Blame Distribution Following Information Security Breaches

Emergent Research Forum

Andrew S. Miller  
Mississippi State University  
asm357@msstate.edu

Kent Marett  
Mississippi State University  
kmarett@business.msstate.edu

Abstract

People distribute blame to the parties they feel responsible in information security breaches. This paper provides propositions of blame distribution based on (a) the source of the breach, (b) the classification of the information that was vulnerable and (c) the classification of stakeholder, and is motivated by gaps in academic literature concerning blame distribution after a breach. The propositions in this paper are grounded in the attribution theory and previous research on institutional trust. Future research methods are discussed, including the data collection. Future research ideas are discussed in this paper.

Introduction

Business organizations collect and store a wealth of information that stakeholders entrust them with. This information may or may not be formally recorded and may or may not be confidential or sensitive in nature. Some smaller businesses, such as sole proprietorships, may not have a lot of formally recorded information. In such cases, the owner or employee(s) would remember the company’s knowledge, such as their suppliers’ contact information, their prices, their customers, peak traffic times, etc. (Iacovou et al. 1995).

However, larger organizations tend to collect more information than smaller firms. While some large organizations may not use technological information systems to store this information, most large firms use some sort of information system (IS) to maintain standardized information, such as their emails, company documents, prices, customer lists, customer billing information, financial documents, etc. (Iacovou et al. 1995).

This information that companies maintain is often valuable to both insiders and outsiders, and can be prone to misuse by many individuals and groups (Pathari and Sonar 2013). These groups are often classified with their relation to the organization as insiders or outsiders (Karlsson et al. 2017). Insiders are commonly classified as people within the organization, including employees, contractors, and others with a direct relationship to the company and its operations. Likewise, outsiders are classified as people who do not have a direct relationship to the company. Both insiders and outsiders can have similar motivations for misusing company information, including financial reasons, vengeance reasons, and to receive recognition.

Regardless of motivation or relationship to the company, however, people ultimately wish to find someone responsible for a criminal or unethical action. This paper makes propositions for how a company’s employees (actors) or the public (observers) place blame after a breach of information security, which occurs whenever information is accessed without proper authorization. This can occur by an insider who has access but is not supposed to access information or release it, or an outsider who obtains access to company systems and information without authorization through some means.

The effects of information security breaches have been studied in previous studies (Arvidsson 2014; Goel and Shawky 2009; McNulty 2007). Arvidsson (2014) examined recent company breaches, namely the Target credit card number breach, and shows how it affected IT operations and Target’s stock price. Goel and Shawky (2009) use financial performance data from 105 publicly-traded corporations and compare the companies’ average rate of return both pre- and post-breach. Lastly, McNulty (2007) focuses on the managerial and reputational effects of a breach, as opposed to the financial approach taken by Arvidsson and Goel and Shawky.
This study attempts to address a significant gap in business literature concerning who is blamed for information security breaches. While the financial impact of an information security breach impacts the firm’s sales and institutional trust, we did not locate any articles discussing the distribution of blame following an information security breach. This research not only pertains to information security, it potentially has a bearing on public relations efforts in the aftermath of a breach. In his development of image restoration theory, Benoit (1997) suggests that it is important for both internal stakeholders and the public to be assured both that the attacked company is making a good faith effort at preventing similar breaches from occurring again and that the offending party is being held responsible. Further, Benoit states that perceptions are often more important than reality, and given the multiple audiences for whom subsequent crisis communication is tailored, the assignment (or mis-assignment) of blame requires understanding how each of the audiences perceived the breach. The following section reviews attribution theory, which has long been a prevailing explanation for how blame is assigned depending on the accuser’s perspective.

**Attribution Theory**

Classic attribution theory is widely credited to Heider (1958) who established an early framework for the distinction of internal and external attributions. Heider classified internal attributions as personal beliefs and personality characteristics. These internal attributions are unique to the individual and tend to not rapidly change. These are often referred to as dispositional attributions.

Likewise, Heider defines external attributions as situational pressures or outside influence (Heider 1958). External attributions relate to something that the individual does not directly control and is based upon a situational basis as opposed to a personal basis. External attributions are frequently called situational attributions.

An attribution is an assignment of cause for an event or phenomenon. For example, if an employee receives poor marks on their annual performance review, some of the employee’s coworkers may say this is because the employee was lazy during the busy season. These coworkers are using internal attributions to explain the employee’s behavior. The employee’s lawyer and psychologist may blame the performance issues on an ongoing divorce battle between a past spouse. In this case, the lawyer and psychologist believe that external attributions lead to the employee’s poor performance review. The actual cause or causes could be anything in this example and may or may not relate to the perceived causes.

The discussion in the following section draws primarily from the attribution theory to determine how people place blame on people and departments regarding information security breaches. Further details about how this will be determined are in the following methods section.

**Model and Research Questions**

To gain a more complete understanding of blame distribution, it is important to view ideas about blame distribution as interconnected rather than as separate and incompatible. To do so, we propose the following research questions:

**RQ1**: How does the information’s classification affect how people assign blame?

**RQ2**: How does the classification of a threat as internal or external affect how people assign blame?

We first study the classification of information involved in the breach to see its impact on the distribution of blame. The possible classifications of information are public, internal use only and confidential (Niemimaa and Niemimaa 2017; Spears and Parrish Jr 2013). Most companies have these exact classifications for their information, and they have progressively strict information handling procedures for each classification (Spears and Parrish Jr 2013). However, governmental organizations often do not have internal use only due to open record laws such as the Freedom of Information Act and other “sunshine” laws that allow the public to request access to what the business community would classify as “internal use only” (Pozen 2017).

Both questions seek to investigate differences in the distribution of blame. This idea comes from the attribution theories external factors and situational attributions. These research questions help guide this
research and aid the development of hypotheses. Additionally, the hypotheses look to the attribution theory for support.

Internal threats are different from external threats in one primary way: the relationship of the alleged perpetrator or potential perpetrator to the organization. Such threats are prevented in different ways according to best practices; therefore, it can be assumed that different parties are responsible in different ways (Moyo et al. 2013). However, individual differences and situational differences will greatly impact the distribution of blame.

This is dependent upon the factors derived from the attribution theory. The relationship to the company variable is derived from the classification of internal and external attributions.

**Proposition 1.** There will be a difference in blame in cases in which the perpetrator was internal or external to the organization, such that the distribution of blame will be more focused on one group for external perpetrators.

There are inherent differences between information classifications. In looking at the types, it can be ascertained that different groups of people in the organization are involved in varying ways with the prevention of the threats. To better understand this, we are interested in the information owner and other parties included in the chain of custody as candidates for blame.

Most organizations view public information as any information that is freely accessible by both internal and external entities. This information can be public information found on forms such as their annual financial report, or information on the company website (Spears and Parrish Jr 2013). The primary concern held for public information is that it remains accurate, as both intentional and unintentional inaccuracies could lose potential clients, erode existing clients’ trust, cause regulatory and legal compliance issues, and cause other financial issues (Yue and Cakanayildirim 2007). Both accuracy and the confidentiality of information is imperative to organizations when the information is classified as internal use only or confidential, as the disclosure of such information could impact the competitive advantages or privacy of its employees or clients (Yue and Cakanayildirim 2007).

To aid in the distinction of knowledge and relationship to the incident, two distinct levels of classification are used: actors and observers. Actors refer to insiders who are directly involved with the situation of interest and have non-public knowledge about the incident (Watson 1982). An observer refers to anyone who is not directly involved in the situation of interest and lacks non-public knowledge (Watson 1982).

The classification of information is similar to the situational factors from the attribution theory, due to these different classifications being highly dependent upon the situation and have a direct impact upon how people blame actors. Likewise, there are several elements often used by people to assign responsibility: agency, accountability and obligation (Harmon 1995). This implies that the perspective of the individual affects their attribution of blame in security incidents.

Institutional trust refers to how honest an organization is perceived, and is shown by the willingness to accept the risk and interact with the organization (Culnan and Armstrong 1999). An organization’s information handling policies and practice can affect the institutional trust the general public holds for the institution (Culnan and Armstrong 1999). Institutional trust can be lost if a violation results from the company causes an individual harm (McKnight et al. 2011; Pienta et al. 2016).

**Proposition 2a.** There will be a lower level of institutional trust for actors than observers when public or internal information is compromised.

**Proposition 2b:** There will be a lower level of institutional trust for observers than actors when confidential information is compromised.

**Proposed Methodology**

For this study, a factorial survey method is proposed. This is to prevent bias, and to reduce the likelihood of deception by the participants, as they are no longer answering who they would blame, but are instead selecting who the person in the scenario would blame (Gefen 2005). A series of scenarios will be developed to test who people blame in each circumstance. To reduce bias and other predispositions, fictitious company and party names will be used.
The specific scenarios will be split into two main groups: insider and outsider breaches. These coincide with the nature of the breach that occurs in each scenario. For example, a scenario of a breach that occurs by an employee selling the contents of the organization’s customer data would be classified as an insider breach. Likewise, a scenario of a breach in which a hacker without direct connection to the company accesses the same information and then sells the information online would be classified as an outsider breach, as the employee did not have an existing relationship with the company.

Additionally, the following categories of data classification are to be examined: public, internal use only and confidential. For each of these categories, two scenarios will be developed. One will be based upon an outsider breach, and one will be based upon an insider breach making this a 3 X 2 design.

Each participant in the survey will receive a single scenario to assign their perceived responsibility of each party to. The actual scenario participants receive is random. Additionally, each scenario will balance completeness of information with succinctness to maintain interest and prevent survey fatigue. The full study will include approximately 400 participants. This sample size of 400 participants was determined a priori using G*Power 3.1.7, with a desired effect size of 0.25, a desired power of 0.95, and an alpha of 0.05 (Faul et al. 2009).

The responses will first be analyzed using descriptive statistics, with respect to each party within the scenario. As the data is provided by the participants in the form of percentage they believe responsible by each party in the scenario, there is no need to normalize the results. Once the descriptive statistics are gathered in each scenario, the results for each pair of the same classification are compared using an ANOVA test and Tukey’s HSD test.

**Discussion and Future Research**

There are potential limitations with the proposed research method and study. First, people may provide who they think is to blame based upon the provided information from the scenario, but it is extremely difficult if not impossible to describe a security event and the organization surrounding it in a length that people will read on a survey, as well as understand. To expand upon this, each participant would not simply answer one scenario; they would instead be tasked with answering 10 scenarios and then deciding who is to blame in each independent scenario. Therefore, survey fatigue is a concern, as people may get tired of reading and simply select an option without reading the entire scenario, question and answer choices.

On the opposite end of the spectrum, if the background information is too short, there is significant risk of leading participants to select certain choices.

Another potential limitation of this is how exactly the surveys will be scored. In real life, it is often a simplification to assume that a single person or department can be blamed for 100% of an issue, while no other person or group is responsible in any way for the issue. To account for this, it is possible to have participants fill in the percentage they believe each party is responsible.

**REFERENCES**


