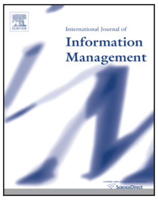
International Journal of Information Management 36 (2016) 987–994

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt



Examining the relationship between firm’s financial records and security vulnerabilities

Yaman Roumani[a,*], Joseph K. Nwankpa[b], Yazan F. Roumani[c]

[a] Computer Information Systems, Eastern Michigan University, 419 Owen Bldg., Ypsilanti, MI 48197, United States
[b] Information Systems, University of Texas Rio Grande Valley, 1201 W. University Drive, Edinburg, TX 78539, United States
[c] Decision and Information Sciences, Oakland University, 342 Elliott Hall, Rochester, MI 48309, United States

ARTICLE INFO

Article history:
Received 15 December 2015
Received in revised form 18 May 2016
Accepted 19 May 2016

Keywords:
Security
Vulnerability
Financial records
Technology firms

ABSTRACT

Security vulnerabilities and breaches remain a major concern for firms as they cost billions of dollars in downtime, maintenance and disruptions. Although researchers in the fields of security and vulnerability prediction have made significant contributions, the number of vulnerabilities continues to increase. Contrary to existing vulnerability studies, this research examines vulnerabilities from a financial perspective. We explore whether firm’s financial records are associated with vulnerabilities. In particular, we examine the correlation between the number of vulnerabilities and each of firm’s size, financial performance, marketing and sales, and research and development expenditures. The empirical analysis of this study is based on data collected from 89 publicly traded technology firms over a 10-year period. Our results reveal that financial records are significantly associated with vulnerabilities. More specifically, our results show that as technology firms increase their marketing and sales expenditures, the number of vulnerabilities increases as well. Interestingly, the analysis shows that firms can counter this rise by increasing their spending on research and development. We also find a positive correlation between the number of vulnerabilities and each of firm’s size and performance.

1. Introduction

Vulnerabilities have been identified as one of the key reasons for computer security breaches which resulted in billions of dollars in losses (Telang & Wattal, 2007). Incidents such as the Conficker worm (2009), MyDoom (2006) and SoBig viruses (2003) occurred when hackers exploited vulnerabilities in information systems. The damages due to Conficker, MyDoom and SoBig viruses were estimated at $9.1 billion, $38 billion and $37.1 billion, respectively. The Sourcefire Vulnerability Research Team reported that in 2012 the number of vulnerabilities increased to levels comparable to 2008–2009 after they decreased in 2010–2011, and the percentage of more critical vulnerabilities has increased as well (Younan, 2013). Moreover, the growth of smartphones has resulted in an increase in vulnerabilities. According to HP Cyber HP Enterprise Security (2013), the rate of mobile vulnerabilities has risen rapidly in 2012 compared to 2011. It was reported that the last five years have seen a 787 percent increase in mobile vulnerability disclosures (HP Enterprise Security, 2013).

As technology infrastructure gets increasingly complex and interconnected, the difficulty of achieving security increases. Furthermore, developing vulnerability-free products which involves thousands or millions of lines of code is not possible, thus vulnerabilities will inevitably be discovered. Moreover, as software managers continue to follow the approach of “I’d rather have it wrong than have it late. We can always fix it later” (Slaughter, Harter, & Krishnan, 1998), and continue to favor achieving cost and schedule goals at the cost of product’s quality, vulnerabilities will always exist. Existing research have developed several vulnerability predictive models (Alhazmi & Malaiya, 2005a, 2005b; Alhazmi, Malaiya, & Ray, 2007; Dacier, Deswarte, & Kaâniche, 1996; Ortalo, Deswarte, & Kaâniche, 1999; Shin and Williams, 2008; Shin, Meneely, Williams, & Osborne, 2011). However, such models relied on technical aspects and historical vulnerability data for prediction and they had shortcomings regarding their assumptions (Ozment, 2007). Additionally, the effectiveness of vulnerability discovery techniques has been questioned (Austin, Holmgreen, & Williams, 2013).

Although significant research attention has been directed at developing vulnerability prediction models, very little attention

[*] Corresponding author.
E-mail addresses: yroumani@emich.edu (Y. Roumani), joseph.nwankpa@UTRGV.edu (J.K. Nwankpa), roumani@oakland.edu (Y.F. Roumani).

http://dx.doi.org/10.1016/j.ijinfomgt.2016.05.016
0268-4012/© 2016 Elsevier Ltd. All rights reserved.

has been paid to vulnerabilities from a financial perspective. This is a significant gap in the literature given the importance of financial information in determining how much firms should spend on security in order to protect their products. Anderson (2001) discussed this issue in his paper and indicated how information insecurity can be explained more clearly using microeconomics. In this paper, and through the theory of network externality, we investigate the association between firm's financial records and vulnerabilities. More specifically, we examine the correlation between the number of vulnerabilities and each of firm's size, financial performance, marketing and sales, and research and development expenditures.

This paper contributes to the improvement of vulnerability literature in a number of ways. First, this paper answers the call of Anderson (2001) for more research to explore information insecurity using microeconomics. Second, it develops a vulnerability model and empirically analyzes the association between firm's financial information and vulnerabilities. Third, contrary to existing studies, results of this paper help in better understanding of vulnerabilities through non-technical aspects. Finally, the findings of the study provide guidance for technology firms and managers who wish to evaluate vulnerabilities of their products through financial means. As this is an unexplored area in the research, the article provides opportunities for future studies.

The remainder of this paper proceeds as follows: First, we offer a review of relevant literature of prior vulnerability prediction models and theory of network externality. We then present the hypotheses and research model. Next, we report an empirical study based on data collected from technology firms, followed by a presentation of the data analysis and the results. Finally, we offer a discussion of implications, limitations and future research.

2. Literature review

2.1. Vulnerability predictive models

Existing studies have focused on using mathematical models (Dacier et al., 1996), vulnerability density functions (Alhazmi & Malaiya, 2005a) and security goal models (Shahmehri et al., 2012) to predict vulnerabilities. For instance, Dacier et al. (1996) and Ortalo et al. (1999) proposed to model vulnerabilities of a UNIX system as a privilege graph where every node represents user privileges and every edge represents a vulnerability. The model was used to construct how attackers exploit vulnerabilities and gain user privileges. The privilege graph was transformed to a Markov chain based on successful attack patterns. Browne, Arbaugh, McHugh, and Fithen (2001) used vulnerability data of Computer Emergency Readiness Team (CERT) to analyze vulnerability incident trends and concluded that the cumulative number of vulnerability incidents is related to the square root of starting time of the exploit. Their proposed mathematical model predicted the severity of future vulnerabilities based on earlier vulnerability reports. Shin et al. (2011) provided empirical evidence that vulnerability prediction models using complexity and code churn metrics are useful to predict the location of vulnerable code with high recall. But since their analysis was performed on Mozilla Firefox web browser and the Red Hat Enterprise Linux kernel, they concluded that their results may not be generalized to other projects.

More recent vulnerability predictive studies have modeled vulnerabilities using density analogies. Vulnerability density relies on the number of vulnerabilities found per x lines of code to predict the future number of undiscovered vulnerabilities based on the maturity of the software. Vulnerability density assumes that different software versions are developed in a similar manner and are comparable to each other and have static code. This type of predictive study requires the use of vulnerability discovery models (VDM). According to Ozment (2007), vulnerability discovery models are probabilistic models used to specify the dependency of the vulnerability discovery process on the factors that affect it. VDMs are based on software reliability models (SRM); therefore their assumptions about the data are often the same for both models. The majority of VDMs are time-based models which maintain the total number of vulnerabilities by calendar time and consider calendar time as the independent variable (Woo, Alhazmi, & Malaiya, 2006). Among the existing VDMs is the work by Gopalakrishna and Spafford (2005); the authors analyzed vulnerability data of IIS, BIND, Lpd, Sendmail and RPC to observe trends in data and determine if existing vulnerabilities suggest new information. They found that measuring vulnerability occurrences can predict future vulnerabilities but claimed that the results may not be applicable to every other software artifact. Along their side, Alhazmi and Malaiya (2005a) proposed two VDMs: Alhazmi-Malaiya logistic model (AML) and Alhazmi-Malaiya effort model (AME). AML is an S-shaped, time-based model which considers calendar time as the independent variable and assumes that vulnerability discovery occurs in three consecutive phases. On the other hand, the AME model is an effort-based model which approximates effort with the number of system users (i.e. number of installations). Both AML and AME models have been tested for goodness-of-fit by numerous studies. Although VDMs have been used in the literature, some of those models have shortcomings regarding their assumptions (Ozment, 2007). It was concluded that researchers should clearly state the assumptions upon which their models rely and define the terms that they use (Ozment, 2007).

2.2. Network externality

Network externality theory refers to the change in the benefit that a consumer derives from a good when the number of other consumers using the same kind of good changes (Katz & Shapiro 1985). Network externality can be positive or negative as individuals using the network can provide value to others or they can become a liability to the network. For example, if more people have Internet access, the network value increases since it allows for interaction among users and enables universal access, however, having too many users on a network simultaneously can create a negative externality effect due to quality degradation caused by traffic.

In the information system (IS) market, positive network externality arises through a large market share which leads to high compatibility among users that enables collaborative work and information sharing. Brynjolfsson and Kemerer (1996) used market share as a proxy for the extent of network installed base in their analysis of the spreadsheet software market. Their results showed that the demand for a spreadsheet software significantly increased as the size of the software's installed base increased. Given the positive effect of network externality, technology firms strive to increase network externality of their products and services by enlarging the installed base through marketing, sales and pricing strategies (Schilling 1999). However, positive network externality in the IS market can also cause security issues (negative network externality). Kunreuther and Heal (2003) examined how the use of popular software increases the risk of security attacks and breaches for firms given the interdependence with business partners and the risk of being attacked and affected by the breaches at their partners. Thus, by joining larger networks and having users share IS, firms face higher security risks. In their work, Chen, Kataria, and Krishnan (2005) conducted a risk management study regarding the positive and negative network externalities of software and the benefits of software diversity through a reduction of security losses. The authors calculated the optimal amount of diversity investment by a firm while considering the negative network externalities through attacks and the positive network effects through uniformity and interoperability. Similarly, Geer et al. (2003) reported on the issue of negative network externality when dealing with security related to the operating system market.

2.3. ***Firm's*** *financial records*

Firm's financial records reveal valuable information for firms and stakeholders and they can be utilized for prediction. Prior research studies have built statistical models using firm's financial records to predict future earnings, cash flow changes, supply and demand, possible failures and crises (Dimitras, Slowinski, Susmaga, & Zopounidis, 1999; Strong & Bambang, 1998). In this section, we explore how four financial constructs, namely marketing and sales, firm performance, firm size and research and development are associated with vulnerabilities.

2.3.1. Marketing and sales

Marketing is structured primarily around customers and markets, and it integrates sales, product strategy, distribution, and marketing communications competencies and activities (Achrol & Kotler, 1999). Moreover, marketing strives to reach profitable business performance as its key objective (Webster, 1997). Sales, on the other hand, include activities designed to promote customer purchase in order to generate positive cash flow for the firm (Levitt, 1960) and to stimulate demand (Weitz & Bradford, 1999). Despite their distinct roles, marketing and sales are both responsible for generating revenue for the company and for achieving profitable outcomes. In their study, Kotabe, Srinivasan, and Aulakh (2002) noted that a firm with higher advertising and promotion expenditures is estimated to generate more sales. Moreover, a firm that promotes its products and spends on advertising is able to increase sales by making customers switch to their brands and by expanding sales of their product. Thus, not surprisingly, firms spend billions of dollars on marketing and sales activities. For example, in 2012, Apple doubled its advertising expenditure to $1 billion, which accounts for only 10% of their sales, general and administrative costs (Sherman, 2013).

For technology firms, more marketing and sales expenditures implies more popularity and larger market share, but from a security perspective, this also means more exposure and an invitation for more attacks. Popular products attract more attacks due to being ubiquitous and having a larger installed user-base where a vulnerability has a greater chance of affecting large number of users. The concept of positive network externality signifies larger installed user-base for firms, but for hackers, it implies more users and thus a lucrative target for more attacks (Kunreuther & Heal, 2003). As stated by Maxcer (2007), popularity might be the most important security factor in today's changing hacker world. It has been cited that one of the main reasons why attackers choose to target Windows operating system is due to its popularity and the large number of users (Honeynet Project, 2004). Furthermore, as alternative operating systems, such as Apple iOS grow in popularity, they also become more attractive targets (Bell, 2013).

Firms with high financial capabilities are able to devote more resources to marketing related activities (McDaniel & Kolari, 1987). Moreover, as technology firms increase their marketing and sales expenditures, their market share and user-base increase as well leading to positive network externality, thus attackers will increase their efforts to find vulnerabilities and exploit their systems. This leads to our first hypothesis:

H1. Marketing and sales expenditures are positively associated with the number of vulnerabilities.

2.3.2. Firm performance

Firm performance refers to how well an organization achieves its market-oriented and financial goals (Yamin, Gunasekruan, & Mavondo, 1999). Performance can be characterized as the firm's success in the market and its ability to create acceptable actions and outcomes. The terms 'firm performance' and 'firm success' are often very closely linked and their definitions seem to be intertwined as both terms are used as synonyms in research. Firm performance is multidimensional as it consists of different theoretical and empirical components (Henri, 2004). Traditionally, firm performance has been measured using financial terms including return on assets (ROA), profit, market share, and non-financial terms such as motivation, job satisfaction and turnover (De Toni & Tonchia, 2001; Murphy, Trailer, & Hill, 1996). Existing literature reveals three general approaches to measuring firm performance. The first approach uses a single performance measure based on a theoretical relationship between the independent variables and the measure (Hawawini, Subramanian, & Verdin, 2003; Roberts & Dowling, 2002). The second approach utilizes multiple performance measures (Miller, 2004; Robert Baum & Wally, 2003) while the third approach utilizes the aggregate of multiple performance measures based on the correlation between them (Cho & Pucik, 2005).

Prior literature has attributed high financial firm performance to high profits and market share (Supapol, Fischer, & Pan, 2008). Indeed, market share and profits have been used as measures of firm performance (Sircar, Turnbow, & Bordoloi, 2000). However, for technology firms, high financial performance has a downside when it comes to security. As firms achieve high financial performance, their success and market share grows as well. This fuels more attacks and greater risks since the potential effects of a vulnerability becomes much higher, thus leading to negative network externality effect. According to a report by Symantec, firms such as Google and Microsoft continue to be the primary targets of attacks since they have large market shares, thus, for hackers, finding vulnerabilities will have the potential to affect many users (Symantec, 2011). This implies that firms with large market share are possible targets for vulnerabilities and attacks. Indeed, Alhazmi and Malaiya (2005a, 2005b) found that the highest occurrence of vulnerabilities happen when software market share increases and the targeted system becomes more popular. Thus we hypothesize the following:

H2. Firm performance is positively associated with the number of vulnerabilities.

2.3.3. Firm size

Firm size refers the scale of operations of an organization (Price & Mueller, 1986) and the scope of available resources (Grant, 1991). Firm size was found to reflect past success and current performance of firms (Ravichandran & Lertwongsatien, 2005). Prior studies have shown that larger firms generate superior performance relative to smaller firms (Penrose, 2009). Additionally, it was concluded that larger firms are more profitable than smaller ones (Shepherd, 1972). In a later study, Shepherd (1986) reported that firm size is also correlated with market power. Furthermore, large firms can produce considerably more products than smaller ones (Chandy & Tellis, 2000); this implies that large firms have more market visibility. Indeed, Brammer and Millington (2006) noted that firm size reflects firm visibility and business exposure. From a security perspective, more visibility means greater exposure and thus, more attention from hackers looking to find and exploit vulnerabilities. According to reports by Symantec and IBM X-Force risk, hackers tend to target large firms. In 2011, 50% of the attacks were targeted against large firms while the remaining attacks were directed towards medium and small firms (IBM, 2010; Symantec, 2011). For attacker's, large firms are more lucrative targets since they have more valuable financial and personal data such as credit cards and banking information. Moreover, with the newest hacking trend “ransomware”, holding data hostage for ransom, hackers have shifted their attention to big firms since they have the financial capabilities to pay higher ransom amounts (Luo & Liao, 2009). Based on the previous arguments, we hypothesize the following:

H3. Firm size is positively associated with the number of vulnerabilities.

2.3.4. *Research and development*

Research and Development (R&D) refers to the activities that increase technical and scientific knowledge and the application of that knowledge to create or improve products and processes (Hagedoorn, 2002). Prior studies have found positive relationship between R&D and efficiency in operations (Hitt, Hoskisson, & Kim, 1997) and innovations (Balachandra & Friar, 1997). Today’s technology firms invest in R&D to create new innovations and to improve existing products and services. Moreover, a technology firm with superior product design can gain advantage and achieve greater returns by differentiating its products from competitors.

In terms of security, technology firms invest their R&D in vulnerability research, mitigations and workarounds and the design of secure systems; while others engage their R&D teams to build security labs to create environments for running hacking and assessment tools and code-scanning software (Thurman, 2013). R&D provides information and innovations which closes the gap between the firm’s products and potential exploiters of vulnerabilities. For example, Microsoft security researchers were among the first to offer analysis of the highly sophisticated worm, Stuxnet, which exploited Windows vulnerabilities (Borland, 2010). Through their analysis, Microsoft researchers were able to find several undiscovered vulnerabilities in Windows system and issue security patches. Similarly, Google’s R&D team constantly reports a list of vulnerabilities discovered or fixed by their employees (Google, 2014).

R&D on vulnerability requires extensive capital resources to acquire skilled researchers and security professionals, and to obtain hardware and software products. For instance, in 2012 Apple spent $3.4 billion on R&D, a 39% increase from 2011 (Lowensohn, 2012). However, R&D on vulnerability is typically a race between attackers and defenders (Ransbotham, Mitra, & Ramsey, 2012) where technology firms invest in R&D to develop vulnerability detection and prevention methods while attackers try to find new innovate ways to exploit vulnerabilities. After all, to conduct proactive vulnerability research, technology firms must invest in R&D to develop more secure products and limit the number of vulnerabilities before attackers exploit them. Drawing on the above arguments, we thus propose the following hypothesis:

H4. R&D expenditure on vulnerability is negatively correlated with the number of vulnerabilities.

3. Research model

Building on the background literature and hypotheses discussed above, we provide a research model underlying our study in Fig. 1.

4. Data and methodology

We obtained a list of 652 public technology firms listed by NASDAQ (NASDAQ, 2014). We then compiled a dataset of all disclosed vulnerabilities for each firm between 2002 and 2012. Our baseline source was the National Vulnerability Database (NVD) (NVD, 2014). NVD provides a publication date, a short description, a severity rating and information about the vendor, version and name of the affected products. To help ensure accuracy, we manually checked and corrected vendor and product information to account for inconsistencies. Of the 652 firms, 155 had vulnerability reports. Furthermore, out of the 155 firms, 66 had missing or incomplete vulnerability information. Our final sample size included 89 technology firms.

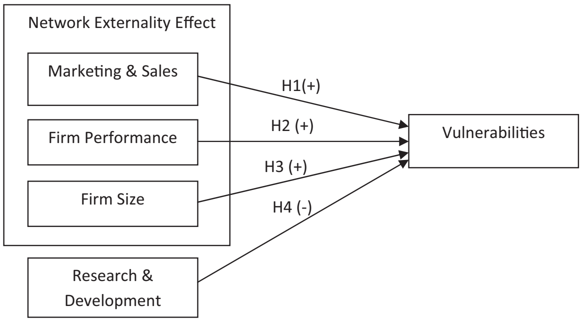


Fig. 1. Research Model.

Table 1
Technology firms.

Activision Blizzard	Facebook	NVIDIA
Adobe Systems	Fortinet	Open Text
AOL	GlobalSCAPE	Oracle
Apple	Google	Palo Alto Networks
Aruba Networks	Groupon	Progress Software
Autodesk	Guidance Software	Proofpoint
AVG Technologies	Imperva	PTC
Baidu	Infoblox	QUALCOMM
BMC Software	Intel	Quantum
Bottomline Technologies	Interactive Intelligence Group	Rackspace Hosting
Broadcom	Intuit	RealNetworks
Brocade Communications Systems	Juniper Networks	RealPage
CA	Kyocera	Red Hat
Check Point Software Technologies	Lantronix	Renren
Cisco Systems	Lattice Semiconductor	SanDisk
Citrix Systems	Lexmark International	SAP AG
Compuware	LinkedIn	Seagate Technology
Cray	Logitech International	Sina
Cypress Semiconductor	LogMein	Smith Micro Software
Dell	Marvell Technology Group	Solarwinds
Demand Media	Microchip Technology	Sourcefire
Digi International	Microsoft	Splunk
Digital River	Mitel Networks	Symantec
EarthLink	Motorola Solutions	TIBCO Software
Eaton	National Instruments	Tucows
Electronic Arts	NetApp	Unisys
EMC	NetScout Systems	VeriSign
Ericsson	Nokia	Vmware
Extreme Networks	NTT DOCOMO	Yandex
F5 Networks	Nuance Communications	

For each of the 89 firms, we used publicly available information listed at the US Securities and Exchange Records Commission’s website (SEC, 2014) and collected quarterly financial records. Financial records included income statements, balance sheets and cash flow statements for the last 10 years (2002–2012). To evaluate our hypotheses, we extracted variables from the financial records and used them as measures. Table 1 shows a list of the 89 technology firms used in this study. Table 2 provides further information about subsectors of these firms as indicated by NASDAQ.

Table 2
Technology firms – Subsectors.

Subsector	Count
Advertising	1
Computer Communications Equipment	6
Computer Manufacturing	4
Computer peripheral equipment	5
Computer Software: Prepackaged Software	32
Computer Software: Programming Data Processing	8
EDP Services	12
Electronic Components	5
Industrial Machinery/Components	1
Radio And Television Broadcasting And Communications Equipment	6
Retail: Computer Software & Peripheral Equipment	1
Semiconductors	8

Table 3
Continuous Variable Information.

	Minimum	Maximum	Mean	Std. Deviation
Number of Vulnerabilities[a]	0	167	12.2598	22.27774
SG&A (in Millions)	24.65	5496.00	878.8730	1006.97626
ROS (%)	−447.40	59.80	20.2968	22.83112
R&D (in Millions)	4.81	2971.00	401.7089	518.42480

[a] aggregated by quarter (2002–2012).

4.1. Control variables

There are various factors that influence vulnerabilities including code size, product age (Woo et al., 2006) and number of products. As technology firms produce more products, the probability of having more vulnerabilities and security attacks increases. Moreover, in their work, Woo et al. (2006) showed how code size and product's age can affect the number of vulnerabilities.

To minimize the confounding effect of spurious correlation, we included the firm's number of products and their average age as control variables. However, given the closed nature of firm's products, obtaining the average code size was not possible in this research.

4.2. Measures

Three popular measures of firm performance were initially considered namely, return on assets (ROA), return on equity (ROE) and return on sales (ROS). Due to data availability, ROS was used. ROS is a popular profitability ratio which is computed as the net profit after taxes as a percentage of net sales. It has been used in prior studies as a measure of firm performance (Grant, 1987; Haar, 1989). As for firm size, the most common measures are: number of employees, market capitalization, and total assets (Cooke, 1989; Inchausti, 1997; Wallace, Naser, & Mora, 1994). Due to data availability and accuracy, we used market capitalization to measure firm size. Market capitalization is calculated as firm's share price multiplied by the number of shares outstanding. Market capitalization is classified in six groups as follows: mega-cap (over $200 billion), large-cap ($200 billion–$10 billion), mid-cap ($10 billion–$2 billion), small-cap ($2 billion–$250 million), micro-cap ($250 million–$50 million), and nano-cap (below $50 million). To measure marketing and sales expenditures, we used Selling, General & Administrative (SG&A) variable. SG&A involves advertising, sales and sales forces, marketing and promotion campaigns and various other administrative and corporate expenses such as travel and office equipment. Furthermore, R&D variable was used to test our last hypothesis. Finally, the number of vulnerabilities was used as the outcome variable. The number of vulnerabilities was aggregated based on the count of vulnerabilities per quarter for each firm. Table 3 provides descriptive statistics of the variables.

Table 4
Goodness of Fit.

	Value	df	Value/df
Deviance	1513.146	736	2.056
Scaled Deviance	1513.146	736	
Pearson Chi-Square	1879.988	736	2.554
Scaled Pearson Chi-Square	1879.988	736	
Log Likelihood	−2274.333		
Akaike's Information Criterion (AIC)	4562.667		
Finite Sample Corrected AIC (AICC)	4562.819		
Bayesian Information Criterion (BIC)	4594.942		
Consistent AIC (CAIC)	4601.942		

Table 5
Omnibus Test.

Likelihood Ratio Chi-Square	Df	Sig.
720.749	8	0.000

4.3. Data analysis

Count data are frequently modeled using Poisson regression, however, the distributional assumption of Poisson regression requires that the mean of the distribution to be equal to the variance (Cohen, Cohen, West, & Aiken, 2003). In our data, the variance was larger than the mean, thus negative binomial regression was deemed appropriate to test our hypotheses. Negative binomial regression is used for dealing with overdispersed count data (Cohen et al., 2003). Negative binomial regression model relaxes the assumption of equality of the mean and the variance of the dependent variable, allowing the variance to exceed the mean (Hilbe, 2011). Moreover, negative binomial regression allows the coefficient estimates to be transformed to give the rate ratio. This implies that our results can be interpreted as the percent increase in the number of vulnerabilities. The empirical analysis was performed using SPSS software (release 20.0.0; SPSS Inc., Chicago, IL) with the number of vulnerabilities as the dependent variable; ROS, market capitalization, SG&A and R&D as the independent variables. In order to account for any potential lag effect as indicated by prior studies (Ravenscraft & Scherer, 1982;Morbey, 1988), we tested several models with lag periods spanning from 0 to 6 lags; where each lag period corresponds to a quarter. Also, we tested the variables for multicollinearity by examining variance inflation factors. Test results indicated no problems with multicollinearity (Belsley, Kuh, & Welsch, 2005).

5. Results

Compared to the models with no lag effects, our results show a significant improvement in goodness of fit where R&D was the only lagged variable at 6 quarters (18 months). Tables 4 and 5 summarize the Goodness of fit test and the Omnibus test. The Omnibus test revealed that the full model is significant (Likelihood Ratio Chi-Square = 720.749, df = 8, $p < 0.001$).

Results of the negative binomial regression analysis are presented in Table 6. H1 predicted that marketing and sales expenditures are positively associated with the number of vulnerabilities. This hypothesis was supported as the results show a significant positive correlation between both variables (β =0.001, $p < 0.001$). Our results suggest that the greater the expenditures of SG&A, the higher the number of vulnerabilities. More specifically, for each $10,000 spent on SG&A, the number of vulnerabilities increases by 10.

H2 examined the association between firm performance and the number of vulnerabilities. The parameter estimate for ROS was positive and highly significant (β = 0.004, $p < 0.004$) thus supporting

Table 6
Parameter Estimates.

Parameter	B	Std. Error	Hypothesis Test			Exp(β)
			Wald Chi-Square	df	Sig.	
(Intercept)	−0.209	0.2252	0.864	1	0.353	0.811
Number of products	2.973	0.4995	0.921	1	0.337	19.550
Average product age	0.485	0.1084	2.005	1	0.157	1.624
SG&A	0.001	0.0001	95.508	1	0.000	1.001
ROS	0.004	0.0015	8.207	1	0.004	1.004
[Market Cap = Mega]	2.272	0.3230	49.478	1	0.000	9.701
[Market Cap = Large]	1.888	0.2374	63.255	1	0.000	6.609
[Market Cap = Med]	1.001	0.2409	17.271	1	0.000	2.721
R&D (lagged)	−0.001	0.0002	50.681	1	0.000	0.999

H2. The analysis indicates that as ROS ratio increases, the number of vulnerabilities increases as well. More specifically, a 1% increase in ROS implies a 0.004 increase in the number of vulnerabilities.

H3 predicted that firm's size is positively associated with the number of vulnerabilities. This hypothesis was also supported. The parameter estimates were positive and highly significant for mega-cap ($\beta = 2.272$, $p < 0.001$), large-cap ($\beta = 1.888$, $p < 0.001$) and medium-cap ($\beta = 1.001$, $p < 0.001$). Our results show that the number of vulnerabilities at mega-cap firms is 2.272 times the number of vulnerabilities at small-cap firms. For large-cap firms, the number of vulnerabilities is 1.888 times the number of vulnerabilities at small-cap firms. Finally, for med-cap firms, the number of vulnerabilities is 1.001 times the number of vulnerabilities at small-cap firms.

Finally, H4 stated that R&D expenditure on vulnerability is negatively associated with the number of vulnerabilities. This hypothesis was supported ($\beta = -0.001$, $p < 0.001$). Results suggest that the greater the expenditure of R&D on vulnerability, the lower the number of vulnerabilities. Thus, as R&D expenditure increases by $10,000, the number of vulnerabilities decreases by 10.

6. Discussion

This research investigates whether financial records of technology firms are associated with vulnerabilities. Prior studies in vulnerability prediction relied mainly on technical and historical trends in vulnerabilities to build a prediction model. However, to our knowledge, this is the first study to examine vulnerabilities through firm's financial records. Our analysis of 89 technology firms suggests that firm's size, performance and expenditures are correlated with vulnerabilities. We find that as technology firms increase SG&A expenditures, they tend to have more vulnerabilities. In a competitive market, as firms spend more money on marketing and sales to attract customers and increase sales, the popularity of their product increases as well, thus increasing product exposure and might be leading to more vulnerabilities and attacks. We further find that more expenditure on research and development is associated with a lesser number of vulnerabilities. This result is interesting for managers because our analysis shows that SG&A and R&D have the same inverse correlation with vulnerabilities. This implies that a corrective action in spending may mitigate the number of vulnerabilities. Indeed in their study, Moitra and Konda (2000) reported that as firms increase their investment in security, survivability from security threats increases rapidly. However, it is important to note that the lag effect of R&D implies that the effectiveness of R&D is delayed by 18 months. Furthermore, our results suggest that as firm performance increases so does the number of vulnerabilities. Consistent with our hypothesis, our results indicated that larger technology firms have more vulnerabilities than smaller ones. A possible reason can be the fact that larger firms tend to disclose vulnerabilities more than smaller firms (Telang and Wattal, 2007). Another possibility can be related to market share; as firm size increases, their market share increases as well resulting in being subject to more attacks.

7. Managerial implications

Given our findings, we believe that technology firms can benefit from their financial records to evaluate and understand security threats. Our study points to the fact that managers need to pay attention to expenditures and how they might relate to vulnerabilities. In particular, the study provides evidence that marketing and sales expenditures are positively associated with security threats. Although technology firms might prefer to spend their resources on marketing and sales activities, managers ought to monitor their expenditures since they correlates with more vulnerabilities. The study provides evidence that research and development is negatively correlated with security threats. However, given the lag effect associated with R&D, technology firms must take into consideration the lag between investment in R&D and product security. Our study also provides preliminary evidence that financial performance is associated with the number of vulnerabilities. This implies that technology firms can use their performance as an indicator of vulnerabilities and plan accordingly. Our analysis finds support for correlation between vulnerabilities and firm size. Thus, as technology firms grow and increase their market capitalization, this should be accompanied by more vulnerabilities and attacks given the firm size. In summary, a firm's expenditures and investment strategies regarding security must be dynamic given the changes in firm's financial structure. Moreover, continual efforts in research and development seem to be the key for better security.

8. Research implications

This study makes key contributions to security and vulnerability prediction fields. As pointed out earlier, although significant research attention has been directed at developing vulnerability prediction models, very little attention has been paid to vulnerabilities from a financial perspective. This is a significant gap in the literature given the importance of financial information in determining how much firms should spend on security in order to protect their products. In this study, we attempted to address this gap by examining the relationship between firm's financial records and vulnerabilities. Insight was provided as to the specific interplay between firm's size, financial performance and expenditures, and vulnerabilities. The empirical results hold important implications for future research that seek to reconcile the association between financial information and security. Our evidence directly supports the contention that financial records are important predictors of number of vulnerabilities. This finding is particularly interesting because it suggests for firms, the real protection may reside in understanding their financial records and its relation to vulnerabilities. This study reveals key predictors of vulnerabilities that have been largely ignored by prior studies and it provides a revealing theoretical lens for further understanding of vulnerabilities.

9. Limitations and future research

Although we believe that our study makes a number of contributions, it has some limitations. Since our data is based on published vulnerabilities, our analysis does not account for undiscovered and unpublished vulnerabilities. However, given the amount and the diversity of our data, we believe that the currently reported vulnerabilities do not jeopardize our results. Also, our study was limited to publicly traded technology firms in NASDAQ, therefore no private firms were included. To generalize our observations from this paper to other firms, further studies should be performed. Although our sample was adequate given the ten years of quarterly data, a higher and more diverse sample of firms would have enhanced the validity and generalizability of the study. The majority of our sample data were large-cap firms; we believe this limitation is due to vulnerability disclosure (Telang & Wattal, 2007). Thus, obtaining vulnerabilities information from smaller firms may enrich the findings of our results as well as offer additional perspectives on the constructs. One path forward for future research is to test whether the proposed model can be used to predict vulnerabilities. Such research can provide further insight on the predictability levels of firm's financial records. Future research can also examine alternative characteristics of vulnerabilities such as severity levels and frequency.

10. Conclusion

The aim of this research was to study the relationship between firm's financial records and vulnerabilities. More specifically, using the network externality theory, this study attempted to find out how key financial information can correlate with the number of vulnerabilities. The results from the empirical evidence showed that each of firm's performance, size, marketing and sales, and research and development expenditures correlate with the number of vulnerabilities. We found that as firms increase their marketing and sales expenditures by $10,000, the number of vulnerabilities increases by 10. On the other hand, as expenditures of R&D increase by $10,000, the number of vulnerabilities decreases by 10. We also found statistically significant evidence that firm performance is positively correlated with the number of vulnerabilities. Furthermore, the analysis showed that market capitalization has a positive relationship with number of vulnerabilities. Based on our findings, firm management are able to employ financial information to examine vulnerabilities of their products by controlling their expenditures and monitoring firm performance and market capitalization.

References

Achrol, R. S., & Kotler, P. (1999). Marketing in the network economy. *The Journal of Marketing*, 146–163.

Alhazmi, O. H., & Malaiya, Y. K. (2005a). Quantitative vulnerability assessment of systems software. In *Proceedings of 51st annual reliability and maintainability symposium* (pp. 615–620).

Alhazmi, O. H., & Malaiya, Y. K. (2005b). Modeling the vulnerability discovery process. *Proceedings of international symposium on software reliability eng*, 129–138.

Alhazmi, O. H., Malaiya, Y. K., & Ray, I. (2007). Measuring, analyzing and predicting security vulnerabilities in software systems. *Computers & Security*, *26*(3), 219–228.

Anderson, R. (2001). Why information security is hard- an economic perspective. *Computer security applications conference, 2001. ACSAC 2001. Proceedings 17th annual*, 358–365. IEEE.

Austin, A., Holmgreen, C., & Williams, L. (2013). A comparison of the efficiency and effectiveness of vulnerability discovery techniques. *Information and Software Technology*, *55*(7), 1279–1288.

Balachandra, R., & Friar, J. H. (1997). Factors for success in R&D projects and new product innovation: a contextual framework. *IEEE Transactions on Engineering Management*, *44*(3), 276–287.

Bell, L. (2013). *Apple's iOS had more security vulnerabilities than Android in 2012*.. Retrieved from. http://www.theinquirer.net/inquirer/news/2262231/apple-ios-had-more-security-vulnerabilities-than-android-in-2012

Belsley, D. A., Kuh, E., & Welsch, R. E. (2005). *. Regression diagnostics: identifying influential data and sources of collinearity* (Vol. 571) John Wiley & Sons.

Borland, J. (2010). *A Four-Day Dive Into Stuxnet's Heart*.. Retrieved from. http://www.wired.com/threatlevel/2010/12/a-four-day-dive-into-stuxnets-heart/

Brammer, S., & Millington, A. (2006). Firm size, organizational visibility and corporate philanthropy: an empirical analysis. *Business Ethics: A European Review*, *15*(1), 6–18.

Browne, H. K., Arbaugh, W. A., McHugh, J., & Fithen, W. L. (2001). A trend analysis of exploitations. *2001 IEEE symposium on security and privacy, 2001. S&P 2001. Proceedings*, 214–229. IEEE.

Brynjolfsson, E., & Kemerer, C. F. (1996). Network externalities in microcomputer software: an econometric analysis of the spreadsheet market. *Management Science*, *42*(12), 1627–1647.

Chandy, R. K., & Tellis, G. J. (2000). The incumbent's curse? Incumbency, size, and radical product innovation. *The Journal of Marketing*, 1–17.

Chen, P. Y., Kataria, G., & Krishnan, R. (2005). Software diversity for information security. *Fourth Workshop on the Economics of Information Security*,. Harvard University.

Cho, H. J., & Pucik, V. (2005). Relationship between innovativeness, quality, growth, profitability, and market value. *Strategic Management Journal*, *26*(6), 555–575.

Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2003). *Applied multiple regression/correlation analysis for the behavioral sciences* (3rd ed.). Hillsdale: Erlbaum.

Cooke, T. E. (1989). Disclosure in the corporate annual reports of Swedish companies. *Accounting and Business Research*, *19*(74), 113–124.

Dacier, M., Deswarte, Y., & Kaâniche, M. (1996). *Quantitative Assessment of Operational Security: Models and Tools Technical Report 96493*. Laboratory for Analysis and Architecture of Systems.

De Toni, A., & Tonchia, S. (2001). Performance measurement systems-Models, characteristics and measures. *International Journal of Operations & Production Management*, *21*(1/2), 46–71.

Dimitras, A. I., Slowinski, R., Susmaga, R., & Zopounidis, C. (1999). Business failure prediction using rough sets. *European Journal of Operational Research*, *114*(2), 263–280.

Geer, D., Bace, R., Gutmann, P., Metzger, P., Pfleeger, C., Querterman, J., & Scheier, B. (2003). *Cyberinsecurity: The cost of monopoly how the dominance of microsoft's products poses a risk to security*. Computer and Communications Industry Association.

Google. (2014). *Research at google*. Retrieved from. http://www.google.com/about/appsecurity/research/

Gopalakrishna, R., & Spafford, E. H. (2005). *A trend analysis of vulnerabilities*. pp. 13. West Lafayette: Purdue University.

Grant, R. M. (1987). Multinationality and performance among British manufacturing companies. *Journal of International Business Studies*, *18*(3), 79–89.

Grant, R. M. (1991). The resource-based theory of competitive advantage: implications for strategy formulation. *California Management Review*, *33*(3), 114–135.

HP Enterprise Security. (2013). *HP 2012 cyber security report*.. Retrieved from. http://www.hpenterprisesecurity.com/register/guarding-against-a-data-breach-hp.com

Haar, J. (1989). A comparative analysis of the profitability performance of the largest US, European and Japanese multinational enterprises. *Management International Review*, *29*(3), 5–18.

Hagedoorn, J. (2002). Inter-firm R&D partnerships: an overview of major trends and patterns since 1960. *Research Policy*, *31*(4), 477–492.

Hawawini, G., Subramanian, V., & Verdin, P. (2003). Is performance driven by industry-or firm-specific factors? A new look at the evidence. *Strategic Management Journal*, *24*(1), 1–16.

Henri, J. F. (2004). Performance measurement and organizational effectiveness: bridging the gap. *Managerial Finance*, *30*(6), 93–123.

Hilbe, J. M. (2011). *Negative binomial regression*. Cambridge University Press.

Hitt, M. A., Hoskisson, R. E., & Kim, H. (1997). International diversification: effects on innovation and firm performance in product-diversified firms. *Academy of Management Journal*, *40*(4), 767–798.

Honeynet Project. (2004). *Know your enemy: trends*.. Retrieved from: http://old.honeynet.org/papers/trends/life-linux.pdf

IBM. (2010). *IBM X-force trend and risk report*.. Retrieved from. http://www.ibm.com/services/fr/gts/..risk/ibm_x-force2010_wgl03007usen.pdf

Inchausti, A. G. (1997). The influence of company characteristics and accounting regulation on information disclosed by Spanish firms. *European Accounting Review*, *6*(1), 45–68.

Katz, M. L., & Shapiro, C. (1985). Network externalities, competition, and compatibility. *The American Economic Review*, *75*(3), 424–440.

Kotabe, M., Srinivasan, S. S., & Aulakh, P. S. (2002). Multinationality and firm performance: the moderating role of R&D and marketing capabilities. *Journal of International Business Studies*, 79–97.

Kunreuther, H., & Heal, G. (2003). Interdependent security. *Journal of Risk and Uncertainty*, *26*(2–3), 231–249.

Levitt, T. (1960). Marketing Myopia, Harvard Business Review, July–August 1960, 45–56.

Lowensohn, J. (2012). *Apple R&D spending up nearly 40 percent in 2012*.. Retrieved from. http://news.cnet.com/8301-13579_3-57543370-37/apple-r-d-spending-up-nearly-40-percent-in-2012/

Luo, X., & Liao, Q. (2009). Ransomware: A New Cyber Hijacking Threat to Enterprises. Handbook of Research on Information Security and Assurance.

Maxcer, C. (2007). *Gates' mac attack: fact vs fiction, MacNewsWorld*.. Retrieved from. http://www.macnewsworld.com/story/56017.html

McDaniel, S. W., & Kolari, J. W. (1987). Marketing strategy implications of the Miles and Snow strategic typology. *The Journal of Marketing*, 19–30.

Miller, D. J. (2004). Firms' technological resources and the performance effects of diversification: a longitudinal study. *Strategic Management Journal*, *25*(11), 1097–1119.

Moitra, S. D., & Konda, S. L. (2000). *The survivability of network systems: an empirical analysis (No. CMU/SEI-2000-TR-021)*. Carnegie-Mellon University, Pittsburgh, Software Engineering Inst.

Morbey, G. K. (1988). R&D: Its relationship to company performance. *Journal of Product Innovation Management*, *5*(3), 191–200.

Murphy, G. B., Trailer, J. W., & Hill, R. C. (1996). Measuring performance in entrepreneurship research. *Journal of Business Research*, *36*(1), 15–23.

NASDAQ. (2014). *Technology companies*. Retrieved from. http://www.nasdaq.com/screening/companies-by-industry.aspx?industry=Technology

NVD. (2014). *National vulnerability database*.. Retrieved from. http://nvd.nist.gov/

Ortalo, R., Deswarte, Y., & Kaâniche, M. (1999). Experimenting with quantitative evaluation tools for monitoring operational security. *IEEE Transactions on Software Engineering*, *25*(5), 633–650.

Ozment, A. (2007). Improving vulnerability discovery models. *Proceedings 2007 ACM workshop on quality of protection*, 6–11. ACM Press.

Penrose, E. (2009). *The theory of the growth of the firm*. Oxford University Press.

Price, J. L., & Mueller, C. W. (1986). *Handbook of organizational measurement*. Marshfield, MA: Pitman Publishing.

Ransbotham, S., Mitra, S., & Ramsey, J. (2012). Are markets for vulnerabilities effective? *MIS Quarterly*, *36*(1), 43–64.

Ravenscraft, D., & Scherer, F. M. (1982). The lag structure of returns to research and development. *Applied Economics*, *14*(6), 603–620.

Ravichandran, T., & Lertwongsatien, C. (2005). Effect of information systems resources and capabilities on firm performance: a resource-based perspective. *Journal of Management Information Systems*, *21*(4), 237–276.

Robert Baum, J., & Wally, S. (2003). Strategic decision speed and firm performance. *Strategic Management Journal*, *24*(11), 1107–1129.

Roberts, P. W., & Dowling, G. R. (2002). Corporate reputation and sustained superior financial performance. *Strategic Management Journal*, *23*(12), 1077–1093.

SEC. (2014). *US securities and exchange commission*.. Retrieved from. http://www.sec.gov/edgar/searchedgar/companysearch.html

Schilling, M. (1999). Winning the standards race: building installed base and the availability of complementary goods. *European Management Journal*, *17*(3), 265–274.

Shahmehri, N., Mammar, A., Montes de Oca, E., Byers, D., Cavalli, A., Ardi, S., et al. (2012). An advanced approach for modeling and detecting software vulnerabilities. *Information and Software Technology*, *54*(9), 997–1013.

Shepherd, W. G. (1972). The elements of market structure. *The Review of Economics and Statistics*, *54*(1), 25–37.

Shepherd, W. G. (1986). *On the core concepts of industrial economics Mainstreams in Industrial Organization*. Dordrecht: Martinus Nijhoff Publishers.

Sherman, E. (2013). *Apple's ad budget hits $1 billion*.. Retrieved from. http://www.cbsnews.com/8301-505124_162-57562380/apples-ad-budget-hits-$1-billion/

Shin, Y., & Williams, L. (2008). An empirical model to predict security vulnerabilities using code complexity metrics. In *IEEE empirical software engineering and metrics (ESEM) 2008 short paper* (pp. 315–317).

Shin, Y., Meneely, A., Williams, L., & Osborne, J. A. (2011). Evaluating complexity, code churn, and developer activity metrics as indicators of software vulnerabilities. *IEEE Transactions on Software Engineering*, *37*(6), 772–787.

Sircar, S., Turnbow, J. L., & Bordoloi, B. (2000). A framework for assessing the relationship between information technology investments and firm performance. *Journal of Management Information Systems*, *16*(4), 69–97.

Slaughter, S. A., Harter, D. E., & Krishnan, M. S. (1998). Evaluating the cost of software quality. *Communications of the ACM*, *41*(8), 67–73.

Strong, S., & Bambang, S. (1998). Predicting stock returns using financial statement information. *Journal of Business Finance & Accounting*, *25*(5–6), 631–657.

Supapol, A. B., Fischer, E., & Pan, Y. (2008). Entrepreneurship in emerging regions around the world: theory. *Evidence and Implications*, 239.

Symantec. (2011). *Internet security threat report*.. Retrieved from. http://symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering*, *33*(8), 544–557.

Thurman, M. (2013). *Security Manager's Journal: r&D's new security lab is a promising step*.. Retrieved from. https://www.computerworld.com/s/article/9237814/Security_Manager_s_Journal_R_D_s_new_security_lab_is_a_promising_step

Wallace, R. O., Naser, K., & Mora, A. (1994). The relationship between the comprehensiveness of corporate annual reports and firm characteristics in Spain. *Accounting and Business Research*, *25*(97), 41–53.

Webster, F. E., Jr. (1997). The future role of marketing in the organisation. In D. R. Lehman, & K. E. Jocz (Eds.), *Reflections on the future of marketing, practice and education*. Cambridge, MA: Marketing Science Institute.

Weitz, B. A., & Bradford, K. D. (1999). Personal selling and sales management: a relationship marketing perspective. *Journal of the Academy of Marketing Science*, *27*(2), 241–254.

Woo, S. W., Alhazmi, O. H., & Malaiya, Y. K. (2006). An analysis of the vulnerability discovery process in web browsers. *Proceedings of the 10th international conference on software engineering and applications*.

Yamin, S., Gunasekruan, A., & Mavondo, F. T. (1999). Relationship between generic strategy, competitive advantage and firm performance: an empirical analysis. *Technovation*, *19*(8), 507–518.

Younan, Y. (2013). *25 years of vulnerabilities*. pp. 1988–2012. 1988–2012. Retrieved from. http://www.terach.com/assets/websites/terach/resources/Sourcefire%2025%20Years%20of%20Vulnerabilities%20Research%20Report.pdf