https://doi.org/10.48009/2_iis_2017_136-147

COMMUNICATION IN CYBERSECURITY: A PUBLIC COMMUNICATION MODEL FOR BUSINESS DATA BREACH INCIDENT HANDLING

Ping Wang, Robert Morris University, wangp@rmu.edu
Sun-A Park, Robert Morris University, park@rmu.edu

ABSTRACT

Cybersecurity attacks such as business data breach incidents have become a significant reality of the digital economy as seen in frequent media reports. These incidents may cause various losses for both consumers and businesses and may turn into business crises. Effective communication is important for successful cyber incident response and handling for business reputation and survivability. This paper draws upon situational crisis communication theories and cybersecurity incident handling guidelines and proposes a public communication model for commercial businesses to share and discuss data breach incidents to the external parties of customers, media, and the general public. A case study of the Yahoo data breach is conducted using the constructs and elements of the proposed model. The paper also discusses implications for cyber incident handling and cybersecurity workforce preparation.

Keywords: Cybersecurity, Incident, Data Breach, Incident Handling, Public Communication

INTRODUCTION

Cybersecurity has been gaining public attention as cyber attacks such as data breach incidents have been frequently reported in the media. The National Initiative for Cybersecurity Careers and Studies (NICCS) under U.S. Department of Homeland Security defines cybersecurity as “[t]he activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation” (NICCS, 2017, c section, para.29). The fundamental goals of cybersecurity are to protect the confidentiality, integrity, and availability (CIA) of sensitive information and relevant information systems from unauthorized access, modification, and interruption. Data breach is an example of unauthorized access to or disclosure of sensitive information. A cybersecurity incident, such as a data breach, is “[a]n occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences” (NICCS, 2017, i section, para.4).

Effective handling of cybersecurity incidents is critical to the survival of businesses in the digital economy as the actual number and impact of data breach incidents may well surpass those of the selected cybercrime cases reported in the media. According to the latest data retrieved on April 27, 2017 from Privacy Rights Clearinghouse (PRC), a nonprofit consumer education and advocacy organization, there have been 5,418 data breach incidents made public since 2005 with a total of 911,887,535 records breached. These data breach cases include 2,152 incidents with commercial businesses, such as retail and financial and insurance services, with 663,789,690 records breached (PRC, 2017). The 2017 report from Hiscox Insurance, a major cybersecurity insurance company, shows that U.S. firms have the highest probability of experiencing a cyberattack with 72% of larger businesses reporting a cyberattack incident in the past year and about half of all US firms experiencing two or more (The Hiscox Cyber Readiness Report, 2017). The data breach incidents may threaten the survivability of impacted businesses. The cybercrime cost the global economy over $450 billion in 2016 alone (Graham, 2017). For example, the cost of the Target data breach affecting 70 million US consumers could reach $1 billion or more in damages along with potential and unforeseeable costs of lawsuits (Seals, 2015). Direct costs from data breach incidents include costs of legal guidance in crisis management, forensic investigations, breach notifications, credit monitoring for affected consumers, business interruptions and recovery, legal defense and settlement, and regulatory fines (Verizon, 2016). In addition, businesses have to be concerned about the much higher indirect costs of cybercrime, which include business reputational damage and loss of customer confidence (Anderson et al., 2012). Therefore, effective handling of cybersecurity incidents is essential to the bottom line and survivability of businesses.

According to National Institute of Standards and Technology (NIST), incident handling in Cybersecurity is to analyze incident-related data and decide the appropriate response to the incident to minimize the impact (NIST, 2012). The NIST Computer Security Incident Handling Guide also emphasizes communication as an important element for effective incident response and handling, which includes discussing and sharing incident-related information with external or outside parties such as customers, stakeholders, partner organizations, and the general public (NIST, 2012). This paper will focus on public communication on business data breach incidents with the outside parties of customers, media, and general public, who have a primary interest in the status and impact of the incident. The rationale for this focus of the communication audience is that public communication has a direct correlation to the business reputation and performance, which are key indicators of the effectiveness of cyber incident handling. For example, the event-study analysis using market valuations conducted by Cavusoglu, Mishra, and Raghunathan (2004) found a negative association between the public announcement of an Internet security breach and the market value of the announcing firm: “The breached firms in the sample lost, on average, 2.1 percent of their market value within two days of the announcement - an average loss in market capitalization of $1.65 billion per breach” (p.69).

A cyber incident could potentially turn into a cyber crisis for business that requires crisis management to minimize damage to business reputation. Communication strategies are among key priorities in cyber crisis management and management must be ready to communicate across all media to assure stakeholders that the organization is taking appropriate actions of response to the situation (Deloitte, 2016). In proposing the public communication model for business data breach incident handling, this paper draws on key communication strategies, such as diminish and rebuild strategies, derived from the situational crisis communication theory for business “to repair reputation, to reduce negative affect and to prevent negative behavioral intentions” (Cooley & Cooley, 2011, p.205). The proposed model will also incorporate cyber incident handling guidelines such as establishing policies and procedures for sharing sensitive information with the media and public.

The main goal of this paper is to propose a model of public communication for businesses to handle cybersecurity incidents effectively with minimal impact on their reputation and performance. To illustrate the proposed model, this paper uses text analysis methods to examine and evaluate the public communication text documents and relevant media reports related to the recent business data breach incidents involving Yahoo using the constructs of the proposed model. The model contribution and case study findings of this paper will not only help to inform business cyber incident response but also will benefit the important cause of preparation and education of cybersecurity workforce. There is a huge and increasing demand for cybersecurity professionals and effective communication is among the top skills expected for cyber workforce and for college and program accreditations (ABET, 2015; MSCHE, 2014; NICE, 2017). The following sections of this paper will review relevant crisis communication theories and incident handling guidelines, formulate and explain the proposed model, describe the case study methodology, discuss the findings and implications for cyber incident handling and cybersecurity workforce preparation and education.

LITERATURE REVIEW

A data breach incident becomes a corporation’s crisis once it appears in the media and stakeholders start reacting to it. Crises are events that produce potential or actual negative outcomes for organizations, industries, publics, and products or services (Fearn-Banks, 1996). A crisis thereby adversely affects the reputation and risks the legitimacy of an organization (Benoit, 1995; Coombs, 1999). Unfortunately, because of the uncertainty of crisis characteristics, corporations cannot avoid crises and do not even know when crises will occur. Further, some crises are perceived to be bigger or smaller than they actually are because each crisis has both actual and perceived dimensions (Heath & Millar, 2004). Many studies have focused on the perceived dimensions of crises in order to investigate how the degree of the public’s blame or attribution of responsibility to an organization varies with crisis situations and strategies (Coombs, 1998; Coombs & Holladay, 1996, 2001; Coombs & Schmidt, 2000; Lee 2005). This perception of crises plays a significant role in influencing crisis outcomes: reputational threat (Coombs, 2007). Organizational reputation refers to an aggregate evaluation the general public make regarding how well an organization is meeting the public’s expectation (Coombs & Holladay, 1996). Benoit (2014) argued that the critical questions for the organization faced with a crisis are "not whether *in fact* the accused caused the damage but whether the relevant audience *believes (perceives)* the accused should be blamed for the reprehensible act" (p. 21). Thus, organizations during a crisis should actively seek an effective communication with the public to lessen and minimize damage to their reputation.

Many studies in crisis communication have focused on what organizations can say and do (crisis response strategies) after a crisis to protect the organization's reputation (Benoit, 1995; Coombs, 1995). For an appropriate communication strategy, various crisis situations should be considered as each situation affects the selection of the best crisis responses (Coombs, 1998; Coombs, 2006). Attribution theory links crisis situations to crisis strategies and posits that people make judgments about the cause of events, especially those that are negative and unexpected (Weiner, 1986). In an organizational crisis situation, stakeholders will make attributions about the cause of a crisis and assess crisis responsibility. For instance, if an organization is perceived as being able to control a crisis, then it will be perceived to have more responsibility for that crisis (Coombs, 1998; Coombs & Holladay, 1996). Attribution theory provided the framework not only for identifying the variables used to assess reputational threat in a crisis situation, but also for integrating crisis communication strategies and crisis situation into a theory of crisis communication. Coombs (1998) tested a system for analyzing crisis situation matched to an array of crisis response strategies based on crisis responsibility and found that the damage to the organization's reputation increases as the perceived attribution of crisis responsibility grows.

Coombs (1998) examined three components of the crisis situation that determine perceptions of crisis responsibility: (1) crisis attributions, (2) performance history, and (3) severity of damage. Crisis attributions involve two dimensions: external control and internal control. External control is the degree to which external agents could control the crisis event, whereas internal control is the degree to which the organization itself could control the crisis event. Coombs (1998) found that the public attributes a strong crisis responsibility to the organization when it perceives that the organization has a higher internal locus of control, because the organization could have acted to prevent the crisis. Performance history refers to whether or not an organization has had similar crises in the past. Similar past crises intensify the public's perception of the crisis responsibility and exacerbate an organizational negative image. Finally, crisis responsibility can also be examined in terms of the severity of damage (Coombs, 1998). Studies on crisis damage hypothesized that the more severe the damage, the greater crisis responsibility the general public would attribute to the organization (Coombs, 1995, 1998; Coombs & Holladay, 1996, 2001, 2002; Claeys, Cauberghe, & Vyncke, 2010).

Coombs (2007) developed the Situational Crisis Communication Theory (SCCT) as a tool for understanding how to protect reputation during a crisis. SCCT is a prescriptive system for matching crisis response strategies to the crisis situation, which is helpful in examining how crisis situations influence the selection and effectiveness of crisis communication strategies. The central focus of SCCT is how to maximize the reputational protection during or after a crisis. SCCT organized the crisis types which are integrated into crisis response strategies and posits that each crisis type generates specific and predictable levels of crisis responsibility, which is the main construct of both attribution and situational crisis communication theories in determining the most effective communication strategies.

Coombs (2007) introduced three clusters of the primary crisis response strategies that an organization can utilize during and after a crisis: 1) Denial; 2) Diminish; and 3) Rebuild. According to SCCT, the denial strategy is appropriate when no evidence exists for the relationship between an organization and the supposed crisis, or when an organization can prove that no crisis exists. When false and damaging information about an organization is being circulated or an external agent causes damage to an organization, it is suitable to use denial strategies by arguing that there is no crisis or by blaming an external party (scapegoat) (Coombs, 2007). The diminish strategy is to limit organizations' responsibility for the crisis (excuse) due to the lack of control/intention or to minimize the amount of damage (justification) by showing that a crisis is not as serious as the public believe. The rebuild strategy is to offer compensation or apologize by taking full responsibility for the crisis. As a supplement to the primary strategies recommended by SCCT, the bolstering strategy emphasizes past good work and is useful only when the organization has a good relationship with stakeholders and a good performance history in the past.

Because crisis types within each crisis cluster produce similar attribution of crisis responsibility, crisis managers can also use similar crisis response strategies to address crisis types within the same cluster. For example, denial strategies would be effective for a victim crisis type producing weak crisis responsibility (Sisco, 2012), and diminish strategies, such as excuse, and justification, would be helpful to address an accidental crisis type producing moderate crisis responsibility (Ma & Zhan, 2016). Finally, rebuild strategies, such as corrective action and full apology, would be effective for an intentional crisis producing strong crisis responsibility (Claeys, Cauberghe, & Vyncke, 2010; Coombs & Holladay, 2012; Sisco, 2012). Thus, once crises are grouped, crisis manager can prepare plans for each cluster, instead of generating plans for every possible crisis type an organization might face. Overall, the crisis situation, determined by the attributed degree of crisis responsibility, should be linked to crisis response strategies in order to select an appropriate strategy for each situation (Coombs, 2007; Sisco, 2012). A recent meta-analysis of SCCT research further supported a strong relationship between attributed responsibility for a crisis and organizational reputation (Ma & Zhan, 2016), and a relatively weak relationship between matching response strategies and reputation due to potential moderating factors, such as locus of control or timing strategies (Claeys, Cauberghe, & Vyncke, 2010; Claeys & Cauberghe, 2012; Ma & Zhan, 2016), which we will discuss in our proposed model.

PROPOSED MODEL

This study proposes a public communication model to help minimize negative effects from business data breach incidents. Many internal guidelines on incident response exist, but few guidelines suggest how to communicate with different external publics to protect reputational assets. Public communication in this paper refers to the formal public discourse that a corporation uses to discuss and share incident-related information with external publics, such as stakeholders, customers, and media, who have a primary interest in the data breach incident and its impact. The goal of public communication is to protect a corporation's reputation. By adopting the dimension of SCCT's crisis response strategies (Coombs, 2007), public communication in this model is a message strategy to explain the corporation's behaviors to its external publics. The model incorporates the three primary communication strategies: 1) denial, 2) diminish, and 3) rebuild strategies, as well as the secondary bolstering strategy.

The ultimate goal of using crisis communication strategies is to protect and maintain organizational reputation. A reputational crisis is "a consequence of a specific critical incident" (Sohn & Lariscy, 2014, p.24), which is applicable to a data breach incident. Since a data breach is a critical event in cybersecurity, this model uses the term "data breach incident" instead of a crisis and labels "incident handling responsibility" for the dimension of crisis responsibility. As seen in Figure 1, an incident response team needs to utilize public communication strategies to mitigate perceptions of a corporation's incident handling responsibility in order to protect an organization's reputation. The model states a negative relationship between incident handling responsibility and reputation: the stronger perceptions of incident handling responsibility significantly decrease the organizational reputation. The incident handling responsibility is determined by the types of public communication strategies and the timing of response by a corporation.

As more accommodative communication strategies (rebuild strategy) an incident response team uses, people perceive the company as taking greater responsibility for the incident compared to defensive strategies (denial or diminish) (Coombs, 2007). The rebuild strategies produce more positive perception and reputation effect compared to the deny or diminish strategies (Claeys, Cauberghe, &Vyncke, 2010). However, the rebuild strategy is not always the preferred response strategy by corporations as it may sometimes worsen the situation (Coombs, 2007). For example, the NIST Computer Security Incident Handling Guide recommends avoiding disclosures of sensitive information to unauthorized parties that may lead to additional disruption and financial loss (NIST, 2012). The timing of incident response may have significant influence on the public's evaluation of incident handling responsibility (NIST, 2012). Perceived delays in reporting or disclosing a breach may increase public perceptions of corporate incident handling responsibility and truthfulness and significantly decrease public perceptions or corporate reputation.

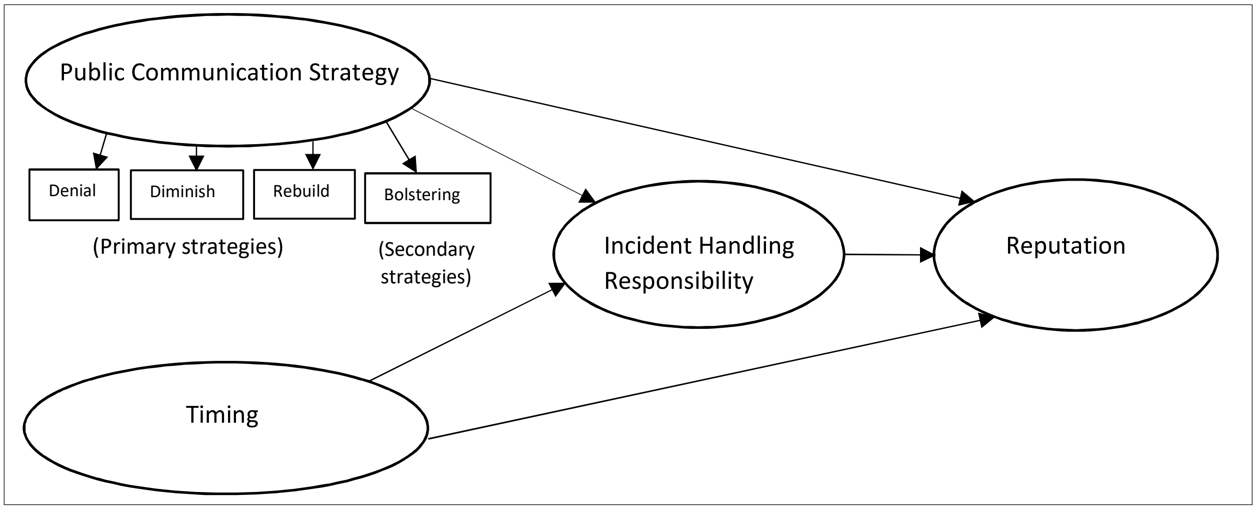


Figure 1. Public Communication Model for Business Data Breach Incident Handling

METHODOLOGY

To illustrate the proposed public communication model for business data breach incident handling, this paper uses content analysis of online business communication text as the primary method for studying the public communication strategies in handling the Yahoo data breach. Company websites have become an important promotional tool for corporate public relations using various forms, such as news and press releases, speeches, corporate identity materials, public-service activities, and investor information and lobbying or cause-related information (Perry & Bodkin, 2000). Accordingly, opinion mining and sentiment analysis including computational treatment of opinion, sentiment, and subjectivity in online text have become an increasingly used research method with extensive applications across various domains from business to government (Pang & Lee, 2008). Much of the online text analysis focuses on sentiment analysis of social media sources with automated evaluations of opinions using publicly available software tools. However, recent research has presented challenges to the reliability and validity of the datasets and judgment assumptions built into such sentiment analysis software systems (Maynard & Bontcheva, 2016). Therefore, the text analysis for this study will focus on formal press release statements posted on the company website with limited use of text analysis software tools for objective linguistic data only without automated sentiment analysis.

This study uses TextSTAT, a simple text analysis tool. The current stable release for Windows is version 2.9c, which is free and downloadable at http://neon.niederlandistik.fu-berlin.de/en/textstat. TextSTAT reads ASCII/ANSI texts including HTML (web pages), Word and OpenOffice files and outputs sortable word frequency lists, and concordances of keywords with searchable contexts and citations. TextSTAT "stands out by its simplicity, clarity, ability to read several file formats, search and link ability, as well as the ability to produce and export word frequency lists" (Benini, 2009, p.14). The simplicity of this tool is highly preferred for reliable and objective linguistic text data analysis by providing quantitative word frequencies and the contexts of these words (Klimova, 2014; Wilson, 2004). This feature fits this study, which needs the quantitative word frequencies and their citation contexts allowing for interpretive analysis in the contexts of the words and the proposed communication model. Word frequencies are significant text data for analysis as they reflect the extent of repetition of key words associated with the communication objectives and strategies. Research by Davidson (2008) on rhetoric, repetition, and business communication techniques indicates that repetition of key words and phrases creates the effects of emphasizing corporate intangible assets, such as good will and innovation leading to positive associations, and projecting corporate identity and presence in a mass market. In addition, repetition not only carries logical emphasis to remind readers of the importance of the key words but also creates a stylistic effect of emotive crescendo similar to that in music and poetry (Kemertelidze & Manjavidze, 2013). The recent data breach of Yahoo is used as the case study for this paper. Yahoo! Inc. (Yahoo) is a global Internet Software/Services company engaged in digital information discovery. The company currently has over 9,000 employees and focuses on informing, connecting and entertaining its users with its search (Yahoo Search), communications, including Yahoo Mail and Yahoo Messenger and digital content products, including Tumblr, Yahoo

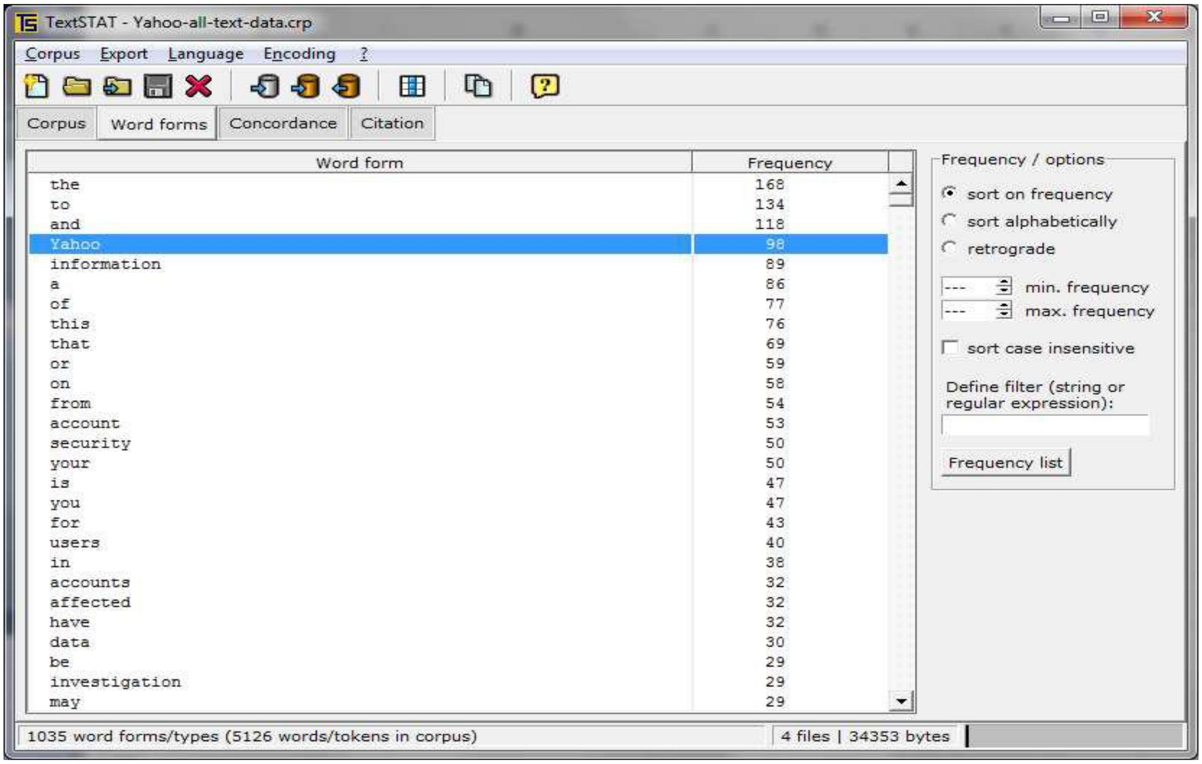
News, Yahoo Sports, Yahoo Finance and Yahoo Lifestyle (CNN Money, 2017; Yahoo Investor Relations, 2016). Verizon has recently acquired Yahoo's core Internet business with the goal of using Yahoo's billion users to build an online advertising powerhouse to compete with Google and Facebook (Fiegerman, 2017).

Yahoo is selected for the case study because it is a large business organization with commercial priorities and large number of users and stakeholders that could be impacted by a data breach incident. Thus, public communication to its users and media as part of the data breach incident response and handling is critical to the company's reputation and market competitiveness. In fact, Yahoo experienced two massive incidents of data breach in recent years disclosed to the public in the last year alone: The 2014 breach incident made public on September 22, 2016 breached records of up to 500 million users; the breach of August 2013 made public on December 14, 2016 compromised over 1 billion user accounts, which is the largest data breach in history (PRC, 2017).

Four publication communication documents from Yahoo regarding the two recent data breach incidents are used for the data analysis. The four documents include formal announcements, notices, and statements representing the official position and opinion of Yahoo. The four documents are publicly available at and retrieved from the official website of Yahoo, which addresses Yahoo users and investors. These documents are: 1) "An Important Message About Yahoo User Security" issued on September 22, 2016 by Bob Lord, CISO (Chief Information Security Officer) of Yahoo (Lord, 2016); 2) "An Important Message to Yahoo Users on Security" (Yahoo Investor Relations, 2016); 3) "Yahoo Security Notice September 22, 2016" (Yahoo, 2016); and 4) "Yahoo Security Notice December 14, 2016" (Yahoo, 2016). The data analysis for this study focuses on the frequencies and interpretations of keywords in light of the proposed communication model. The following section will present and discuss the findings.

FINDINGS AND DISCUSSIONS

The TextSTAT software is used in extracting the word frequencies from the four public communication documents from Yahoo. Figure 2 below shows the screen capture of the aggregate word frequencies sorted from highest frequency to the lowest frequency. The top 10 non-accessory words and their total occurrences in the four documents are: *Yahoo (98), information (89), account (53), security (50), your (50), you (47), users (40), accounts (32), affected (32), data (30)*. The repetitions or high frequencies of these key words may help create the public communication effects of emphasizing intangible assets and projecting a positive image of the company (Davidson, 2008; Kemertelidze & Manjavidze, 2013). For example, the high frequency of *Yahoo* creates the blockbuster marketing effect and presence for the company. The high frequency of *information* signals Yahoo's willingness and transparency for information sharing. The high frequencies of *account, security, accounts, affected*, and *data* project the impression that Yahoo understands and is concerned with the security of affected accounts. The high frequencies of the words *your, you, users* indicate Yahoo's goodwill and respect for their users and customers. These quantitative word frequencies suggest Yahoo's conscious or subconscious attempts to mitigate the damage of the data breach incidents and rebuild the company reputation by means of positive public communication.


TextSTAT - Yahoo-all-text-data.crp
Corpus Export Language Encoding ?
Corpus
Word forms
Concordance
Citation
Frequency list

Word form	Frequency
the	168
to	134
and	118
Yahoo	98
information	89
a	86
of	77
this	76
that	69
or	59
on	58
from	54
account	53
security	50
your	50
is	47
you	47
for	43
users	40
in	38
accounts	32
affected	32
have	32
data	30
be	29
investigation	29
may	29

Frequency / options

● sort on frequency
○ sort alphabetically
○ retrograde

--- min. frequency
--- max. frequency

□ sort case insensitive

Define filter (string or regular expression):

1035 word forms/types (5126 words/tokens in corpus) | 4 files | 34353 bytes

Figure 2. TextSTAT Word Frequencies

Contextual analysis of the Yahoo documents released in handling the data breach incidents does reveal examples of the components and strategies outlined in the proposed public communication model. As an example of the denial or scapegoat strategy, Yahoo blamed “a state-sponsored actor” for stealing a copy of certain user account information from the company’s network according to all three documents released to Yahoo users and investors on September 22, 2016 regarding the 2014 breach that affected 500 million accounts. Similarly, Yahoo blamed “an unauthorized third party” for stealing data associated with over a billion user accounts in the August 2013 Yahoo breach.

Yahoo’s post-breach public communication also shows examples the diminish strategy. In all three release documents regarding the 2014 breach, Yahoo emphasized that the “state-sponsored actor” is no longer in the company network, suggesting the breach was historical and no longer existing. In the investor relations message, Yahoo also tried to diminish the breach by saying that state-sponsored cyber attacks are increasingly common in the technology industry. In addition, in all four release documents addressing the 2014 and the 2013 attacks, Yahoo further diminished the significance of the two massive data breach incidents by consistently emphasizing that the stolen account information did not include unprotected passwords, payment card data, or bank account data. However, in addressing the August 2013 breach, Yahoo attributed some of the attack activities to the same state-sponsored actor responsible for the 2014 breach. This diminish strategy may not have worked well for Yahoo as it reflects Yahoo’s repeated failing performance in securing their networks. The negative performance record may have also limited the use of the supplemental bolstering strategy of emphasizing one’s good track record. There is no evidence of bolstering effort found in the four public release documents from Yahoo for this study.

In terms of the rebuild strategy, Yahoo’s communication documents show efforts of good will, close cooperation with the law enforcement on investigations, as well as taking actions such as giving alerts and recommendations to help secure user accounts. In addition, Yahoo stated their commitment to continuous improvements of their protection and prevention technology to safeguard user accounts. Although Yahoo is not offering any apology or compensation in these public communication documents, it does encourage users to seek Yahoo’s online customer support for assistance with their accounts and emphasizes that Yahoo does not charge any fee for such support. The minimal rebuild effort by Yahoo may have helped to lower the public perception of Yahoo’s responsibility for the breach.

The timing of incident response is an important factor and maybe more important than the communication strategies in shaping public perception on the company's incident handling responsibility and subsequently the company's reputation in this case. The timing of response refers to not only prompt response to the public but also punctual reporting and disclosure to appropriate industry regulation authorities for compliance. Yahoo published their acknowledgement notices on the 2014 breach about two years later in September 2016 and the 2013 breach about three years later in December 2016. The respective 2-year and 3-year absolute lapses in announcing the two massive data breach incidents may not have helped Yahoo's corporate reputation regardless of the actual timing of Yahoo's knowledge of the incidents. In fact, it was later revealed that Yahoo's CEO Marissa Mayer was aware of the 2014 breach in July 2016 or about two months before Yahoo's public disclosure of the breach incident by filing Form 8-K on September 22, 2016 whereas regulations mandate that such filing be submitted within four business days of the incident to keep the public and investors informed; US Senator Warner questioned Yahoo's truthfulness in representations to the public and called for an investigation into Yahoo's incident handling (Blake, 2016).

The effectiveness of the public communication model for corporate data breach incident handling is measured by the company's subsequent performance. It was observed that within 3 days after Yahoo announced the 2014 data breach on September 22, 2016, Yahoo's stock value lost about 3.75 percent (Blake, 2016). This may have been caused by the late announcement of the breach and the question over Yahoo's timing of disclosure. The U.S. Securities and Exchange Commission (SEC) has since launched an investigation into the timing of Yahoo's disclosure of the data breach (Masters, 2017). In addition, the data breach incidents and Yahoo's handling of the incidents have led to Verizon to lower its price for acquiring Yahoo by $350 million (Moritz, 2017). In spite of Yahoo's public communication efforts and strategies of denial, diminish, and rebuild in handling the data breach incidents, the considerably long lapses of time before public announcements and delayed reporting of the incidents may have had a significant negative impact on Yahoo's reputation and market value.

CONCLUSIONS

This paper identifies the importance of communication skills in Cybersecurity and proposes a public communication model for business data breach incident handling. The model consists of important situational crisis communication strategies, such as denial, diminish, rebuild, and bolstering, and the timing of incident response, which jointly impact the public perceptions on incident handling responsibility and the company reputation. The case study using the breach incident communication documents from Yahoo illustrates the elements and effects of the proposed model. Despite Yahoo's public communication efforts and strategies, the delayed timing of disclosing the breach incidents appeared to have a negative impact on the company's reputation and market value.

This study has important value and implications for cybersecurity incident handling and cyber workforce preparation. For cybersecurity incident handling, it is most important to report and disclose identified data breach incidents promptly per compliance regulations to avoid any legal penalties and negative public perceptions of the organization. The public communication strategies in the proposed model should be carefully considered against the organization's priorities and performance record in order to be effectively used to help mitigate the damage of cyberattacks and improve the reputation and intangible assets of the organization. Given the increasing demand for qualified workforce for cybersecurity work, educational and training institutions should incorporate and emphasize public communication competency and skills in their cybersecurity curriculum and courses. Cybersecurity program assessment and certifications should reflect the public communication competency for cyber incident response and handling as well.

This paper is only a preliminary research effort in a new and cross-disciplinary area. The data collection and analysis for this study is limited to formal company release documents related to the Yahoo breach case. Future studies may involve more business breach case examples and text documents for larger data collection and representation. It is also a promising area for a follow-up study to identify and compare any different effects on corporate reputation between the official business statements and less formal and more emotional social media postings. The Protection Motivation Theory (PMT) is an important theory that can be used to measure one's coping behavior or response under threat (Woon, Tan, & Low, 2005; Rahman & Choo, 2015). Empirical studies could be conducted via a survey of corporate organizations to measure correlations between the PMT factor of Response Cost (perceived costs of money, time, and effort for adopting a recommended response) and corporate willingness to use public communication strategies for reputation protection. The research scope may be extended to public communication strategies in cybersecurity incident handling for government and non-profit organizations, which have less commercial motivation for reputation protection.

REFERENCES

ABET. (2015). *Criteria for Accrediting Computing Programs (2016-2017 accreditation cycle).* Retrieved from http://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2016-2017/

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M., & Savage, S. (2012). *Measuring the cost of cybercrime.* In Proceedings of Workshop on Economics of Information Security (WEIS 2012), Berlin, Germany, June 2012, 1-31.

Benini, A. (2009). *Text analysis under time pressure: Tools for humanitarian and development workers.* Retrieved from http://www.aldo-benini.org/Level2/HumanitData/Benini_TextAnalysis_100301.pdf

Benoit, W. L. (1995). *Accounts, excuses and apologies: Image restoration strategies.* Albany, NY: University of New York Press.

Benoit, W. L. (2014). *Accounts, excuses, and apologies: Image repair theory and research* (2nd ed.). Albany, NY: University of New York Press.

Blake, P. (2016, September 26). *Senator questions Yahoo's handling of data breach disclosure, calls for SEC investigation.* Retrieved from http://abcnews.go.com/Business/senator-questions-yahoos-handling-data-breach-disclosure-calls/story?id=42364672

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce, 9*(1), 69-104.

Claeys, A.-S., Cauberghe, V., & Vyncke, P. (2010). Restoring reputations in times of crisis: An experimental study of the situational crisis communication theory and the moderating effects of locus of control. *Public Relations Review, 36*(3), 256-262.

CNN Money. (2017). Yahoo! Inc (NASDAQ: YHOO). Retrieved from http://money.cnn.com/quote/profile/profile.html?symb=YHOO

Claeys, A.-S., Cauberghe, V., & Vyncke, P. (2010). Restoring reputations in times of crisis: An experimental study of the situational crisis communication theory and the moderating effects of locus of control. *Public Relations Review, 36*(3), 256-262.

Claeys, A. S., & Cauberghe, V. (2012). Crisis response and crisis timing strategies, two sides of the same coin. *Public Relations Review*, *38,* 83–88.

Cooley, S.C., & Cooley, A. B. (2011, June). An examination of the situational crisis communication theory through the general motors bankruptcy. *Journal of Media and Communication Studies, 3*(6), 203-211.

Coombs, W. T. (1995). Choosing the right word: The development of guidelines for the selection of the “appropriate” crisis response strategies. *Management Communication Quarterly, 8,* 447-476.

Coombs, W. T. (1998). An analytic framework for crisis situations: Better responses from a better understanding of the situation. *Journal of Public Relations Research, 10*(3), 177-191.

Coombs, W. T. (1999). *Ongoing crisis communication: Planning, managing, and responding*. Thousand Oaks, CA: Sage.

Coombs, W. T. (2006). The protective powers of crisis response strategies: Managing reputational assets during a crisis. *Journal of Promotion Management, 12*(3/4), 241-260.

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review, 10*(3), 163-176.

Coombs, W. T., & Holladay, S. J. (1996). Communication and attributions in a crisis: An experimental study in crisis communication. *Journal of Public Relations Research, 8, 279–295.*

Coombs, W. T., & Holladay, S. J. (2001). An extended examination of the crisis situations: A fusion of the relational management and symbolic approaches. *Journal of Public Relations Research, 13*, 321–340.

Coombs, W. T., & Holladay, S. J. (2002). Helping crisis managers protect reputational assets: Initial tests of the situational crisis communication theory. *Management Communication Quarterly, 16,*165–186.

Coombs, W. T., & Holladay, S. J. (2012). Amazon.com's Orwellian nightmare: Exploring apology in an online environment. *Journal of Communication Management, 16*(3), 280-295.

Coombs, W. T, & Schmidt, L. (2000). An empirical analysis of image restoration: Texaco's racism crisis. *Journal of Public Relations Research, 12,* 163–178.

Deloitte. (2016). *Cyber crisis management: Readiness, response, and recovery.* Retrieved from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf

Fearn-Banks, K. (1996). *Crisis communications: A casebook approach.* Mahwah, NJ: Lawrence Erlbaum Associates, Inc.

Fiegerman, S. (2017, April 3). *Yahoo and AOL will form new company called ... Oath*. Retrieved from http://money.cnn.com/2017/04/03/technology/verizon-yahoo-aol-oath/

Graham, L. (2017, February 7). *Cybercrime costs the global economy $450 billion: CEO.* Retrieved from http://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html

Heath, R. L. & Millar, D. P. (2004). A rhetorical approach to crisis communication: management, communication processes, and strategic responses. In Dan P. Millar & Robert L. Heath (Eds.), *Responding to crisis: A rhetorical approach to crisis communication* (pp. 33-35). Mahwah, NJ: Lawrence Erlbaum.

Kemertelidze, N., & Manjavidze, T. (2013). Stylistic repetition, its peculiarities and types in modern English. *European Scientific Journal, July 2013 Special Edition,* 1-8.

Klimova, B. F. (2014). Using corpus linguistics in the development of writing. *Procedia - Social and Behavioral Sciences, 141*(2014), 124-128.

Lee, B. K. (2005). Hong Kong consumers' evaluation in an airline crash: A path model analysis. *Journal of public relations research. 17*(4), 363-391.

Lord, B. (2016, September 22). An important message about Yahoo user security. Retrieved from https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security

Ma, L., & Zhan, M. (2016). Effects of attributed responsibility and response strategies on organizational reputation: A meta-analysis of situational crisis communication theory research. *Journal of Public Relations Research, 28*(2), 102-119.

Masters, G. (2017, January 23). SEC probing Yahoo over timing of breach disclosure. *SC Magazine.* Retrieved from https://www.scmagazine.com/sec-probing-yahoo-over-timing-of-breach-disclosure/article/633102/

Maynard, D., & Bontcheva, K. (2016). Challenges of evaluating sentiment analysis tools on social media. *Proceedings of Language Resources Evaluation Conference (LREC 2016),* 1142-1148.

Moritz, S. (2017, February 21). Verizon reaches deal for lowered Yahoo price after hacks. *Bloomberg Technology.* Retrieved from https://www.bloomberg.com/news/articles/2017-02-21/verizon-said-to-reach-deal-for-lowered-yahoo-price-after-hacks

MSCHE (Middle States Commission on Higher Education). (2014). *Standards for accreditation and requirements of affiliation* (13th ed.). Retrieved from http://www.msche.org/documents/RevisedStandardsFINAL.pdf

NICCS (National Initiative for Cybersecurity Careers and Studies). (2017). Retrieved from https://niccs.us-cert.gov/glossary

NICE (National Initiative for Cybersecurity Education). (2017). *Cybersecurity workforce demand*. Retrieved from http://csrc.nist.gov/nice/NICE_Workforce_Demand.pdf

NIST (National Institute of Standards and Technology). (2012). *Computer security incident handling guide* (Special Publication 800-61 Revision 2). Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Pang, B., & Lee, L. (2008). Opinion mining and sentiment analysis. *Foundations and Trends in Information Retrieval, 2*(1-2), 1-135.

Perry, M., & Bodkin, C. (2000). Content analysis of Fortune 100 company web sites. *Corporate Communications: An International Journal, 5*(2), 87-96.

PRC (Privacy Rights Clearinghouse). (2017). *Data breaches.* Retrieved from https://www.privacyrights.org/data-breaches

Rahman, N. H. A., & Choo, K.R. (2015). *Factors influencing the adoption of cloud incident handling strategy: A preliminary study in Malaysia.* Proceedings of 21st Americas Conference on Information Systems (AMCIS 2015), 1-15.

Seals, T. (2015, February 28). *Target breach costs could total $1Bn*. *Infosecurity.* https://www.infosecurity-magazine.com/news/target-breach-costs-could-total-1bn/

Sisco, H. F. (2012). Nonprofit in Crisis: An Examination of the Applicability of Situational Crisis Communication Theory. *Journal of Public Relations Research, 24*(1), 1-17.

Sohn, Y. J., & Lariscy, R. W. (2014). Understanding reputational crisis: Definition, properties, and consequences. *Journal of Public Relations Research, 26*(1), 23-43.

The Hiscox Cyber Readiness Report. (2017). Retrieved from http://www.hiscox.com/cyber-readiness-report/

Verizon. (2016). *2016 Data Breach Investigations Report*. Retrieved from http://www.verizonenterprise.com/

Wilson, T. D. (2004). Talking about the problem: A content analysis of pre-search interviews. *Information Research, 10*(1), paper 206. Retrieved from http://InformationR.net/ir/10-1/paper206.html.

Woon, I.M.Y., Tan, G.W., & Low, R.T. (2005). A protection motivation theory approach to home wireless security. *Proceedings of Twenty-Sixth International Conference on Information Systems,* 367-380.

Yahoo. (2016, September 22). *Yahoo security notice* September 22, 2016. Retrieved from https://help.yahoo.com/kb/sln28092.html

Yahoo. (2016, December 14). *Yahoo security notice* December 14, 2016. Retrieved from https://help.yahoo.com/kb/SLN27925.html

Yahoo Investor Relations. (2016, September 22). *An important message to Yahoo users on security*. Retrieved from https://investor.yahoo.net/releasedetail.cfm?releaseid=990570