An Exploration of Public Reaction to the OPM Data Breach Notifications

Research-in-Progress

Abstract

With the number of data breaches swelling, people are likely to not respond adequately and ignore the breach notifications altogether. Ignorance of breach notifications creates a perfect storm of cyclical outrage and apathy that criminals can use to their advantage. In this research-in-progress paper, we explore public reactions to breach notifications for addressing two research questions: (1) with more and more information related to the breach, do people become apathetic towards that breach? (2) at what point do people simply tune out information related to the breach? The results of the sentiment analysis show that public express anxiety when there is a fear of being affected by the breach, and public express anger when there are lack of measures to safeguard the data. Sadness is the most strongly expressed emotion in response to the severity of the breach. After the public has received sufficient details about the event, they start to tune out information related to the breach event. The findings of this paper provide foundations for identifying when public experiences data breach fatigue, a feeling of numbness or emotional exhaustion to the breach event.

Keywords

OPM breach, Twitter microblog, Public reaction, Emotions, Sentiments

Introduction

According to the Identity Theft Resource Center, there occurred a total of 5,810 data breaches with a total of 847,807,830 individual records stolen between 2005 and 2015 (IRTC, 2016). Data breaches have been reported by companies such as JP Morgan Chase, Target, Neiman Marcus, LinkedIn, Ebay, Adobe, Home Depot, and Sony Pictures. Each of these data breaches represent an incident where private data has been reviewed, stolen, or used by unauthorized parties. This data may include personally identifiable information (PII), personal health information (PHI), or other information protected with the purpose of limiting access to authorized users. Data from the Privacy Rights Clearinghouse shows that external hacking is the leading source of breaches, followed by insider disclosure, physical loss, and lost or stolen devices (Williamson, 2015). According to CSID, a leading provider of global identity protection and fraud detection technology, the financial, educational, and government sectors have the highest number of breaches reported (CSID, 2015). Compromised data can be exploited by criminals to commit crimes affecting a victim's identity and finances.

Vulnerable consumers who do not take protective measures may incur losses that may have otherwise been preventable. Anecdotes have shown that consumers may not respond adequately to data breaches. Examples include a lack of post-breach vigilance, no alteration in their behavior, and neglecting to subscribe to fraud protection services (O'Farrell, 2014; Perlberg, 2014). Some may ignore alarms, alerts, or breach notifications. A 2014 Ponemon Institute report found 32% of consumers surveyed "ignored the notifications and did nothing" when alerted to a data breach involving their information (PonemonInstitute, 2014). The same report also found that 55% of consumers surveyed had taken no steps to protect themselves from future identity thefts. A YouGov BrandIndex report found that consumers turned numb to breach incidents (Marzilli,

2013). Criminals can take advantage of people if they do not care about the breach notifications, a result of which they will be continued targets of criminal activity. Indeed, it is clear that investigating public's reactions to breaches is of paramount importance.

Most of the work studying public reaction to breaches has focused on a macro-level understanding of people's response to multitude of data breaches as the number of breaches have multiplied from 2011 to 2016 (the year of mega breaches). The idea behind the macro-level investigation of public reaction is that the more people are confronted with breaches, the less likely they are to care about other breaches. To date, however, there is little micro-level understanding of public reaction in the aftermath of an individual data breach. With more and more information related to the breach, do people become apathetic towards that breach? At what point do people simply tune out information related to that breach? In this research-in-progress paper, we explore negative emotions (anger, anxiety, fear and sadness) in the aftermath of the breach notifications within the context of a single breach event. The contributions of this research-in-progress paper are two-fold: First, it determines the pattern of emotional responses to breach notifications. Second, it investigates if people will start treating breach notifications apathetically.

The study is organized as follows. In the next section, we review the background of public reaction to breaches and specify the context of the research. We then explore the data about a recent breach and conduct an analysis of emotions related to the breach. Subsequently we analyze the breach related data to identify two critical dimensions that need to be considered in studying people's reaction to breaches. Finally we end this study with the conclusion.

Background

OPM Breach and Twitter Microblog

For the purposes of this paper, we focus on the April 2015 data breach of the U.S. Office of Personnel Management (OPM). In this incident, personnel data – full name, birth date, home address, and social security number – of millions of Federal employees was stolen. It was a large data breach in the recent past and its sheer number of victims allows us rich data in understanding publics' reaction to breaches. This preliminary study lays the foundation for subsequent projects (e.g., model extensions or victims and non-victims comparisons).

The widespread use and the rapid growth of microblogging services have resulted in new mechanisms for people to share their emotions regarding specific events. Microblogging services have afforded broadcasting information to the public in real time thereby enabling people to express their emotions without any time or location restrictions (Lee et al., 2015). In this way, microblogging services can be considered as useful tools for corporate entities and government organizations alike in understanding people's reaction in the aftermath of data breaches. In this paper, we focus on Twitter messages in the aftermath of OPM breach.

Public Reaction to Breaches

Industry reports have suggested that consumers demonstrate a lack of interest in breach incidents with increasing occurrences of breach events (Humphries, 2014). Public reaction to breaches is a result of their prior experience, both direct and indirect, with data breaches. It remains relatively consistent across situations and may act as an important cognitive bias that distorts people's sense making in the aftermath of a breach event. Lee et al. (2015) argue that emotional factors can inform public's reaction to events. A decision maker's apathy may be explained by his or her insensitivity

to data breach notifications, which results from an over exposure to frequent media reports on similar incidents in the past (Lazzarotti, 2014). When one becomes drained by hearing about data breach events, he or she tends to lose interest in breach events.

To best of our knowledge, most of the studies investigating breach events have ignored the micro-level view that examines publics' reaction to individual aspects of the breach events. In order to examine the breach event from a micro-level view, we investigate people's emotional state in response to the data breach notifications. Following Lee et al. (2015), who suggest that three negative emotions – anger, anxiety, and sadness – help in understanding the people's response to a crisis event, we explore negative emotions (anger, anxiety and sadness) in the aftermath of the breach notifications within the context of OPM breach event. Anger is denotes an uncomfortable response to a grievance (Videbeck, 2013); Anxiety is the fear caused by being aware of danger (Lee et al., 2015); Sadness is the opposite of happiness (Lee et al., 2015).

Methodology

OPM Timeline

While the adversarial access to OPM's network dates back to mid-2012, the breach was only detected in mid-2014 when OPM was notified by a third party. The adversary managed to obtain an elevated access to the OPM's network, and successfully exfiltrated personnel information, including fingerprints. OPM released public notifications in June 2015. The data we utilize in this research-in-progress paper provides the key events in the timeline post the public notification of the OPM breach (see Table 2).

Table 2. Timeline of OPM Breach

Date	**Event**	**Importance**
6/4/15 – First time #opmhack concept enters public sphere – Begin data collection		
6/4/15	First Public Notification	First time #opmhack concept enters public sphere
6/8/15	H. Comm. brief confirming lost data	News reports relay briefing: Public now aware of data significance
6/12/15	Fed Union: Hackers took SSNs of everyone	News report claiming SSNs of all federal employees taken
6/16/15	OPM Director Archuleta acknowledgement	OPM Director finally acknowledges breach
7/9/15	Press release confirming breach magnitude (21.5 million affected)	Magnitude of impact revealed to be larger than thought
7/10/15	OPM Director Archuleta resigns	Director resigns (1 day after major press release)
7/31/15 – End data collection		

Data Collection

We purchased data following the OPM data breach using third party vendor. Twitter provides three APIs to enable researchers and developers to collect data, namely STREAMING, REST and SEARCH APIs. Satisfying user specified filtering criteria (based on keywords, location, language,

etc.), streaming API is used to get tweets and their corresponding user's data in real time, REST API is used to get the data in select historical time period, and search API provides data on relevant searches on Twitter. For this research, the purchased tweets were collected from Twitter microblogs through the REST APIs using the keyword #opmhack. We requested purchased data from the time when OPM publicly announced the breach (June 4th 2015) till two months after the announcement (July 31st 2015). This time window allowed us to gather 18,764 tweets that provided information during the time with the greatest propensity for public reaction to data breach. Table 1 provides the descriptive of the data collected. Figure 1 shows a distribution of the tweets collected.

Table 1. Data Descriptive

Month	Tweets (N)	Percent (%)
June 2015	9018	48.06%
July 2015	9746	51.94%

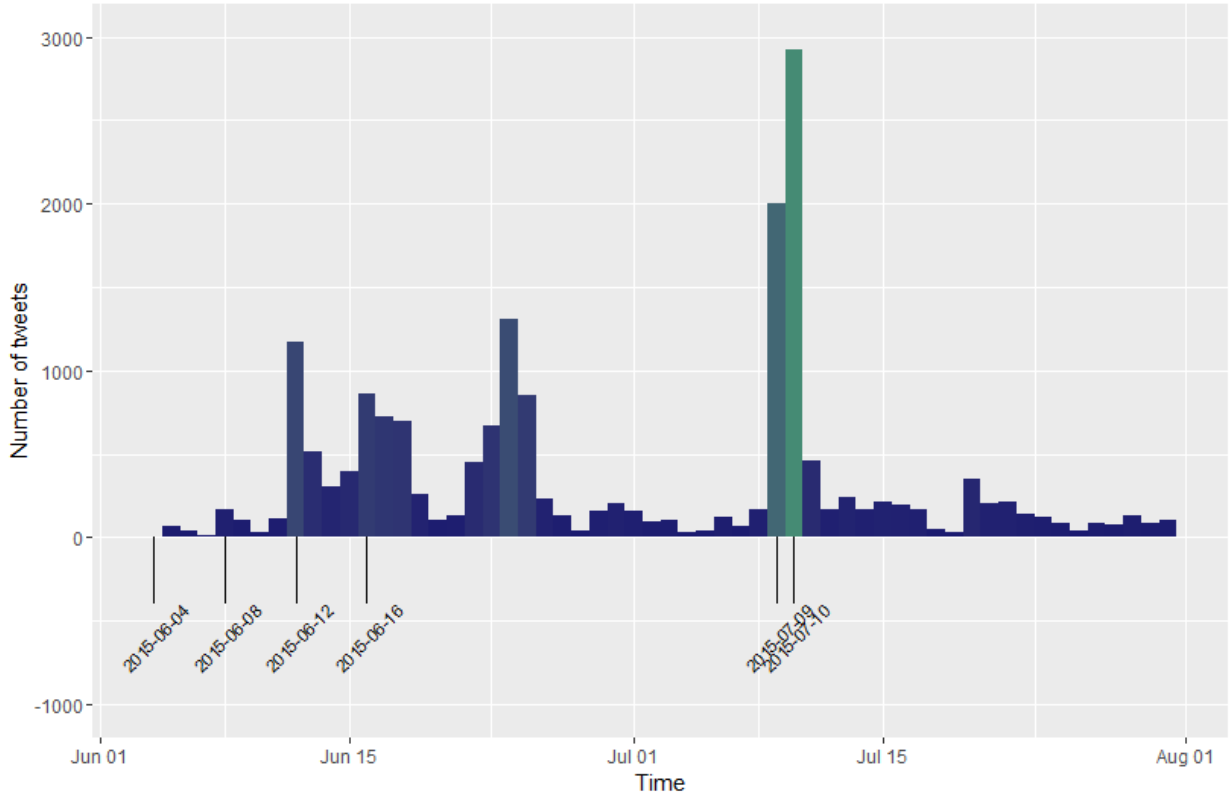

Figure 1. Distribution of the tweets collected

Sentiment Analysis

In order to investigate people's reaction to OPM breach notifications, we conducted sentiment analysis of the tweet messages. Sentiment analysis allows us to identify the expression of sentiments in the text messages (Nasukawa & Yi, 2003). Sentiment analysis combines natural language process and text analysis to extract emotion information from the text (Stieglitz &

Krüger, 2011). We used a text analysis software, Linguistic Inquiry and Word Count (LIWC), for analysis of anger, anxiety and sadness expressed within the tweets. LIWC uses a psychometrically validated dictionary to measure the inherent emotions in the text (Lee et al., 2015). LIWC is a popular tool for sentiment analysis and has been used in research to extract emotions from plain tweets (Pennebaker et al., 2015; Tausczik & Pennebaker, 2010)

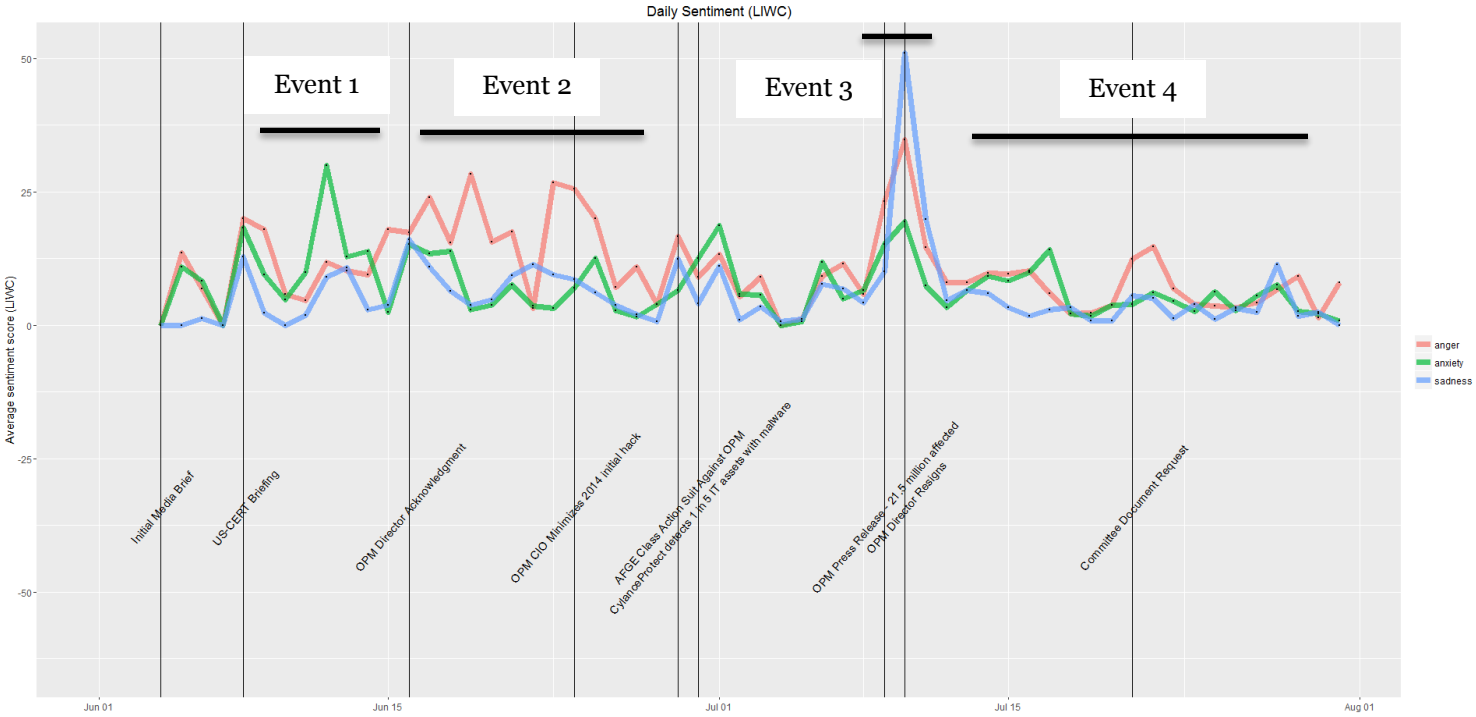

Figure 2. Public Reaction to OPM Breach over the Timeline

Emotional Reaction to OPM Data Breach

In this section, we present analysis results to answer the two research questions: First, we investigate the research question – "With more and more information related to the breach, do people become apathetic towards that breach?" From Figure 2, we can see that when the information about suspicious traffic on OPM network is confirmed by US-CERT and when the federal union claims that SSNs of all federal employees are stolen, people express anxiety because of the fear of being affected by the event (event 1). As OPM Director acknowledges the compromise of background data, public express their anger that stems from the lack of measures in place to safeguard the personnel data (event 2). When OPM releases a public statement that 21.5 million personnel have been affected, people experience sadness for the extent of damage the breach caused (event 3).

Second, we investigate the research question – "At what point do people simply tune out information related to that breach?" After the press release, people have obtained sufficient detail about the incident, which is visible in the less volatile patterns (somewhat stable patterns) of anger, anxiety and sadness (event 4). In this phase, people start tuning out information related to the OPM breach. This phase provides important clues to data breach fatigue – an emotional exhaustion in relation to the information about the breach. Prior studies have considered the sensation of fatigue as an emotion rather than a physical state (Noakes et al., 2004). The sensation of fatigue is a

complex emotion affected by other emotions such as anger and fear (Gibson et al., 2003). LeDoux (1998) has suggested that fatigue is an emotion itself. Gibson et al. (2003) also argue, "the sensation of fatigue can be classified as an emotional construct" (p. 174).

Discussion and Conclusion

The existing research, for the most part, has been silent on online public's reactions in response to data breaches (Chakraborty et al., 2016). Our paper makes a twofold contribution. First, it determines the emotional responses to breach notifications. Second, it investigates if people will start treating breach notifications apathetically. In the case of breach events, people expressed anxiety in the early stages when there is a danger from the event. In addition, public also showed anger for OPM's incapability to safeguard personnel information. In reaction to the sizeable loss of data (21.5 million records), sadness was the most strongly expressed emotion. In this way, the results confirm that expressed emotions reflect the characteristics of the breach event.

Findings of our study offer directions to the practitioners and policy makers in conceiving plans that promote protection in the aftermath of data breach incidents despite challenges such as breach fatigue. For example, educational or awareness campaign may be employed to encourage emotion focused coping strategy in order to reduce chaos and uncertainty related to the event. This preliminary study lays the foundation for future studies targeting at uncovering more complex issues. We plan to test the model among non-victim populations and to include other constructs that may better explain this research phenomenon.

This study has the following limitations. First, the information about OPM hack was available much before it was publicly announced. Second, in the timeline, we have only focused on those events that were available to public. Third, we only focus on one microblogging platform, Twitter. This could affect the generalizability of the results. One possibility of future work would be to look at positive emotions and contrast its patterns with the negative emotions. Yet another future option would be to breakdown the timeline to accommodate events that were not necessarily available to public in the OPM context. Finally, the emotional reactions over the timeline can be constructed for each user and then compared it with the social reaction (as reported in this paper).

By the time of the workshop, we will incorporate an event study analysis (following Wang et al., 2010) that provides details on why certain events in the timeline have higher levels of emotions (anger, anxiety or sadness). We will also test mean differences for the three emotions for different events on the timeline. This will allow a richer understanding of public's reaction to the OPM breach event.

References

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., and Rao, H. R. (2016). Online Shopping Intention in the Context of Data Breach in Online Retail Stores. Decision Support Systems (83), pp. 47-56.

CSID. (2015). Data Breaches Pose a Threat across All Industries. In: CSID. Austin, TX.

Gibson, A. S. C., Baden, D. A., Lambert, M. I., Lambert, E. V., Harley, Y. X., Hampson, D., ... & Noakes, T. D. (2003). The conscious perception of the sensation of fatigue. Sports Medicine, 33(3), 167-176.

Humphries, D. (2014). Public Awareness of Security Breaches: Industry View 2014. In: Software Advice. Gartner.

IRTC. (2016). Data Breaches. In: Identity Theft Resource Center. San Diego, CA.

Lazzarotti, J. (2014). Report Says Russian Hackers Stole 1.2 Billion Usernames and Passwords, but Don't Let "Breach Fatigue" Take Hold. In: Workplace Privacy, Data Management & Security Report. White Plains, NY: Jackson Lewis P.C.

LeDoux J. (1998). The emotional brain. London: Weidenfeld and Nicolson.

Lee, J., Rehman, B. A., Agrawal, M., & Rao, H. R. Sentiment Analysis of Twitter users over Time: The Case of the Boston Bombing Tragedy. In 15th Workshop on e-Business, WEB 2015, Fort Worth, Texas, USA, Springer.

Marzilli, T. (2013). Target Perception Falls after Data Breach. In: YouGovBrandIndex. London, UK: YouGov plc.

Nasukawa, T., & Yi, J. (2003). Sentiment analysis: Capturing favorability using natural language processing. In Proceedings of the 2nd international conference on Knowledge capture (pp. 70-77). ACM.

Noakes, T. D., Gibson, A. S. C., & Lambert, E. V. (2004). From catastrophe to complexity: a novel model of integrative central neural regulation of effort and fatigue during exercise in humans. British journal of sports medicine, 38(4), 511-514.

O'Farrell, N. (2014). Data Breach Fatigue: Consumers Pay the Highest Price. Mountain View, CA: CreditSesame.com.

Pennebaker, J. W., Boyd, R. L., Jordan, K., & Blackburn, K. (2015). The development and psychometric properties of LIWC2015. UT Faculty/Researcher Works.

Perlberg, S. (2014). Do Consumers Have Data Breach Fatigue? In: WSJ.com. New York, NY.

PonemonInstitute. (2014). The Aftermath of a Mega Data Breach: Consumer Sentiment. Ponemon Institute.

Stieglitz, S., & Krüger, N. (2011). Analysis of sentiments in corporate Twitter communication–A case study on an issue of Toyota. Analysis, 1, 1-2011.

Tausczik, Y. R., & Pennebaker, J. W. (2010). The psychological meaning of words: LIWC and computerized text analysis methods. Journal of language and social psychology, 29(1), 24-54.

Videbeck, S. (2013). Psychiatric-mental health nursing. Lippincott Williams & Wilkins.

Wang, J., Xiao, N., & Rao, H. R. (2010). Drivers of information security search behavior: An investigation of network attacks and vulnerability disclosures. ACM Transactions on Management Information Systems (TMIS), 1(1), 3.

Williamson, W. (2015). Data Breaches by Teh Numbers. In: Security Week. Wired Business Media.