https://doi.org/10.48009/3_iis_2018_150-159
Issues in Information Systems
Volume 19, Issue 3, pp. 150-159, 2018

CYBERSECURITY INCIDENT HANDLING: A CASE STUDY OF THE EQUIFAX DATA BREACH

Ping Wang, Robert Morris University, wangp@rmu.edu
Christopher Johnson, Robert Morris University, chris@chrisjohnsonit.com

ABSTRACT

Public communication strategies are an important component of corporate cybersecurity incident handling and crisis management. This paper studies the recent Equifax data breach using an improved version of business communication model for cybersecurity incident handling, which highlights and examines the scapegoating strategy often used in corporate crisis management. This study uses Equifax public release documents for text data analysis and evaluates the effectiveness of Equifax incident handling strategies for the massive data breach. The paper also discusses implications for cybersecurity education and workforce preparation.

Keywords: Cybersecurity, Incident Handling, Public Communication, Scapegoating, Equifax

INTRODUCTION

Corporate cybersecurity incidents such as data breaches are frequently seen in media reports and may cause business crises that demand effective incident handling and crisis management in public communication (Wang & Park, 2017). A cybersecurity incident is defined as "[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). Data breach is a common example incident of unauthorized access to or disclosure of sensitive information violating the confidentiality of protected data assets. Known cyber attacks and data breaches have been on the rise. According to the latest data retrieved on May 11, 2018 from Privacy Rights Clearinghouse (PRC), a nonprofit consumer education and advocacy organization, there have been 8,137 data breach incidents made public since 2005 with a total of 10,326,390,393 records breached. Among all the data breach cases so far, there are 2,397 incidents with commercial businesses, including online retail, financial and insurance services and other businesses, with a total of 9,839,228,876 records breached (PRC, 2018). The commercial data breach cases are far more substantial than in other sectors as the number of records breached make up the lion's share (over 95% of all records breached) whereas the commercial data breach cases only account for 29% of all data breach cases. The average direct financial cost of a data breach is over $3.6 million according to the 2017 study report by IBM Security and Ponemon Institute (Ponemon Institute, 2017). There may also be substantial hidden and indirect costs such as damage to corporate reputation and loss of customer confidence as a result of the data breach (Anderson et al., 2012). The recent Equifax data breach not only costs hundreds of millions of dollars for the company but also may create problems that could impact hundreds of millions of consumers in the US for decades (U.S. News, 2017). Therefore, it is critical to the bottom line and survivability of businesses to handle such cybersecurity incidents and crises effectively (Wang & Park, 2017).

Cybersecurity incident handling is defined by the US National Institute of Standards and Technology (NIST) as analyzing incident-related data and deciding the appropriate response to the incident to minimize the impact, including strategies of communication of incident-related information with external or outside parties such as customers, stakeholders, partner organizations, and with the general public (NIST, 2012). Public communication on the cybersecurity incident is important for the handling of the incident and for managing any subsequent corporate crisis as it has a direct correlation to the business reputation and performance, such as on the impact of market valuations in the study by Cavusoglu, Mishra, & Raghunathan (2004) and in the study of Yahoo data breaches published by Wang and Park (2017). Effective communication strategies will help rebuild the corporate image, restore customer confidence in the company, and minimize direct and indirect losses.

The study by Wang and Park (2017) proposed a comprehensive public communication model for handling business data breach incidents and illustrated the model with the case study of Yahoo data breaches. The model includes important business communication strategies of denial, diminish, rebuild, bolstering, and timing. This paper is to review the strategies of the model with a more in-depth pursuit of and focus on the scapegoating strategy as a special type of denial. Although there has been little research on the scapegoating strategy in handling cybersecurity incidents, it is of significant value because in reality the board often demands a scapegoat in the wake of a data security breach (Seijts, 2015). This paper will also focus on the study of the recent Equifax data breach for data analysis and discussion.

The purpose of this paper is to further the study of Wang and Park (2017) and propose an improved model of public communication for businesses to handle cybersecurity incidents effectively with special focus on the scapegoating strategy. To illustrate the proposed model and strategies, this paper uses text mining and analysis methods to examine and evaluate the public communication documents and relevant media reports related to the recent Equifax data breach incident as the case study. The following sections of this paper will review relevant background theories, formulate and explain the proposed model, describe the Equifax and the case study methodology, discuss the findings and implications for cyber incident handling and cybersecurity workforce preparation and education.

BACKGROUND & MODEL

The aftermath of a massive corporate data breach could easily turn into a crisis. Lessons and theories on corporate crisis management are useful for handling such incidents to minimize the financial losses and reputational damage. The Situational Crisis Communication Theory (SCCT) by Coombs (2007) has been frequently referenced in understanding how to protect reputation during a crisis. SCCT is a prescriptive system for matching crisis response strategies to the crisis situation. There are three primary response strategies in SCCT that an organization can employ during and after a crisis: denial, diminish, and rebuild. The denial strategy is to argue against the existence of a crisis or blame a scapegoat if there is no presence of evidence for a crisis (Coombs, 2007). The diminish strategy is to excuses to downplay the extent of the crisis and the organization's responsibility for the crisis, and the rebuild strategy is to offer compensation or apologies for the crisis. The bolstering strategy may be used as a supplemental strategy to emphasize positive past performance record, and selection of response strategies should take into account of the attributed incident handling responsibility for a crisis (Wang & Park, 2017).

The scapegoating strategy is a special example of denial response to a crisis. Scapegoating, which is to transfer the blame to a third party to deflect public perceptions or criticisms of one's own responsibility for a disaster, has been a pattern of social behavior since ancient times, and "in a large number of instances it is clearly being employed as an objective strategy designed specifically not just to ensure survival in the face of hostile censure, but actually to maintain the status quo" (Douglas, 1995, p. 107). Scapegoating is found to be a frequent tool used by global corporations to divert media attention and public perception of incident handling responsibility for crises. If there are multiple but separate peer organizations involved in a crisis, the scapegoat strategy may be sharing the blame or shifting part of the blame to others to lessen the burden for a single actor (Bamber & Parry, 2016). However, if there are multiple parties within the same organization for a crisis, a different form of scapegoating strategy is to assign a single scapegoat to reduce the damage if there are multiple causes for the crisis (Cinarh, 2016). This is not just a quantitative reduction of responsible parties but qualitatively a possible strategy to shift blame within the same organization to a single party who is less important to the organization and can be sacrificed in order to protect responsible parties that are more valuable or profitable to the organization.

There should be cautions, however, in using the scapegoat strategy. The study by Coombs, Holladay, and Claeys (2016) finds an increase in reputational damage and stakeholder anger if an organization denies responsibility for the crisis but is later found responsible. The study also finds that denials and no response conditions are significantly less effective than positive actions taken by the responsible organization in mitigating stakeholder anger and reputational damage if the organization is later found to be guilty (Coomb, Holladay, & Claeys, 2016). The findings suggest that timing or delay in acknowledging organizational responsibility for the crisis will have a negative effect on the corporate reputation and stakeholder perception. It is quite common to expect and find a scapegoat in cases of data security breach, but forcing a scapegoat to resign may backfire and hurt the corporate image instead for two reasons: (1) it would shift blame away from the real actor if the real perpetrator is later found and identified to be different and

external; (2) forcing a senior executive to leave may undermine the corporate image of having recovered from the incident and hurt consumer and public confidence in the company (Seijts, 2015).
The public communication model for data incident breach handling by Wang and Park (2017) incorporates the communication strategies of denial, diminish, rebuild, and bolstering from the SCCT theory and considers rebuild and bolstering strategies more positive than denial and diminish in terms of their impact on perceptions of incident handling responsibility and corporate reputation. The model includes a negative relationship between public perceptions of corporate incident handling responsibility and the corporate reputation. The model also argues that the incident handling responsibility is determined by the types of public communication strategies and the timing of response by a corporation as perceived delays in reporting or disclosing a breach may increase public perceptions of corporate incident handling responsibility and lower the reputation of the company (Wang & Park, 2017).

However, the strategy of scapegoating is not adequately addressed in the data breach incident handling model by Wang and Park (2017). The model only mentions scapegoating as a form of denial in general but does not specify the conditions and outcomes of different types of scapegoating. This study is to address the limitation of the model and propose an adapted and improved version of the model. Figure 1 below presents an improved version of the public communication model for business data breach incident handling based on the original model by Wang and Park (2017). The adapted model retains original strategies of denial, diminish, rebuild, bolstering, and the timing factor and their relationships to incident handling responsibility and corporate reputation but adds the important scapegoating strategy and its impact on perceptions of incident handling responsibility in two different ways: sharing blame with multiple peers and reducing blame to a single party. The scapegoating strategy of sharing blame with multiple peers is used in the environment of multiple peer organizations experiencing the same type of incident in order to divide and lessen public and media attention to the responsibility of just one company (Bamber & Parry, 2016). The scapegoating strategy of reducing blame to a single party, however, is often used when there are multiple people or causes within the same organization that are responsible for the incident or crisis (Cinarh, 2016). The purpose of reducing the blame to a single cause or individual is to sacrifice one and protect others who may be more valuable and less dispensable to the organization. Both scapegoating strategies are subtle forms of denial and may be subject to the constraints of the denial effect and the timing factor as discussed above.

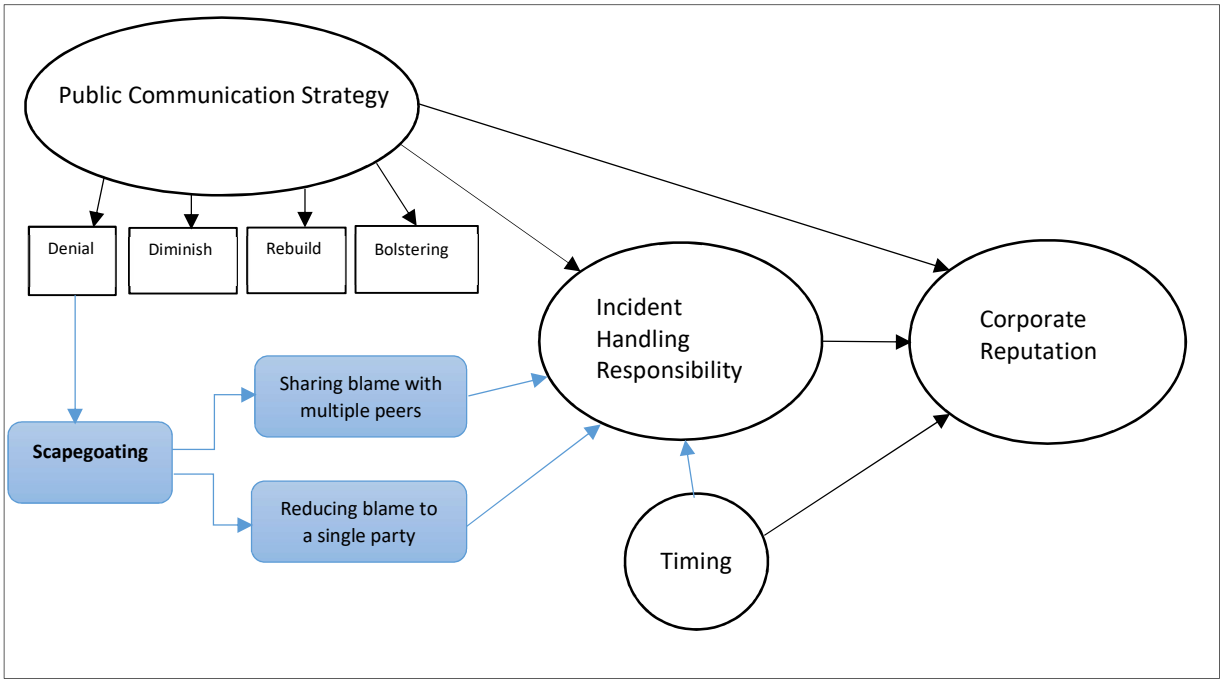

Figure 1. Adapted Public Communication Model for Business Data Breach Incident Handling

METHODOLOGY: EQUAFAX CASE STUDY

To illustrate the improved data breach incident handling model proposed above, this paper uses the case study of the recent data breach of Equifax. The Equifax case is selected because it not only happened recently but also is a massive breach of sensitive personal and financial information including social security numbers, birth dates and addresses, and in some cases driver license numbers, credit card information and financial dispute documents of over 140 million U.S. consumers (or over 44% of U.S. population) (U.S. News, 2017). Ironically, Equifax is one of the major credit reporting agencies that are supposed to safeguard the sensitive credit records and personal information of consumers who place their trust in. Here is Equifax's current company profile posted at its website:

> Equifax is a global information solutions company that uses unique data, innovative analytics, technology and industry expertise to power organizations and individuals around the world by transforming knowledge into insights that help make more informed business and personal decisions.
>
> Headquartered in Atlanta, Ga., Equifax operates or has investments in 24 countries in North America, Central and South America, Europe and the Asia Pacific region. It is a member of Standard & Poor's (S&P) 500® Index, and its common stock is traded on the New York Stock Exchange (NYSE) under the symbol EFX. Equifax employs 10,400 employees worldwide. (Equifax, 2018, para.1-2)

Figure 2 below shows a timeline of the major events in Equifax's data breach based on Equifax's public releases and media reports. United States Computer Emergency Readiness Team (US-CERT) issued a release on March 8, 2017, announcing a patch that would address a vulnerability in Apache's Struts 2 software. Equifax received that release, and issued a notification internally requesting that the software be patched on March 9, 2017. The Equifax breach began with the exploitation of this vulnerability on March 10, 2017. The actors behind the attack spent the next two months elevating their access and exploring the Equifax network, until they finally began accessing files with Personally Identifiable Information (PII) on May 13, 2017. The actors remained inside the Equifax network until their presence was finally detected on July 29, 2017, and security flaws allowing their access were remediated on July 30, 2017. This included updating the Struts 2 software, eliminating the vulnerability announced in March. Equifax then engaged the FBI and other third-parties for assistance on August 2, 2017. Richard Smith, Equifax CEO, was notified on August 15, 2017 that PII was taken during the breach. Equifax made their initial announcement regarding the breach to the public on September 7, 2017. The retirement of Equifax Chief Information Security (CISO) and Chief Information (CIO) officers was announced on September 15, 2017. Richard Smith followed the suit on September 26, 2017. Earlier this year, news outlets reported that other types of PII including email addresses and phone numbers were also included in the breach and that an additional 2.4 million Americans were impacted by the breach (Davidson, 2018; LA Times, 2018). Equifax press release announced Mark Begor as its new permanent CEO on March 28, 2018.

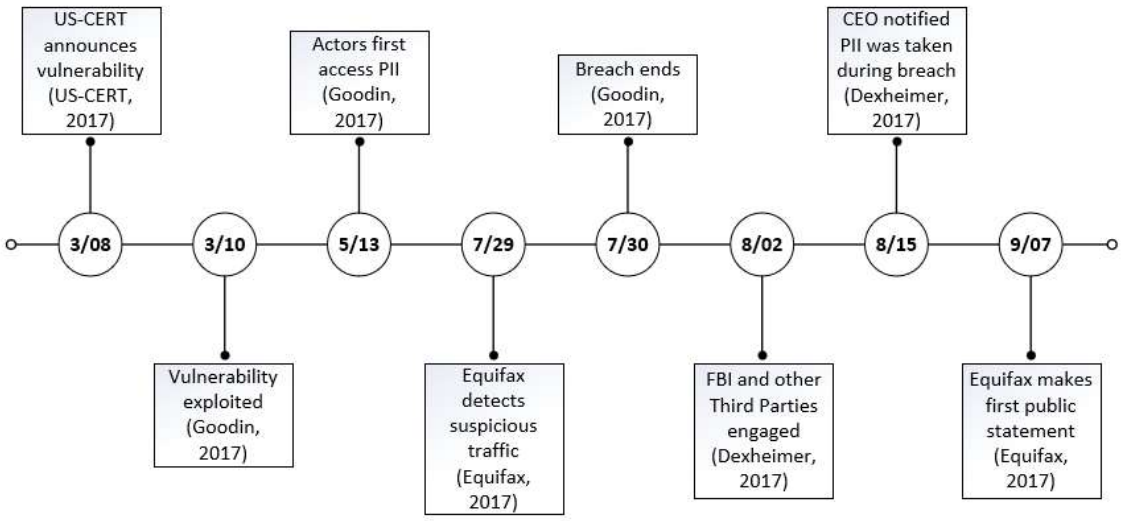

Figure 2. A timeline illustrating the Equifax Data Breach

To illustrate the proposed public communication model for business data breach incident handling, this paper uses the content analysis of online business communication texts as the primary method as previously used by Wang and Park (2017) in studying the public communication strategies in handling the Yahoo data breach. This study also uses the TextSTAT text mining and analysis tool for word frequency analysis with outputs of sortable word frequency lists, and concordances of keywords with searchable contexts and citations. TextStat is selected for this study because 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 (Benini, 2009; Klimova, 2014; Wang & Park, 2017; Wilson, 2004). Word frequencies reflect the extent of repetition of key words associated with the communication objectives and strategies, and repetition of key words and phrases creates the crescendo type of effects of progressive emphasis, positive associations, and favorable image projections (Davidson, 2008; Kemertelidze & Manjavidze, 2013; Wang & Park, 2017).

The text mining and analysis for the Equifax case study uses three public press release documents issued by Equifax that are most relevant to the data breach incident. The four documents are currently still available to the public at Equifax website. These press release documents are: (1) "Equifax Announces Cybersecurity Incident Involving Consumer Information" issued on September 7, 2017 (Equifax, September 7, 2017); (2) "Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes" issued on September 15, 2017 (Equifax, September 15, 2017); and (3) "Equifax Announces Cybersecurity Firm Has Concluded Forensic Investigation of Cybersecurity Incident" issued on October 2, 2017 (Equifax, October 2, 2017). The text data analysis focuses on the identified word frequencies and interpretations of keywords related to the proposed communication model. The following section presents and discusses the findings.

FINDINGS AND DISCUSSIONS

This study uses the TextSTAT software in extracting the keyword frequencies from the three public release documents published by Equifax regarding the data breach last year. Figure 3 below shows the screen capture of the aggregate word frequencies sorted from highest frequency to the lowest frequency. Among the top 30 non-accessory words of highest frequencies, there is no presence of any keywords with negative associations to the corporate image. The high-frequency keywords with possible associations with communication and the company image and reputation and their frequencies in the three documents are: *Consumers (94)=Consumer (53)+consumers (41), (Equifax (76), Services (75), News (66), Products (63), Policy (60), Technology (60), Consumer (53), Business (52), Media (49), Public (43), Health (42), Financial (39), People (30),* and *Security (28)*. The high frequencies or repetitions of these keywords may help create the public communication effects of emphasis and projecting a positive corporate image (Davidson, 2008; Kemertelidze & Manjavidze, 2013; Wang & Park, 2017). For example, while the words *News* and *Media* suggest that the company is aware of the news media, the overwhelmingly high frequencies of *Consumer, consumers, Public,* and *People* combined indicate the company's constant and priority attention to consumers and people. The high frequencies of *Services, Products, Policy, Technology, Health, Financial,* and *Security* also show the company's emphasis of the things that consumers are most interested in. Finally, the high frequency of *Equifax* may help generate the blockbuster marketing effect and presence for the company similar to the effect of buzz words.

Contextual analysis of the Equifax press release documents released issued in the wake of the data breach incident does reveal examples of the components and strategies outlined in the proposed public communication model above. As an example of the diminish strategy, the initial press release highlighted the statement "No Evidence of Unauthorized Access to Core Consumer or Commercial Credit Reporting Databases" at the top of the public document (Equifax, September 7, 2017). In the same document, the company also tried to shift part of the blame to a third party by saying that "Criminals exploited a U.S. website application vulnerability to gain access to certain files" (para. 1). As examples of rebuild efforts and positive actions, Equifax has issued repeated apologies to impacted consumers and business customers for the concern and frustrations caused by the breach, promised free identify theft protection and credit monitoring to impacted consumers as well as independent investigations into the incident and improvements in information security protection for all consumers (Equifax, September 7, 2017; Equifax, September 15, 2017; Equifax, October 2, 2017). Equifax also attempted the bolstering strategy in the initial press release by saying that they are proud of themselves as a "leader in managing and protecting data" (Equifax, September 7, 2017). In addition, Equifax has shown good will by releasing the technical details of the breach, a timeline of developments, its engagement with

law enforcement (FBI) and the independent firm Mandiant for forensic investigations, as well as additional support efforts and actions for impacted consumers (September 15, 2017).

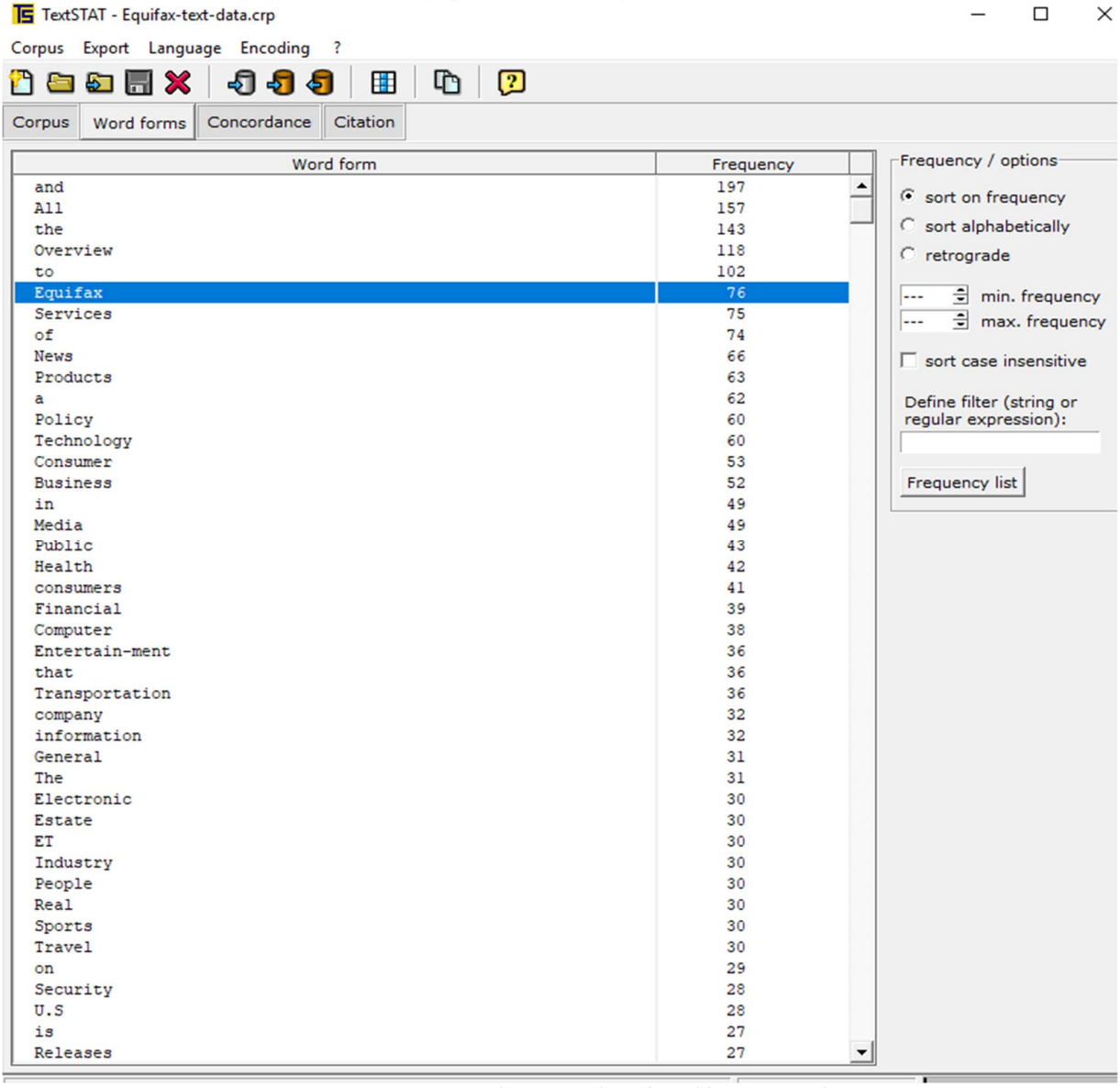

Figure 3. TextSTAT Word Frequencies of Equifax Press Releases

In terms of scapegoating strategies, there is no indication that Equifax attempted to share the blame with peer organizations with data breach incidents except for blaming third party criminals for the unauthorized access. However, Equifax did try to reduce the blame to a single scapegoat – former Chairman and CEO Richard Smith. Equifax announced Smith's sudden retirement on September 26, 2017 effective immediately but three weeks after its announcement of the data breach (Egan, 2017). After his retirement, Smith testified at the U.S. House Energy and Commerce Committee hearing on October 3, 2017 and stated that he takes "full responsibility" for the breach (Moyer, 2017). By taking all the blame, the newly retired former CEO serves as the scapegoat for the Equifax organization in an attempt to reduce the blame to a single party and protect everyone else in the same organization who may be found responsible.

The intended effects of the incident handling strategies may be moderated by the facts and responsibilities found later

and impacted by the timing issues. For example, initial announcement and handling of the data breach by Equifax was given negative reviews because it was found that Equifax waited six weeks before it announced its massive data breach affecting 143 million Americans and that three Equifax executives sold their company stock shares days after the company found out about the hack and before this corporate disclosure of the breach (Wiener-Bronner, 2017). In terms of improving security protection, in the weeks since Equifax disclosed the breach, the company's official Twitter account mistakenly tweeted a phishing link four times instead of the company's actual breach response page (Newman, 2017). In addition, it was reported after Equifax's initial breach disclosure that an Equifax web portal was secured with the worst username and password combination possible: admin and admin, which can be easily guessed and cracked (Matthews, 2017).

Equifax's handling of the massive data breach incident does not appear effective so far. The effectiveness of the public communication model for corporate data breach incident handling is measured by the company's subsequent performance. Soon after Equifax's initial press release of the data breach, its stock value closed down about 14 percent and the cost estimates for the company by the breach would be in hundreds of millions of dollars (U.S. News, 2017). In addition, Equifx was hit with 23 class-action lawsuits filed through the weekend after its initial announcement of the data breach (McCoy, 2017). An assessment of Equifax's public communication in its initial handling of the data breach was a "public relations catastrophe" (Wiener-Bronner, 2017).

CONCLUSIONS

This paper proposes an improved version of the public communication model for business data breach incident handling. The model added different manners of the scapegoating strategy often used in corporate crisis management in addition to the situational crisis communication strategies of denial, diminish, rebuild, and bolstering, and the timing of incident response. The case study of the recent massive Equifax data breach is used to illustrate the elements and effects of the proposed model. The case study has significant value because of the massive size and impact of the Equifax breach and the fact that Equifax is one of the three major credit reporting agencies that are supposed to safeguard consumer credit information.

This study has important implications and lessons learned for cybersecurity incident handling and cyber workforce preparation. 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 upon latent discovery of responsibilities. Effective communication skills are an important part of educational programs and assessment of student learning outcomes (ABET, 2015; MSCHE, 2014). Given the increasing demand for qualified workforce for cybersecurity work, public communication competency and skills should be incorporated in their cybersecurity curriculum and courses. In addition, cybersecurity program assessment and certifications should address the public communication competency for cyber incident response and handling (Wang & Park, 2017).

This is a case study of a commercial business data breach incident. Future studies in this area may be extended to cybersecurity incident handling for government and non-profit organizations such as healthcare institutions with less commercial motivation. Given the fact that ransomware incidents have been on the rise, future studies on cybersecurity incident handling may consider cases of ransomware attacks.

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.

Bamber, M., & Parry, S. (2016). A study of the employment of denial during a complex and unstable crisis involving multiple actors. *International Journal of Business Communication, 53*(3), 343-366.

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

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.

Cinarh, I. (2016). In search of a scapegoat: The global corporate blame game. *Proceedings of International Conference on Communication, Media, Technology and Design, May 27-29, 2016, Zagreb, Croatia,* 125-132.

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., & Claeys, A. (2016). Debunking the myth of denial's effectiveness in crisis communication: Context matters. *Journal of Communication Management, 20*(4), 381-395.

Davidson, P. (2018, March 1). Equifax finds an additional 2.4 million Americans impacted by 2017 data breach. Retrieved from https://www.usatoday.com/story/money/personalfinance/2018/03/01/equifax-finds-additional-2-4-million-americans-impacted-2017-breach/384381002/

Dexheimer, E. (2017, October 02). Equifax Made Major Errors That Led to Hack, Ex-CEO Concedes. Retrieved from https://www.bloomberg.com/news/articles/2017-10-02/ex-equifax-ceo-says-human-tech-failures-allowed-breach-to-occur

Douglas, T. (1995). *Scapegoats: Transferring blame.* New York, NY: Routledge.

Egan, M. (2017, September 26). Equifax CEO Richard Smith is out after stunning data breach. Retrieved from http://money.cnn.com/2017/09/26/investing/equifax-ceo-richard-smith-out/index.html

Equifax. (2017, September 7). Equifax announces cybersecurity incident involving consumer information. Retrieved from https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628

Equifax. (2017, September 15). Equifax releases details on cybersecurity incident, announces personnel changes. Retrieved from https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832

Equifax. (2017, October 2). Equifax announces cybersecurity firm has concluded forensic investigation of cybersecurity incident. Retrieved from https://investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821

Equifax. (2018). Company Profile. Retrieved from https://www.equifax.com/about-equifax/company-profile/

Eyal, N. (2017, February 6). Why you need an imaginary scapegoat. *Harvard Business Review.* Retrieved from https://hbr.org/2017/02/why-you-need-an-imaginary-scapegoat

Goodin, D. (2017, September 21). Massive Equifax hack reportedly started 4 months before it was detected. Retrieved from https://arstechnica.com/information-technology/2017/09/massive-equifax-hack-reportedly-started-4-months-before-it-was-detected/

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.

LA Times. (2018, February 09). Equifax hack exposed more information than we thought, documents show. Retrieved from http://www.latimes.com/business/la-fi-equifax-hack-20180209-story.html

Matthews, L. (2017, September 13). Equifax website secured by the worst username and password possible. Retrieved from https://www.forbes.com/sites/leemathews/2017/09/13/equifax-website-secured-by-the-worst-username-and-password-possible/#7d833287457d

McCoy, K. (2017, September 11). Equifax hit with at least 23 class-action lawsuits over massive cyberbreach. Retrieved from https://www.usatoday.com/story/money/2017/09/11/equifax-hit-least-23-class-action-lawsuits-over-massive-cyberbreach/653909001/

Moyer, L. (2017, October 3). Equifax ex-CEO tells Congress he takes 'full responsibility' for massive data hack. Retrieved from https://www.cnbc.com/2017/10/03/equifax-ex-ceo-tells-congress-he-takes-full-responsibility-for-massive-data-hack.html

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

Newman, L. H. (2017, September 24). All the Ways Equifax Epically Bungled Its Breach Response. Retrieved from https://www.wired.com/story/equifax-breach-response/

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

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

Ponemon Institute. (2017). 2017 Cost of data breach study. Retrieved from https://www.ibm.com/security/data-breach

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.*

Seijts, J. (2015). Case study: Who should take the fall? *Harvard Business Review,* July-August, 123-127.

US-CERT. (2017, March 8). Apache software foundation releases security updates. Retrieved from https://www.us-cert.gov/ncas/current-activity/2017/03/08/Apache-Software-Foundation-Releases-Security-Updates

U.S. News. (2017, September 8). Equifax breach could have 'decades of impact'. Retrieved from https://www.usnews.com/news/articles/2017-09-08/equifax-breach-could-have-decades-of-impact-on-consumers

Wang, P., & Park, S. (2017). Communication in Cybersecurity: A public communication model for business data breach incident handling. *Issues in Information Systems, 18*(2), 136-147.

Wiener-Bronner, Danielle (2017, September 13). Equifax breach: How a hack became a public relations catastrophe. Retrieved from http://money.cnn.com/2017/09/12/news/companies/equifax-pr-response/index.html

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.