UNDERSTANDING THE IMPACT OF INTERNET SECURITY BREACH ON MARKET VALUE: MANAGEMENT DETERRENCE POLICIES PERSPECTIVE

Francis Kofi Andoh-Baidoo
University of Texas – Pan American
1201 W University Drive
Edinburg, TX 78539
andohbaidoof@utpa.edu

ABSTRACT
This study employs the deterrence theory to examine the factors that impact firm damage associated with announcements of Internet security breaches in the public media. Firm damage is measured as the observed cumulative abnormal returns associated with the announcement. The findings suggest that investors interpret a security breach as management’s inaction to deter potential computer abusers from violating organizational security policies and controls. Specifically, investors are more likely to react negatively to Internet firms than Non-Internet firms. In addition, investors react more negatively to more recent attacks.

Keywords: Internet security breach, deterrence theory, risk management, market value, cumulative abnormal returns, event studies, decision tree induction, firm damage

1. INTRODUCTION
Internet security breach has been identified as one of the important challenging issues of management practice in the information age. Despite its increasing use to provide electronic commerce activities, the internet is very susceptible to security vulnerabilities. Quite recently, it was reported that over two-thirds of Americans are seriously concerned about cyber criminals and hackers (McCrohan 2003).

Information security has been identified as the most critical factor that influences people’s intention to purchase online (Salisbury et al. 2001; Yang et al. 2002). Salisbury et al. (2001) note that buyers are concerned about the lack of protection of their information to security breaches. Buyers might perceive security breaches as management’s failure to provide effective mechanisms to protect their information assets held within the organization and or in transit during electronic commerce transactions from security breach attacks.

The deterrence theory stipulates that managers can deter, prevent, and detect abuse as well as pursue remedies and or punish offenders for computer abuse (Straub et al. 1998). Thus, lack of effective management policies could be cited as a reason why a firm would be hit with security breach. Event studies on internet security breaches report that the announcements of internet security breaches lead to loss of market value (e.g., Andoh-Baidoo et al. 2007; Campbell et al. 2003; Cavusoglu et al. 2004a; Gordon et al. 2002; Hovav et al. 2003). However, none of these studies has explored investors’ reaction to management practices that could lead to security breaches. The purpose of this study is to use the deterrence theory to investigate how investors link internet security breaches to managements’ security policies and actions. We use the traditional event study analysis to measure the market value decline that results from announcements of internet security breaches in the public media. Firm damage can be operationalized as the observed cumulative abnormal return (CAR) attributable to the announcement of Internet security breach over the event window.
We use Decision Tree induction to examine the likelihood firm type and period of attack influence the damage to the firms arising from internet security breaches. The deterrence theory is used to explain how investors interpret management policies and actions that lead to security breaches.

The rest of the paper is organized as follows. We first discuss the theoretical foundations and hypotheses. We then present our research methodology followed by the results and a discussion of the results. We finally conclude the paper highlighting the managerial implications and limitations.

2. THEORIES AND HYPOTHESES

2.1. Theoretical background

The deterrence theory (e.g., Straub et al. 1998) forms the theoretical foundation for the hypotheses developed and tested to explain the relationships between firm damage (observed negative cumulative abnormal returns) and firm type and period of attack.

Deterrence Theory and Internet Security Breaches

The deterrence theory posits that the administration of appropriate strong disincentives and sanctions can be used to deter an individual’s intention to commit antisocial acts. This theory is extensively used in criminology research (Blumstein 1978; Pearson et al. 1985). Straub and others have used the deterrence theory to study information systems security risks (Hoffer et al. 1989; Straub 1990; Straub et al. 1992; Straub et al. 1993; Straub et al. 1990; Straub et al. 1998). In general, this stream of research argues that actions taken by management can deter potential computer abusers from violating organizational security policies.

Given that a great majority of computer security breaches are perpetrated by legitimate users, with most of these users being internal, the expectation is that countermeasures taken within the organization can serve as effective controls against breaches. The effectiveness of security countermeasures as deterrence mechanisms depends a great deal on user actions and awareness (D’Arcy et al. 2007). Making users aware of the existence of deterrence mechanisms can discourage inappropriate behavior because of the increased perception of being caught and punished (D’Arcy et al. 2007). To summarize, the Deterrence theory suggests that firms should be able to develop effective policies that would deter intruders from attacking their networks and systems. Thus, investors would interpret the announcements of internet security breaches as lack of effective actions by management to prevent security breaches.

2.2 Hypotheses

Cumulative abnormal returns (firm damage)

According to the deterrence theory, investors believe that internet security breach is a result of management failure to implement effective security policies and controls to deter intruders. Thus, Internet security breach is bad news to investors and our expectation is that investors will react negatively to any announcement that a firm has been breached. We therefore state the first hypothesis as:

Hypothesis 1: The CAR attributable to the announcement of an Internet security breach is negative.

Firm Type

Previous related studies and the information systems security literature suggest that firms that depend heavily on the Internet (referred to as “Net” firms, such as Amazon.com and eBay) are found to have greater interest in Internet security issues than do other firms (e.g., Cavusoglu et al. 2004a). In the case of Net firms, an incident that shuts down the network could result in no sales, whilst a conventional firm that suffers the same incident may generate sales from traditional markets. The Deterrence theory suggests
that investors would expect that Net firms would have effective controls and policies that would deter attackers from breaching their web sites and other information resources. Since Hence investors’ reaction to internet security breach on Net firms would be higher than for Non-net firms. We hypothesize that:

**Hypothesis 2:** All else equal, the likelihood of negative CAR attributable to announcements of Internet security breaches by Net firms is significantly higher than the likelihood of negative CAR attributable to announcements of Internet security breaches by Non-Net firms.

**Time Lag**

In February 2000, several major firms such as Yahoo, E-Bay, Amazon, and E-trade had their web sites shut down by a Denial of Service attack. This is the time when major firms were hit by the Denial of Service attack and most firms experienced a security breach for the first time. Since then several organizations have developed several proactive countermeasures and security controls as response to security threats. Thus, investors would react more negatively to attacks that are more recent than those that occurred prior to February 2000. This is because they expect that management should have taken major steps to prevent security incidents after they have learnt a lot from their own experiences and those of others. Thus, we hypothesize that:

**Hypothesis 3:** All else equal, the likelihood of negative CAR attributable to announcements of Internet security breaches for Post February 2000 is significantly higher than the likelihood of negative CAR attributable to announcements of internet security breaches for Pre February 2000 announcements.

### 3. RESEARCH METHODOLOGY

Our research approach involves using traditional event study methodology to estimate the CAR associated with announcements of internet security breaches in the public media. We then use decision tree induction to examine the relationship between the independent variables (firm characteristics, attack characteristics) and CAR. Details of the methodology are presented in the sections below.

#### 3.1 Data Collection

We define an event as an announcement about a firm’s Internet security breach in one of the major newspapers. Using Lexis-Nexis Academic online feature, we include in our sample all announcements in the Wall Street Journal, New York Times, Financial Times, Washington Post, and USA Today for the period 1997 through 2003. The list of keywords used for searching events include: virus names (e.g., love bug, soBig, and blaster worm); Attacker Type (e.g., Hacker, Vandal); Results of the attack (e.g., Denial of Service, Theft of Service), names of organizations reported in previous studies (e.g., Yahoo, eBay), or a term or combination of such terms (e.g., information security breach, computer system security, Internet security incident, and breach).

Only events involving publicly traded firms were considered in this study. We recorded 110 events. However, we eliminated some events using the following criteria: (1) when an event was reported more than once in a single or in different newspapers, we kept only the first announcement; (2) only firms that were listed on New York Stock Exchange (NYSE), NASDAQ, or American Stock Exchange (AMEX) and had return data in the CRSP database were included for analysis; (3) for firms in the CRSP database, the returns data had to be available for 120 days before the event for the computation of stock market return; and (4) where there were confounding effects such as earning announcements, dividends or any major announcement in the event window involving the breached firm that could impact return, the event was dropped. Our final sample size after the eliminations was 41.
3.2 Coding
We classified Firms as Net and Non-Net. We used Internet Stock listing™ and Morgan Stanley Dean Witter’s Internet Company list to identify “Net” and “Non-Net” firms (e.g., Cavusoglu et al. 2004b; Im et al. 2001). We use February 2000 as the “cutoff date”. This is the time when major firms were hit by the Denial of Service attack and most firms experienced security breaches for the first time. We believe that this period would be recognized as the time that businesses and investors became more aware of security breaches. Attack was classified as Pre February 2000 when they occurred on or before the cutoff date and Post February otherwise.

3.3 Event Study and CAR
To compute the abnormal return from the announcement, we first have to estimate the returns in the absence of the event. The market model developed by Sharpe (1963), which is used to estimate return, is represented as:

\[ R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it} \]

where \( R_{it} \) is the return of stock \( i \) on day \( t \); \( R_{mt} \) is the return of the market portfolio on day \( t \), \( \alpha_i \) and \( \beta_i \) are the intercept and slope parameters respectively for firm \( i \), and \( \varepsilon_{it} \) is the disturbance term for stock \( i \) on day \( t \).

According to the Efficient Market Hypothesis (Fama et al. 1969), if investors feel that internet security breach causes decreases in future cash flow, the firm will observe a negative abnormal return. This reflects the market reaction to the announcement which is quickly absorbed into the firm’s stock. The abnormal return for firm \( i \) on day \( t \) of the event window can be estimated as:

\[ AR_{it} = R_{it} - (\hat{\alpha}_i + \hat{\beta}_i R_{mt}) \]

where \( \hat{\alpha} \) and \( \hat{\beta} \) are the ordinary least square estimates of \( \alpha \) and \( \beta \). These parameters are estimated using the market model over 120 day period ending with the day immediately preceding the first day of the event window, i.e. day (-2).

The summation of the daily abnormal returns over the event window is the cumulative abnormal return. The cumulative abnormal return for stock \( i \) over the event window \((T_1, T_2)\) is computed as:

\[ CAR_{i(T_1,T_2)} = \sum_{t=T_1}^{T_2} AR_{it} \]

For a sample of \( n \) stocks the cumulative abnormal return over the event window is

\[ CARR_{(T_1,T_2)} = \frac{1}{n} \sum_{i=1}^{n} CAR_{i(T_1,T_2)} \]

3.4. Decision Tree Induction
A decision tree (DT) is a representation of a given decision problem in tree structure where every non-leaf node is associated with one of the decision variables, and every branch from a non-leaf node is associated with a subset of the values of the corresponding decision variable, and each leaf node is associated with a value of the target (or dependent) variable. If the target variable is discrete then the DT is considered to be a classification tree and for each node the DT generation algorithm generates the relative frequencies
(probabilities) for the classes of the target variable. At every leaf a class is assigned, with the winning
class being the one that provides the largest class probability (even if the probability is less than 50%). In
this paper we use classification trees.

Decision tree induction identifies those variables most significant in predicting the outcome. The most
significant attribute is located at the root of the tree and succeeding attributes further discriminate
between the outcomes. The sequence of attribute values in the decision tree can easily be converted to the
rules of an expert system. Several DTs may be generated by varying the splitting methods (e.g. Entropy,
Gini) and/or excluding selected independent variables as potential predictors.

In this study, every case at the leaf node is assigned to one possible class, Negative or Normal. Negative
refers to negative CAR while Normal means a CAR value greater or equal to zero. For the given target
event (e.g. CAR is Negative), the posterior probabilities for each sibling node are compared.

4. RESULTS

In this section, we present and discuss the results for the Internet security breach sample. First, we present
the results and discussion of the cumulative abnormal return attributed to the announcement of Internet
security breach. We also discuss the results of the DT induction.

4.1 Event Study and CAR

We present the results of the Eventus® analysis for the sample of events from the Internet security breach
announcements.

<table>
<thead>
<tr>
<th>Days</th>
<th>Cumulative Average Abnormal Return</th>
<th>Median Cumulative Abnormal Return</th>
<th>Positive: Negative</th>
<th>Generalized Sign Z</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Equally Weighted</td>
<td>Precision Weighted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(-1, +1)</td>
<td>-3.18%</td>
<td>-1.75%</td>
<td>-1.45%</td>
<td>14:27</td>
</tr>
</tbody>
</table>

* Significant at .05
** Significant at .01

The generalized sign test (one–tail test) shows that the results are significant at the 5% level. Thus,
Hypothesis 1 is confirmed by our data. Within a three day window of security breach announcements,
firms on an average lost 3.18% of their market value.

4.2 DT Induction, Firm Type and Period of Attack

We used SAS Enterprise Miner 4.3 tool to generate the Decision Trees. We generated several DTs, using
three splitting methods (i.e. Chi-Square, Entropy and Gini). These methods are presented as the sources of
the rules generated in Table 3 as DT_C, DT_E, and DT_G respectively.
**Firm Type**

**Table 2: Sets of Rules that include Firm Type as a Discriminating Predictor**

<table>
<thead>
<tr>
<th>Source</th>
<th>Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>DT_EGa</td>
<td>IF <strong>Firm Type</strong> = ‘NET’ &amp; <strong>Results</strong> ∈ {'THEFT OF SERVICE', ‘CORRUPTION OF INFORMATION’} &amp; <strong>Attacker</strong> ∈ {'CORPORATE RAIDERS’, ‘VANDALS’} THEN N = 3 CAR: {POSITIVE: 0.0%; NEGATIVE: 100.0%}</td>
</tr>
<tr>
<td></td>
<td>IF <strong>Firm Type</strong> = ‘NON.NET’ &amp; <strong>Results</strong> ∈ {'THEFT OF SERVICE', ‘CORRUPTION OF INFORMATION’} &amp; <strong>Attacker</strong> ∈ {'CORPORATE RAIDERS’, ‘VANDALS’} THEN N = 9 CAR: {POSITIVE: 44.4%; NEGATIVE: 55.6%}</td>
</tr>
<tr>
<td>DT_Gc</td>
<td>IF <strong>Firm Type</strong> = ‘NON.NET’ &amp; <strong>Access</strong> = ‘UNAUTHORIZED USE’ THEN N = 6 CAR: {POSITIVE: 83.3%; NEGATIVE: 16.7%}</td>
</tr>
<tr>
<td></td>
<td>IF <strong>Firm Type</strong> = ‘NET’ &amp; <strong>Access</strong> = ‘UNAUTHORIZED USE’ THEN N = 3 CAR: {POSITIVE: 33.3%; NEGATIVE: 66.7%}</td>
</tr>
<tr>
<td></td>
<td>IF <strong>Firm Type</strong> = ‘NET’ &amp; <strong>Period</strong> = ‘PRE FEB 2000’ &amp; <strong>Access</strong> = ‘UNAUTHORIZED ACC’ THEN N = 5 CAR: {POSITIVE: 40.0%; NEGATIVE: 60.0%}</td>
</tr>
<tr>
<td></td>
<td>IF <strong>Firm Type</strong> = ‘NON.NET’ &amp; <strong>Period</strong> = ‘PRE FEB 2000’ &amp; <strong>Access</strong> = ‘UNAUTHORIZE ACC’ THEN N = 3 CAR: {POSITIVE: 66.7%; NEGATIVE: 33.3%}</td>
</tr>
</tbody>
</table>

All three rules (See Table 2) for the firm type variable show that the likelihood of negative CAR attributable to the announcement of an internet security breach is higher for net firms than non-net firms thus providing support for Hypothesis 2.

**Period of Attack**

**Table 3: Sets of Rules that include Period (Time) as a Discriminating Predictor**

<table>
<thead>
<tr>
<th>Source</th>
<th>Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>DT_C</td>
<td>IF <strong>Access</strong> = ‘UNAUTHORIZED ACC’ &amp; <strong>Period</strong> = ‘PRE FEB 2000’ THEN N : 8 CAR: {POSITIVE: 50.0%; NEGATIVE: 50.0%}</td>
</tr>
<tr>
<td></td>
<td>IF <strong>Period</strong> = ‘POST FEB 2000’ &amp; <strong>Access</strong> = ‘UNAUTHORIZED ACC’ THEN N : 24 CAR: {POSITIVE: 16.7%; NEGATIVE: 83.3%}</td>
</tr>
</tbody>
</table>

The pair of rules in Table 3 suggests that for attacks involving Unauthorized Access, those that occurred Pre February 2000 are less likely to lead to negative CAR than those that occurred Post February 2000 (50% vs 83%) and therefore the data provides support for H3.
5. DISCUSSIONS
Generally, the announcement of internet security breach in the public media leads to negative CAR, which is an operationalization of firm damage. The DT analysis provides evidence to suggest that the firm type and period of attack are good predictors of the likelihood of firm damage. In the following, we explain the findings using the deterrence theory.

5.1 Firm Type
Since Net firms depend solely on the internet, a security breach on a firm’s web site or information resources could prevent the firm from performing any transactions. The Deterrence theory suggests that investors would expect that Net firms would spend considerable effort in implementing effective countermeasure policies and controls to prevent security breaches. Hence, the finding from the data that Net firms are more likely to suffer firm damage than Non-Net firms is in agreement with the expectation of the deterrence theory.

5.2 Period of Attack
The results suggest that prior to the widespread knowledge about Internet security breaches in February 2000, investors did not link announcements on Internet security breaches to market value (Pre February 2000) when the breach was perpetrated by Unauthorized users, i.e. the outsider, much as they do Post February 2000 when many individuals and firms became more aware of security breaches. Security Managers have become more aware of security and techniques to proactively actively deal with them (D'Arcy et al. 2007). The deterrence theory suggests that managers are expected to use these techniques to prevent security breaches. This expectation explains why we observe that most recent attacks are more likely to cause damage.

6. MANAGERIAL IMPLICATIONS
As organizations make conscientious efforts to eliminate or reduce Internet security breaches, it would increase consumer confidence in e-commerce activities and assure investors of firm’s commitment to secure their business systems, which eventually may enhance business activities and improve the stock market performance. As the public becomes more aware of the information technology issues, they are better informed in interpreting the implications of Internet security and the impact Internet security breaches have on market value of breached firms. Security managers should implement effective policies and controls that would take into consideration some of the findings such as minimizing vulnerabilities as investors do not take it lightly when hackers notify firms about their systems’ vulnerabilities. In addition, Net firms should take extra efforts in avoiding security breach because investors expect them to do better than Non-Net firms in protecting information and network resources.

7. CONCLUSION
Previous relevant studies on security and firm damage have observed that announcements of internet security breaches in the public media and further that firm and attack characteristics influence the likelihood of firm damage. However, there is lack of theoretical basis for explaining the phenomena. In this paper, we explored the relationships between firm damage and firm characteristics and attack characteristics using the deterrence theory. The paper seeks to contribute to theory development in Internet security breaches and firm damage as measured by abnormal returns observed when a security breach is announced in the public media. The findings suggest that investors interpret security breach as management’s inaction to deter potential computer abusers from violating organizational security policies. We examine some of the limitations of our study in this section. One of the problems with performing an event study on Internet security breaches is that of sample size. While firms are eager to make public e-commerce initiatives, the same is not true for Internet security breaches.
Although one may consider the sample size of 41 used in the current study to be small, it is greater than the size of events that Campbell et al. (2003) and Hovav and D’Arcy (2003) used. Nevertheless, a large sample size would enhance the validity of the findings.

8. REFERENCES


