Decision Support Systems 51 (2011) 745–759

Contents lists available at ScienceDirect

Decision Support Systems

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

Predicting stock market returns from malicious attacks: A comparative analysis of vector autoregression and time-delayed neural networks

Lara Khansa [a,*], Divakaran Liginlal [b]

[a] Department of Business Information Technology, Virginia Polytechnic Institute and State University, Blacksburg, VA, United States
[b] Carnegie Mellon University in Qatar, Doha, Qatar

ARTICLE INFO

Available online 1 February 2011

Keywords:
Malicious attacks
Stock price
Time-delayed artificial neural network
Vector autoregression

ABSTRACT

With the growing importance of Internet-based businesses, malicious code attacks on information technology infrastructures have been on the rise. Prior studies have indicated that these malicious attacks are associated with detrimental economic effects on the attacked firms. On the other hand, we conjecture that more intense malicious attacks boost the stock price of information security firms. Furthermore, we use artificial neural networks and vector autoregression analyses as complementary methods to study the relationship between the stock market returns of information security firms and the intensity of malicious attacks, computed as the product of the number of malicious attacks and their severity levels. A major contribution of this work is the resulting time-delayed artificial neural network model that allows stock return predictions and is particularly useful as an investment decision support system for hedge funds and other investors, whose portfolios are at risk of losing market value during malicious attacks.

1. Introduction

Malicious code consists of software or firmware intended to execute an unauthorized computer process with the purpose of disrupting the target's information systems [48]. Viruses, worms, Trojans, and other code-based entities that infect a host fall into this category. The growth of Internet-based businesses and globalization have exposed information technology (IT) infrastructures of firms to malicious code attacks of increasing intensity. In response, information security firms, i.e. the vendors of products that protect information systems from such malicious attacks, have invested heavily in research and development to come up with more resilient products. While malicious attacks have been associated with detrimental economic effects on attacked firms [8,10,22,23,30,40], we conjecture that they are beneficial to the market value of information security firms. The basis for this argument is that higher intensity of malicious attacks leads to higher investments in information security products and services [38], which, in turn, should have a positive effect on the stock price of the information security firms who sell these products and services. In this paper, we attempt to investigate two research questions: (i) *Are malicious attacks beneficial to the stock price of information security firms*, and *(ii) How well can the stock market returns of information security firms be predicted from these malicious attacks?*

Artificial neural networks (ANNs) have been widely used in the areas of intrusion detection and prevention, spam control, and financial prediction. The unpredictability in the arrival and intensity of malicious attacks makes it ideal to exploit the adaptability of ANNs to forecast the stock market returns of information security firms, given a certain level of intensity of malicious attacks. Our literature survey indicated that prior studies have not attempted to relate the market performance of information security firms to the intensity levels of malicious attacks, computed as the product of the severity of malicious attacks, which are assessed by antivirus providers' subject matter experts, and the number of malicious attacks. By adopting a complementary approach using both vector autoregression (VAR) methods and ANNs, we attempt to fill this gap in the literature.

Forecasting models proposed in the information security economics literature include risk management models [38,54], game theoretical models [11], real options (RO)-based models [37], and event study analyses [10,22]. Risk management models generally take into account both a risk analysis phase and a risk assessment phase. The risk analysis phase involves the identification of threats to system security, the probability of their occurrence, and their resulting impact. The risk assessment phase consists of identifying safeguards to mitigate the impact of the threats, followed by a cost-benefit analysis. Commonly used risk metrics such as Average Loss Expectancy (ALE) have been criticized for being overly complex when they attempt to address all threats and vulnerabilities [54]. RO-based models that quantify the benefits of information security investments

* Corresponding author at: Pamplin College of Business, Department of Business Information technology, 2062 Pamplin Hall (0235), Blacksburg, VA 24061–0101, United States. Tel.: +1 540 231 5003.
E-mail addresses: larak@vt.edu (L. Khansa), liginlal@cmu.edu (D. Liginlal).

0167-9236/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2011.01.010

have also been developed [37]. However, these RO-based models impose assumptions on the distribution of malicious attacks. In contrast, our analyses in this paper are based on actual records of malicious attacks and hard financial stock market data. Further, event study analyses have been conducted to relate security breaches resulting from malicious attacks to the stock price of information security firms [10,22]. Event studies only capture the momentary impacts of security breaches around the time of their announcements. In this paper, we relate the time series of malicious attacks to that of the stock market returns of information security firms and study their dynamic relationship over time. We first make use of VAR analysis to investigate this relationship, in the Granger causality sense [24]. VAR analysis, in the context of this paper, is a better fit than other regression methods because it captures time-lagged effects and feedback between variables. These effects and feedback are particularly relevant in time series data where relationships between variables could go both ways. One could argue that when the market value of information security firms increases, their ability to innovate and reduce the intensity of future malicious attacks increases as well. Sims [52] advocated the use of VAR models for such analyses because they make no a-priori assumptions regarding the relationships between variables, thus avoiding the identification restrictions of structural models. After we have established the significance between our model's variables and the time lag using VAR analysis, we use ANN-based analytical methods that complement VAR analysis by effectively mapping complex nonlinearities without specification of assumptions regarding the statistical distribution or properties of the underlying data.

The remainder of this paper is organized as follows. Section 2 provides a background to the research in the subject disciplines, surveys contemporary literature, and develops our hypothesis. Section 3 covers the research design, including a discussion of the data collection methods and measures. VAR analysis and results are presented in Section 4. The time-delayed ANN-based analysis, comparisons with the results of VAR, and sensitivity analyses with respect to ANN parameters and data quality are presented in Section 5. Section 6 discusses the implications, contributions, and limitations of the study, and avenues for future research.

2. Theoretical background

Malicious attackers can be classified as one of three types: a masquerader who is not a legitimate user but attempts to exploit a legitimate user account, a misfeasor who is a legitimate user but attempts to access resources to which he/she does not have usage permission, and a clandestine user who attempts to gain administrative control of the system [56]. What all these types of intruders have in common is that they all need a way into the system they desire to access. There exist many ways in which to gain access to a system, such as tricking a legitimate user over the telephone or by email into releasing account details. However, one of the most popular means of gaining entry is by exploiting software bugs, also called vulnerabilities, in host operating systems or Web applications that are running on Web servers. Software vendors have been shown to follow the strategy of releasing their products early and fixing them later through patching [3,44], especially when the market size and the degree of competition are high. Spier [55] showed that if manufacturers have the ability to repurchase their defective product, they have fewer incentives to design safer products. In a sense, software vendors have the ability to "repurchase their product" or more accurately they can repair their product without a physical recall. They can "ship" a patch to a user and have the user "install" the solution. The fact that software vendors do not have to physically recall their products from the customer could lessen their incentives to reduce vulnerabilities. Anderson [2] concluded that software vendors are capable of creating more secure software but that the economics of the software industry provide few incentives to encourage the development of more secure products and that the idea of shipping the product now and fixing the bugs later is a perfectly rational approach. The number of software vulnerabilities has increased dramatically over the years. Even in recent years, Symantec, a major antivirus provider (http://www.symantec.com), reported a 19% increase in documented vulnerabilities from 2007 to 2008, and that, in parallel, new malicious code signatures have increased by an astonishing 265% in 2008 compared to 2007.

A parallel exists between vulnerabilities in software and vulnerabilities in manufactured products. This paper, therefore, draws upon the research stream studying the effect of product defects on the market value of related firms, whether attacked firms or firms producing solutions for these defects. Bad reputation and lack of customer satisfaction have been shown to affect future customer behavior and, in turn, the level, timing, and risk of future cash flows of suppliers [5,12,29,32,33,35,48,50,51,63]. Chen et al. [12] showed that firms are better off being passive in responding to product recalls because proactive strategies are perceived by investors as a signal of larger financial losses to the firm. Rhee and Haunschild [48] tested automobile recalls from 1975 to 1999 and found that highly reputable firms are punished more upon product recalls than less reputable firms. Rupp [51] found that recalls initiated by the government were as damaging to shareholders as other recalls. White and Pomponi [63] reported the costs of recalls to consumer products companies to be more than 6 billion US$ per year. Kamp and Burton [35] reported that Medtronic's fourth quarter 2008 earnings fell 69% due to charges of product flaws and a safety notice. Mattel recalled millions of toys in 2007 and reported a cost of 30 million US$ related to those recalls. The costs (tangible and intangible) to Toyota of their recent recalls are expected to be astronomical. Early estimates of the cost of these recalls reach 2 billion US$ [32]. There are several studies that illustrate the negative effects of product recalls on firm value. Jarrell and Peltzman [33] found that drug recalls by the Food and Drug Administration (FDA) resulted in an average 6% loss in stock equity values for the affected firms. Moreover, some of the effects of the recall on stock equity values spilled over to other drug companies not directly affected by the recall. Similarly, Rubin et al. [50] estimated that product recalls by the U.S. Consumer Product Safety Commission resulted in an average 7% reduction in the stock equity values of the firms involved. Hendricks and Singhal [29] recounted the negative effects of supply chain glitches that resulted in production and shipment delays, on the market value of suppliers.

In the particular realm of information security, several researchers have investigated the impact of information security breaches on the market value of affected firms. Goel and Shawky [23] studied security breaches over the period 2004–2008 and noted a significantly negative impact on the market value of breached firms. Campbell et al. [8] found that only breaches linked to loss of confidential information had significant negative effects on the stock price of firms, while the impact of non-confidential breaches were not significantly different from zero. Hovav and D'Arcy [30] also studied the impact of denial-of-service attack announcements on the market over 4.5 years and showed that the market penalizes "Internet-specific" companies more than other companies. Liginlal et al. [40] found that investors' confidence in a financial firm's continuity is particularly abated after a human error-related privacy breach. Cavusoglu et al. [10] studied the change in market value of firms whose systems had been breached. The study showed that the announcement of a security breach decreased the market capitalization values of a firm, on average, by 2.1 billion US$ within two days of the breach. Furthermore, the study demonstrated a significant information transfer effect to information security firms. Garg et al. [22] reported similar findings and confirmed this transfer