a decrease in customer base. Before the breach, 44 percent of US households shopped at Target, while only 33 percent did so immediately after the breach (Quick 2017). While this level of impact has not accompanied all large data breaches, the general thinking has been that data breaches result in significant financial losses.

The technology literature has also covered other large breaches with negative consequences. Heartland Payment System was breached in March 2008 (Cheney 2010). The breach was not discovered until January 2009. Heartland was deemed out of compliance with the Payment Card Industry Data Security Standard (PCI DSS) and was prevented from processing payments for major credit cards until May of 2009. Other data breaches, for example, TJXX Companies in December 2006, Sony PlayStation Network in April 2011,

and JP Morgan Chase in July 2014, were also believed to have had significant financial effects on those corporations.

On the other hand, Home Depot suffered a major breach in September of 2014. More than 56 million card numbers were exposed. Unlike Target, Home Depot suffered very little financial consequences (Hill 2014). Similarly, Marriot International data breach had very little impact on their financials. Notwithstanding the fact that their breach started in 2014 and was not discovered and addressed until September of 2018 (Aivazpour et al., 2022). Also, eBay's May 2014 breach affected 145 million customer records and lasted 229 days (Alharbi 2020). The breach led to a downturn in visitor statistics but had little financial impact on the company.

While data breaches are not limited to e-commerce businesses, the ongoing pace of breaches appears to be correlated with e-commerce growth (Dalmadge, 2020). Macro-level analysis shows that as eCommerce increases, so does the number of data breaches; however, data breaches have not had a negative impact on short-term macro-level eCommerce growth. This paper addresses firm level performance and examines specifically whether data breaches are having adverse effects on profit margins of breached firms.

RELATED WORK

The Information Systems literature has addressed the impacts of breaches in several ways. First, focus has been placed on the short-term impacts of breaches on the market value of breached firms (Cavusoglu et al., 2002; Muntermann and Roßnagel 2009; Kannan et al., 2007; Goel and Shawky 2009; Hovav and D'Arcy 2003; Spears J. L., H. Barki 2010; Lebek and Uffen 2014). These studies have largely found negative outcomes over the days immediately following the breach announcements. Goel and Shawky (2009) found that a corporate security breach had a negative impact of approximately 1% of the firm's market value during the days surrounding the event. Kannan et al (2007) also found that there were negative short-term changes in market value but that the downturn did not hold in the long term. Hovav and Gray (2014) found that while some firms suffered losses after breaches, others were the winners.

Another popular focus was the effect of data breaches on consumer confidence and trust in the breached organization. O'Cass and Fenech (2003) and Shih (2004) found a negative relationship between security breaches and consumers' attitudes towards the breached businesses. Berezina et al. (2012) found that data breaches negatively affect satisfaction and the likelihood of customers recommending a hotel to others.

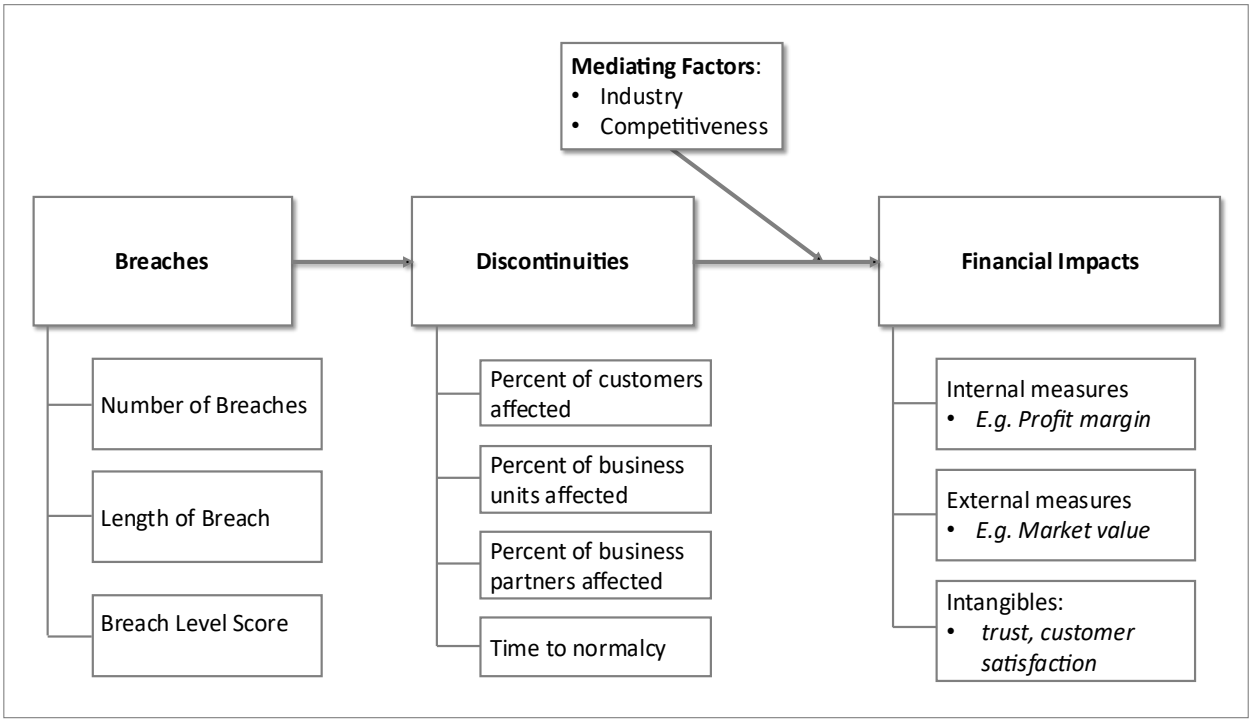
While trust and consumer confidence represent intangible measures, these are likely to impact firm value in the short term. Van der Heijden et al. (2003) found that the negative consumer attitudes affect customer adoption of eCommerce. More specifically, Suh and Han (2003) found that trust influences the customer's likelihood of accepting ecommerce.

Several works have addressed the recovery costs associated with breaches. Laytona and Watters (2007) found that businesses often incur large expenditure for remediation work and that these tangible costs are significant and often have a greater impact on businesses than the intangible costs such as consumer confidence.

CONCEPTUAL DEVELOPMENT

Figure 1 presents the theoretical model for analyzing breach impacts. Triggers cause discontinuities. When a tornado hits a production center it often destroys the company's building and equipment causing disruptions in the production processes. Similarly, when a business suffers a security breach, it often loses its ability to continue providing high-quality service to its customers and other stakeholders. Discontinuities represent the firm's inability to provide the service quality to which its customers are accustomed. The firm returns to a state of continuity when it regains normalcy, that is, all stakeholders regain the high-quality service that existed before the discontinuity. These discontinuities can adversely affect business performance.

FIGURE 1
THE DATA BREACH TO BUSINESS IMPACT MODEL



Target's 2013 data breach and Sony's 2014 breach are well known for being large-scale breaches that resulted in significant business disruptions. A large security breach, however, could result in little or no business disruption. Home Depot's 2014 data breach did not receive the same level of media coverage as Target and Sony's, and had far less disruptive impact on business operations, despite the fact that more than 56 million card numbers were exposed. This seems to suggest a disconnect between the size of the data breach and the resulting business discontinuity and in some cases the resulting financial impacts.

The scope of the discontinuities also varies. In some cases, information systems become unavailable to businesses because breached systems are not deemed fit for return to normal business use. In other cases, while the firms have all systems fully available and accessible to their customers, the resulting loss of trust hampers the natural business dynamics. The size and scope of the discontinuities, rather than the size of the initial data breach, seem to dictate the likelihood of the firm suffering adverse financial impacts.

The focal point of reporting on most data breaches has been the number of customers whose data has been compromised, and in many cases, the extent to which their financial data, such as credit card numbers, was exposed. These measures explain the trigger, that is the initial breach, not the discontinuity caused by the breach. Figure 1 addresses some of the classification elements for addressing discontinuity. First, many of today's large firms have multiple product lines, are supported by multiple and often geographically dispersed business units, and have customers that interact with some but not all of these business units. A discontinuity may therefore affect some business units – rather than the entire business. Second, discontinuities may have ripple effects throughout the entire value chain, rather than just in small sections of it. Thirdly, discontinuities may affect the entire customer base or be limited to small parts of it. Finally, discontinuities vary in duration. In some cases, businesses quickly repair and recover the affected systems and return to normal operations. In other cases, the effects of the breach are felt long after the system recovery is completed. That is, the resulting discontinuity lasts well beyond the duration of the breach and recovery period.

The resulting discontinuities have the potential to cause differing financial impacts. The operational impacts may take the form of recovery costs, lost sales, lost customers, remediation costs, and legal

liabilities, among others. This may translate to decreases in internal measures such as a decreased profit margin. In other cases, there are significant external impacts, for example falling market value. Breached businesses also suffer intangible costs such as loss of trust and decreased customer satisfaction.

Several factors may mediate the financial impacts of the discontinuity. Anecdotal evidence suggests that manufacturing firms are impacted less than service firms. Their ability to maintain inventory often allows them to survive the discontinuities without necessarily losing the ability to serve their customers. Service firms are often unavailable to their customers during periods of discontinuity.

DATA AND METHODOLOGY

Data necessary to test the full model is not yet publicly available. As such the statistical analysis is limited to the relationship between data breaches and internal financial metrics. The central question here is whether the data breaches and the resulting discontinuities have a significant impact on short-term financial performance. Specifically, does the profit margin in the breached business decline in the quarter following the security breach compared to performance over the prior quarters? Furthermore, given the unique nature of the retail sector, is the relationship between retailers the same as it is for the broader collection of firms?

Existing literature has assessed security breaches in three ways: (i) length of breach, (ii) severity of the breach (addressed here as the breach level score) and (iii) the number of breaches faced by affected firms. Several major breaches lasted for months before being discovered by the affected firms. These are deemed more harmful than breaches that lasted for very short periods. Other breaches, such as Target's 2013 breach were renowned for the number of records accessed during the breach. The popular breach level index website further classifies the level/severity of breaches on a 10-point scale. While their ranking algorithm is not public, the renowned breaches that have exposed millions of records are ranked at the top of the scale. Smaller breaches with few records accessed are ranked at the bottom.

Data is collected from two sources. First, security breach data is collected from the 'Breach Level Index' website. The online database provides information on the nature of the security breach, the company identity (which is now being suppressed), the breach level, and the number of customers whose data is affected. A full list of data points is presented in Table 1.

TABLE 1
DATA FIELDS FOR THE BREACH DATASET

Data Field	Description
Rank	Monthly ranking for the severity of the breach
Organization	Name of the breached organization
Records Breached	Number of customers whose data was affected
Type of Breach	Account Access; Financial Access; Identity Theft; Existential Data; Nuisance
Source of Breach	Accidental loss; hacktivist; malicious insider; malicious outsider; state sponsored; unknown
Location	Country – location for the company
Industry	Education; entertainment; financial; government; healthcare; hospitality; industrial; insurance; non-profit; professional services; retail; social media; technology; other.
Risk Score	0-10 score assigned by the breach level team – measure of severity of the breaches
Date of Breach	Day, month & year information

The data types shown in Table 1 are self-explanatory except for the 'Type of Breach'. This is further detailed in table 2. The data classification utilized in table 2 is also as presented in the breach index site. Breach data is collected for the period second quarter 2013 to second quarter 2018. This yielded 9,730 rows of data. Unfortunately, many of these firms have no publicly reported financial data.

TABLE 2
TYPE OF BREACH

Name	Description
Financial Access	Bank account credentials, credit card data.
Existential Data	National Security or Business ID
Account Access	username/password to social media sites, websites.
Identity Theft	SSN, ID number, name, medical records, date of birth
Nuisance	email address, affiliation etc.

The second data source was Macrotrends online financial data repository. The data site provides a large source of company financials for publicly traded firms. Profit margin data was pulled from this site. The resulting dataset comprises companies that have breached and have available financial data for the period 2013-2018 in the Macrotrends repository. The resulting data pertains to 166 companies and comprises 441 records, representing 441 individual data breaches. One hundred and twenty-seven of these breaches were for retail firms. Table 3 shows the distribution of the other breaches by industry.

TABLE 1
BREACH COUNT BY INDUSTRY

Industry	Account Access	Existential Data	Financial Access	Identity Theft	Nuisance	Total
Retail	8	5	71	40	3	**127**
Technology	21	10	6	41	15	**93**
Financial	5	2	38	43	2	**90**
Healthcare	1		4	72	1	**78**
Insurance				5		**5**
Industrial			1	3		**4**
Social media			1	3		**4**
Education				3		**3**
Entertainment	1			2		**3**
Government	1	1			1	**3**
Professional Services		1	1		1	**3**
Hospitality				1		**1**
Other	7	2	4	13	1	**27**
Grand Total	**44**	**21**	**126**	**226**	**24**	**441**

Each record in the combined dataset represents the profit margin for a company and the breach activity for the quarter in question. The data enabled the calculation of each company's profit margin for the period preceding the data breach and facilitated a comparison with the profit margin in the breached quarter. The prior profit margin is utilized as the 5-year same quarters average for the company. For example, a breach in the 4th quarter of 2014 would require the average of the profit margins for fourth quarters from 2009 to 2013. 't-Test: Paired Two Sample for Means' was utilized to measure the difference between the two sets of results. The outputs are presented in Tables 4 and 5.

RESULTS/FINDINGS

Table 4 shows the results for retail businesses only. The reports for the actual quarter in which the data breach took place were as follows. The present profit margin was (M = 0.0358, SD = 0.0712, N = 113) and was hypothesized to be less than the profit margins for the prior period average (M = 0.0604, SD = 0.0064, N =113). However, this difference was not significant, $t(112) = 1.082$, $p = 0.141$ (1-tail). While the 3.58 percent margin was markedly lower than the 6.04 percent margins for the preceding quarters, the analysis delivered a *p-value* of 0.141. Therefore, the performance for the breach quarters is not significantly different from those for the non-breached prior quarters.

Table 5 shows the results for all businesses in the dataset. Unlike the results for the retailers, the mean profit margin does not diminish for the affected quarter. In fact, the profit margin increases from 0.73% to 3.72%. The analysis also delivers a negative t-value. This implies that the hypothesis does not hold, that is, data breaches do not affect the short-term profit margin of businesses in the broader group.

TABLE 4
T-TEST: PAIRED TWO SAMPLE FOR MEANS FOR RETAIL FIRMS ONLY

	Prior	***Present***
Mean	6.0447061%	3.5773451%
Variance	0.006393686	0.071190951
Observations	113	113
Pearson Correlation	0.44009934	
Hypothesized Mean Difference	0	
df	112	
t Stat	1.081587939	
P(T<=t) one-tail	0.140879489	
t Critical one-tail	1.658572629	
P(T<=t) two-tail	0.281758977	
t Critical two-tail	1.981371815	

TABLE 5
T-TEST: PAIRED TWO SAMPLE FOR MEANS FOR ALL INDUSTRY DATA

	Prior	***Present***
Mean	0.73%	3.72%
Variance	0.802767725	0.1870816
Observations	360	360
Pearson Correlation	0.325302625	
Hypothesized Mean Difference	0	
df	359	
t Stat	-0.659134141	
P(T<=t) one-tail	0.255116096	
t Critical one-tail	1.64910915	
P(T<=t) two-tail	0.510232191	
t Critical two-tail	1.966593938	

DISCUSSION

There is broad support in academic literature for the negative short-term impacts of data breaches. These primarily address the negative impacts on shareholder wealth (Cavusoglu et al., 2002; Kannan et al., 2007; Yayla and Hu, 2011; Campbell, 2003; Gatzlaff and McCullough, 2010; Garget et al., 2003). Cavusoglu et. al (2002) and Hovav and D'Arcy (2003) found that data breaches impose significant costs on the affected companies both in the short and medium term. Short-term costs include investigation and remediation activities, legal advisory services, fines, and lost transactions (Aral 2013). However, these costs do not necessarily translate to a downwards movement in profitability.

The findings here (as shown in tables 4 and 5) do not challenge the earlier findings. Rather, it suggests that while security breaches result in significant costs to affected firms, these costs do not necessarily lead to decreased profitability measures for these firms over the ensuing quarter. This is especially important for firms that are small to medium-sized businesses that are often not publicly traded.

Large firms are often assessed on their ability to recover their market value after an adverse event, for example a security breach. Firms that are not publicly traded and smaller firms without large financial reserves are much more likely to be distressed by a strong quarterly downturn in profits. Tables 4 and 5 suggest that the feared decrease in profitability has not occurred for most firms that have breached their contracts.

The contribution of this paper is twofold. First, it challenges the broad presumption that data breaches naturally generate negative financial outcomes. The analysis failed to reveal a negative and significant relationship between data breaches and profit margins for both the retail subset of firms and the larger dataset.

Secondly, retailers are affected uniquely. Their results, although not statistically significant, were quite different from those of the larger collection of firms. This may be a result of the often intense levels of competition in the retail space, particularly in the general retail marketplace. For example, when Target suffers a data breach many of its customers simply move to Walmart or online to Amazon.com. There is very little effort required in that act of switching retailers. The process of switching would be a lot more challenging and time-consuming for many other types of businesses.

Furthermore, anecdotal evidence suggests that in the event of discontinuity, firms in highly competitive sectors are more affected than those in less competitive sectors. In the absence of true competitors, customers will have to wait for the business to recover. However, in very competitive marketplaces, customers are likely to move to a competitor.

There are also factors in play that currently lack quantifiable data for inclusion in an analysis of this nature. For example, how does the degree of media coverage and the choice of media outlets affect the customer's reaction to breaches and, hence, influence the financial outcome? Rosati et al. (2019) found a relationship between the short-term market value of firms after a breach and the nature of the breach communication.

The limitations of the study have all been woven into the discussion. A dataset based on small businesses, rather than publicly traded firms, would deliver a model uniquely tailored to these smaller firms that rely heavily on short-term profitability. However, these smaller (non-traded firms) do not provide much publicly available data. In addition to this, additional data on the competitive nature of the industries, the ranking of the firms within the competitive structure of the industry, and degree of media coverage will serve to refine the thesis.

Finally, the inability to categorize the discontinuities resulting from the breach is a major challenge for all breach impact studies. The relationship neglects a critical internal step in the larger breach impact model. This is so, irrespective of the choice of dependent variables. Anecdotal evidence suggests that data breaches pose challenges for businesses, and these challenges often result in a decline in business performance. Further studies are needed to classify discontinuities and address the long-term impacts of breaches. That is, do breached firms recover and continue to perform well in the long term, or do their performance lag behind that of their competitors who did not suffer similar breaches?

REFERENCES

Aivazpour, Z., Valecha, R., & Chakraborty, R. (2022). Data breaches: An empirical study of the effect of monitoring services. *ACM SIGMIS Database: The Database for Advances in Information Systems*, *53*(4), 65–82. https://doi.org/10.1145/3571823.3571829

Alharbi, F.S. (2020). Dealing with data breaches amidst changes in technology. *International Journal of Computer Science and Security*, *14*(3).

Aral, S., Dellarocas, C., & Godes, D. (2013). Introduction to the special issue—Social media and business transformation: A framework for research. *Information Systems Research*, *24*(1), 3–13.

Berezina, K., Cobanoglu, C., Miller, B.L., & Kwansa, F.A. (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 Hospitality Management*, *24*(7), 991–1010.

Breach Level Index. (n.d.). Retrieved from https://breachlevelindex.com/

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

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2002). The effect of internet security breach announcements on market value of breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*.

Cheney, J.S. (2010). *Heartland Payment Systems: Lessons learned from a data breach.* Federal Reserve Bank of Philadelphia.

Dalmadge, C.L. (2019). Impacts of data breaches on ecommerce growth. *International Journal of Business Research*, *19*(1), 81–86.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, *11*, 74–83.

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

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

Hill, C. (2014, September 25). Home Depot's data breach is worse than Target's, so where's the outrage? *MarketWatch*. Retrieved from http://www.marketwatch.com/story/yawn-who-cares-about-home-depots-data-breach-2014-09-24

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, *6*(2), 97–121.

Hovav, A., & Gray, P. (2014). The ripple effect of an information security breach event: A stakeholder analysis. *Communications of the Association for Information Systems*, *34*(50). https://doi.org/10.17705/1CAIS.03450

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce*, *12*(1), 69–91.

Layton, R., & Watters, P.A. (2014). A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications*, *19*(6), 321–330.

Lebek, B., & Uffen, J. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049–1092.

Muntermann, J., & Roßnagel, H. (2009). On the effectiveness of privacy breach disclosure legislation in Europe: Empirical evidence from the US stock market. In A. Jøsang, T. Maseng, & S.J. Knapskog (Eds.), *NordSec LNCS* (Vol. 5838, pp. 1–14). Springer.

O'Cass, A., & Fenech, T. (2003). Web retailing adoption: Exploring the nature of internet users' web retailing behavior. *Journal of Retailing and Consumer Services*, *10*(2), 81–94. https://doi.org/10.1016/S0969-6989(02)00004-8

Plachkinova, M., & Maurer, C. (2018). Security breach at Target: A teaching case. *Journal of Information Systems Education*, *29*(1), 11–20.
Quick, M., et al. (2017). World's biggest data breaches. *Information is Beautiful*. Retrieved from http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Rashid, F.Y. (2017). Target's data breach settlement sets a low bar for industry security standards. *CSO*. Retrieved from https://www.csoonline.com/article/3199064/security/targets-data-breach-settlement-sets-a-low-bar-for-industry-security-standards.html
Rosati, P., Deeney, P., Cummins, M., Van der Werff, L., & Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance*, *47*, 458–469.
Scanio, S., & Glasgow, J.W. (2015). Payment card fraud, data breaches, and emerging payment technologies. *Fidelity Law Journal*, *21*.
Shih, H.P. (2004). An empirical study on predicting user acceptance of e-shopping on the Web. *Information & Management*, *41*(3), 351–368. https://doi.org/10.1016/S0378-7206(03)00079-X
Spears, J.L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, *34*(3), 503–522.
Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce*, *7*(3), 135–161.
Van der Heijden, H., Verhagen, T., & Creemers, M. (2003). Understanding online purchase intentions: Contributions from technology and trust perspectives. *European Journal of Information Systems*, *12*(1), 41–48. https://doi.org/10.1057/palgrave.ejis.3000445
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.