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.

© 2016 Elsevier Ltd. All rights reserved.

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

Download English Version:

https://daneshyari.com/en/article/1025465

Download Persian Version:

https://daneshyari.com/article/1025465

Daneshyari.com