Decision Support Systems 50 (2011) 662–672

Contents lists available at ScienceDirect

Decision Support Systems

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

Assessing the severity of phishing attacks: A hybrid data mining approach

Xi Chen [a,*], Indranil Bose [b], Alvin Chung Man Leung [b,c], Chenhui Guo [d]

[a] School of Management, Zhejiang University, China
[b] School of Business, The University of Hong Kong, Hong Kong
[c] McCombs School of Business, The University of Texas at Austin, TX, United States
[d] Eller College of Management, The University of Arizona, AZ, United States

ARTICLE INFO

Available online 19 August 2010

Keywords:
Financial loss
Phishing
Risk
Supervised classification
Text phrase extraction
Variable importance

ABSTRACT

Phishing is an online crime that increasingly plagues firms and their consumers. We assess the severity of phishing attacks in terms of their risk levels and the potential loss in market value suffered by the targeted firms. We analyze 1030 phishing alerts released on a public database as well as financial data related to the targeted firms using a hybrid method that predicts the severity of the attack with up to 89% accuracy using text phrase extraction and supervised classification. Our research identifies some important textual and financial variables that impact the severity of the attacks and potential financial loss.

1. Introduction

Phishing is a major security threat to the online community. It is a kind of identity theft that makes use of social engineering skills and technical subterfuge to entice the unsuspecting online consumer to give away their personal information and financial credentials [5]. A typical phishing attack consists of four phases, namely, preparation, mass broadcast, mature, and account hijack [8]. The tremendous financial impact of phishing is borne by the fact that phishing caused an estimated financial loss of US $3.2 billion affecting 3.6 million people from September 2006 to August 2007 [40]. The number of reported phishing incidents grew exponentially, and increased by 293.7% from 8829 in December 2004 to 34,758 in October 2008 [4,5]. Not only do phishing attacks cause financial loss, but they also shatter the confidence of customers in conducting e-commerce. Managers of some of the US super regional banks have indicated that the deteriorating customer trust is a major concern with respect to phishing [46]. A recent survey found that most customers of European banks only use online banking to check their account balances instead of conducting online transactions due to the fear of getting phished [15]. Another study also reported that the customer fear psychosis has resulted in a 20% decrease in the rate of opening of genuine emails [10].

To make customers aware of latest phishing attacks, some international organizations and government statutory bodies, such as the Anti-phishing Working Group (APWG), have published phishing alerts on their websites. To assess the risk level of each phishing attack, some firms have sought help from information security experts who evaluated reported phishing incidents based on the contents of the phishing email and the phishing websites. However, as phishing incidents continue to increase at a tremendous rate, the manual risk assessment method involving experts may be too slow. Data mining techniques can improve the assessment of phishing attacks. They can discover the knowledge embedded in the traits of prior phishing attacks and identify the inherent characteristics that contribute to the different risk levels of a phishing attack. This can help predict the associated risk level of a new phishing incident in a short period of time with a reasonable accuracy. Furthermore, the risk level, which is based on the technical sophistication of phishing attacks, may not be directly related to financial loss caused by an attack. Past research has shown that the impact of sophisticated phishing alerts on stock markets is not as significant as phishing alerts whose risk level is considered to be moderate [33]. However, the financial loss resulting from a phishing attack is always of great concern to security administrators as well as consumers of an organization. Therefore, a warning mechanism that can identify the phishing incidents that are either very risky or likely to cause a large financial loss will be of great interest to shareholders and senior managers of the targeted companies.

In this research we use supervised classification techniques, which is a major stream of data mining, to assess the severity of phishing attacks. At the same time, we identify the key antecedents that contribute to a high risk level or a high financial loss generation by a phishing attack. We use a hybrid approach which combines key phrase extraction and supervised classification methods that makes use of the textual data description of the phishing attack as well as financial data of the targeted company to assess the severity of a phishing attack according to its risk level or financial loss generating

* Corresponding author.
E-mail addresses: chen_xi@zju.edu.cn (X. Chen), bose@business.hku.hk (I. Bose), aleung@mail.utexas.edu (A.C.M. Leung), chguo@email.arizona.edu (C. Guo).

0167-9236/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2010.08.020

potential. The three classifiers used for this purpose result in a classification accuracy of up to 89%. Our results also show that the key identifying variables for risk level and potential financial loss of phishing attacks are different from each other. High risk level is associated with phishing emails that ask customers of large firms to update their accounts whereas high financial loss is characterized by phishing attacks targeted to customers of large firms that have high total liabilities.

2. Literature review

Phishing has aroused great interest among information security researchers. Understanding the critical success factors of phishing and determining methods that can prevent or detect such a crime has been a popular area of research. We can roughly split current research on phishing into three streams, namely, phenomenal studies, economic analysis, and technical research.

As an example of a phenomenal study related to phishing, Jagatic et al. found that the social engineering skill of the adversary was a critical success factor for phishing [26]. Dhamija and Tygar discovered that lack of knowledge, inability to control visual deception, and lack of attentiveness to detail are the major weaknesses of people who fall prey to phishing attacks [14]. Interestingly, Workman found that the critical success factors for some marketing strategies were applicable to phishing attacks as well [51]. Researchers also found that education of customers, standardization of technology, and sharing of phishing information were among the most important policies that could deter phishing attacks [35]. Some researchers conducted experimental studies and confirmed that if a user was trained to identify phishing attacks, the chance of being cheated in future was significantly lowered [32].

Among economic studies related to phishing, Jakobsson classified the costs of phishing into three categories, namely, direct cost, indirect cost, and opportunity cost [27]. Singh studied a number of international phishing incidents and found that the direct financial loss per incident ranged from US $900 to 6.5 million pounds [45]. However, it is widely believed that as companies are quite reluctant to disclose information related to direct financial loss caused by phishing, the actual financial loss might be ten times more than the estimated numbers that appeared in research reports [21]. In their attempt to estimate the indirect financial loss caused by phishing, Leung and Bose found that phishing related announcements caused a significant negative reaction among investors of targeted companies [33]. It is interesting to note that a significant negative investor reaction of 2.1% loss in market value within two days of the announcement was reported in the broader context of analyzing the economic impact of information security breaches [30].

In the area of technical research, information security researchers have toiled to discover better countermeasures of phishing. A number of anti-phishing toolbars and phishing filters have been developed. Data mining based approaches have been frequently adopted in the development of such countermeasures. Data mining techniques have been used to filter out phishing emails that contained fraudulent messages [1]. By analyzing the headers of emails, researchers were able to prevent the spread of malicious emails containing virus/worms/Trojans, and stop crimes such as phishing and distributed denial of service attacks with an accuracy of 99% [52]. Among the various data mining techniques that have been adopted for determination of phishing emails are support vector machines [12], random forest [18], one-step ternary and repeated binary classification techniques [19], and ensemble methods [43]. To authenticate the URL embedded in the emails, logistic regression [20] and decision trees have also been used [37]. The focus of the extant research was on the analysis of the characteristics of the emails and determination of the malicious nature of the emails. However, the focus of the current research is on the assessment of the influence of such phishing emails.

The use of data mining techniques in research related to information security is not new. Zhu et al. had used rough sets, neural networks, and decision trees for detection of network intrusion [55]. They tried different combinations of classification tools and data representation format, and experimented with variation in the proportion of training and testing data. They showed that rough sets performed best when the data was presented in binary format, and the proportion of training and testing data was balanced [55]. Zhao et al. proposed a hybrid system for network intrusion detection [54]. The system consisted of three main components: service pattern databases that were used to detect the network traffic patterns for different services, anomaly detection module that was based on unsupervised clustering and detected anomalous network traffic patterns, and a random forest module that was used to differentiate between intrusion cases and normal cases of service usage. Zhao and Huang proposed a data mining approach that mimicked the human immune system and detected network intrusion [53]. Ansari et al. detected misuse and anomalies using a soft computing method like fuzzy logic [3]. From the various examples cited in this paragraph we can see that data mining techniques have been favored by researchers in the area of information security. For a comprehensive review on this topic the interested reader may refer to Tsai et al. [47]. However, past research mainly focused on the detection of security events such as misuse, anomalies, intrusion, and other types of security breaches. Research on the use of data mining techniques to assess the influence of security events such as phishing attacks was limited.

In this paper, we used neural network (NN), decision tree (DT), and support vector machine (SVM) to classify the risk levels. The three classifiers have different characteristics. NN consists of three interconnected layers, namely, input layer, hidden layer, and output layer. Each layer contains interconnected nodes than can process the data. The interconnections are assigned weights that continue to change as the NN 'learns' the pattern from the input data. Inputs and intermediate results are passed from the input layer to the output layer to produce the final classification results [9]. Because of the structure, NN is good at learning non-linear relationships between input data and output data. SVM views data sets as vector spaces and performs classification by constructing a hyperplane that maximizes the separation in order to divide the vectors into different classes. SVM can perform either linear or non-linear classification [11]. DT can tolerate the presence of outliers and missing data, and so minimum effort is required for data preprocessing using DT. When processing categorical data with more than two levels of value, NN and SVM create dummy variables for each level of value of the related input variable, and this adds to the computational burden. In contrast, DT can derive rules directly from categorical data without creating dummy variables. However, DT cannot use continuous variables directly, and has to convert them to categorical data. The DT model adopted in this research was C5.0, an upgraded version of C4.5 developed by Quinlan [41]. Compared to C4.5, C5.0 is faster, more accurate, and less memory intensive [42]. Furthermore, C5.0 allowed multiple splits at any level of the DT.

Similar to data mining, text mining has also gained popularity as a research tool due to its ability to mine digital content available on the Internet. Text mining was used to convert free text of the phishing alerts to structural data in the form of a document-term matrix. Since a document is composed of various terms, if we used all terms as attributes, the dimensionality of the document-term matrix would be very high. We grouped similar terms together so that the dimensionality of the document-term matrix was significantly reduced following the example of prior research [16]. In fact, we found that some of the frequently occurring words had almost similar meaning, and thus it was more efficient to group such words together under a higher level concept. For example, the terms 'cash', 'refund', and 'savings' could be grouped under the concept 'money'. Usually, a dictionary which contained the linguistic and semantic relationships

between words is used for grouping of concepts. WordNet is a popular dictionary that is used for grouping in natural language processing [17]. In WordNet, nouns are organized into hierarchies with their hypernyms and hyponyms. For noun y, if every y is a type of x, then y is a hyponym of x. On the other hand, if every x is a type of z, then z is hypernym of x. In Fig. 1, the hyponym and hypernym hierarchies of the word 'bank' are shown. According to Fig. 1, words such as 'credit union', 'agent bank', 'acquirer', and other phrases under the hyponym are grouped under the same concept 'bank'. At the same time, the concept 'bank' belonged to the concept 'financial institution', which in turn belonged to the higher level concepts 'institution' and 'organization'.

The most typical application of text mining is in document management involving tasks such as text segmentation, key words extraction, indexing, and text categorization. Wei et al. have used clustering techniques and integrated information on personal preferences for document management [49]. A hybrid methodology that combined text mining with data mining has been adopted by some researchers as well. Ma et al. used text mining to analyze company news and discover social networks among companies, and utilized the discovered characteristics of the social networks to predict the revenue of the associated companies using decision trees and logistic regression [38]. Holton employed document clustering to identify those documents that showed disgruntled messages. He then extracted key terms from those documents, and used those terms as input to a Bayesian network to classify disgruntled messages and non-disgruntled messages. The accuracy of the classification was as high as 89% [25]. Although text mining has been frequently used in a number of domains, its application in the area of information security is not so common. Wang et al. used text mining techniques such as key phrase extraction, cluster analysis, and concept links to discover different types of disclosures about information security incidents in financial reports [48]. They used memory based reasoning to classify the disclosures about information security incidents into three groups. Each of these groups represented different levels of fluctuations in stock prices caused by the disclosures. However, the classification was only based on the textual content of the disclosures about information security incidents, and no financial information about the company was used. We believe that text mining techniques can be used to analyze text-based phishing alerts for identification of important textual variables that characterize phishing attacks.

Prior research has demonstrated that phishing as an online crime is growing in terms of frequency of occurrences, financial loss imparted to firms and their customers, as well as technical sophistication. In fact, Berghel reported that the technical sophistication marked the difference between severity of attacks caused by phishing mongers and posers [7]. To the best of our knowledge, there is no prior research that predicted the severity of a phishing attack using data mining techniques. As numerous phishing emails and websites appear every day, a warning system that could identify severe phishing incidents and their characteristics, and alert senior managers and information security specialists to take immediate action could be quite useful for preventing the escalating direct and indirect financial loss due to phishing. As there is a lack of research in this area, we are motivated to construct a warning system using a data mining approach that makes use of textual data obtained from phishing alerts as well as financial data of companies. Data mining approaches have shown their superiority over traditional statistical approaches in building classification systems [6,22,23,28], and this motivated us to use a hybrid text and data mining method to assess the severity of phishing attacks in two ways—the associated risk level of the attack, and the loss in market value for the firm caused by the phishing alerts. Direct financial loss due to a phishing attack is difficult to calculate, and is generally not immediately available at the time of release of phishing alerts. This is partially due to the fact that many companies try to conceal such data to prevent any damage to their reputation. An alternative measure of financial loss is the indirect financial loss in market value caused by phishing alerts. As phishing attacks occur, potential customers may get scared and avoid using the e-commerce services offered by the company. Investors may foresee the shrunk future revenue due to the reduced number of customers or transactions, and react by decreasing the market value of the company. In the context of security breaches, past research has evaluated the impact of the characteristics of the attack on the financial loss generated by the security breach [2,30], but did not find any significant relationship between them. In fact, both risk level and indirect financial loss are complementary measures that indicate the severity of a phishing attack because the two indicators may not be correlated, and a high risk level of a phishing alert does not necessarily imply that the phishing attack will result in a high loss in market value [33]. In this research, we estimate risk level and loss in market value using both textual data obtained from the description of the phishing alerts, and financial data from the financial statements of the companies.

3. Theoretical framework

A theoretical model showing the impact of any type of threat on corporate performance was proposed by Crockford [13] and called the risk-components model. In this model, it was proposed that threats may compromise corporate resources, and thus negatively affect firm performance. This impact may be reflected as drop in earnings or

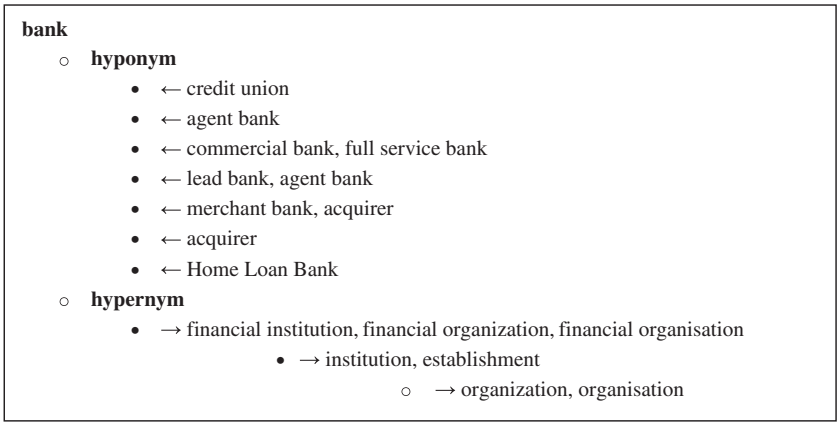

Fig. 1. Possible lexical relationships for the concept 'bank'.

market value of the firm. We adopted this model for assessment of the impact of security threats. Loch et al. categorized security threats according to their potential impacts on corporate assets. These categories included disclosure, modification, destruction, and denial of service [36]. The level of severity of security threats affected firm value, and it was reported that the potential impact of such threats on corporate performance could be determined by ranking these threats according to their severity [50]. Furthermore, Crockford proposed some modifying factors that might augment the impact of threats. Organizational factors, such as IT resources and firm size, have been found to significantly affect security management [31]. Such factors have also been found to pose deterrent effects on the security effectiveness, and hence indirectly determine the impact of security threats on firm value [29]. Based on extant literature discussed above, we conceived our theoretical model as shown in Fig. 2. Phishing alerts were found to drive down market value in prior empirical research [33]. In this study, we investigate the relationships between nature of phishing alerts, and various organizational factors on one hand with the decline in market value of firms on the other hand.

4. Data collection and analysis

In this section we describe how we collect, prepare, and analyze phishing alerts to assess their severity, and determine important antecedents that influence the classification.

4.1. Data collection and preparation

To determine the severity of phishing attacks, we utilized two types of input data, namely, phishing alerts available from the database Millersmiles, and financial data available from the financial statements of the firms. The phishing alerts data used in this research is the largest available phishing alerts data set at the time of research, and was collected from mid-2005 to mid-2008.

As phishing is primarily motivated by financial gains [24,34], corporate financial data may be relevant for the assessment of severity of phishing. Relevant financial data, reported in the last month of the year prior to the release of the phishing alert, was retrieved from The Center for Research in Security Prices (CRSP). In the raw data set, there were 168 financial variables. The four authors conferred with each other, and an expert in the area of finance to choose relevant financial variables that were appropriate for the context of this research. This resulted in the choice of 75 attributes related to the financial performance of a firm. Then we used the Pearson's Chi-square statistic to determine the strength of the relationship between those 75 financial variables and the target variables. The top 25 variables for the classification tasks (in terms of the Pearson's Chi-square statistic) were selected. The list of those 25 financial variables appears in Table 1. As some targets of phishing attacks did not have publicly available financial data, (e.g., Internal Revenue Service) some sample data was discarded at this stage. The average total assets of the targeted firms were about US $484,000 million with average earnings about US $10,000 million and average number of employees approximately 61,000.

The technical sophistication of the phishing attack was measured in terms of the risk level of the attack that was determined by the information security specialists of Millersmiles. As for financial impact, because the direct financial loss was rarely disclosed by the targeted companies, we measured the indirect financial loss in terms of loss of market value of the firm. An event study was conducted to determine the change in market value of the firm after the release of the phishing alerts. This methodology was adopted because it could immediately measure the impact of phishing alerts on market value of firms, which indirectly reflected the expectation of the investors about the performance of the companies that became targets to phishing attacks. The adopted method was similar to that of Leung and Bose [33]. First, all events related to private firms were removed. Then events that were affected by some confounding events such as mergers, acquisitions, dividend announcements, and changeovers were eliminated from further consideration. Next, the stock return of the firm was compared with that of a market index to determine the cumulative abnormal return (CAR) of stock prices. We used CAR in this study because the change in the stock price of a firm is a synthesized reflection of various consequences due to phishing attacks, such as loss of clients, shrinkage in market share, and reduced confidence of consumers as well as investors. The direct financial loss is rarely reported by victims of phishing attacks, and the actual financial performance of the victims is reported only on a quarterly or annual basis. Within this time frame the companies may be subject to the influence of other events that are unrelated to the phishing attacks, making it difficult to isolate the direct financial loss due to phishing attacks. On the contrary, CAR provides an immediate measure of the impact of phishing alerts on firm value. Making use of the event study methodology and removing cases with confounding events that may have an influence on the market value of the companies, we ensured that the CAR only captured the effect of phishing alerts, albeit in the form of indirect financial loss.

The computation procedure of CAR is based on the capital asset pricing model as shown in (1):

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it} \quad (1)$$

where R_{it} is the rate of return for firm i on day t, R_{mt} is the rate of return of market index m on day t, α is the y-intercept, β is the slope that measures the sensitivity of R_{mt}, and ε_{it} is the disturbance term with Ordinary Least Squares properties. Following the convention of prior event studies, we constructed the regression model using stock price data for 200 trading days that started one month prior to the event announcement date. The abnormal return in stock price (AR_{it}) on the event announcement i on date t is computed using Eq. (2):

$$AR_{it} = R_{it} - (a_i + b_i R_{mt}) \quad (2)$$

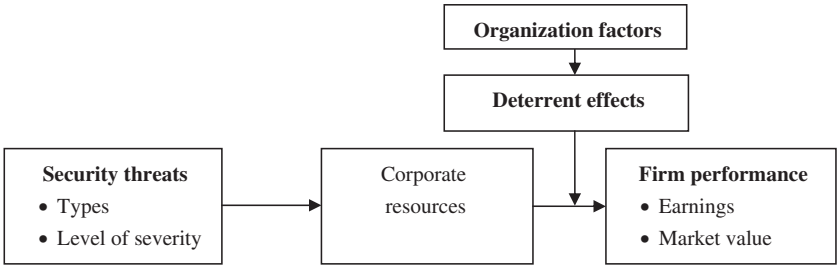

Fig. 2. Theoretical model for assessing the impact of security threats on firm performance.

Table 1
List of financial data used in classification.

Variables	Meaning	Mean[a]	Std. dev[a]
Advertising_Expense	Expenditure in advertising	527.62	549.77
Assets_Total	Total assets	483,838.59	668,759.88
Book_Value_Per_Share	Book value per share	24.59	30.90
Common_Equity_Tangible	Value of tangible common equity	14,627.22	19,126.68
Cost_of_Goods_Sold	Cost of goods sold	13,983.46	20,462.61
Debt_in_Current_Liabilities_Total	Total debt in current liabilities	51,929.49	102,443.34
Earnings_Before_Interest_and_Taxes	Earnings before interest and taxes	10,021.76	11,641.15
Employees	Number of employees	61.12[b]	111.18[b]
Income_Before_Extraordinary_Items	Income before extra-ordinary items	4256.40	5301.25
Inventories_Total	Total inventories	7666.51	19,516.20
Invested_Capital_Total	Total amount of invested capital	86,789.72	110,956.03
Liabilities_Total	Total liabilities	452,367.84	634,786.36
Long_Term_Debt_Total	Total long term debt	60,489.73	86,810.73
Market_Value_Total_Fiscal	Total market value in fiscal year	47,572.94	49,770.37
Net_Income_Loss	Net loss in income	4265.04	5322.35
Notes_Payable_Short_Term_Borrowings	Notes payable in short-term borrowings	44,948.64	94,289.16
Operating_Expenses_Total	Total operating expenses	20,741.33	27,870.43
Other_Intangibles	Value of other intangibles	3276.60	6337.16
Preferred_Preference_Stock_Capital_Total	Total preferred/preference stock (capital)	406.48	1028.74
Price_High_Annual_Fiscal	Annual high price in fiscal year	51.17	21.30
Price_Low_Annual_Fiscal	Annual low price in fiscal year	35.90	16.57
Receivables_Total	Total receivables	244,330.45	310,778.64
Revenue_Total	Total revenue	31,537.03	38,754.69
S_P_Core_Earnings	Standard and Poor's core earnings	4206.22	5050.33
Selling_General_and_Administrative_Expense	General sales and administrative expense	7633.71	7659.20

[a] Figures in million US dollars unless otherwise specified.
[b] Figures in thousand.

CAR_i, which is the cumulative abnormal return of announcement i over a 3-day event window $[-1, 1]$ is computed using the following formula:

$$CAR_i = \sum_{t=-1}^{1} AR_{it} \tag{3}$$

where $t=[-1, 1]$ is one day before the date of release of phishing alert to one day after that date. Following the convention of prior event studies, a 3-day event window for computation of CAR is adopted because information about the event may be leaked one day prior to the event announcement day, and the investors may take 1–2 trading days to fully realize the consequence of the event. A short event window is preferred to a long event window due to the probable occurrence of other unrelated events that may lead to false statistical inference [39]. A total of 1030 phishing alerts in our sample data had relevant CAR_i data that ranged from −7.9% to 5.7% with a mean of 0% and standard deviation of 1.3%, and were subsequently used in the numerical experiments.

4.2. Numerical experimentation

We used a $3\times3\times2$ experimental design in this research incorporating three sets of input data, three classifiers, and two classification tasks. The design included:

- Textual data from phishing alerts, financial data of the targeted companies, and combined textual and financial data. Key phrase extraction techniques were used on the textual data to determine important semantic concepts that could act as input variables to the classifiers.
- 3 classifiers—decision tree (DT), support vector machines (SVM), and neural network (NN).
- Classification of risk level and CAR.

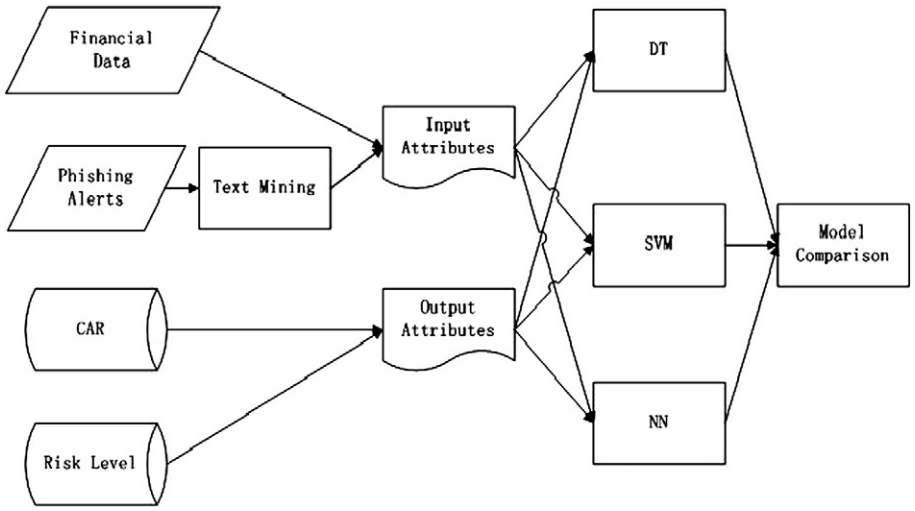

Fig. 3. Schematic diagram for data analysis.

After the models were built, their performances were compared using accuracy and top decile lift as performance metrics. In addition, we also evaluated the relative importance of the different input variables for the various models. A schematic diagram representing the overall procedure for data analysis is shown in Fig. 3.

4.2.1. Textual content analysis

We used the text mining module of the SPSS Clementine to extract the key semantic concepts from the phishing alerts. The text mining had its own built-in dictionary which was similar to WordNet. After grouping various terms under the broader semantic concepts, a document-concept matrix was built. Each cell of the matrix represented the frequency of occurrence of the concepts within a document (i.e., a phishing alert). By performing this analysis, the natural language of phishing alerts was converted to structural data that could be used as input variables to the classification models.

4.2.2. Development of classification models for risk level and CAR

There were two dependent variables in our research to measure the severity of phishing alerts, namely, risk level and CAR. We first categorized phishing alerts according to the five risk levels assigned by Millersmiles. These risk levels were: Low, Low-Medium, Medium, Medium-High, and High. The majority of the alerts belonged to the category of Medium. For the sake of simplicity, we grouped risk levels Low and Low-Medium to form a new group 'Low', and Medium-High and High to form a new group 'High'. Next, we categorized phishing alerts according to the CAR generated by them. Positive CAR indicated that the market responded favorably to the phishing alert whereas a negative CAR indicated unfavorable market response. Although CAR is a continuous variable we categorized it into three groups, namely, positive, stable, and negative. The positive group consisted of phishing alerts that resulted in CAR greater than 3%. The negative group consisted of phishing alerts associated with a CAR less than −3%. The rest of the phishing alerts belonged to the stable group. This method of creating groups with the choice of 3% as a threshold value was used in prior research [48].

In the subsequent modeling phase, we classified various levels of severity (i.e., risk level and CAR) using input variables obtained from textual categories or financial data or both. NN, SVM, and DT were used in this research due to their history of superior performance in other applications related to information security [12,37,55]. The risk levels and the CAR for the phishing alerts were not evenly distributed. Figs. 4 and 5 show the distributions of the two variables. Therefore, for classification of risk level, we oversampled the high risk and low risk instances of data but kept the medium risk instances the same so that the distribution of the three groups became 1:1:1 in the training and testing data sets. For classification of CAR, we repeated the process by oversampling the negative and positive instances while retaining the stable instances in its original form. To build the classification model,

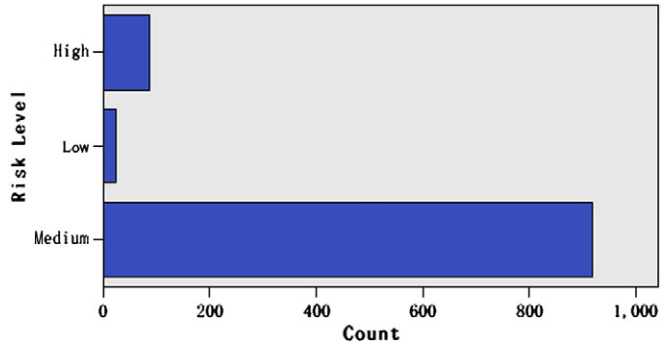

Fig. 4. Distribution of risk level of phishing alerts.

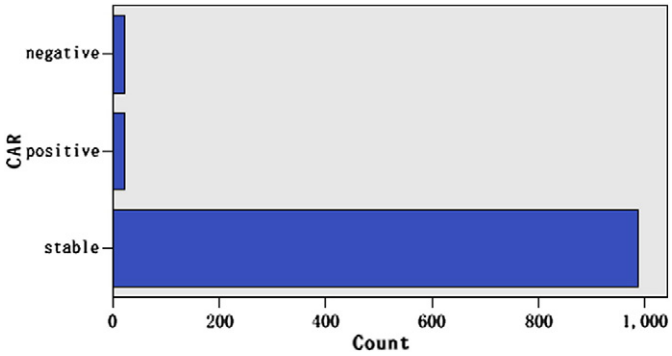

Fig. 5. Distribution of CAR generated by phishing alerts.

70% of the oversampled data was used for training, and 30% was used for testing. However, in the validation data set, we retained the original distribution of data. We also used 10-fold cross validation, and calculated the average accuracy of the model from the cross-validation models.

4.2.3. Evaluation of importance of variables

To find out which variables played an important role in the classification process we evaluated the importance of the variable i (VI_i) as the normalized sensitivity using the following formula:

$$VI_i = \frac{S_i}{\sum_{j=1}^{K} S_j} \tag{4}$$

where K is the number of input variables, and S_i is the ratio of the variance in the expected value of the output when all input variables are known except i to the unconditional variance in the value of the output. It is obtained using the formula:

$$S_i = \frac{Var\left(E\left(Y|X_{j,i\neq j}\right)\right)}{Var(Y)} \tag{5}$$

where Y denotes the output variable, and X denotes the input variables. Saltelli et al. showed that S_i is the proper measure of sensitivity to rank the predictors in order of importance for any combination of interaction and non-orthogonality among predictors, and when the size of the dataset was larger than a few hundred records [44]. We calculated the importance of all input variables for classification of risk level and CAR separately, and ranked the input variables in terms of their importance for both cases.

5. Results

In this section, the results obtained by applying the trained classification models on the validation data are presented. We evaluated the classification accuracy of the models, and then identified the important variables discovered by the models for the two classification tasks.

5.1. Classification accuracy

In Tables 2 and 3, we showed the lift values obtained for the two classification tasks. For classification of risk level, the models assigned likelihood scores to phishing alerts that indicated how likely it was for the phishing alerts to be high risk. The top decile lift was equal to the ratio of true high risk phishing alerts among the top 10% of phishing alerts in terms of the likelihood score of high risk divided by the ratio of high risk phishing alerts in the whole population of phishing alerts.

Table 2
Lift values for classification of risk level.

Deciles	Combined	Text.	Fin.	Combined	Text.	Fin.	Combined	Text.	Fin.
	DT	DT	DT	SVM	SVM	SVM	NN	NN	NN
1	5.26	4.07	4.09	6.40	4.40	2.44	4.77	4.19	2.75
2	4.35	3.17	2.98	3.95	3.52	1.82	3.49	3.07	2.51
3	3.02	2.50	2.40	2.91	2.54	1.98	2.55	2.36	1.97
4	2.33	2.02	1.99	2.31	2.00	1.76	2.06	1.80	1.69
5	1.93	1.73	1.70	1.93	1.75	1.52	1.67	1.51	1.58
6	1.61	1.55	1.50	1.61	1.59	1.37	1.47	1.38	1.46
7	1.38	1.35	1.38	1.43	1.38	1.24	1.28	1.24	1.33
8	1.21	1.24	1.25	1.25	1.21	1.16	1.13	1.15	1.18
9	1.11	1.11	1.11	1.11	1.11	1.09	1.06	1.06	1.07
10	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

Table 3
Lift values for classification of CAR.

Deciles	Combined	Text.	Fin.	Combined	Text.	Fin.	Combined	Text.	Fin.
	DT	DT	DT	SVM	SVM	SVM	NN	NN	NN
1	5.91	4.76	2.90	8.52	7.72	2.86	7.62	7.14	5.63
2	3.10	2.75	2.86	4.76	5.00	4.03	4.76	4.29	4.07
3	2.75	2.70	2.68	3.17	3.33	3.17	3.17	3.17	3.17
4	2.38	2.20	2.50	2.50	2.50	2.50	2.38	2.38	2.50
5	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00
6	1.67	1.67	1.67	1.67	1.67	1.67	1.67	1.67	1.67
7	1.43	1.43	1.43	1.43	1.43	1.43	1.43	1.43	1.43
8	1.25	1.25	1.25	1.25	1.25	1.25	1.25	1.25	1.25
9	1.11	1.11	1.11	1.11	1.11	1.11	1.11	1.11	1.11
10	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

For example, suppose there were 10,000 phishing alerts and the percentage of true high risk phishing alerts was 1.8%. If the top decile lift was two, this implied that the model could identify 36 true high risk phishing alerts by selecting 1000 phishing alerts that made up the top 10% of phishing alerts in terms of likelihood scores for high risk. In contrast, by random targeting, the expected number of true high risk phishing alerts that could be captured among 10% of all phishing alerts was only 18. Therefore the higher the top decile lift, the better was the model. We used lift values to compare the model's ability to capture high risk phishing alerts. As shown in Table 2, the combined textual and financial data always performed best in terms of top decile lift up to the 7th decile. For SVM, the use of only textual data was consistently better than the use of only financial data in terms of top decile lift. For DT, the performance using textual data was not as good as that using financial data in the first decile, but was consistently better up to the 6th decile. For NN, the performance using textual data was better than that using financial data up to the 4th decile. The results indicated that analyzing the textual content of the phishing alerts was important for the classification of risk levels of the phishing alerts. The results also illustrated that combining textual data with financial data made the classification more accurate. Among the three classifiers, the performance of SVM was the best. The top decile lift using the hybrid textual and financial data as input was 6.40 implying that the model was 6.4 times more likely to capture true high risk phishing alerts than random selection.

The lift values obtained for the classification of CAR are shown in Table 3. The results shown are consistent with those in Table 2. Again, the combined textual and financial data performed best in terms of lift in most cases, and the use of only textual data was consistently better than the use of only financial data only for SVM but not for DT and NN. Table 3 again illustrated the importance of combining textual data with financial data for the purpose of classification. As in the case of risk level classification, the SVM model using combined textual and financial data as inputs obtained the highest lift value of 8.52.

The confusion matrices for classification of risk level and CAR are shown in Tables 4 and 5 respectively. As the dependent variables had three levels, we showed the number of correct classifications (i.e., sum of true positives and true negatives), and the number of wrong classifications (i.e., sum of false positives and false negatives) for each class in Tables 4 and 5. From the confusion matrix shown in Table 4, it can be seen that for classification of risk level, the use of the combined textual and financial data as input led to better performance of the models in terms of accuracy than the use of other types of input. Also, the use of only textual data as input gave rise to better accuracy of classification of risk level compared to the use of only financial data. For classification of CAR, use of textual data gave rise to higher accuracy compared to the use of financial data as in the case of classification of risk level. Interestingly, although the combined textual and financial data gave rise to better performance in case of SVM and NN, the best performance in terms of overall accuracy was obtained when DT was used with textual data as input.

Taking the classification of high risk cases as well as overall performance into account, the DT model using combined textual and financial data performed the best, and was able to correctly classify 75 high risk cases out of 86. The SVM model using combined textual and financial data ranked second by classifying 68 high risk cases out of 86 correctly. For classification of CAR, the SVM model using only textual data as input performed the best and correctly classified all 21 negative CAR cases. The SVM model using combined textual and

Table 4
Confusion matrix for classification of risk level.

		Combined			Text.			Fin.		
		High	Low	Medium	High	Low	Medium	High	Low	Medium
DT	High	75	5	6	64	4	18	59	11	16
	Low	0	23	0	3	18	2	0	22	1
	Medium	133	64	724	234	82	605	218	126	577
	Correct	822	79.81%		687	66.70%		658	63.88%	
	Wrong	208	20.19%		343	33.30%		372	36.12%	
SVM	High	68	4	14	65	4	17	44	11	31
	Low	1	21	1	3	19	1	1	19	3
	Medium	141	47	733	202	99	620	229	176	516
	Correct	822	79.81%		704	68.35%		579	56.21%	
	Wrong	208	20.19%		326	31.65%		451	43.79%	
NN	High	65	3	18	55	8	23	47	16	23
	Low	1	18	4	2	19	2	0	21	2
	Medium	181	34	706	171	101	649	214	212	495
	Correct	789	76.60%		723	70.19%		563	54.66%	
	Wrong	241	23.40%		307	29.81%		467	45.34%	

Table 5
Confusion matrix for classification of CAR.

		Combined			Text.			Fin.		
		Neg.	Pos.	Stable	Neg.	Pos.	Stable	Neg.	Pos.	Stable
DT	Negative	13	1	7	10	1	10	12	9	0
	Positive	1	18	4	2	13	8	8	14	1
	Stable	95	24	867	64	27	895	183	146	657
	Correct	898	87.18%		918	89.13%		683	66.31%	
	Wrong	132	12.82%		112	10.87%		347	33.69%	
SVM	Negative	20	0	1	21	0	0	19	2	0
	Positive	3	19	1	3	20	0	8	12	3
	Stable	99	26	861	120	51	815	209	99	678
	Correct	900	87.38%		856	83.11%		709	68.83%	
	Wrong	130	12.62%		174	16.89%		321	31.17%	
NN	Negative	19	0	2	18	2	1	19	2	0
	Positive	3	19	1	3	19	1	7	12	4
	Stable	115	74	797	130	78	778	219	70	697
	Correct	835	81.07%		815	79.13%		728	70.68%	
	Wrong	195	18.93%		215	20.87%		302	29.32%	

financial data ranked second, and correctly classified 20 negative CAR cases out of 21.

5.2. Comparison of important variables

In order to understand the antecedents that governed the classification of risk level and CAR of phishing alerts, we calculated the importance of all input variables. As the combined textual and financial data gave rise to good accuracies, we listed the top five most important textual variables and the top five most important financial variables identified for each of the classification tasks using the three classifiers with the combined textual and financial data as input. The variables are listed in order of their importance in Tables 6 and 7, where the column 'Identifying Classifier(s)' showed the corresponding classifiers that identified these variables as important. The top five textual categories that were common between classification of risk level and CAR are shown in italics in Table 6.

We found that the top five textual categories for the two classifications were not similar. Only four categories 'confirmation', 'account', 'information', and 'computers' were common to both classifications. Also, there was no general agreement among the classifiers about the most important textual category. For classification of risk level, 'update' was identified as an important textual category by all three classifiers. This implied that phishing attacks with messages requesting recipients to update their personal information were of high risk level. 'Security', 'email', 'bank account', and 'bank' were regarded as top five textual categories by two of the three classifiers. These findings demonstrated that high risk phishing attacks were usually associated with security messages related to bank accounts in the form of emails and targeted to customers of banks. For classification of CAR, 'consumers' was identified as an important textual category by all three classifiers, whereas 'information' and 'writing' were identified as top five categories by two of the three classifiers. This reflected the perception of investors about the potential financial loss to be generated by the phishing attacks. When phishers pretended to be authenticated service providers and requested their customers to reveal personal information, then such attacks became likely to cause financial loss to the customers, hurt brand reputation, and affect present and future revenues of the company. The textual concept of 'writing' was related to words such as 'service access', 'limited access', and 'promotion code'. Those words were baits used by phishers to capture the attention of customers.

In Table 7, the top five most important financial variables identified by the three classifiers are listed. There were no common financial variables for classification of risk level and CAR. This showed that the underlying financial variables determining the two measures of severity of phishing attacks were significantly different. For classification of risk level, total inventories was identified as an important financial variable by all three classifiers whereas other intangibles and advertising expense was identified as a top five financial variable by two out of three classifiers. These financial variables indicated the preference of phishers towards launching attacks on large firms. High total inventories and intangibles is a hallmark of a large firm, and high advertising expense identified a company that had greater media exposure. This meant that large companies were preferred targets for high risk phishing attacks because they had a strong customer base, and their customers were likely to be misled by fake emails due to their inherent trust on these companies. For classification of CAR, number of employees, total invested capital, and total liabilities were identified as top five financial variables by two out of three classifiers. Again, the number of employees and total invested capital indirectly hinted at the large size of the firm. It was interesting to note that firms that already had high total liabilities were at greater risk of being penalized by investors when phishing attacks took place.

Table 6
Textual concepts listed in order of importance with identifying classifiers.

Risk Level*	Identifying Classifier(s)	CAR[a]	Identifying Classifier(s)
Update	DT, SVM, NN	Consumers	DT, SVM, NN
Security	DT, SVM	*Information*	DT, SVM
Email	DT, SVM	Writing	SVM, NN
Bank account	DT, NN	eBay	DT
Bank	SVM, NN	*Confirmation*	DT
Confirmation	DT	Warning	DT
Account	SVM	Person	SVM
Information	NN	*Account*	SVM
Computers	NN	Work	NN
		Computers	NN
		Assets	NN

[a] Textual concepts common to both classifications are shown in italics.

6. Discussion

Information security analysts generally assess the severity of phishing attacks on the basis of technical sophistication. The financial loss that is likely to result from phishing attacks is rarely estimated. However, senior managers and shareholders of companies are quite

Table 7
Financial variables listed in order of importance with identifying classifiers.

Risk level	Identifying Classifier(s)	CAR	Identifying Classifier(s)
Inventories_Total	DT, SVM, NN	Employees	DT, SVM
Other_Intangibles	DT, NN	Invested_Capital_Total	SVM, NN
Advertising_Expense	SVM, NN	Liabilities_Total	SVM, NN
Price_High_Annual_Fiscal	DT	Receivables_Total	DT
Operating_Expenses_Total	DT	Net_Income_Loss	DT
Income_Before_Extraordinary_Items	DT	Price_Low_Annual_Fiscal	DT
S_P_Core_Earnings	SVM	Long_Term_Debt_Total	DT
Preferred_Preference_Stock_Capital_Total	SVM	Assets_Total	SVM
Market_Value_Total_Fiscal	SVM	Book_Value_Per_Share	SVM
Common_Equity_Tangible	NN	Notes_Payable_Short_Term_Bors.	NN
Earnings_Before_Interest_and_Taxes	NN	Debt_in_Current_Liabilities_Total	NN
		Cost_of_Goods_Sold	NN

interested to know the economic impact of phishing attacks. Keeping in mind that it is important to evaluate the technical sophistication as well as the potential financial impact of phishing attacks, we conducted this research and developed a mechanism to predict the severity of phishing alerts in terms of risk level and potential loss in market value indicated by CAR of stock prices. Our research results showed that the two types of severity measures were complementary because there were different variables that were impacting each of them. From the list of top five most important input variables generated using the three classifiers, we found that the overlap for the two types of classifications was consistently low and this implied that risk level of a phishing alert was not indicative of the CAR generated by it. This finding is similar to that of a prior study where it was shown that a phishing alert with high risk did not result in significantly negative CAR [33]. This implied that instead of only providing ratings of the risk level of phishing attacks, anti-phishing organizations should develop some predictions for the potential financial loss caused by phishing attacks. The loss in market value of the targeted firm could be added with the information of the risk level to give a complete picture of the impact of a phishing attack. Furthermore, our research results indicated that assessment based on data that consisted of important textual categories discovered from the text of phishing alerts as well as financial data of the targeted companies, outperformed assessment based on any of the above data items alone. Information security specialists usually assess risk level of phishing incidents based on the textual description of phishing alerts. Our results indicated that for assessing severity it was important to consider the financial condition of the targeted company as well.

From an academic perspective, our research made an important contribution in terms of application of a hybrid text and data mining method for solving a problem in the area of information security. Text mining was used in the first stage to extract key semantic concepts from the textual content of the phishing alerts, and in the second stage these important concepts as well as financial data of the organizations were input to classifiers to classify the risk level and CAR of the phishing alerts. The performance of the classifiers in terms of accuracy and top decile lift showed that the hybrid text and data mining model was successful in classifying different levels of risks and different types of financial impact caused by phishing attacks. The results were more or less consistent for the three different classifiers, and indicated that a hybrid data mining model was able to generate consistent results of high accuracy. Our research showed that data mining techniques could be used to assess severity of phishing attacks effectively. This is an important academic implication, and we hope other researchers can further explore the use of data mining in assessing other security breaches in future.

From a managerial perspective, our study paved the way for automating the assessment of severity of phishing attacks. As there are an increasing number of phishing incidents that are reported around the world every day, manual assessment of such incidents could be time consuming as well as inaccurate due to the subjective bias of the evaluator. The method proposed in this paper automated the assessment of severity of phishing incidents using past data and provided a richer assessment of such incidents than what is currently being done by the anti-phishing organizations. We hope that the findings of this study can encourage anti-phishing organizations to adopt our proposed method to predict the risk level as well as potential financial impact of a phishing alert as soon as it is reported on their website. A system for assessment of phishing alerts can be divided into two parts: offline processing and online processing. For the offline processing part, a database of phishing attacks will be maintained. Data on phishing attacks need to be collected and updated continuously in this database. The second component of the offline system will be the financial data of the organization that will be updated only when financial statements are issued by the company. A third component of the offline system will be the training module where classifiers will be re-trained regularly in order to capture new patterns of phishing attacks. The main component of the online processing part will be the parsing of the new phishing alert for keyword extraction, collection of latest financial data for the company, and classification. As soon as a new phishing alert appears, the classifiers will determine the risk level of the alert, and assess the level of financial impact of the alert based on the knowledge base of the classifiers. The predictions will need to be checked by human experts from time to time to ensure that the classifier system is performing appropriately.

7. Conclusion

Phishing has become one of the biggest threats to the online community. Many researchers have explored ways to deter such crime. Information security specialists and anti-phishing organizations have set up phishing alerts databases that assess each reported phishing incident in terms of its risk level. In the view of increasing number of reported phishing incidents, we believe that such a manual assessment approach is not efficient enough to provide a timely report, and is also not complete as it ignores the possible financial impact of phishing incidents. In this research, we adopted a hybrid text and data mining model that used key phrase extraction technique to discover important semantic categories from the textual content of the phishing alerts, and combined those discovered categories with financial data of the targeted companies to come up with classification of risk level of the attack and the loss in market value of the firm that it was likely to cause. The performance of the hybrid model was quite superior in terms of top decile lift and accuracy, and demonstrated the need to consider textual data as well as financial data for making

prediction about the severity of the phishing alert. Furthermore, our results showed that risk level and CAR were fundamentally different from each other as we discovered that different textual and financial factors impacted them. This implied that it was important to evaluate both for fully assessing the severity of the phishing alerts—a practice we recommend that all anti-phishing organizations should adopt in future to make their members more knowledgeable about the severity of phishing attacks. In this research, we assume equal misclassification cost. However, in future researchers can conduct the experiments using unequal misclassification cost. For example, if the false positive alarm is issued, it will mislead the investors and other stakeholders of the company. In that case, classifying low risk or low CAR attacks as high risk or high CAR will cause unnecessary worry among investors. However, the impact of misclassifying a high risk or high CAR phishing attack can be quite severe. Such a false negative misclassification may turn out to be very costly for the firm. It will be interesting to see if the assumption of unequal misclassification cost leads to similar prediction as the current research.

References

[1] E. Airoldi, B. Malin, Data mining challenges for electronic safety: the case of fraudulent intent detection in e-mails, Proceedings of the Workshop on Privacy and Security Aspects of Data Mining 2004, Brighton, UK, 2004, pp. 57–66.
[2] F.K. Andoh-Baidoo, K.-M. Osei-Bryson, Exploring the characteristics of internet security breaches that impact the market value of breached firms, Expert Systems with Applications 32 (3) (2007) 703–725.
[3] A.Q. Ansari, T. Patki, A.B. Patki, V. Kumar, Integrated fuzzy logic and data mining: impact on cyber security, Proceedings of the Fourth International Conference on Fuzzy Systems and Knowledge Discovery, Haikou, China, 2007.
[4] APWG, Phishing Activity Trends Report December 2005, Anti-Phishing Working Group, 2005, pp. 1–15, (http://www.antiphishing.org/reports/apwg_report_DEC2005_FINAL.pdf).
[5] APWG, Phishing Activity Trends Report Second Half 2008, Anti-Phishing Working Group, 2009, pp. 1–12, (http://www.antiphishing.org/reports/apwg_report_H2_2008.pdf).
[6] B. Baesens, S. Viaene, D. Van den Poel, J. Vanthienen, G. Dedene, Bayesian neural network learning for repeat purchase modeling in direct marketing, European Journal of Operational Research 138 (1) (2002) 191–211.
[7] H. Berghel, Phishing mongers, and posers, Communications of the ACM 49 (4) (2006) 21–25.
[8] I. Bose, A.C.M. Leung, Unveiling the mask of phishing: threats, preventive measures, and responsibilities, Communications of the Association for Information Systems 19 (24) (2007) 544–566.
[9] I. Bose, R.K. Mahapatra, Business data mining—a machine learning perspective, Information & Management 39 (3) (2001) 211–225.
[10] A. Brandt, Phishing anxiety may make you miss messages, PC World 23 (10) (2005) 34.
[11] C.J.C. Burges, A tutorial on support vector machines for pattern recognition, Data Mining and Knowledge Discovery 2 (2) (1998) 121–167.
[12] M. Chandrasekaran, K. Narayanan, S. Upadhyaya, Phishing e-mail detection based on structural properties, Proceedings of NYS Cyber Security Conference, Albany, NY, USA, 2006.
[13] N. Crockford, An Introduction to Risk Management, Woodhead-Faulkner, Cambridge, 1986.
[14] R. Dhamija, J.D. Tygar, Phish, and HIPs: human interactive proofs to detect phishing attacks, in: H.S. Baird, D.P. Lopresti (Eds.), Proceedings of the Second International Workshop on Human Interactive Proofs, Bethlehem, PA, USA, 2005, pp. 127–141.
[15] B. Ensor, A. Giordanelli, M.d. Lussanet, T.v. Tongeren, Many online banking users use few features, Forrester Research, 2007, pp. 1–6.
[16] R. Feldman, J. Sanger, The Text Mining Handbook: Advanced Approaches in Analyzing Unstructured Data, Cambridge University Press, Cambridge, UK, 2007.
[17] C. Fellbaum, WordNet: An Electronic Lexical Database, The MIT Press, Boston, MA, USA, 1998.
[18] I. Fette, N. Sadeh, A. Tomasic, Learning to detect phishing emails, Proceedings of the Sixteenth International Conference on World Wide Web, Banff, Alberta, Canada, 2007, pp. 649–656.
[19] W.N. Gansterer, D. Polz, E-mail classification for phishing defense, advances in information retrieval, Proceedings of the Thirty-First European Conference on IR Research, Toulouse, France, 2009, pp. 449–460.
[20] S. Garera, N. Provos, M. Chew, A.D. Rubin, A framework for detection and measurement of phishing attacks, Proceedings of the 2007 ACM Workshop on Recurring Malcode, Alexandria, VA, USA, 2007, pp. 1–8.
[21] G. Goth, Phishing attacks rising, but dollar losses down, IEEE Security & Privacy Magazine 3 (1) (2005) 8.
[22] K. Ha, S. Cho, D. MacLachlan, Response models based on bagging neural networks, Journal of Interactive Marketing 19 (1) (2005) 17.
[23] C.M. Heilman, F. Kaefer, S.D. Ramenofsky, Determining the appropriate amount of data for classifying consumers for direct marketing purposes, Journal of Interactive Marketing 17 (3) (2003) 5–28.
[24] S. Hinde, ID theft: the US legal fight back, Computer Fraud & Security 2004 (10) (2004) 7–9.
[25] C. Holton, Identifying disgruntled employee systems fraud risk through text mining: a simple solution for a multi-billion dollar problem, Decision Support Systems 46 (4) (2009) 853–864.
[26] T. Jagatic, N. Johnson, M. Jakobsson, F. Menczer, Social phishing, Communications of the ACM 50 (10) (2006) 1–10.
[27] M. Jakobsson, S. Myers, Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft, Wiley-Interscience, Hoboken, NJ, USA, 2007.
[28] F. Kaefer, C.M. Heilman, S.D. Ramenofsky, A neural network application to consumer classification to improve the timing of direct marketing activities, Computers & Operations Research 32 (10) (2005) 2595–2615.
[29] A. Kankanhalli, H.-H. Teo, B.C.Y. Tan, K.-K. Wei, An integrative study of information systems security effectiveness, International Journal of Information Management 23 (2) (2003) 139–154.
[30] K. Kannan, J. Rees, S. Sridhar, Market reactions to information security breach announcements: an empirical analysis, International Journal of Electronic Commerce 12 (1) (2007) 69–91.
[31] A.G. Kotulic, J.G. Clark, Why there aren't more information security research studies? Information & Management 41 (5) (2004) 597–607.
[32] P. Kumaraguru, S. Sheng, A. Acquisti, L. Cranor, J. Hong, Lessons from a real world evaluation of anti-phishing training, Proceedings of the eCrime Researchers Summit 2008, Anti-phishing Working Group, Atlanta, GA, USA, 2008, pp. 1–12.
[33] A.C.M. Leung, I. Bose, Indirect financial loss of phishing to global market, Proceedings of the Twenty-Ninth International Conference on Information Systems, Paris, France, 2008, pp. 1–15.
[34] E. Levy, Criminals become tech savvy, IEEE Security & Privacy 2 (2) (2004) 65–68.
[35] Q. Liao, X. Luo, The phishing hook: issues and reality, Journal of Internet Banking and Commerce 9 (3) (2004) 1.
[36] K.D. Loch, H.H. Carr, M.E. Warkentin, Threats to information systems: today's reality, yesterday's understanding, MIS Quarterly 16 (2) (1992) 173–186.
[37] C. Ludl, S. McAllister, E. Kirda, C. Kruegel, On the effectiveness of techniques to detect phishing sites, in: B.M. Hämmerli, R. Sommer (Eds.), Proceedings of the Fourth International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Lucerne, Switzerland, 2007, pp. 20–39.
[38] Z. Ma, O.R.L. Sheng, G. Pant, Discovering company revenue relations from news: a network approach, Decision Support Systems 47 (4) (2009) 408–414.
[39] A. McWilliams, D. Siegel, Event studies in management research: theoretical and empirical issues, Academy of Management Journal 40 (3) (1997) 626–657.
[40] T. Powell, Ounce of ID theft protection worth more than agony of restoring good name, MyWestTexas.com, 2008 (http://www.mywesttexas.com/articles/2008/05/26/news/opinion/columns/trish_powell/bbb_5_23.txt).
[41] J.R. Quinlan, C4.5: Programs for Machine Learning, Morgan Kaufmann Publishers, San Mateo, CA, USA, 1993.
[42] Rulequest Research, Is See5/C5.0 Better Than C4.5? Rulequest Research, 2008, (http://www.rulequest.com/see5-comparison.html).
[43] A. Saberi, M. Vahidi, B.M. Bidgoli, Learn to detect phishing scams using learning and ensemble methods, Proceedings of the International Conferences on Web Intelligence and Intelligent Agent Technology Workshop, Silicon Valley, CA, USA, 2007, pp. 311–314.
[44] A. Saltelli, K. Chan, E.M. Scott, Sensitivity Analysis, Wiley, Chichester, West Sussex, UK, 2000.
[45] N.P. Singh, Online frauds in banks with phishing, Journal of Internet Banking and Commerce 12 (2) (2007) 1–27.
[46] T. Smith, J. Jordan, Banks' Top Phishing Fears—Financial Loss and Lost Customer Trust, MarkMonitor, San Francisco, CA, USA, 2007.
[47] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, W.-Y. Lin, Intrusion detection by machine learning: a review, Expert Systems with Applications 36 (10) (2009) 1194–1200.
[48] T.-W. Wang, J. Rees, K. Kannan, Reading the disclosures with new eyes: bridging the gap between information security disclosures and incidents, February 1, 2008 (http://ssrn.com/abstract=1083992).
[49] C.-P. Wei, R.H.L. Chiang, C.-C. Wu, Accommodating individual preferences in the categorization of documents: a personalized clustering approach, Journal of Management Information Systems 23 (2) (2006) 173–201.
[50] M.E. Whitman, Threats to information security, Communications of the ACM 46 (8) (2003) 91–95.
[51] M. Workman, Wisecrackers, a theory-grounded investigation of phishing and pretext social engineering threats to information security, Journal of the American Society for Information Science and Technology 59 (4) (2008) 662–674.
[52] J. Zhang, Z.-H. Du, W. Liu, A behavior-based detection approach to mass-mailing host, Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, China, 2007, pp. 2140–2144.
[53] J.–.Z. Zhao, H.–.K. Huang, An intrusion detection system based on data mining and immune principles, Proceedings of the First International Conference on Machine Learning and Cybernetics, Beijing, China, 2002.
[54] J. Zhao, M. Zulkernine, A. Haque, Random-forests-based network intrusion detection systems, IEEE Transactions on Systems, Man, and Cybernetics – Part C: Applications and Reviews 38 (5) (2008) 649–659.
[55] D. Zhu, G. Premkumar, X. Zhang, C.–.H. Chu, Data mining for network intrusion detection: a comparison of alternative methods, Decision Sciences 32 (4) (2001) 635–660.

Xi Chen is a lecturer of Information Systems at the School of Management, Zhejiang University, China. He obtained his BS (Management Information Systems) from Fudan University, MS (Information Systems) from the National University of Singapore, and Ph.D. (Information Systems) from the University of Hong Kong. His research interests are in the areas of data mining, mobile services, and churn management. His research has appeared or is forthcoming in Decision Support Systems, European Journal of Operational Research, Journal of Organizational Computing and Electronic Commerce, Journal of the American Society for Information Science and Technology, Electronic Commerce Research and Applications, and in the proceedings of several international conferences.

Indranil Bose is an associate professor of Information Systems at the School of Business, The University of Hong Kong. He holds a B. Tech. from the Indian Institute of Technology, MS from the University of Iowa, MS and Ph.D. from Purdue University. His research interests are in telecommunications, data mining, information security, and supply chain management. His publications have appeared in Communications of the ACM, Communications of AIS, Computers and Operations Research, Decision Support Systems, Ergonomics, European Journal of Operational Research, Information & Management, Journal of Organizational Computing and Electronic Commerce, Journal of the American Society for Information Science and Technology, and Operations Research Letters. He is listed in the International Who's Who of Professionals 2005–2006, Marquis Who's Who in the World 2006, Marquis Who's Who in Asia 2007, Marquis Who's Who in Science and Engineering 2007, and Marquis Who's Who of Emerging Leaders 2007. He serves on the editorial board of Information & Management, Communications of AIS, and several other IS journals.

Alvin Chung Man Leung is currently a Ph.D. student of McCombs School of Business, The University of Texas at Austin specializing in Information Systems. He has obtained his MPhil, BBA(IS), and BEng(SE) degrees from The University of Hong Kong. His research interests include social network, information security, and data mining. His publications have appeared in various international journals and conference proceedings such as Decision Support Systems, Communications of the ACM, Communications of the AIS, and International Conference on Information Systems (ICIS). He was also the recipient of Best Student Paper Award in International MultiConference of Engineers and Computer Scientists 2008.

(Julian) Chenhui Guo studies as a Ph.D. student in the Department of MIS, Eller College of Management, The University of Arizona. He obtained his Bachelor of Business Administration degree from Zhejiang University, Hangzhou, China. His current research interests include data/text mining, business intelligence, and behavioral science in IS usage.