The effect of data breaches on company performance

Ahmad H. Juma'h
Department of Accountancy, University of Illinois, Springfield, Illinois, USA, and
Yazan Alnsour
Department of Computer Information Systems, University of Northern Colorado, Greeley, Colorado, USA

Received 19 January 2019
Revised 20 April 2019
27 June 2019
Accepted 5 August 2019

Abstract

Purpose – This paper aims to analyze the effect of data breaches – whose concerns and implications can be legal, social and economic – on companies' overall performance.

Design/methodology/approach – Information on data breaches was collected from online compilations, and financial data on breached companies was collected from the Mergent Online database. The financial variables used were related to profitability, liquidity, solvency and company size to analyze the financial performance of the breached companies before and after the data breach event. Nonfinancial data, such as the type and the size of the breaches, was also collected. The data was analyzed using multiple regression.

Findings – The results confirm that nonmandatory information related to announcements of data breaches is a signal of companies' overall performance, as measured by profitability ratios, return on assets and return on equity. The study does not confirm a relationship between data breaches and stock market reaction when measuring quarterly changes in share prices.

Research limitations/implications – The main limitation of the study relates to ratio and trend analyses. Such analyses are commonly used when researching accounting information. However, they do not directly reflect the companies' conditions and realities, and they rely on companies' released financial reports. Another limitation concerns the confounding factors. The major confounding factors around the data breaches' dates were identified; however, this was not enough to assure that other factors were not affecting the companies' financial performance. Because of the nature of such events, this study needs to be replicated to include specific information about the companies using case studies. Therefore, the authors recommend replicating the research to validate the article's findings when each industry makes more announcements available.

Practical implications – To remediate the risks and losses associated with data breaches, companies may use their reserved funds.

Social implications – Company data breach announcements signal internal deficiencies. Therefore, the affected companies become liable to their employees, customers and investors.

Originality/value – The paper contributes to both theory and practice in the areas of accounting finance, and information management.

Keywords Financial performance, Data breaches, Nonfinancial factors, Number of breached records

Paper type Research paper

Declaration of interest: The authors report no conflicts of interest. The authors alone are responsible for the content and writing of this paper.

International Journal of Accounting & Information Management
Vol. 28 No. 2, 2020
pp. 275-301

1834-7649
DOI 10.1108/IJAIM-01-2019-0006

1. Introduction

Accelerated progress in communication, networks and information technologies is shaping global business, and it is estimated to continue changing business structures for the foreseeable future. This development has many advantages and disadvantages for all organizations' stakeholders. Information systems management is increasingly considering information security and privacy due to their potential critical issues for all company activities. The magnitude of the importance of breached data was described in the California Data Breach Report 2012-2015 (Harris, 2016) as follows:

> In the past four years, the Attorney General has received reports on 657 data breaches, affecting a total of over 49 million records of Californians. In 2012, there were 131 breaches, involving 2.6 million records of Californians; in 2015, 178 breaches put over 24 million records at risk. This means that nearly three in five Californians were victims of a data breach in 2015 alone (p. 8).

Multinational companies rely heavily on technology and always have some technical vulnerabilities, which means data breaches and losses are inevitable. Data is one of the company's most important assets, and the threat of losing data control is becoming an issue that affects everyone. No matter whether companies establish guidelines and controls to mitigate the risk of data breaches, hacking and phishing threats still exist. Information security and privacy is a determining factor for companies' continuity and sustainability. Companies are adopting several protection techniques such as system authentication, data encryption, user access control and firewalls as well as practices that aim to minimize such risks such as employee training and user orientation to the company's information security policy and protocols. Despite these measures, perpetrators are becoming more organized and sophisticated, and the risk is growing.

There are many recent examples of companies that have suffered from major data breaches – Equifax, Anthem, eBay, JPMorgan Chase, Home Depot, Yahoo and Target, among others. Assessing the economic effects of data breaches is a challenge for both accounting and information security management (Schatz and Bashroush, 2016). Research concerning the implications of data breaches is considered an emerging area (Ghosh and Swaminatha, 2001; Spanos and Angelis, 2015, 2016). Event studies have mostly shown that data breaches have a negative effect on cumulative abnormal returns of publicly traded companies. However, these same studies have shown mixed results concerning the significance of the relationship between data breaches and company value/share. Event studies using daily share prices investigate the immediate effect of a breach. Over a longer timeframe, Kannan *et al.* (2007) found no significant negative effect of information security breaches on company value. In descriptive and comparative studies, Ko and Dorantes (2006) found that sales increased significantly for the breached firms in the fourth quarter after a security breach, contradicting the negative effects shown in most event studies performed using daily share prices.

Stoel and Muhanna (2011) found that companies with information technology (IT) weaknesses performed worse than firms with no weaknesses. Data breaches indicate deficiencies in internal controls – particularly IT internal controls. Companies that are continually improving their IT controls to avoid cyber-incidents can reduce the risk of data breaches. However, hackers' ability to penetrate larger companies' records, such as those of Apple, Walmart and Equifax, indicates that hackers are becoming threats even to companies that invest heavily in IT. Brody *et al.* (2018) indicate that the potentially harmful effects of malware, which can be financial and nonfinancial, are often not well known.

To contribute to the existing literature, the goal of this article is to analyze the intermediate (quarterly) term effect of data breaches on companies' performance by

including qualitative and quantitative factors. Qualitative factors are increasingly being used by researchers in accounting, finance and IT studies (Arnold *et al.*, 2012; Vasarhelyi, 2012; No and Vasarhelyi, 2017). The article aims to verify the effect of data breach announcements on the overall performance of affected companies, as measured by changes in return on assets (ROA) and changes in return on equity (ROE). The study used nonfinancial variables such as the number of records breached and the type of breach. The nonfinancial information was obtained from online databases. The yearly fixed and industry-fixed effects were also incorporated. The financial variables used were ratios related to liquidity, solvency, leverage, book-to-market and capitalization. The Mergent Online database was used to obtain the companies' quarterly financial information.

The following section discusses the theoretical background to develop research statements. Section 3 discusses the data collection and research methodology. Section 4 presents the results. The last two sections present a summary of the main findings, notable conclusions, limitations and suggestions for future research.

2. Theoretical background

Since 2000, researchers have been increasingly more interested in the effect of information security events – such as privacy violations, denials of service and website defacements – on the confidentiality, integrity and availability of information systems (Spanos and Angelis, 2016). In the executive summary of the California Data Breach Report 2012-2015, these types of breaches are identified as generally being caused by malware and hacking, physical loss and human error. Data breaches are mostly breaches of sensitive personal information such as social security numbers, bank account information and medical information. The industry sectors most affected by data breaches are retail, finance, healthcare and small business.

Internal and external perpetrators have different motives and methods for accessing company data. External perpetrators or hackers are more skilled, organized and innovative. Therefore, the data breach type depends on the perpetrator, their intentions and the source of the threat. The source is important because outsider activities will be more dangerous than those from the inside (Jouini *et al.*, 2014). Therefore, this study anticipates that the data breaches characterized by a large number of breached records and perpetrated by external hackers affect companies' financial performance most negatively.

Parallel to advances in IT, companies are accumulating data to serve their customers better and become more competitive in the market. According to Muhanna and Stoel (2010), investors reward companies that have superior IT capability. However, using the internet is not without cost. Stakeholders are concerned when they see a company with a less-than-optimal level of IT security and information privacy (Schmidt *et al.*, 2016). Securing personal data is an ethical and legal responsibility of every organization that stores and uses that data. Several rules, regulations, enforcement actions, common law duties, contracts and self-regulatory regimes address secure information. Laws in the USA and European Union have security requirements for specific types of entities. The Federal Trade Commission (FTC) has the authority to fine a firm responsible for data breaches – but this does not limit the companies' possible liability for the occurrence of data breaches (Silverman, 2014).

The main objective of management is to pursue the perpetual growth of a corporation such that the wealth of its stockholders is maximized. The agency theory (Jensen and Meckling, 1976), and information asymmetry are crucial to understanding how and when management report information about data breach incidents; firms can improve their corporate governance and business ethics to reduce the self-interested motives of management and to avoid moral hazard. The agency theory examines how management's

behavior could be directed at stockholders' interest by reducing agency costs (Wang, 2010; Chen *et al.*, 2012). According to Brush *et al.* (2000) and Wang (2010), the agency theory is related to a manager's goal to maximize his or her personal wealth instead of the stockholders' wealth: management's self-interest produces waste and inefficiency in the presence of free cash flows, and the burden of agency costs is incurred by stockholders because of weak corporate governance (Jensen, 1986).

The Committee of Sponsoring Organizations (COSO), US Securities and Exchange Commission (SEC), Public Company Accounting Oversight Board (PCAOB), American Institute of Certified Public Accountants (AICPA), International Federation of Accountants (IFAC) and other regulators have created an ongoing field for internal controls discussion (Leach and Newsom, 2007). The SEC requires that publicly held corporations submit their audited financial statements and other supplementary information annually. Public data unavailability implies that investors cannot use frequently released financial information as an opportunity to generate profit from private information (Fu *et al.*, 2012). Companies that choose not to disclose material data breaches, losses or damage may face legal issues for not complying with the 2011 SEC disclosure guidance for cybersecurity and other released SEC requirements for cybersecurity disclosure (Trope, 2012). Companies are required to report material cybersecurity incidents to make the information available to stakeholders and investors.

There is a need for greater specification of systematic, policy-related controls to reduce the differences between software, mathematical models and accounting procedures to increase company efficiency (Karimi *et al.*, 2014). Auditors use different types of software and systems verifications; these verifications cannot assure that the data cannot be breached (Bradford and Florin, 2003; Eden *et al.*, 2014). The understanding of internal controls helps external auditors determine the scope of their audits (Gramling *et al.*, 2004). According to the PCAOB (2007) and the IFAC (2012), the external auditors may choose to rely on internal audit functions depending on their understanding of their strength. Sarbanes–Oxley Act (2002) increased researchers' interest in evaluating the internal controls of organizations (Desai *et al.*, 2011).

Further research can be carried out in this area to link internal controls and company events (Messier *et al.*, 2011; Weisner and Sutton, 2015). Noncompliance with the mandatory disclosure of an activity (e.g. corporate social responsibility) might affect companies' financial performance (Chen *et al.*, 2017). Data breaches, as company events, are related to a company's internal controls and its operational and overall efficiency.

According to the PCAOB, internal control deficiencies are related to significant single or combined deficiencies that result in the likelihood of a material misstatement on the annual or interim financial statements not being prevented or detected. In addition, significant deficiency and material weakness are both shortfalls in the design and administration of the internal controls. Deficiencies are less pervasive than material weaknesses, but multiple significant deficiencies such as data breaches could lead to material weakness.

According to Leach and Newsom (2007), control activities include top-level reviews, information processing, physical controls, performance indicators, duty segregation, control over information systems and ongoing monitoring. Doyle *et al.* (2007) investigate the relationship between internal control (material weakness), firm size and market value, but they do not make a correlation with bankruptcy. According to Ashbaugh-Skaife *et al.* (2007), there is a positive relationship between internal control deficiencies, control failure and unavailability of internal control resources. Kuhn *et al.* (2013) indicate that companies reporting IT weaknesses perform worse financially than companies with non-IT weaknesses.

To meet company needs, managers should seek operational and overall efficiency. Operational efficiency requires investing in new technologies such as software and maintaining training programs for employees to assure compliance with goals and policies; seeking a satisfactory relationship with customers, creditors and investors enables companies to maintain their overall performance (Haislip and Richardson, 2017). Data breach costs may be considered immaterial for larger companies, but data breaches signal inadequate investment in IT assets. This motivates comparing financial ratios of the performance of a company that suffered from data breaches.

According to Baird and Morrison (2005) and Lajili and Zéghal (2010), financial variables and ratios are suitable for performing financial data analysis. The use of financial ratios is common in accounting and finance research – ratios like indicators related to solvency, liquidity, leverage and effect size (Beaver, 1966, 1968; Roumani *et al.*, 2016). Altman (1968) designed a discriminatory model that, until now, had retained a predictive value for companies with financial difficulties. Discriminant analyses permit the use of qualitative and quantitative information for group firms according to similarities and differences. Grouping firms by observations leads to discriminant analysis. Some economic studies combine nonparametric approaches with parametric discrimination, as used by Altman (1968); logit analysis for distress prediction, as used by Ohlson (1980); and multiple regression univariate analysis, as used by Theodossiou (1993). The variables included in these studies were the following: earning per share (EPS), growth, ROA, assets, liabilities, rate of increase in sales, rate of increase in equity, rate of increase in assets, ROE, accounts receivables, inventory, debts, interest expense and dummy variables.

Fu *et al.* (2012) argue that more frequent financial reporting reduces information asymmetry. Some companies tend to deliberately exclude outsiders from the critical early phases of incident response to prevent a negative perception of their performance (Ahmad *et al.*, 2015). The quality and timing of reporting are important to investors' decisions. Leach and Newsom (2007), Stubben (2010) and Beaver *et al.* (2005, 2012) indicate that financial information quality is a considerable constraint for any reportage of financial information. The ratio analysis is affected by common variations when applying accounting principles, including inventory valuation, depreciation and amortization methods, capitalization and expenses recognitions, leasing, post-retirement benefit costs and recognition of specific items in the financial statements such as discontinued operations, impairments and significant operational and non-operational deficiencies.

In this article, we considered nonfinancial variables that include the type of data breach, number of records, whether the perpetrators were internal or external and industry classification; this is consistent of the materiality concept in accounting (Juma'h, 2009, 2014, 2019). These qualitative variables indicate the data breaches' materiality. For example, the performance was affected more in companies that suffered from a large breach of records (e.g. Yahoo, Sony and Equifax) than in those that suffered a smaller breach of records. Moreover, internal perpetrators did not affect companies' overall performance as much as sophisticated external ones. Operational deficiencies are reflected in a company's operational performance, and therefore, the authors of this article anticipate that, in the companies that suffered from data breaches, changes in operational performance are related to the changes in the companies' operational measures of liquidity, solvency and leverage.

The incidence of the data breaches is related to the deficiencies linked to internal controls, especially the preventive controls to protect a company's data (Stoel and Muhanna, 2011). The data breach announcements affect customer satisfaction and trust, which affect the breached companies' performance (Martin *et al.*, 2017). Bose and Luo (2014) state that managers should view security investment from a more comprehensive perspective,

considering IT- and non-IT-related factors related to firm performance, for example, to identifying and measuring companies' IT risks, which is linked to the data regarding information assets, threats, system vulnerability and security controls (Jerman-Blažič, 2008).

Companies use their resources to face and mitigate risks associated with severe data breaches; increase internal controls efficiency; increase investment in assets related to information systems; improve the relationship with affected parties through intensive marketing programs; compensate customers; improve the companies' image, reputation and trust (Martin, 2018; Mathur, 2018); and (in some cases) deal with charges or penalties from government agencies such as the SEC on accusations of not reporting events according to SEC regulation deadlines.

In relation to the stock market, there is evidence indicating that investors perceive the occurrence of data breaches negatively (Spanos and Angelis, 2016). Empirical investigations concerning companies' announcements are associated with stock market reactions. This is because companies' share prices and returns are commonly referenced, and the data is easy to access. Frino *et al.* (2007) indicate that market behaviors could be used to predict financial distress or difficulties, which includes data breaches. A more holistic approach to information security is needed to enable managers to play an effective role in information security (Soomro *et al.*, 2016; Marriott *et al.*, 2017). SEC requires that publicly held corporations annually submit their number of outstanding shares and closing market price (using firms' fiscal years as the valuation date). Based on finance theories related to the efficient market hypothesis, and at least in a semi-strong manner, the stock market is informationally efficient and reflects new information (Fama, 1970; Fama and French, 2015). The implications of the data breaches, as well as the implications of other financial and nonfinancial announcements or events, may affect the breached companies' market value. To consider the market price as an explanatory variable, this study used quarterly share prices around the data breach incidences.

3. Data and methodology

After 2000, many empirical studies (Campbell *et al.*, 2003; Ettredge and Richardson, 2003; Garg *et al.*, 2003; Hovav and D'Arcy, 2003; Kannan *et al.*, 2007; Gordon *et al.*, 2010) discussed the effect of data breaches on a firm's value. By searching the existing empirical studies, Spanos and Angelis (2016) found 37 related articles about 45 studies. They indicate that 75.6 per cent of the event studies show that data breaches have significant negative effects on companies' values. In general, the previous studies are limited to a few indicators, such as company and market return and the announcement of the data breaches. According to Spanos and Angelis (2016), there is a need to conduct more studies on the general effects of data breaches on a company's performance – such as the effects and implications in terms of sales, revenue, liquidity, solvency profitability and sustainability indicators.

3.1 Data collection

According to Pindado *et al.* (2008), panel data allows the elimination of unobservable heterogeneity by adding a large range of observations in a data set. Similar to Altman and Sabato (2007), panel data was used to organize the collected data in this study, and secondary data was used. To relate the data breaches to company performance, data is collected related to the announcements of data breaches that occurred due to security deficiencies, attacks, lost data, thefts or any other data privacy mismanagement. The authors search for announcements in online databases, namely, PrivacyRights.org and InformationIsBeautiful.net. The primary data source is PrivacyRights.org, which stores more than 8,000 events, most of which are related to governmental units, nonprofits and

private entities. InformationIsBeautiful.net is used to validate data content and to identify major breaches. Google Search is used to validate the announcements' content when discrepancies arose among them. For the purpose of the study, companies included in the sample must have financial reporting before and after the data breach announcements. From 2005 to 2017, the authors identified 795 data breach events from 450 companies that report ROA yearly. From these, the authors found 441 events for 290 companies that report ROA quarterly. These constitute the sample size of the analysis, which is comparable to that of contemporary accounting research on cybersecurity (Higgs *et al.*, 2016; Ettredge *et al.*, 2018).

The financial variables and ratios the authors use in this article are obtained from Mergent Online by the FTSE Russell database. The authors consider public firms traded in US stock markets – firms that have announced data breaches – for the study because they are required to report any major issues to the SEC within four days using 8-k reports. The companies' data is publicly accessible through the EDGAR database. The definitions of the financial variables are provided in Table X. The authors use the two-digit North American Industry Classification System (NAICS) for industry classification. The data collected for each breach includes the type of breach, number of records affected, date of the breach, type of industry and whether the company is publicly traded. The definitions of the nonfinancial variables are provided in Table XI.

3.2 Data description

Tables I and II provide some data-related descriptions of the sample used. Table I shows that there were more incidences of data breaches in 2010 and 2014 than in other years, and that about two-third of the sample occurred in or after 2010. The number of records hacked is an indicator of the data breaches' materiality (Table II).

According to Stoel and Muhanna (2009), the effect of IT capability on company performance depends on the external environment, such as industry characteristics. Table III shows the industry classifications using the two-digit NAICS. The finance and insurance industry demonstrates the most frequent occurrence of data breaches. This industry is targeted by hackers because of the sensitivity of the information on record; in addition, the black-market price motivates hackers to target the records of firms in the financial and insurance industry.

Year	Frequency	Cumulative frequency	(%)	Cumulative (%)	Total number of breached records
2005	10	10	2.27	2.27	27,934,500
2006	36	46	8.16	10.43	238,602
2007	36	82	8.16	18.59	84,329
2008	19	101	4.31	22.90	24,300
2009	15	116	3.40	26.30	23,829
2010	53	169	12.02	38.32	786,264
2011	37	206	8.39	46.71	2,771,782
2012	41	247	9.30	56.01	50,116,187
2013	43	290	9.75	65.76	36,491,461
2014	65	355	14.74	80.50	155,186,775
2015	30	385	6.80	87.30	90,379,471
2016	27	412	6.12	93.42	32,312
2017	29	441	6.58	100.00	34,086,353
Total	441		100.00		

Table I.
Distribution of data breaches by year

We used financial ratios as financial indicators related to a specific event such as a data breach. Changes in each company's overall performance for each company are used to measure the data breaches' effects on company performance. To determine the degree of change in a specific ratio as an indicator of such effects, the indicator (R) is considered in the quarter of the data breach incident, namely, (R_{t_0}); as a benchmark, the average of R in the four quarters immediately before the event is used, namely, ($A(R_{t_{-1}}\_R_{t_{-4}})$. The degree of change in R (dΔR) is defined as $(R_{t_0}/(A(R_{t_{-1}}\_R_{t_{-4}}) - 1)$. For example, the degree of change in ROA is $(ROA_{t_0}/(A(ROA_{t_{-1}}\_ROA_{t_{-4}}) - 1)$.

Table IV presents the variables used in the correlation analysis using multiple linear regression (MLR) with financial variables or ratios and MLR with financial variables or ratios and dummy variables (MLRDV).

The variables' descriptions as mean, median and standard deviations are provided in Table V. The mean values of dΔROA and dΔROE are –54.4 and –46.1 per cent, respectively. And, 23 per cent of the breaches are due to outside hackers. For major data breaches, the study considers companies with more than 100,000 records breached; examples of these companies are provided in Table XII. For these breaches, on average, the quarter (t_0) represents the minimum of the selected ratios. For example, ROAper cent on a subset of the sample related to major hacks shows, on average, a minimum level of ROAper cent at the event quarter (t_0). The polynomial function (ROAper cent = $0.0196t^2 - 0.0317t + 6.76$; R^2 = 0.569) is a better estimate than the linear function (ROAper cent = $-0.0149t + 6.947$; R^2 = 0.454). From Figure 1, we can observe that after the quarter t_0, ROAper cent began to increase.

Table II.
Data breach volume

Data breach volume range	Frequency	(%)
2-499	60	13.2
500-4,999	62	14.1
5,000-19,999	43	9.8
20,000-999,999	17	3.9
1,000,000-25,000,000	8	2
>25,000,000	4	1
No reported records	247	56
Total announcements	441	100.00

Table III.
Industry classification

Industry classification	Frequency	(%)
Finance and insurance	165	37.4
Manufacturing	58	13.2
Retail trade	44	10.0
Information and culture	44	10.0
Accommodation and food services	21	4.8
Administration and support services	21	4.8
Transportation and warehousing	19	4.3
Healthcare and social assistance	14	3.2
Professional, scientific and technical services	12	2.7
Wholesale trade	7	1.6
Others	36	8.2
	441	100

Variable	Variable description
dΔROA	The degree of change in returns on assets (dependent variable)
dΔROE	The degree of change in returns on equity (dependent variable)
Recs	The reported number of records
RecsM	The number of records affected by the data breach in millions
BInsd	Data breach conducted by an insider (someone with legitimate access intentionally breaching information, such as an employee, contractor or customer)
BHack	Data breach due to being hacked by an outside party or being infected by malware
BPhys	Data breach due to paper (nonelectronic) documents being lost, discarded or stolen
BDisc	Unintended disclosure (not involving hacking, intentional breaching or physical loss – e.g. sensitive information being posted publicly, mishandled or sent to the wrong party via online publishing, email, mail or fax)
BStat	Data breach due to stationary computer loss (lost, inappropriately accessed, discarded or stolen computer or server not designed for mobility)
BCard	Fraud involving debit and credit cards not accomplished via hacking (e.g. skimming devices at point-of-service terminals)
BUnkn	The data breach cause is unknown
CapM	The total capitalization in millions
dΔSP	The degree of change in the share price
dΔCR	The degree of change in the current ratio
dΔTAT	The degree of change in the total asset turnover
dΔCFS	The degree of change in the cash flow per share
dΔB/M	The degree of change in the book-to-market ratio
dΔCET	The degree of change in the cash and equivalent turnover
NAICS	The first two digits of the NAICS industry classification
Year	The year of the data breach

Table IV.
The classification of variables as either dependent or independent in MLR and MLRDV

Variable	Mean	SD	Minimum	Maximum
dΔROA	−0.544	20.980	−25.673	4.600
dΔROE	−0.461	20.262	−17.000	4.500
RecsM	7.749	30.435	0.693	18.792
BInsd	0.121	00.327	0.000	1.000
BHack	0.232	00.423	0.000	1.000
BPhys	0.158	00.366	0.000	1.000
BDisc	0.221	00.416	0.000	1.000
BStat	0.026	00.160	0.000	1.000
BUnkn	0.042	00.201	0.000	1.000
CapM	37,621	481,039	0.001	6,198,039
dΔSP	0.000	00.188	−0.504	0.976
dΔCR	0.000	00.188	−0.504	0.976
dΔTAT	0.003	00.135	−0.259	1.281
dΔCFS	1.527	17.388	−4.160	233.000
dΔB/M	−0.009	00.339	−2.622	1.569
dΔCET	0.0212	00.420	−0.838	2.560
NAICS	–	–	21	72
Year	–	–	2005	2017

Table V.
Descriptive statistics

3.3 Statistical tests

The *p-test*, *t-test*, *F-statistic test* and R^2 *values* are used to analyze regression results. Usually, *p-values* use 0.05 as a threshold. The *t-test* is used to verify multiple regressions' coefficient significance (Black, 2009). According to Iqbal and French (2005) and Tinoco and Wilson (2013), regression analysis is suitable for financial data analysis. This analysis uses the ordinary least squares (OLS) model to analyze the effect of data breaches on the affected companies' performance. Three measures are identified for performance measures (Table IV): dΔROA and dΔROE, acting as measures of overall performance; and dΔSP, acting as a measure of the reactions of investors in the stock markets to the data breach announcements.

Panel data sets have a fundamental advantage over cross-sections: they enable flexibility in modeling differences across individual companies in the sample. For the OLS model, this is the following: $y_{it} = X_{it}^{'}\beta + Z_{it}^{'}\alpha + e_{it}$; $y_{it} = X_{it}^{'}\beta + C_{it} + e_{it}$. The individual company effect is $Z_{it}^{'}\alpha$, where Z_i contains a constant term and a set of specific variables related to an individual (a company) or a group (a business classification). The specific variables are those that can be identified, such as financial ratios or variables, and those that are unobserved, such as a company's or a business's specific characteristics. If Z_i contains only a constant term, pooled regression can be used. For model structuring, the fixed and random effects are considered in panel data research. For fixed effects, if Z_i is unobserved but correlated with X_{it}, the OLS of β is biased and inconsistent because of omitted variable(s), and the model is $y_{it} = X_{it}^{'}\beta + \alpha_{it} + e_{it}$. Considering the random effect, the unobserved variables can be assumed to be uncorrelated with the included variables, and the model can be formulated as $y_{it} = X_{it}^{'}\beta + \alpha + u_{it} + e_{it}$. The random-effects approach specifies that u_{it} is a group-specific random element. The crucial difference between fixed and random effects is whether the omitted (unobserved) variables are correlated with the regressors in the model, not whether these effects are stochastic or not (Greene, 2012).

The authors use dummy variables for year-fixed effects and for business-classification-fixed effects to minimize the effect of omitted variable bias. A dummy variable is assigned, starting with 2005 and ending with 2017, for year-fixed effects, and the industry classifications are considered according to the two digits of the NAICS classification. The treatment of fixed effect assists in dealing with variation between inter-data breaches (variation from one data breach to another) and intra-data breaches (the variation within each data breach over time; Greene, 2012). The regression used is defined as $y_{it} = X_{it}^{'}\beta + year^{*}\ dummies + industry\ classifications^{*}\ dummies + e_{it}$. One year and one business classification are omitted to avoid perfect multcolinearity in the regression.

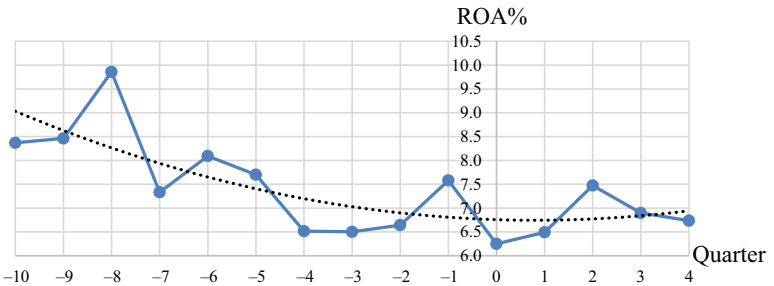

Figure 1.
ROA% polynomial trend

3.4 Results

Table VI shows the pairwise correlation coefficients of the dependent and independent variables. The dΔROA and dΔROE correlate with the BHack and the number of records in millions (RecsM) with a level of significance of 10 per cent. Because most of the companies use technology in some way, finding a higher correlation between dΔROA and dΔROE and the business classification is not expected. As expected, the correlation between dΔROA and dΔROE is high; this is because both ROA and ROE ratios are dependent on each other and are used as proxies to understand a company's overall performance.

The models of overall performance (proxies: dΔROA and dΔROE) are explained by the controlling variables. Table VII shows 12 models to explain dΔROA. In the models that include the natural logarithm of the number of records (LnRecs) as explanatory variables for dΔROA, the *t*-test is significant at the 1 per cent level. This indicates that larger data breaches had a greater effect than smaller ones. Using other controlling variables and including industry classification- and year-fixed effect, the LnRecs are significant at the 5 per cent level. Equation (1) shows F = 2.44 with $p < 0.01$. The data breaches affect the overall companies' performance as measured by dΔROA. The magnitude of the data breaches can be measured by the number of records affected (Table VII). The number of records is considered the key factor in determining the materiality of the effect of a data breach on a company's performance:

$$\begin{aligned} d\Delta ROA \;=\; & 0.777 - 0.114\,RecsM \;+\; 1.110\,BInsd \;+\; 1.111\,BHack \;+\; 1.668\,BPhys \\ & +\; 0.720\,BDisc - 0.033\,BStat \;+\; 0.755\,BUnkn \;+\; 0.001\,CapM \\ & -\; 1.497\,d\Delta CR \;+\; 0.511\,d\Delta TAT - 0.097\,CFS - 0.254\,B/M \\ & -\; 0.629\,d\Delta CET \;+\; NAICS^{*}\,dummies \;+\; Yearit^{*}\,dummies \;+\; e_{it} \end{aligned} \tag{1}$$

Like with dΔROA, equation (2) shows that dΔROE was found significant (F = 1.47, $p < 0.01$; see Table VIII). Furthermore, the number of records breached is considered the material factor in explaining the decrease in company performance, measured by dΔROE (Table VIII):

$$\begin{aligned} d\Delta ROE \;=\; & 1.76 - 0.056\,RecsM \;+\; 0.869\,BInsd \;+\; 1.195\,BHack \;+\; 2.287\,BPhys \\ & +\; 1.111\,BDisc \;+\; 0.331\,BStat \;+\; 0.855\,BUnkn \;+\; 0.001\,CapM - 2.392\,d\Delta CR \\ & +\; 0.567\,d\Delta TAT - 0.171\,CFS \;-\; 0.435\,B/M - 0.761\,d\Delta CET \\ & +\; NAICS^{*}\,dummies \;+\; Yearit^{*}\,dummies \;+\; e_{it} \end{aligned} \tag{2}$$

However, for the model of stock market reaction (proxy: dΔSP), the F-test is not significant at the 10 per cent level. Investors in stock markets may react to data breach announcements on a daily basis, as indicated by previous research (Spanos and Angelis, 2016), and not on a quarterly basis; this is because other confounding events may minimize the effect of the announcements over time.

4. Conclusion

From the trend analysis, the evidence showed that breached companies suffered in terms of performance during the quarter of the breach. This confirms that the financial statements

Table VI.
Pairwise correlation coefficient between variables

Variables	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. RecsM	1.000														
2. BInsd	−0.056	1.000													
3. BHack	0.285*	−0.204*	1.000												
4. BPhys	−0.069	−0.161*	−0.238*	1.000											
5. BDisc	−0.085	−0.198*	−0.292*	−0.231*	1.000										
6. BStat	−0.026	−0.061	−0.090	−0.071	−0.088	1.000									
7. BUnkn	−0.034	−0.078	−0.115	−0.091	−0.112	−0.035	1.000								
8. CapM	−0.013	−0.027	−0.044	−0.032	0.138	−0.014	−0.018	1.000							
9. dΔROA	−0.498*	0.064	−0.113	−0.008	0.060	0.033	0.023	0.005	1.000						
10. dΔROE	−0.319	0.045	−0.129	0.023	−0.019	0.046	0.022	0.012	0.869	1.000					
11. dΔCR	−0.134	0.110	−0.049	−0.051	−0.090	0.029	−0.021	0.040	0.126	−0.007	1.000				
12. dΔTAT	−0.019	0.064	−0.103	0.102	−0.021	−0.012	−0.033	0.090	−0.011	−0.016	−0.036	1.000			
13. dΔCFS	−0.013	−0.030	−0.055	−0.032	−0.023	−0.015	−0.019	−0.010	0.013	0.021	0.056	0.028	1.000		
14. dΔB/M	−0.007	0.085	0.047	−0.053	−0.167*	0.032	0.043	−0.065	0.017	0.100	0.093	−0.107	0.016	1.000	
15. dΔCET	0.035	−0.045	−0.040	0.192*	0.015	−0.045	0.026	0.034	−0.085	−0.043	−0.333*	0.383*	0.004	−0.166*	1.000

Note: *$p < 0.1$

Variables	1 dΔROA	2 dΔROA	3 dΔROA	4 dΔROA	5 dΔROA	6 dΔROA
RecsM	−0.114*** (0.014)	−0.115*** (0.015)	−0.116*** (0.015)	−0.119*** (0.016)	−0.116*** (0.015)	−0.116*** (0.016)
BInsd					0.585 (0.693)	0.453 (0.736)
BHack					0.475 (0.596)	0.290 (0.627)
BPhys					0.006 (0.641)	0.256 (0.677)
BDisc					0.400 (0.587)	0.075 (0.611)
BStat					0.654 (1.248)	0.059 (1.247)
BUnkn					0.395 (1.020)	0.079 (1.046)
CapM						
dΔCR						
dΔTAT						
dΔCFS						
dΔB/M						
dΔCET						
Industry included		Yes	Yes	Yes		Yes
Years included				Yes		
Constant	−0.307 (0.190)	−0.303 (2.529)	−0.206 (1.297)	−0.931 (2.955)	−0.607 (0.426)	−0.593 (2.646)
Number of breaches	190	190	190	190	190	190
R^2	0.248	0.348	0.294	0.389	0.254	0.351
Adjusted R^2	0.244	0.280	0.242	0.274	0.225	0.256
F-test	61.950	5.080	5.650	3.380	8.850	3.710

Notes: Standard errors in parentheses; ***$p < 0.01$; **$p < 0.05$; *$p < 0.1$

(*continued*)

Table VII.
OLSDV results for variables predicting dΔROA

Variables	7 dΔROA	8 dΔROA	9 dΔROA	10 dΔROA	11 dΔROA	12 dΔROA
RecsM	−0.116*** (0.015)	−0.118*** (0.017)	−0.116*** (0.014)	−0.116*** (0.015)	−0.116*** (0.014)	−0.114*** (0.017)
BInsd	1.395* (0.747)	1.090 (0.799)	0.271 (0.793)	−0.018 (0.930)	1.229 (0.972)	1.110 (1.174)
BHack	0.522 (0.704)	0.243 (0.742)	0.018 (0.658)	0.017 (0.736)	0.946 (0.944)	1.111 (1.110)
BPhys	0.453 (0.762)	0.467 (0.824)	0.146 (0.749)	0.394 (0.847)	1.228 (1.052)	1.668 (1.268)
BDisc	0.663 (0.670)	0.227 (0.725)	0.139 (0.692)	−0.144 (0.771)	0.784 (0.895)	0.720 (1.069)
BStat	0.850 (1.274)	0.265 (1.286)	0.099 (1.253)	−0.340 (1.281)	0.602 (1.369)	−0.0334 (1.476)
BUnkn	1.518 (1.094)	1.149 (1.147)	0.149 (0.950)	−0.515 (1.041)	0.914 (1.136)	0.755 (1.313)
CapM			−0.001 (0.001)	−0.001 (0.001)	−0.001 (0.001)	−0.001 (0.001)
dΔCR			−1.010 (1.393)	−0.711 (1.537)	−1.925 (1.517)	−1.497 (1.723)
dΔTAT			−0.079 (1.636)	0.004 (1.756)	0.346 (1.747)	0.511 (1.977)
dΔCFS			0.061 (0.172)	−0.044 (0.179)	−0.011 (0.188)	−0.097 (0.199)
dΔB/M			−0.739 (0.690)	−0.619 (0.762)	−0.397 (0.737)	−0.254 (0.856)
dΔCET			−0.602 (0.684)	−0.435 (0.727)	−0.753 (0.778)	−0.629 (0.841)
Industry included		Yes		Yes		Yes
Years included	Yes	Yes			Yes	Yes
Constant	−1.1 (1.388)	−1.599 (3.045)	−0.288 (0.487)	−0.369 (2.437)	−0.391 (1.438)	0.777 (3.053)
Number of breaches	190	190	122	122	122	122
R^2	0.312	0.4000	0.434	0.534	0.483	0.565
Adjusted R^2	0.236	0.258	0.366	0.380	0.349	0.334
F-test	4.070	2.830	6.380	3.470	3.590	2.440

Table VII.

Variables	1 dΔROE	2 dΔROE	3 dΔROE	4 dΔROE	5 dΔROE	6 dΔROE
RecsM	−0.054*** −0.0122	−0.058*** (0.013)	−0.054*** (0.013)	−0.060*** (0.014)	−0.052*** (0.013)	−0.057*** (0.014)
BInsd					−0.030 (0.593)	−0.366 (0.656)
BHack					−0.382 (0.517)	−0.443 (0.554)
BPhys					−0.187 (0.558)	−0.134 (0.599)
BDisc					−0.384 (0.502)	−0.595 (0.528)
BStat					0.302 (1.042)	−0.0483 (1.053)
BUnkn					−0.079 (0.854)	−0.254 (0.882)
CapM						
dΔCR						
dΔTAT						
dΔCFS						
dΔB/M						
dΔCET						
Industry included		Yes		Yes		Yes
Years included			Yes	Yes		
Constant	−0.351** (0.163)	−0.249 (2.124)	0.487 (1.092)	−0.302 (2.531)	−0.154 (0.368)	0.195 (2.224)
Number of breaches	178	178	178	178	178	178
R^2	0.101	0.208	0.142	0.241	0.108	0.216
Adjusted R^2	0.096	0.118	0.074	0.087	0.072	0.093
F-test	19.870	2.320	2.080	1.560	2.940	1.760

Notes: Standard errors in parentheses; ***$p < 0.01$; **$p < 0.05$; *$p < 0.1$

(*continued*)

Table VIII.
OLSDV results for variables predicting dΔROE

Variables	7 dΔROE	8 dΔROE	9 dΔROE	10 dΔROE	11 dΔROE	12 dΔROE
RecsM	−0.052*** (0.013)	−0.058*** (0.014)	−0.053*** (0.013)	−0.055*** (0.014)	−0.054*** (0.013)	−0.056*** (0.015)
BInsd	0.484 (0.654)	0.086 (0.732)	0.147 (0.724)	−0.513 (0.857)	1.299 (0.881)	0.869 (1.072)
BHack	−0.304 (0.622)	−0.498 (0.669)	−0.448 (0.604)	−0.636 (0.662)	1.047 (0.900)	1.195 (1.038)
BPhys	0.121 (0.688)	−0.013 (0.761)	0.0771 (0.702)	0.341 (0.765)	1.508 (0.990)	2.287* (1.169)
BDisc	−0.229 (0.593)	−0.492 (0.651)	0.136 (0.623)	−0.225 (0.677)	1.029 (0.825)	1.111 (0.959)
BStat	0.534 (1.087)	0.029 (1.117)	0.204 (1.120)	−0.273 (1.112)	0.930 (1.215)	0.331 (1.264)
BUnkn	0.705 (0.947)	0.542 (1.006)	0.125 (0.850)	−0.514 (0.906)	0.997 (1.018)	0.855 (1.146)
CapM			−0.001 (0.001)	−0.001 (0.001)	−0.001 (0.001)	−0.001 (0.001)
dΔCR			−1.444 (1.295)	−1.534 (1.381)	−2.533* (1.418)	−2.392 (1.536)
dΔTAT			0.334 (1.487)	0.116 (1.531)	0.905 (1.576)	0.567 (1.701)
dΔCFS			0.027 (0.156)	−0.064 (0.157)	−0.068 (0.168)	−0.171 (0.172)
dΔB/M			−0.470 (1.000)	−0.344 (1.029)	−0.351 (1.030)	−0.435 (1.087)
dΔCET			−0.433 (0.627)	−0.406 (0.651)	−0.688 (0.700)	−0.761 (0.734)
Industry included		Yes		Yes		Yes
Years included	Yes	Yes			Yes	Yes
Constant	−0.53 (1.179)	0.970 (2.595)	−0.314 (0.436)	−0.760 (1.420)	−0.523 (1.272)	1.76 (2.629)
Number of breaches	178	178	115	115	115	115
R^2	0.156	0.253	0.202	0.393	0.293	0.462
Adjusted R^2	0.055	0.063	0.1000	0.176	0.095	0.148
F-test	1.540	1.330	1.970	1.810	1.480	1.470

Table VIII.

Variables	1 roeMod 1	2 roeMod 2	3 roeMod 3	4 roeMod 4	5 roeMod 5	6 roeMod 6
RecsM	0.001 (0.001)	0.001 (0.001)	0.001 (0.001)	0.001 (0.001)	0.001 (0.001)	0.001 (0.001)
BInsd					−0.068 (0.058)	−0.093 (0.063)
BHack					−0.032 (0.048)	−0.038 (0.052)
BPhys					−0.012 (0.054)	−0.030 (0.060)
BDisc					−0.015 (0.049)	−0.039 (0.051)
BStat					−0.136 (0.097)	−0.117 (0.099)
BUnkn					−0.005 (0.090)	−0.043 (0.092)
CapM						
dΔCR						
dΔTAT						
dΔCFS						
dΔB/M						
dΔCET						
Industry included		Yes	Yes	Yes		Yes
Years included				Yes		
Constant	0.0534*** (0.016)	0.166 (0.140)	−0.0784 (0.100)	−0.126 (0.177)	0.0788** (0.036)	0.166 (0.142)
Number of breaches	168	168	168	168	168	168
R^2	0.002	0.124	0.08	0.208	0.022	0.143

Notes: Standard errors in parentheses; ***$p < 0.01$; **$p < 0.05$; *$p < 0.1$

(*continued*)

Table IX.
OLSDV results for variables predicting dΔSP

Table IX.

Variables	7 roeMod 7	8 roeMod 8	9 roeMod 9	10 roeMod 10	11 roeMod 11	12 roeMod 12
RecsM	0.001 (0.001)	0.001 (0.001)	0.001 (0.001)	0.001 (0.001)	0.001 (0.001)	0.001 (0.001)
BInsd	−0.077 (0.063)	−0.107 (0.068)	−0.027 (0.071)	−0.074 (0.083)	−0.075 (0.081)	−0.140 (0.086)
BHack	−0.021 (0.057)	−0.030 (0.061)	−0.054 (0.060)	−0.037 (0.067)	−0.138** (0.078)	−0.137* (0.082)
BPhys	−0.019 (0.064)	−0.024 (0.072)	−0.032 (0.072)	−0.057 (0.085)	−0.110 (0.090)	−0.124 (0.100)
BDisc	−0.017 (0.056)	−0.047 (0.060)	−0.048 (0.064)	−0.083 (0.070)	−0.109 (0.075)	−0.179** (0.078)
BStat	−0.093 (0.101)	−0.048 (0.103)	−0.160 (0.110)	−0.115 (0.111)	−0.111 (0.110)	−0.020 (0.106)
BUnkn	−0.019 (0.096)	−0.076 (0.100)	−0.026 (0.095)	−0.127 (0.102)	−0.057 (0.101)	−0.182* (0.103)
CapM			0.000 (0.000)	0.000 (0.000)	0.000 (0.000)	0.000 (0.000)
dΔCR			0.080 (0.127)	0.154 (0.136)	0.065 (0.127)	0.140 (0.124)
dΔTAT			−0.057 (0.144)	−0.010 (0.152)	−0.115 (0.142)	−0.042 (0.141)
dΔCFS			0.002 (0.015)	−0.010 (0.016)	0.011 (0.015)	0.005 (0.014)
dΔB/M			0.060 (0.060)	0.044 (0.064)	0.057 (0.060)	0.014 (0.059)
dΔCET			0.055 (0.062)	0.040 (0.064)	0.068 (0.064)	0.031 (0.062)
Industry included		Yes		Yes		Yes
Years included	Yes	Yes			Yes	Yes
Constant	−0.0504 (0.109)	0.0879 (0.182)	0.0891* (0.046)	0.164 (0.138)	0.694*** (0.208)	0.554** (0.218)
Number of breaches	168	168	112	112	112	112
R^2	0.093	0.225	0.048	0.284	0.273	0.559

and their accompanying notes, as mandatory information adhering to generally accepted accounting principles and SEC guidelines and requirements, are an important source of information for all stakeholders. The information voluntarily released by companies regarding data breaches and cybersecurity incidents can be considered an indication of their performance. The number of records affected and the type of breach (as proxies for the importance of data breach incidents) are shown to be significant explanatory variables for dΔROA and dΔROE, as shown by pairwise correlation coefficient analysis and MLRDV analysis. This supports the argument that nonmandatory information can assist stakeholders in determining the effect of events on companies' performance.

In summary, the occurrence of a data breach affects a company's overall performance as measured by dΔROA and dΔROE. Data breach announcements signal internal deficiencies in breached companies; therefore, the affected companies become liable to their employees, customers and investors. To remediate the risks and losses associated with data breaches, companies may use their reserved funds. The findings of this research contribute to both theory and practice in the areas of accounting, finance and information management.

Variable	Symbol	Definition	Purpose
Return on assets	ROA	Net income divided by average total assets	Overall financial performance; signals effective uses of both assets and capital
Return on equity	ROE	Net income divided by average stockholders' equity	Indicates how efficiently a company uses the capital it receives from its owners to generate an investment return to those shareholders
Share price	SP	Market value per common share	Measures the stock market valuation of the company's assets
Current ratio	CR	Current assets divided by current liabilities	Proxy for company financial health; the ability to pay back company liabilities with its assets
Total assets turnover ratio	TAT	Net sales revenue divided by average total assets	Measures the value of a company's sales or revenues generated relative to the value of its assets; efficiency measurement
Cash flow per share	CFS	Net income divided by the number of outstanding shares	Proxy for financial strength
Book value to market value	B/M	Book value by market value per share	Proxy for the value of a company
Cash and equivalents turnover	CET	Sales revenue divided by average cash and equivalents	Proxy for immediate liquidity

Table X.
Financial variables definitions and purposes

Variable	Description
Number of records	A numeric variable that indicates the number of breached records. For normalization purposes, the number of records in millions was used in the regression analysis
Reported number of records	1 – for events announcements reporting the number of records.0 – for announcements not reporting the number of records
NAICS	The first two digits of NAICS to present industry classification
Date of the breach	The date of the breach in MM/DD/YYYY

Table XI.
Description of nonfinancial explanatory variables

Table XII.
Examples of data breached

Name	Business class	Records (1,000)	Breach method	The content of the announcement	Source
Yahoo	BSO	3,000,000	Hack	2016: "Yahoo warned on that it had uncovered a massive cyber-attack, saying data from more than 1 billion user accounts were compromised in 2013, making it the largest breach in history. The number of affected accounts was double the number implicated in 2014 breach that the internet company disclosed and blamed on hackers working on behalf of a government. Yahoo required all of its customers to reset their passwords. Yahoo also said that it believes hackers responsible for the previous breach had also accessed the company proprietary code to learn how to forge 'cookies' that would allow hackers to access an account without a password"	privacyrights.org
eBay	BSO	145,000	Hack	2014: "The company has said hackers attacked between late February and early March with login credentials obtained from 'a small number' of employees. They then accessed a database containing all user records and copied "a large part" of those credentials"	informationisbeautiful.net
Equifax	BSF	143,000	Hack	2017: "One of the largest credit bureaus in the U.S. said on Sept. 7, 2017, that an application vulnerability on one of their websites led to a data breach that exposed about 147.9 million consumers. The breach was discovered in July, but the company says that it started in May"	csoonline.com
TJX	BSO	94,000	Hack	2007: "Hackers hacked a Minnesota store Wi-Fi network and stole data from credit and debit cards of shoppers at off-price retailers TJX, owners of nearly 2,500 stores, including T.J. Maxx and Marshalls. This case is believed to be the largest such breach of consumer information"	informationisbeautiful.net

(*continued*)

Name	Business class	Records (1,000)	Breach method	The content of the announcement	Source
Anthem	MED	80,000	Hack	2016: "The second-largest health insurer in the U.S., formerly known as WellPoint, said a cyber attack had exposed the names, addresses, Social Security numbers, dates of birth and employment histories of current and former customers—everything necessary to steal an identity"	csoonline.com
Chase	BSF	76,000	Hack	2014: "The US's largest bank was compromised by hackers, stealing names, addresses, phone numbers and emails of account holders. The hack began in June but was not discovered until July, when the hackers had already obtained the highest level of administrative privilege to dozens of the bank's computer servers"	informationisbeautiful.net
Target Stores	BSR	70,000	Hack	2014: "Investigators believe the data was obtained via software installed on machines that customers use to swipe magnetic strips on their cards when paying for merchandise at Target"	informationisbeautiful.net
Home Depot	BSO	56,000	Hack	2014: "Malware installed on cash register system across 2,200 stores syphoned credit card details of up to 56 million customers. Maybe the same group of Russian and Ukrainian hackers responsible for the data breaches at Target, Sally Beauty and P.F. Chang's . . ."	informationisbeautiful.net
Adobe	BSO	36,000	Hack	2013: "Hackers obtained access to a large swath of Adobe customer IDs and encrypted passwords and removed sensitive information (i.e., names, encrypted credit or debit card numbers, expiration dates, etc.). Approximately 36 million Adobe customers were involved: 3.1 million whose credit or debit card information was taken and nearly 33 million active users whose current, encrypted passwords were in the database [were] taken"	informationisbeautiful.net

(*continued*)

Table XII.

Name	Business class	Records (1,000)	Breach method	The content of the announcement	Source
Dun and Bradstreet	BSO	33,600	Hack	2014: "Hackers stole millions of social security numbers from large US data brokers Dun and Bradstreet Corp and Kroll Background America Inc, owned by Altegrity. Correction 7 Jan 2015: we previously stated that records were stolen from LexisNexis. LexisNexis conducted a thorough investigation of the malware intrusion and found no evidence that the malware accessed or stole any customer or consumer data"	informationisbeautiful.net
Sony	BSO	24,600	Hack	2011: "Hacked by LulzSec. In addition to the Sony PlayStation Network breach, compromised 77 million records. More than 23,000 lost financial data, according to Sony"	informationisbeautiful.net

Table XII.

5. Limitations and future research

The main limitation of this study, as in all empirical studies, relates to ratio and trend analyses. Such analyses are commonly used in researching accounting information. However, they are mere proxies of the companies' conditions and realities, and they rely on companies' released financial reports. Companies use and make different accounting treatments, estimations and decisions to report their financial performance. The consistency or reliability of such information is a matter of judgment. Another limitation concerns the confounding events. The authors have attempted to identify the major confounding events around the dates of the data breaches; however, this is not enough to rule out the possibility that other events do not affect these companies' financial performance. Therefore, the authors recommend replicating the research when more announcements become available per industry type to enable the validation of the findings.

Risk assessment is another avenue to be addressed. This would verify how investors perceive data breaches, taking into consideration several factors such as the size of the companies, the type of industry, whether the effects are local or global, the hackers' ability to penetrate larger companies' records and other nonfinancial items. Stakeholders are concerned by the companies' level of IT security and information privacy (Schmidt *et al.*, 2016). More research is needed on the integration of qualitative factors regarding the risk of cyber exposure in auditing works (No and Vasarhelyi, 2017). Further research can be carried out to link internal accounting controls and information technology controls and the occurrence of data breaches as part of company events related to companies' operational and overall financial and nonfinancial efficiency. Acquiring new technologies, such as software and hardware, should be considered by information security management. Investing in IT can reduce the likelihood of a data breach. Future research can investigate the relationship between investing in IT and the occurrence of data breaches (Table IX-XII).

References

Ahmad, A., Maynard, S.B. and Shanks, G. (2015), "A case analysis of information systems and security incident responses", *International Journal of Information Management*, Vol. 35 No. 6, pp. 717-723.

Altman, E.I. (1968), "Financial ratios, discriminant analysis and the prediction of corporate bankruptcy", *The Journal of Finance*, Vol. 23 No. 4, pp. 589-609.

Altman, E.I. and Sabato, G. (2007), "Modelling credit risk for SMEs: evidence from the US market", *Abacus*, Vol. 43 No. 3, pp. 332-357.

Arnold, V., Bedard, J.C., Phillips, J.R. and Sutton, S.G. (2012), "The impact of tagging qualitative financial information on investor decision making: implications for XBRL", *International Journal of Accounting Information Systems*, Vol. 13 No. 1, pp. 2-20.

Ashbaugh-Skaife, H., Collins, D.W. and Kinney, W.R. Jr, (2007), "The discovery and reporting of internal control deficiencies prior to SOX-mandated audits", *Journal of Accounting and Economics*, Vol. 44 Nos 1/2, pp. 166-192.

Baird, D.G. and Morrison, E.R. (2005), "Serial entrepreneurs and small business bankruptcies", *Columbia Law Review*, Vol. 105, p. 2310.

Beaver, W.H. (1966), "Financial ratios as predictors of failure", *Journal of Accounting Research*, Vol. 4, pp. 71-111.

Beaver, W.H. (1968), "Market prices, financial ratios, and the prediction of failure", *Journal of Accounting Research*, Vol. 6 No. 2, pp. 179-192.

Beaver, W.H., Correia, M. and McNichols, M.F. (2012), "Do differences in financial reporting attributes impair the predictive ability of financial ratios for bankruptcy?", *Review of Accounting Studies*, Vol. 17 No. 4, pp. 969-1010.

Beaver, W.H., McNichols, M.F. and Rhie, J.-W. (2005), "Have financial statements become less informative? Evidence from the ability of financial ratios to predict bankruptcy", *Review of Accounting Studies*, Vol. 10 No. 1, pp. 93-122.

Black, K. (2009), *Business Statistics: Contemporary Decision Making*, John Wiley and Sons, Hoboken, NJ.

Bose, R. and Luo, X. (2014), "Investigating security investment impact on firm performance", *International Journal of Accounting and Information Management*, Vol. 22 No. 3, pp. 194-208.

Bradford, M. and Florin, J. (2003), "Examining the role of innovation diffusion factors on the implementation success of enterprise resource planning systems", *International Journal of Accounting Information Systems*, Vol. 4 No. 3, pp. 205-225.

Brody, R.G., Chang, H.U. and Schoenberg, E.S. (2018), "Malware at its worst: death and destruction", *International Journal of Accounting and Information Management*, Vol. 26 No. 4, pp. 527-540.

Brush, T.H., Bromiley, P. and Hendrickx, M. (2000), "The free cash flow hypothesis for sales growth and firm performance", *Strategic Management Journal*, Vol. 21 No. 4, pp. 455-472.

Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L. (2003), "The economic cost of publicly announced information security breaches: empirical evidence from the stock market", *Journal of Computer Security*, Vol. 11 No. 3, pp. 431-448.

Chen, C.X., Lu, H. and Sougiannis, T. (2012), "The agency problem, corporate governance, and the asymmetrical behavior of selling, general, and administrative costs", *Contemporary Accounting Research*, Vol. 29 No. 1, pp. 252-282.

Chen, Y.C., Hung, M. and Wang, Y. (2017), "The effect of mandatory CSR disclosure on firm profitability and social externalities: evidence from China", *Journal of Accounting and Economics*, Vol. 65 No. 1, pp. 169-190.

Desai, N.K., Gerard, G.J. and Tripathy, A. (2011), "Internal audit sourcing arrangements and reliance by external auditors", *Auditing: A Journal of Practice and Theory*, Vol. 30 No. 1, pp. 149-171.

Doyle, J., Ge, W. and McVay, S. (2007), "Determinants of weaknesses in internal control over financial reporting", *Journal of Accounting and Economics*, Vol. 44 Nos 1/2, pp. 193-223.

Eden, R., Sedera, D. and Tan, F.B. (2014), "Sustaining the momentum: archival analysis of enterprise resource planning systems (2006-2012)", *Communications of the Association for Information Systems*, Vol. 35, p. 3.

Ettredge, M., Guo, F. and Li, Y. (2018), "Trade secrets and cyber security breaches", *Journal of Accounting and Public Policy*, Vol. 37 No. 6, pp. 564-585.

Ettredge, M. and Richardson, V.J. (2003), "Information transfer among internet firms: the case of hacker attacks", *Journal of Information Systems*, Vol. 17 No. 2, pp. 71-82.

Fama, E.F. (1970), "Efficient Capital markets: a review of theory and empirical work", *The Journal of Finance*, Vol. 25 No. 2, pp. 383-417.

Fama, E.F. and French, K.R. (2015), "Incremental variables and the investment opportunity set", *Journal of Financial Economics*, Vol. 117 No. 3, pp. 470-488.

Frino, A., Jones, S. and Wong, J.B. (2007), "Market behaviour around bankruptcy announcements: evidence from the Australian stock exchange", *Accounting and Finance*, Vol. 47 No. 4, pp. 713-730.

Fu, R., Kraft, A. and Zhang, H. (2012), "Financial reporting frequency, information asymmetry, and the cost of equity", *Journal of Accounting and Economics*, Vol. 54 Nos 2/3, pp. 132-149.

Garg, A., Curtis, J. and Halper, H. (2003), "Quantifying the financial impact of IT security breaches", *Information Management and Computer Security*, Vol. 11 No. 2, pp. 74-83.

Ghosh, A.K. and Swaminatha, T.M. (2001), "Software security and privacy risks in mobile e-commerce", *Communications of the ACM*, Vol. 44 No. 2, pp. 51-57.

Gordon, L.A., Loeb, M.P. and Sohail, T. (2010), "Market value of voluntary disclosures concerning information security", *MIS Quarterly*, Vol. 34, No. 3, pp. 567-594.

Gramling, A.A., Maletta, M.J., Schneider, A. and Church, B.K. (2004), "The role of the internal audit function in corporate governance: a synthesis of the extant internal auditing literature and directions for future research", *Journal of Accounting Literature*, Vol. 23, p. 194.

Greene, W.H. (2012), *Econometric Analysis, 71e*, Stern School of Business, New York University, New York, NY.

Haislip, J.Z. and Richardson, V.J. (2017), "The effect of customer relationship management systems on firm performance", *International Journal of Accounting Information Systems*, Vol. 27, pp. 16-29.

Harris, K. (2016), "California data breach report 2012-2015", available at: https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf (accessed 26 June 2019).

Higgs, J.L., Pinsker, R.E., Smith, T.J. and Young, G.R. (2016), "The relationship between board-level technology committees and reported security breaches", *Journal of Information Systems*, Vol. 30 No. 3, pp. 79-98.

Hovav, A. and D'Arcy, J. (2003), "The impact of denial-of-service attack announcements on the market value of firms", *Risk Management and Insurance Review*, Vol. 6 No. 2, pp. 97-121.

Iqbal, Z. and French, D. (2005), "Managerial actions and stock transactions during financial distress: some empirical evidence", *Journal of Economics and Finance*, Vol. 29 No. 2, pp. 154-171.

Jensen, M.C. (1986), "Agency costs of free cash flow, corporate finance, and takeovers", *The American Economic Review*, Vol. 76 No. 2, pp. 323-329.

Jensen, M.C. and Meckling, W.H. (1976), "Theory of the firm: managerial behavior, agency costs and ownership structure", *Journal of Financial Economics*, Vol. 3 No. 4, pp. 305-360.

Jerman-Blažič, B. (2008), "An economic modelling approach to information security risk management", *International Journal of Information Management*, Vol. 28 No. 5, pp. 413-422.

Jouini, M., Rabai, L.B.A. and Aissa, A.B. (2014), "Classification of security threats in information systems", *Procedia Computer Science*, Vol. 32, pp. 489-496.

Juma'h, A.H. (2009), "The implications of materiality concept on accounting practices and decision making", *Revista Empresarial Inter Metro/Inter Metro Business Journal*, Vol. 5 No. 1, pp. 22-37.

Juma'h, A.H. (2014), "The materiality concept: implications for managers and investors", *Revista Finanzas y Politica Económica*, Vol. 6 No. 1, pp. 159-168.

Juma'h, A.H. (2019), "Behavioral elements related to consideration and use of materiality concept in accounting practices, accountancy business and the public interest".

Kannan, K., Rees, J. and Sridhar, S. (2007), "Market reactions to information security breach announcements: an empirical analysis", *International Journal of Electronic Commerce*, Vol. 12 No. 1, pp. 69-91.

Karimi, V., Cowan, D. and Alencar, P. (2014), "An approach to correctness of security and operational business policies", *International Journal of Accounting Information Systems*, Vol. 15 No. 4, pp. 323-334.

Ko, M. and Dorantes, C. (2006), "The impact of information security breaches on financial performance of the breached firms: an empirical investigation", *Journal of Information Technology Management*, Vol. 17 No. 2, pp. 13-22.

Kuhn, J.R., Jr, Ahuja, M. and Mueller, J. (2013), "An examination of the relationship of IT control weakness to company financial performance and health", *International Journal of Accounting and Information Management*, Vol. 21 No. 3, pp. 227-240.

Lajili, K. and Zéghal, D. (2010), "Corporate governance and bankruptcy filing decisions", *Journal of General Management*, Vol. 35 No. 4, pp. 3-26.

Leach, R. and Newsom, P. (2007), "Do firms manage their earnings prior to filing for bankruptcy?", *Academy of Accounting and Financial Studies Journal*, Vol. 11 No. 3, pp. 125.

Marriott, H.R., Williams, M.D. and Dwivedi, Y.K. (2017), "Risk, privacy and security concerns in digital retail", *The Marketing Review*, Vol. 17 No. 3, pp. 337-365.

Martin, K. (2018), "The penalty for privacy violations: how privacy violations impact trust online", *Journal of Business Research*, Vol. 82, pp. 103-116.

Martin, K.D., Borah, A. and Palmatier, R.W. (2017), "Data privacy: effects on customer and firm performance", *Journal of Marketing*, Vol. 81 No. 1, pp. 36-58.

Mathur, M. (2018), "Where is the security blanket? Developing social media marketing capability as a shield from perceived cybersecurity risk", *Journal of Promotion Management*, Vol. 25 No. 2, pp. 1-25.

Messier, W.F., Jr, Reynolds, J.K., Simon, C.A. and Wood, D.A. (2011), "The effect of using the internal audit function as a management training ground on the external auditor's reliance decision", *The Accounting Review*, Vol. 86 No. 6, pp. 2131-2154.

Muhanna, W.A. and Stoel, M.D. (2010), "How do investors value IT? An empirical investigation of the value relevance of IT capability and IT spending across industries", *Journal of Information Systems*, Vol. 24 No. 1, pp. 43-66.

No, W.G. and Vasarhelyi, M.A. (2017), "Cybersecurity and continuous assurance", *Journal of Emerging Technologies in Accounting*, Vol. 14 No. 1, pp. 1-12.

Ohlson, J.A. (1980), "Financial ratios and the probabilistic prediction of bankruptcy", *Journal of Accounting Research*, Vol. 18 No. 1, pp. 109-131.

Pindado, J., Rodrigues, L. and de la Torre, C. (2008), "Estimating financial distress likelihood", *Journal of Business Research*, Vol. 61 No. 9, pp. 995-1003.

Roumani, Y., Nwankpa, J.K. and Roumani, Y.F. (2016), "Examining the relationship between firm's financial records and security vulnerabilities", *International Journal of Information Management*, Vol. 36 No. 6, pp. 987-994.

Schatz, D. and Bashroush, R. (2016), "The impact of repeated data breach events on organisations' market value", *Information and Computer Security*, Vol. 24 No. 1, pp. 73-92.

Schmidt, P.J., Wood, J.T. and Grabski, S.V. (2016), "Business in the cloud: research questions on governance, audit, and assurance", *Journal of Information Systems*, Vol. 30 No. 3, pp. 173-189.

Silverman, D.L. (2014), "Developments in data security breach liability", *The Business Lawyer*, Vol. 70 No. 1, pp. 231-245.

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: a literature review", *International Journal of Information Management*, Vol. 36 No. 2, pp. 215-225.

Spanos, G. and Angelis, L. (2015), "Impact metrics of security vulnerabilities: analysis and weighing", *Information Security Journal: A Global Perspective*, Vol. 24 Nos 1/3, pp. 57-71.

Spanos, G. and Angelis, L. (2016), "The impact of information security events to the stock market: a systematic literature review", *Computers and Security*, Vol. 58, pp. 216-229.

Stoel, M.D. and Muhanna, W.A. (2009), "IT capabilities and firm performance: a contingency analysis of the role of industry and IT capability type", *Information and Management*, Vol. 46 No. 3, pp. 181-189.

Stoel, M.D. and Muhanna, W.A. (2011), "IT internal control weaknesses and firm performance: an organizational liability lens", *International Journal of Accounting Information Systems*, Vol. 12 No. 4, pp. 280-304.

Stubben, S.R. (2010), "Discretionary revenues as a measure of earnings management", *The Accounting Review*, Vol. 85 No. 2, pp. 695-717.

Theodossiou, P.T. (1993), "Predicting shifts in the mean of a multivariate time series process: an application in predicting business failures", *Journal of the American Statistical Association*, Vol. 88 No. 422, pp. 441-449.

Tinoco, M.H. and Wilson, N. (2013), "Financial distress and bankruptcy prediction among listed companies using accounting, market and macroeconomic variables", *International Review of Financial Analysis*, Vol. 30, pp. 394-419.

Trope, R.L. (2012), "'There's no app for that': calibrating cybersecurity safeguards and disclosures", *The Business Lawyer*, Vol. 68 No. 1, pp. 183-195.

Vasarhelyi, M.A. (2012), "Financial accounting standards should not matter: it's just a layer", *Journal of Information Systems*, Vol. 26 No. 2, pp. 1-11.

Wang, G.Y. (2010), "The impacts of free cash flows and agency costs on firm performance", *Journal of Service Science and Management*, Vol. 03 No. 4, pp. 408-418.

Weisner, M.M. and Sutton, S.G. (2015), "When the world isn't always flat: the impact of psychological distance on auditors' reliance on specialists", *International Journal of Accounting Information Systems*, Vol. 16, pp. 23-41.

Corresponding author
Ahmad H. Juma'h can be contacted at: jumah@uis.edu