2017

Corporate apology and cultural difference: A comparison of the United States and South Korea in cyber-security breach crisis

Nahyun Kim
Iowa State University

Corporate apology and cultural difference: A comparison of the United States and South Korea in cyber-security breach crisis

by

Nahyun Kim

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Journalism and Mass Communication

Program of Study Committee:
Suman Lee, Major Professor
Dara Wald
Huaiqing Wu

Iowa State University

Ames, Iowa

2017

TABLE OF CONTENTS

LIST OF TABLES

ACKNOWLEDGEMENTS

I would like to thank my committee members for their guidance and support throughout the thesis. My deepest gratitude goes first to my major professor, Dr. Suman Lee, for his knowledge, advice, and encouragement that has helped me grow in the process. My appreciation extends to Dr. Dara Wald and Dr. Huaiqing Wu for their expertise and advice that has become a vital part of this thesis.

Additionally, I am also indebted to my colleagues, department faculty and staff in the Greenlee School of Journalism. My time at Iowa State University could not have been this valuable without their help and inspiration.

Finally, I would like to thank my family and friends for their unwavering support and belief in me. I am happy and feel blessed to take this journey in life with you.

ABSTRACT

The purpose of this study is to examine characteristics of apology (responsibility admittance, sympathetic expression, compensation, reassurance) and other features of crisis response such as use of excuses, function of apology, and organizational representation appearing in official statements when cyber-security breaches threaten an organizational reputation. Ultimately, 108 official statements issued by organizations in the United States and South Korea were analyzed through a quantitative content analysis. The results showed that (1) the most common type of data breach is identity theft, and almost all types of industry are exposed to the risk of data breach incidents; (2) internal security vulnerabilities including "malicious insider" and "accidental loss" are the second most frequent cause of cyber-security breaches; and (3) culture plays a significant role in the characteristics of apology (responsibility, sympathy, compensation, reassurance), use of excuse, function of apology, and organizational representation in official statements.

CHAPTER 1. INTRODUCTION

The digital world has brought not only positive changes to our lives, such as convenience, efficiency, and interconnectedness, but also negative consequences, such as privacy threats and cybercrimes. The potential for theft of digital information has increased due to the ease of data collection and its massive distribution. Personally identifying information (PII) is digitally stored in cyberspace, where it is exposed to the potential risk of misuse. People are seriously concerned about this risk. According to the TRUSTe's Consumer Confidence Privacy Index (2015), only 55% of Americans trust a company's ability to manage consumers' personal information. More than 90% of consumers surveyed said they are concerned about cyber privacy (TRUSTe, 2015).

To ease the concern and distrust, companies dealing with customers' personal information make efforts to update their technical infrastructures for cyber security and try hard to communicate with their customers when cyber-security breaches occur. However, society has witnessed an increasing trend of data breach crises. A few mega breaches, such as Target in 2013 and Home Depot in 2015, have been highly publicized by the media, but the number of reported cases suggests that the problem is much broader. According to the Identity Theft Resource Center (2017), the number of data breach cases in the United States reached a record high of 1,093 cases in 2016. Furthermore, this trend appears to be similar on a global scale. For all types of organizations, the explicit costs of stolen or lost records have increased by 23% since 2013 (Ponemon Institute, 2015).

Data breach incidents are an irrevocable crisis. Issuing an apology statement is a common practice among organizations when a cyber-security crisis happens. Making a cautious public apology may be more complicated now with the prevalence of internet

communications, through which apologies are seen and evaluated by people who have both direct and indirect relationships to the issues. Therefore, a successful public apology should not be a simple statement saying "sorry", but rather a highly articulated and sincere response guided by communication strategies.

The effectiveness of an apology depends on many factors, such as nuances of language, audience characteristics, and socioeconomic situations. This study expects culture to have an impact on making an apology as a crisis response and explores official statements issued by organizations in the United States and South Korea when cyber-security breaches threaten corporate reputations. The purpose of this study is to examine whether apology statements differ by cultural difference (individualistic versus collectivistic) in terms of the four components of corporate apology (responsibility admittance, sympathetic expression, compensation, reassurance), the use of an excusatory gesture, the function of the apology, and organizational representation.

CHAPTER 2: LITERATURE REVIEW

Cyber-Security Breach

A cyber-security breach means an event in which data that can identify an individual (e.g. name, driver's license number, social security number, medical record, and financial record etc.) is endangered by potential risk of exposure either in paper or electronic format (Identity Theft Resource Center, 2017). Cyber-security breaches are irrevocable once personal data is forcefully publicized in cyberspace. The stolen data is uncontrollable, and information can diffuse almost boundlessly in cyberspace.

There is no consensus on the definition of cyber security among scholars; a study that explored 18 countries' national cyber-security strategies (NCSS) found that each nation had a different understanding of the issue, and six of them discussed cyber security without defining it (Luiijf, Besseling, & De Graaf, 2013). Similarly, researchers do not use unified terms when exploring cyber-security issues; rather, they choose different words that fit most into the scope of their study. For example, Prakash and Singaravel (2015) used "privacy breach" to refer to the potential invasion of privacy from information leakage in data mining. Others used "data breach" to generally describe the leak of health information in the United States (e.g. Appari & Johnson, 2010).

Considering the scope of precious study and context, cyber security is widely used to indicate the issue as a risk or crisis that needs to be managed before or after an event of occurrence (Boyes, 2015; Davis, Garcia, & Zhang, 2009; Öğüt, Raghunathan, & Menon, 2011). A cyber-security breach brings both tangible (e.g., loss of sales) and intangible (e.g., loss of reputation) negative consequences to organizations. Scholars have found that a cyber-

security breach negatively affects the financial performance of a corporation. After a firm announces a data breach, the firm's market value significantly drops (Andoh-Baidooo & Osei-Bryson, 2007; Goel & Shasky, 2009). According to Veltsos (2012), data-security breaches threaten the reputation and credibility of corporations.

Despite the magnitude of this issue, cyber-security has rarely been studied in regards to a public relations crisis. Cyber-security breaches can happen at the individual, organizational, state, or national level. This study examines the cyber-security breach at the organizational level (e.g., corporate and non-profit organizations, such as schools) when the organization failed to protect its clients' personal data.

Crisis and Crisis Response Strategy

People often describe bad experience as a crisis, however, not all bad experiences are necessarily crises (Ulmer, Sellnow, & Seeger, 2014). This brings up the question, what makes a crisis distinct from other unpleasant or undesirable events in life? The three essential attributes of a crisis are unpredictability, representation of threats (Coombs, 2012), and its magnitude (Barton, 1993; Coombs, 2010). Being unpredictable means that an event violates people's expectation (Coombs, 2010). With heuristics, people have expectations for external objectives in situations and know what is desirable or not. For example, buildings are built to be structurally stable and are not expected to collapse, or downturn in economy should not last for a long time as it is not a desirable situation. When a situation unfolds opposite to people's expectations, the situation is perceived as being unusual or abnormal (Coombs, 2010). Scholars also agree that a crisis threatens an organization's major values or expectancies (Hermann, 1963; Coombs, 2012) and negatively affects its stakeholders

(Coombs, 2010; Barton, 1993). Since a crisis generates negative outcomes, it is something that needs to be prevented or avoided for both the organization and its stakeholders through proper management (Coombs, 2010). Lastly, a crisis stands out because a crisis is typically much grander than an unpleasant occurrence. Crisis is a serious event that can bring significant damage to organizations (Barton, 1993; Coombs, 2010). Sometimes, the existence of an organization can be threatened by the crisis (Fearn-Banks, 2017). With its magnitude, a crisis is described as "a major, unpredictable event" (Barton, 1993, p. 2), "a major occurrence" (Fearn-Banks, 2017, p. 1), or "turning points in organizational life" (Regester, 1989, p. 38). Unlike other incidents, a crises requires substantial resources for restoration and careful management-level attention (Coombs, 2010). For example, an individual loss of money from stock market investments is not generally called a crisis, but people recognize a stock market crash as an economic crisis because it brings a huge loss in resources and negative consequences from which a society seriously suffers.

The meaning of a crisis is socially constructed (Coombs, 2010). What defines a situation as a crisis is largely depends on how people view a situation. Moreover, people's perception of an event can affect whether that event turns into a crisis or not (Coombs, 2010). Empathizing the perceptual nature of a crisis, Coombs (2012) defined a crisis as "the perception of an unpredictable event that threatens important expectancies of stakeholders and can seriously impact an organization's performance and generate negative outcomes" (p. 2). A crisis situation can unfold even before the actual crisis event happens if people perceive it as a crisis in advance, or it can last even after the occurrence of an actual crisis as long as people suffer from the event. The definition is meaningful in that it can reflect three phases of crisis management, which are pre-crisis management to prevent crisis, crisis response to

deal with ongoing crisis, and post-crisis management to repair damaged reputation and trust (Coombs, 2007a).

A crisis can be momentum for an organization to be better or worse (Fink, 1986) depending on how an organization manages the crisis (Coombs, 2010). Communication is critical in crisis management as information is collected, processed, and disseminated through communication (Coombs, 2010). Successful crisis management will reduce the negative consequences of the crisis and reputational damage (Coombs & Holladay, 2005; Kiambi & Shafer, 2016). When a crisis happens, people need information to cope with the crisis situation and expect organizations to provide them such information. In addition, people in an uncertain or threatening situation tend to engage in rumor activities to make their own sense about the situation (DiFonzo & Bordia, 2000; DiFonzo & Bordia, 2007). Rumor is another type of crisis situation that organizations need to deal with (Coombs, 2000; Coombs, 2012). Therefore, it is important to provide people with related information.

Speed and clarity of communication is critical in crisis communication (Coombs, 2012). Crisis managers are expected for immediate responses and to keep the public updated with the present situation (Coombs, 2012). A quick response to a crisis is highly recommended in order to ensure effective crisis communication (Benoit, 1997; Coombs, 2010; Coombs, 2012) even though a crisis limits the amount of time to make responses with its nature of being unpredictable, (Hermann, 1972). Delayed crisis communication may fail to deliver appropriate information to the public in a timely manner, letting the message lose its power for the changed situation. In addition, it is important to deliver clear messages to inform people. People in a crisis situation might be overwhelmed with the unusual situation and tend to experience negative feelings such as anger, anxiety, sadness, and fright (Jin, Pang,

& Cameron, 2007). They might not be able to properly process information with such negative emotions (Coombs, 2012). In addition, ambiguity of messages will be another burden for the victims in crisis situations. People engage with coping behavior when facing emotional stress or life strains in order to protect themselves from any harm that may threaten their well-being (Lazarus, 1966; Pearlin & Schooler, 1978). Coping behavior involves cognitive appraisal of whether or not an environment is harmful or beneficial to an individual, and ultimately the efficacy of the particular coping behavior (Folkman, Lazarus, Dunkel-Schetter, DeLongis, & Gruen, 1986). In a crisis situation, people engage with a cognitive process to assess the crisis situation itself, and put cognitive effort into seeking ways to avoid or reduce any harm. However, an individual's cognitive resources are limited and people need to allocate their cognitive resources to encode, store, and retrieve mediated messages (Lang, 2000). Therefore, people may get annoyed when given too much additional information to process, or when additional cognitive works are needed to explore all of possible meanings of the unclear message.

Researchers have identified various types of crisis response strategies. Benoit (1997) identified five crisis response strategies: (1) denial (denying the occurrence of the event, that the organization performed it, or that the event was not harmful); (2) evasion of responsibility (by framing the act as an response to another's harmful act, explaining the event happened from defeasibility or by accident, or asserting that the original intention was good); (3) reduction of offensiveness (by increasing positive feelings or minimizing negative feelings associated with the negative event, differentiating the event from the past similar event, placing the negative act in a favorable context, counter-attacking the accusers, or providing compensation); (4) corrective action (restoring the status as before or promising to

prevent the reoccurrence of the negative event); and (5) mortification (apologizing and begging for forgiveness). The denial and evasion of responsibility are used to eliminate or reduce the organization's responsibility. Reducing offensiveness and corrective action diminishes any negativity associated with the organization. Mortification involves accepting the fault and making an apology. The effectiveness of each strategy is contingent upon its situation (Benoit, 1997). Organizations should analyze the accusation they face (blame or offensiveness) and the audience's beliefs and values that constitute their attitudes because it will provides insight about which options will be appropriate for the situation to change people's attitudes in the process of image restoration (Benoit, 1997; Benoit, 2015).

Situational crisis communication theory (SCCT) provides crisis managers with a useful framework to select effective crisis communication responses (Coombs, 2007b). There are three types of crises based on the level of an organization's attribution of crisis responsibility (Coombs, 2007b). First, a crisis with a weak attribution belongs to the victim cluster (Coombs, 2007b). The cause of crisis is outside of the company's control, such as a natural disaster, malicious agents trying to damage the organization, or false information (Coombs, 2007b). Second, a crisis with minimal attributions is categorized as an accidental cluster (Coombs, 2007b). The organization's action is unintentional, but the cause of the crisis is attributed to the organization (e.g., malpractice in operation or a technical error) (Coombs, 2007b). Last, a crisis with a strong attribution is called an intentional cluster (Coombs, 2007b). In this case, organizations know that they are taking inappropriate actions that may generate negative outcomes (e.g., human error or organizational misdeed) (Coombs, 2007b).

Three crisis response strategies are recommended for each crisis type which are denial, diminishment, and rebuilding (Coombs, 2007b). The denial strategy involves deleting any association between the organization and the crisis and can be executed through the simple denial of the event, attacking the accuser, and finding a scapegoat (Coombs, 2007b; Coombs 2012). The diminishment strategy weakens the organization's attributions for crisis or reduces the offensiveness of the crisis and can be performed using an excuse and justification (Coombs, 2007b; Coombs 2012). The rebuilding strategy improves the organization's reputation and involves making an apology or providing financial compensation (Coombs, 2007b; Coombs, 2012).

In addition to the crisis type, history of similar crises and prior reputation are also important considerations in SCCT when choosing crisis response strategies. (Coombs, 2007b; Coombs 2012). Even when for a same crisis type, different crisis response strategies are recommended. For example, diminish strategies are recommended for an accidental crisis when an organization has not experienced a similar event in the past and received an unfavorable reputation (Coombs 2012). However, when an organization has a similar crisis history or unfavorable prior reputation, rebuilding strategies are recommended for accidental crisis (Coombs, 2012).

A bolstering strategy serves as a supplemental strategy to the other three crisis response strategies (Coombs, 2012). A bolstering strategy builds a favorable connection between the organization and the public and includes reminding the public of past good events, praising publics, or victimizing the organization itself (Coombs, 2007b; Coombs, 2012).

Each strategy has its own power to minimize reputational damage and restore its tarnished image in different situations. However, despite the variety of crisis response strategies, audiences typically want to receive apology most when they are offended and perceive an organization as responsible for the offensive events.

Corporate Apology as a Crisis Response

Apology and its components

An apology is a communicative response that acknowledges guilt for a wrongdoing (Hearit, 2006). When a corporation involves issues that have been publicly criticized, the corporation seeks for forgiveness of the public by delivering public apologies to restore its damaged images (Hearit, 2006; Benoit, 2015). Corporate apology, a company-crafted response, has similar propositions with the one made by an individual because it is organized by individual members of the organization (e.g. executives, lawyers, and public relations managers etc.) who act in concert for a corporate advocacy (Hearit, 2006). Scholars agree that an apology or mortification reduces the negative consequences of a crisis and helps restore the organization's image or reputation (Benoit 1997; Benoit & Drew 1997; Kim, Avery, & Lariscy, 2009). Apologies are also known to ease public anger (Thomas & Millar, 2008) and the victims' aggression towards harm-doers (Ohbuchi, Kameda, & Agarie, 1989). Lyon and Cameron (2004) further argued that an apology helps corporations gain ethos, a pro-social status, and favor after a crisis.

The main components that are widely used for a corporate apology are responsibility admittance, sympathetic expression, compensation, and reassurance (Lee & Chung, 2012).

Gill (2000) argued that a full apology includes acknowledgement of responsibility, expression of remorse, and intention to prevent future similar event. Compensation can be added to the main components of a full apology as victims' financial damage or physical loss cannot be fully reimbursed with the other three components of apology.

The most essential component of an apology is the admission of responsibility, or accepting fault for a crisis (Benoit 1997; Benoit & Drew, 1997; Fuchs-Burnett, 2002). Lazare (2005) found that not admitting responsibility in an apology could lead to a negative situation, such as a major loss in reputation. Depending on how the corporation takes responsibility, the level of responsibility admittance can differ between active or passive. A company can rebuild its reputation through active responsibility admittance; however, passive responsibility admittance does not decrease the victims' negative feelings when it is clear that the company is responsible for the crisis situation (Robbennolt, 2003). Lee and Chung (2012) tested the effect of active versus passive responsibility admittance on public anger and found that an apology statement that admits responsibility relieves the public's anger more than an apology statement which passively acknowledges responsibility.

Sympathy is perceived in apologies in which corporations try to express their understanding and concern for the stakeholders involved in the crisis. A strong sympathetic expression makes apologies appear more sincere (Gonodo-Madikizela, 2003), having an effect equivalent to when corporations admit responsibility (Coombs & Holladay, 2008). However, expression of concern and sympathy for victims does not necessarily mean that an organization admits that they are responsible for the crisis (Coombs, 2012). Thus, an organization can express sympathy to increase the efficacy of making an apology without taking responsibility.

Sympathy is distinguished from empathy, where people experience another's situation. Sympathy with another individual's predicament leads to emotional identification; however, empathy makes people more intensely conscious about another's situation (Switankowsky, 2000). Previous studies have focused on sympathy because it requires a minimum level of emotional involvement with the situation that victims face. People with sympathy are considered "with-feeling" while people with empathy are "in-feeling" (Escalas & Stern, 2003, p. 53). Organizations may decide to stay at the level of sympathy to not lose their voice in managing the situation.

Compensation refers to offering something that can offset the suffering of victims (Coombs & Holladay, 2008). The form of compensation can vary such as providing goods or services, or monetary offerings (Benoit, 2015). The victim's perceived severity of damage or offensiveness of the events reduce with the compensation, therefore, organizations can strategically use compensation for image restoration (Benoit, 2015), Compensation alone is not a major component of an apology; however, it can increase the likelihood of a successful apology when integrated with other components. For instance, Braaten, Cody, and DeTienne (1993) found out that an apologetic statement can have a greater impact when responsibility admittance includes compensation.

Reassurance is a corporation's effort to prevent the same or similar negative event from happening again (Lazare, 2005; Leape, 2012). Furthermore, reassurance can be interpreted as a responsibility component indicating that actual efforts will be made to ensure that a similar crisis does not occur again (Lee, 2004).

The four components of apology stipulate what an apology should include to be successful. In the real world, there can be other notable attributes of apology to consider.

Use of excuse

Making an apology means admitting responsibility (Benoit, 1997); however, an excuse can appear in apology statements as well. An excuse is a type of account that denies full responsibility while admitting the inappropriateness of an event (Scott & Lyman, 1968). Apologies that involve responsibility admittance can be costly to corporations, as they can be used as evidence in lawsuits against them (Patel & Reinsch, 2003; Tyler, 1997). In this sense, some scholars argue that not admitting responsibility can be a strategic option for organizations when responsibility is ambiguous or unknown (Coombs & Holladay, 2008).

There are four ways that an organization can reduce or evade responsibility, either by emphasizing (1) that the situation was due to inadequate information or lack of control over the crisis (defeasibility), (2) the crisis was an accidental event (accident), (3) the trigger of the crisis was in response to other's wrongful behavior (provocation), or (4) the original intention of an action or event was benevolent (good intention) (Benoit, 2015). The first two tactics are denying an organizations' free will in controlling the trigger of the event. An organization can also deny its volition by asserting that they could not do anything about the crisis because a third party was involved in the crisis (Coombs, 1995). Or, an organization can insist that they were fully committed but the crisis was unavoidable. However, such a claim can be made without providing any further information or proof of their commitments. On the other hand, the last two options are related to the intentions of an organization and may not be appropriate for the context of cyber security breaches. These options can be utilized only when an organization had malicious intentions resulting in wrongful actions. For example, only individuals who planned for and carry out data breaches can claim that what happened was a counterattack of a provocation or that its intentions were

good. However, it would be safe to say that no organization has a desire to leak their own data. Organizations are blamed for their failure to secure personal data online. In this situation, organizations need different types of excuses for 'what happened', not for 'what they intended and did'.

An organization can also use victimization as an excuse strategy. Victimization involves coercion and reduces culpability (Fingarette, 1985). An organization can pose as a victim of the crisis by saying that it was also the victim of a malicious act (Coombs, 2010).

Function of apology

An official statement of apology is a message that the organization sends to its public. The function of an apology is marked by its content. Organizations should prioritize to protect their public by sending them messages that include two types of information: instructing information and adjusting information (Coombs, 2012). Instructing information is about what to do for physical safety in a crisis while adjusting information is concerned with how to handle psychological threats or distress (Coombs, 2012). A cyber-attack is not supposed to be physically harmful to its public. Therefore, it is safe to say that official apology statements regarding a cyber-security breach tend to focus on adjusting information. The two types of adjusting information can be about analyzing the crisis situation or expressing concern and sympathy. People engage emotional or rational coping strategies to logically understand the crisis situation or ease their negative emotions (Jin, 2009). Specifically, people wants to know what happened or what was done about the crisis to be reassured, and they may need to receive an expression of concern and sympathy to handle their psychological sufferings (Coombs, 2012). Based on the type of adjusting information,

the functions of an apology statement can be classified as providing analytic accounts, expressing concern and sympathy, or both.

Organizational representation

As much as what is said, who delivers the statement is also important to acquire a desirable outcome of communication. A spokesperson can appear in the discourse itself (e.g., "I am a manager of…") or be identifiable in an apology statement through signatures or names at the end of the written statement. For major issues, people expect an individual in a higher position to communicate with the public. Men (2012) mentioned that a natural association exists between a CEO and organization, indicating that a CEO can serve as a representative spokesperson regarding the event. A corporation's reputation is affected by the CEO's own reputation (Alsop, 2006), and the CEO's credibility is positively linked with the corporate reputation (Men, 2012). Several scholars have demonstrated the significant role of the CEO as a spokesperson in a crisis response (Luceero, Tan Teng Kwang, & Pang, 2009; Murray & Shohen, 1992; Turk, Jin, Stewart, Kim, & Hipple, 2012). Specifically, Lucero et al. (2009) found that a CEO needs to come to the forefront when the crisis is caused by the organization's transgression or when the crisis negatively affects the organization's reputation. Presumably, the visibility of a CEO as part of the response to a crisis can affect the effectiveness of the message. However, it is still possible that an organization does not identify its spokesperson in its public written statement or might use a different type of spokesperson, such as middle-level managers or collectively naming itself by using the company's name.

Along with these key components of an apology, cultural characteristics are also mirrored in an apology statement. In other words, the norms of an apology vary from culture to culture (Maddux, Kim, Okumura, & Brett, 2011).

Cultural Differences

The definition of culture is a complex whole acquired by man during his adaptation to given human and physical surroundings (Kluckhohn & Kelly, 1945; Tylor, 1871). It includes not only material acquisitions, such as physical artifacts, but also capabilities and habits, such as knowledge, belief, art, and customs (Tylor, 1871).

As a standardized social procedure (Kroeber & Kluckhohn, 1952), culture tells people what is desirable or what should be avoided within society. Individual patterns of feeling, thinking, and potential behavior are influenced by the social environment as these patterns are acquired through social contacts throughout early childhood (Hofstede & Hofstede, 2005). By observing, assimilating, and talking with others, members within a certain society internalize the shared norms, rules, and values that shape how people interact and communicate with others within a society (Hofstede & Hofstede, 2001; Hofstede & Hofstede, 2005).

Diverse perspectives explain how culture influences the way people think, communicate, behave, and build relationships with other people. Each culture originated from its own natural setting of society and, accordingly, cultures differ from place to place and from time to time. Therefore, distinguishing one culture from another does not evaluate its superiority or inferiority to others, but rather provides a basic foundation for understanding an individual culture's social behavior and background. One of the most

popular categorizations is the individualist–collectivist culture suggested by Hofstede (1984). The distinction between an individualistic and a collectivistic society is the degree to which individuals integrate into or separate themselves from a group (Hofstede, 1994). People in individualistic cultures see themselves as being independent from their in-groups, thereby favoring values such as individual efforts and goals (Hofstede, 1994; Ju & Power, 1998; Triandis, 2001). In a similar sense, an intentional action or event is regarded as the result of an individual behavior in an individualistic culture (Morris, Menon, & Ames, 2001; Taylor, 1985). People's misbehavior in individualist societies may result in guilt and the loss of self-respect for individuals (Hofstede & Hofstede, 2005). On the other hand, people in collectivistic cultures view themselves as being interdependent within their in-groups, favoring collective efforts, group goals, and unquestioning loyalty (Hofstede, 1994; Ju & Power 1998; Triandis, 2001). Therefore, the responsibility for an event is attributed to groups in a collectivistic culture (Morris et al., 2001), and individual misbehavior tends to be associated with shame and loss of face for groups (Hofstede & Hofstede, 2005).

The different perception of the self also influences communication styles. According to Gudykunst and Nishida (1986) and Gudykunst, Ting-Toomey, and Chua (1988), an individualistic culture mostly entails low-context communication while a collectivist culture involves more high-context communication. Hall (1976) determined that culture can be identified as a high- or low-context culture based on communication style. High-context and low-context are relative concepts on a continuum, where some cultures place at a higher or lower ends of the continuum. Context means "the information that surrounds an event" (Hall & Hall, 1989, p. 6), and the level of context determines whether the meaning is contained in a message itself or outside the context. In a high-context culture (e.g., South Korea, Japan,

Arabian countries), communication involves indirect and implicit messages (Hall, 1976) and not everything is stated explicitly in writing or speech (Nishimura, Nevgi, & Tella, 2008). Non-verbal communication cues, closeness of relationship, and sociocultural contexts such as social hierarchy or norms greatly influence the communication process in a high-context culture (Hall & Hall, 1989; Kim, Pan, & Park, 1998). For example, if people share a similar background, it would be easier for them to understand the unsaid meaning and get to the point of the messages while avoiding potential misunderstandings. The focus of communication in a high-context culture is on listeners, who need to or are expected to "read between the lines" to get the true meaning of the message (Gudykunst & Nishida, 1994). In contrast, in a low-context culture (e.g., the United States, Germany, and other Northern European countries), communication uses direct and explicit messages in which most of the information is transmitted as a part of the message (Hall, 1976). The interpretation of the message tends to be univocal; therefore, the focus of communication is on the speaker (Gudykunst & Nishida, 1994). The listeners' different backgrounds or diverse contexts may not affect the interpretation of the message because what a speaker expresses is actually what he or she intended.

The connection between individualistic culture-low context communication and collectivist culture-high context communication makes sense when considering that people in a collectivist culture recognize themselves as members of their in-groups. Relationship is another context in communication; thus, communication in a collectivist culture involves a higher level of context. On the other hand, communication in an individualistic culture mainly concerns whether the message itself is well delivered as people in such a culture care less about how the relational context affects the interpretation of the message.

An apology statement consists of highly articulated language to resolve conflict within a society. As language is one of the important forms of culture, apology and culture are closely interrelated.

Corporate Apology and Cultural Differences

A corporate apology statement is supposed to reflect the prevailing values in a particular society and follow its accepted social norms. The same text may be interpreted differently across cultures (Janssens, Lambert, & Steyaert, 2004). In other words, cultural contexts affect the language used to deliver similar content. For example, Ju and Power (1998) compared apology statements from the presidents of the United States and South Korea. Both statements made a clear apology while admitting responsibility and expressing sorrow. However, each apology generated different public responses in the United States and South Korea; the apology statement from South Korea did not make people feel better while the apology from the United States was a success. Among several possible explanations, the authors pointed out that the efficacy of the apology statement did not work in South Korea because people in collectivist cultures think words are less important and think highly of showing empathy.

Cultural differences also affect the function of apologies. For example, Maddux et al. (2011) found that people in an individualistic culture (e.g., the United States) tended to regard apologies as analytical statements to assess blame, while those in a collectivistic culture (e.g., Japan) viewed apologies as a mean of expressing remorse. The results align with the idea that an individualistic culture often uses explicit expressions, avoiding any

uncertainty (low-context message), while a collectivist culture focuses more on the sociocultural context of communication (high-context message).

The main research question of this study is whether the cultural differences in value orientation and communication style appear in an apology statement when cyber-security breaches threaten the corporate reputation. The communication style of a high- or low-context culture may result in differences in expressing the four components of an apology. In addition, organizations from a collectivist culture may tend to use more excuses when apologizing because reducing responsibility can help save face (Hofstede & Hofstede, 2001). Furthermore, two different cultures will recognize the function of an apology differently: individualistic cultures may use an apology to provide facts in an analytical manner whereas collectivistic cultures are more likely to use one to express an organization's concern and sympathy in a crisis situation. Lastly, the individualist–collectivist cultural dimension may affect who appears as an organizational representative in an apology. Individualistic societies are supposed to present an organizational representative as an independent self and individual whereas collectivistic societies tend to use both an interdependent self and collectives to represent an organization.

Based on the literature reviewed, this study asks the following research questions.

Research question 1: What are the overall characteristics of organizations and cyber-security breaches?

Research question 2: Is there any difference between the United States (low-context culture) and South Korea (high-context culture) in terms of the characteristics of apologies (responsibility admittance, sympathetic expression, compensation, and

reassurance) appearing in official statements when cyber-security breaches threaten corporate reputation?

Research question 3: Is there any difference between the United States (individualistic culture) and South Korea (collectivistic culture) in use of excuse in apologies?

Research question 4: Is there any difference between the United States (individualistic culture) and South Korea (collectivistic culture) in the function of apologies?

Research question 5: Is there any difference between the United States (individualistic culture) and South Korea (collectivistic culture) when describing organizational representation in apologies?

CHAPTER 3. METHODS

A content analysis was conducted to examine the research questions. The samples for this study were composed of apology statements officially published by organizations.

Sample

This study chose the United States (individualistic and low-context culture) and South Korea (collectivistic and high-context culture) as the target countries. Apart from the differences in the cultural dimension, the two nations are similar in terms of internet infrastructure. For example, both countries are known for their high rate of Internet access, at 74% for the United States and 89% for South Korea (International Telecommunication Union, 2016), and have experienced mega-data breach crises that leaked large proportions of their populations' personal data in the 2000s.

The unit of analysis in this research is a written statement officially released by an organization to handle a cyber-security breach crisis in the United States or South Korea from 2008 to 2016. The statements included official website announcements, email letters, official blog posts, and so on. To avoid duplication, the study analyzed the original version of the statements; updated versions were not included in the sample.

To compose a sampling frame with the apology statements, this research implemented two different types of selection process for each country: cyber-security breach incident selection and apology statement selection.

For the incident selection for organizations in the United States, this study used a website (http://breachlevelindex.com) called the Gemalto Breach Level Index. The website

provides data breach databases and regularly updates the list of cyber-security breaches per country around the world. The list also includes a risk score for each crisis, which ranks each crisis case from highest to lowest. The total number of data breaches in the database was more than a hundred since 2013.

To get an official apology statement for each case from the United States, this study searched each incident from the one with the highest risk score. Cases were removed from the sample (1) if the organization did not release any written apology statement or (2) it was impossible to find the original copy of the apology statement. For example, if the company originally released the public apology statement on their official website and it was still accessible, the apology statement was included in the study. If the apology statement was not found from the official website, other sources such as related news articles, open sources from legal organizations, or postings from blogs were used to obtain the original apology statement issued by the organization.

The data breach database by Gemalto Breach Level Index only provided 20 cases for Korean organizations, which was not sufficient to provide a sampling frame of apology statements from Korean organizations. To compose a sampling frame for data breach cases in Korea, this study explored all the images that appeared when using the search terms of "personally identifying information breach cases" and "statement of apology for personally identifying information breach cases" via Google's image search feature. Duplicate statements were not included.

The final number of 108 official statements included 54 from each country. From the Google image search for the apology statements from South Korea, the total number of statements was 54 after eliminating the duplicates. The apology statement selection process

for organizations in the United States stopped when the 54th statement was found to match the number of cases for both countries for a better comparison.

Operationalization of Variables

The descriptive variables such as country, industry, source of breach, and type of breach were adopted from the Gemalto Breach Level Index. Country was coded as 1 = the United States and 2 = South Korea. Industry was coded as 0 = education, 1 = financial, 2 = government, 3 = healthcare, 4 = retail, 5 = technology, and 6 = others. Source of breach was coded as 0 = accidental loss, 1 = malicious insider, 2 = malicious outsider, and 3 = others. Type of breach was coded as 0 = nuisance, 1 = account access, 2 = financial access, 3 = identity theft, and 4 = existential data.

Responsibility admittance was coded as 0 = absence of responsibility admittance, 1 = presence of passive responsibility admittance, and 2 = presence of active responsibility admittance. Passive responsibility was coded when organizations made general apologies for what happened without specifying responsibility attribution (e.g., "We are sorry for the incident. . . ."). A statement was coded as active only when responsibility admittance explicitly appeared in the statement (e.g., "We take full responsibility. . . ." or "We admit our fault in. . . .").

Sympathetic expression was coded as 0 = absence of sympathetic expression, 1 = presence of low sympathetic expression, and 2 = presence of high sympathetic expression. A statement was coded as a low sympathetic expression when phrases simply acknowledged victims' feelings, pain, or frustration about their loss of personal information (e.g., "We are sorry/regretful for your concern/frustration/inconveniences. . . ."). A statement was coded as

a high sympathetic expression when phrases explicitly mentioned a connection between an organization's sympathy and victims' feelings, pain, or frustration about their loss of personal information (e.g., "Your pain is our pain. . . ." or "We join/understand your pain/frustration. . . .").

Compensation was coded as 0 = absence of compensation and 1 = presence of compensation. A statement was coded as having a presence of compensation when it explicitly offered free privacy protection consultation, service upgrades, discounted fees, and so on.

Reassurance was coded as 0 = absence of reassurance and 1 = presence of reassurance. A statement was coded as having a presence of reassurance when it explicitly promised innovating, reforming, or restructuring the system to prevent future data breaches (e.g., "We assure you that we will do everything we can to further secure your data. . . ." or "We will do our best to avoid a similar breach from reoccurring. . . .").

Use of excuse was coded as 0 = absence of excuse and 1 = presence of excuse. A statement was coded as having a presence of excuse when organizations emphasized inevitable circumstances under which data breach crises could happen regardless of their devotion in protecting personal data or when they pose themselves as a victim of the crisis too (e.g., "Despite our efforts and the state-of-the-art security system, this data breach happened. . . ." or "We were the victims of. . . .").

Function of apology was operationalized as either analytic accounts or expression of concern and sympathy in the first paragraph of an apology, as the opening paragraph is supposed to provide readers with the initiative to continue reading. The introduction should capture an indifferent reader's attention with the most important messages that the

organization wants to deliver. The variable was coded as 0 = providing analytic accounts, 1 = expressing concern and sympathy, and 2 = others. Analytic accounts were coded when organizations provided detailed information, such as how the data breach incidents occurred and what the corporation did during the crisis situation in the opening paragraph of an apology. Expression of concern and sympathy was coded when organizations made notions about their concern and compassion for the victims in the first paragraph of an apology.

Organizational representation in an apology was operationalized as the signing authority of an official statement. It was coded as 0 = CEO or president, 1 = all members of the organization, 2 = name of organization, 3 = other managers (public relations head, human resources manager, or IT manager), and 4 = unknown.

Inter-Coder Reliability

Two coders recruited from a large Midwestern research university were trained to code the components of apology (responsibility, sympathy, compensation, reassurance), use of excuse, function of apology, and organizational representation in official apology statements. A pre-test was conducted for the coding scheme to meet the acceptable inter-coder reliability using 20% of all statements. Two coders studied the codebook (see Appendix B) and coded the content independently. Based on the results, the codebook was revised and elaborated until inter-coder reliability for each variable reached an acceptable level of .80 or higher. Using Holsti's formula, the inter-coder reliability coefficients for all variables ranged from 0.83 to 0.96 (see Table 1).

Table 1.

Results of Inter-coder Reliability of Variables

Variables	Reliability	Variables	Reliability
Descriptive variables		Others	
Industry	0.96	Use of excuse	0.96
Source of breach	0.93	Function of apology	0.94
Type of breach	0.93	Organizational representation	0.95
Component of apology			
Responsibility	0.83		
Sympathy	0.83		
Compensation	0.91		
Reassurance	0.86		

Note. The percentage agreement was calculated based on Holsti's formula.

In order to ensure the reliability of the coding sheets in two different languages (English and Korean), the original coding sheet in English was translated into Korean. It was then re-translated into English by another translator. Both translators were bilingual and fluent in both languages. Finally, the original version of the coding sheet was compared to the re-translated version, and there seemed to be no issues in using the original coding sheet.

CHAPTER 4. FINDINGS

Ultimately, 108 official written statements—54 statements each from the United States and South Korea—were analyzed. For research question 1, the descriptive statistics for industry, source, and type of data breaches were as follows (see Table 2). The most frequent area of data breaches was retail, accounting for 26% with 28 cases, followed by technology (14%, 15 cases) and healthcare (12%, 13 cases). Organizations of education, finance, and government combined were 22%. Meanwhile, 79% of the incidents were caused by malicious outsiders, indicating that hacking activity was the most common cause of a data breach crisis. Identity theft (71%), account access (14%), and financial access (12%) were the most prevalent types of incidents.

Table 2.

Count and Percentage for Country, Industry, Source, and Type of Breach (N = 108)

Variables	% (Count)	Variables	% (Count)
Country		Source of Breach	
United States	50.0 (54)	Accidental Loss	8.3 (9)
South Korea	50.0 (54)	Malicious Insider	8.3 (9)
	100.0 (108)	Malicious Outsider	78.7 (85)
Industry		Unknown	4.6 (5)
Education	3.7 (4)		100.0 (108)
Financial	10.2 (11)	Type of Breach	
Government	8.3 (9)	Nuisance	0.9 (1)
Healthcare	12.0 (13)	Account Access	13.9 (15)
Retail	25.9 (28)	Financial Access	12.0 (13)
Technology	13.9 (15)	Identity Theft	71.3 (77)
Others	25.9 (28)	Existential Data	1.9 (2)
	100.0 (108)		100.0 (108)

For research question 2, Table 3 presents chi-square tests of the four components of apology (responsibility, sympathy, compensation, reassurance) by different cultural origins (individualistic versus collectivistic). Presence was recoded for responsibility and sympathy by combining passive–active responsibility admittance and low–high sympathetic expression.

After combining both passive and active responsibility admittance, the result showed that the responsibility admittance was significantly more visible in the statements from South Korea (67%) while more than half of the statements from the United States did not show any intention of taking responsibility for the incidents (57%; $\chi^2 = 5.380$, $df = 1$, $p < .05$).

After combining low and high sympathetic expression, 63% of the statements from the United States and 72% of the statements from South Korea used sympathetic expression. However, the difference was not significant ($\chi^2 = 0.676$, $df = 1$, $p < .05$).

With passive and active responsibility admittance separated, responsibility admittance was significantly more visible in the statements from South Korea for both active and passive manner (20% and 40%, respectively) while more than half of the statements from the United States did not show any intention of taking responsibility for the incidents (57%; $\chi^2 = 10.028$, $df = 2$, $p < .05$).

With low and high sympathetic expression separate, we conducted Fisher's exact test because some of the categories were smaller than 10. The test was used to get a *p*-value instead of using the chi-square test when any cells of the contingency table were less than 5 or 10. The interpretation of the *p*-value was the same as the chi-square test. Organizations from both countries appeared to be sparing with their sympathetic expressions: 57% of the statements from the United States showed a low level of sympathy for those affected while 37% of the statements from the United States did not express any sympathy. On the other

hand, 72% of the statements from South Korea expressed low sympathy while 28% of the statements from South Korea did not show any sympathy ($p < .05$).

For compensation, more than half of the statements from the United States mentioned compensation (56%) compared to only 11% from South Korea ($\chi^2 = 22.042$, $df = 1$, $p < .05$).

Regarding reassurance, 56% of the statements from the United States provided reassurance while 89% of the statements from South Korea showed reassurances that data protection would prevent similar crises in the future ($\chi^2 = 13.338$, $df = 1$, $p < .05$).

Table 3.

Cross-Tabulation of Responsibility, Sympathy, Compensation, and Reassurance by Country

(N = 54 for each country)

Variables	% (*n*)		Chi-squared test		
	United States	South Korea	χ^2	*df*	*p*
Responsibility (passive-active admittance combined)					
Absence	57.4 (31)	33.3 (18)	5.380	1	.02
Presence*	42.6 (23)	66.7 (36)			
	100.0 (54)	100.0 (54)			
Sympathy (low-high expression combined)					
Absence	37.0 (20)	27.8 (15)	0.676	1	.41
Presence**	63.0 (34)	72.2 (39)			
	100.0 (54)	100.0 (54)			
Responsibility					
Absence	57.4 (31)	33.3 (18)			
Passive responsibility admittance	38.9 (21)	46.3 (25)	10.028	2	.01
Active responsibility admittance	3.7 (2)	20.4 (11)			
	100.0 (54)	100.0 (54)			
Sympathy					
Absence	37.0 (20)	27.8 (15)			
Low sympathetic expression	57.4 (31)	72.2 (39)	4.629	2	.00***
Highly sympathetic expression	5.6 (3)	0.0 (0)			
	100.0 (54)	100.0 (54)			
Compensation					
Absence	44.4 (24)	88.9 (48)	22.042	1	.00
Presence	55.6 (30)	11.1 (6)			
	100.0 (54)	100.0 (54)			
Reassurance					
Absence	44.4 (24)	11.1 (6)	13.338	1	.00
Presence	55.6 (30)	88.9 (48)			
	100.0 (54)	100.0 (54)			

* Presence was re-coded by combing active and passive responsibility admittance.

** Presence was re-coded by combining high and low sympathetic expression.

*** *P*-value became lower than any significant α when conducting Fisher's test instead of chi-squared test due to the small observations in some categories, decreasing from 0.1 to 2.2e-16.

For research questions 3 through 5, Table 4 shows the chi-square tests of use of excuse, function of apology, and organizational representation in apology by cultural difference (individualistic versus collectivistic). Regarding the use of excuse in apology, more than 46% of statements from South Korea excused the companies while only 15% of statements from the United States attempted to evade responsibility (χ^2 = 11.171, *df* = 1, *p* < .05).

Regarding the function of apology, statements from the United States tended to provide analytic accounts in the first paragraph (72%) whereas apology statements from South Korea tended to express concern or sympathy for the victims first (74%; χ^2 = 38.833, *df* = 2, *p* < .05).

As for organizational representation, a Fisher's test was conducted due to the small observations in some categories. The results showed that the most visible organizational representative was CEO and president (61%), followed by other managers (OR, HR, or IT) (15%) in the statements from the United States whereas it was unidentifiable (43%) or appeared as all members of the organization (32%) in the statements from South Korea (*p* < .05).

Organizational representation was recoded by combining CEO or president and other managers (individuals) as well as all members of the organization and name of the organization (collectives). The difference between the two countries was still clear: 76% of the statements from the United States was delivered by an individual while only 14% of the statements from South Korea was presented by an individual representative (χ^2 = 42.730, *df* = 1, *p* < .05).

Table 4.

Cross-Tabulation of Use of Excuse, Function of Apology, and Organizational Representation by Country (N = 54 for each country)

Variables	% (*n*)		Chi-squared test		
	United States	South Korea	χ^2	*df*	*p*
Use of excuse					
Absent	85.2 (46)	53.7 (29)	11.171	1	.00
Present	14.8 (8)	46.3 (25)			
	100.0 (54)	100.0 (54)			
Function of apology					
Providing analytic accounts	72.2 (39)	24.1 (13)			
Expressing concern/sympathy	14.8 (8)	74.1 (40)	38.830	2	.00*
Others	13.0 (7)	1.9 (1)			
	100.0 (54)	100.0 (54)			
Organizational Representation					
CEO or president	61.1 (33)	13.0 (7)			
All members of organization	1.9 (1)	31.5 (17)			
Name of organization	3.7 (2)	11.1 (6)	43.688	4	.00**
Other managers (OR, HR, or IT)	14.8 (8)	1.9 (1)			
Unknown	18.5(10)	42.6 (23)			
	100.0 (54)	100.0 (54)			
Organizational Representation (Combined)					
Individual***	75.9 (41)	13.8 (8)	42.730	2	.00
Collectives****	5.6 (3)	42.6 (23)			
Unknown	18.5 (10)	42.6 (23)			
	100.0 (54)	100.0 (54)			

* *P*-value increased to 6.288e-10 when conducting Fisher's test instead of Chi-squared test due to the small observations in some categories, however, was still lower than any significant α.

** *P*-value was still lower than any significant α when conducting Fisher's test instead of Chi-squared test due to the small observations in some categories.

*** Individual was re-coded by combing CEO or president, and other managers (OR, HR, or IT).

**** Collectives was re-coded by combining all members of organization, and name of organizations.

CHAPTER 5. DISCUSSION

Significance of the Study

The results of this study provides several implications about crisis responses to cyber-security breaches. First, identity theft is the most common type of cyber-security breach, and almost every industry is vulnerable to this risk. E-commerce and digital payment rapidly increase retail shopping online, but cyber-security technology does not necessarily catch up to the speed of transactions. Healthcare organizations digitize and share sensitive patient information; even the technology industry, including social media companies, are vulnerable to hackers and malicious insiders. People live in risky societies where the severity of risk and vulnerability of cyber security are substantially high while response and self-efficacy are relatively low. In this climate, public relations professionals face cyber-security crises more frequently than before, regardless of the type of organization and industry they represent.

Second, the fact that the internal security vulnerability of the organizations was the second major factor (18%) in data breach crises should be a wake-up call to many organizations: The combined proportion of malicious insiders (9%) and accidental loss (9%) accounted for almost one-fifth of all breach incidents. Usually organizations assume that cyberattacks are perpetrated by external factors such as professional hackers and malicious outsiders. This study confirms this general assumption, but it also reveals that betrayal by employees and inadvertent mistakes should not be ignored. This can serve as a reminder for organizations of the sheer importance of internal public relations in building and retaining mutually beneficial relationships with their employees. Winning the hearts and minds of

employees is a front-line battle for organizations to protect themselves, especially with regard to cyber-security breaches.

Third, different cultural origins affect the characteristics of apology. Our study revealed that South Korean organizations were less hesitant to admit responsibility in both passive and active manners and express higher sympathy. In addition, the statements from South Korea displayed reassurance by vigorously promising that a data breach would never happen again. One possible explanation is that people from a high-context culture (collectivist culture) tend to be more effective and intuitive in conflict situations while members from a low-context culture (individualistic culture) are likely to be more factual and inductive (Ting-Toomey, 1985). Organizations in South Korea might have expected affective response (e.g., anger, anxiety) from their public and, thus, chose to focus on using strategies to reduce the hostile feelings. Another possible explanation for the difference can be understood by how people from each country manage conflict. Power distance is the extent to which the less powerful individual of an organization accepts the power unequally distributed within the organization (Hofstede & Hofstede, 2005). When power distance is high, subordinates of the organization are unlikely to contradict their bosses who have more power within an organization. Usually, a collectivist culture has a higher power distance than individualistic culture. In South Korea, there is a saying that “customers are the king”; it reflects the high power distance in the market and organization in South Korea.

The differences are more distinctive when it comes to compensation; most of the corporations from the United States clearly mentioned compensation while many of the organizations from South Korea did not. It is interesting that the level of responsibility admittance and sympathetic expression were not proportionate to the intention of providing

compensation. However, compensation will not be effective unless it is provided with substantial responsibility admittance and sympathetic expression.

Fourth, the use of excuse, function of apology, and organizational representation differed considerably depending on the national culture. The use of excuses was more visible in the statements from South Korea. The level of reputational damage is closely related to the amount of responsibility that an organization has to do with the crisis (Coombs, 2007b; Coombs, 2012). By reducing the responsibility, an organization can minimize the negative impact on its reputation. This finding can be interpreted as organizations in South Korea trying harder to avoid blame.

Individuals from a high-context culture are more likely to prefer analytical accounts from messages because they prefer to manage crises in a factual and axiomatic style (Ting-Toomey, 1985). On the other hand, people from a low-context culture are more likely to favor messages that touch their feelings as they have more effective manners with conflicts (Ting-Toomey, 1985). The different audience expectations are likely to be differently reflected in organizations' messages to the public. The finding of the study concurs with this argument. Statements from the United States (low-context culture) emphasized delivering analytic accounts while statements from South Korea (high-context culture) tended to express their concern for the incidents and show sympathy for the victims.

Statements from the United States (individualistic culture) were also more likely to refer to individual representatives, such as CEOs, presidents, and other managers (PR, HR, and IT). On the other hand, statements from South Korea (collectivist culture) tended to use collective group identities, such as all members of an organization and the name of an organization. This finding provides evidence related to how individualistic and collectivist

cultures form different individual and organizational identities, suggesting the need to select organizational representation based on this finding.

There is no right or wrong in terms of cultural differences because every culture has its own systems of values, beliefs, and norms. One lesson we can learn from the findings of this study is the importance of tailoring apology messages to satisfy cultural cues and expectations. An apology issued during a crisis should be sincere in order to comfort people's anger and eliminate uncertainty. A keen understanding about cultural cues and expectations of the public is a sure path toward effective public relations.

Finally, the relationship between responsibility admittance and the use of an excuse as a crisis response strategy may be overlooked when considering the impact of an apology statement. The purpose of making an excuse is to reduce one's responsibility (Benoit & Drew, 1997); thus, one might expect a negative relationship between active responsibility and excuses. However, at least from this study, Korean organizations often showed both active responsibility and excuses. In other words, even when organizations fully accepted responsibility, they still tried to avoid further blame by saying that there could have been no way to prevent the crisis from occurring because they had done everything they could.

Limitations of the Study

There are several limitations to be discussed in this research. First, this study is based on the quantitative content analysis and descriptive in nature. The possible causal relationship among the efficacy of apology statement, the components of apology, and culture is not identifiable using the method.

When comparing the United States and South Korea, there may be factors other than cultural differences that explain the differences in results found in this study; these potential confounding factors were not identified or controlled for in the current study. The type of industry and type of data breach can mediate the effect of cultural differences. For example, a financial organization's primary goal is to protect customers' data as people are increasingly worried about cyber-security issues related to their financial data, such as bank accounts. When financial information is stolen, the organization will try hard to manage the crisis situation, using all of the apology components regardless of cultural differences.

Finally, selection bias when identifying cyber-breach crises and sampling bias when searching for apology statements may have occurred. The bias can be reduced by constructing sampling frames based on the same criteria for each country. As previously stated, different methods were used for the United States and South Korea in the data breach case selection process and apology statement selection process. The number of samples from each country was also intentionally matched to ensure a numerical equivalence for both samples. The different criteria to compose each country's sampling frame was reasonable, but could not avoid potential selection bias.

Suggestions for Future Research

Hopefully, the findings of the study can lead to more rigorous relationship testing in future studies. A future study can use an experimental setting to directly measure the impact of cultural differences on apology. For example, efficacy of a certain type of apology statement can be tested by engaging with subjects from different cultures.

Another interesting study can involve testing interrelationships among the four apology components and use of excuse. Lee and Chung (2012) empirically tested a different type of apology statement with different levels of responsibility admittance and sympathetic expression, and found out no interaction between the two components in soothing public anger (Lee & Chung, 2012); however, future studies can attempt to measure the efficacy of apology statements using different combinations of apology components. For example, this study found that responsibility admittance and the use of an excuse often appear together; therefore, future studies can look into if an apology statement using both strategies is more effective than when showing only responsibility admittance in protecting an organization's reputation. Some audiences may agree with the reason why the organization makes excuses while others might think the apology with the excuse is not sincere.

Future studies should also adopt the situation social crisis model (Coombs, 2007b) to identify the optimal combination of apology statements. The optimal combination of apology statements to minimize reputational damage will be different based on the source of the cyber-security breach. For example, people think that an organization is less responsible for cyber-security breaches if the breach is caused by malicious hacking activities targeting the organization. In this case, the organization may not need to excessively admit its fault in the apology statement, but rather can focus on expressing sympathy, providing compensation, or reassuring its public. However, if the cyber-security breach occurs due to the organization's malpractice, making the organization responsible for the crisis, the organization will need to clearly accept its responsibility before talking about sympathy, compensation, and reassurance.

Finally, future studies can use data breach cases from the same source, if possible, or collect data using the identical selection method for both countries to avoid sampling bias. Future researchers could also investigate different countries, which would enable random sampling.

REFERENCES

Alsop, R. J. (2006). *The 18 immutable laws of corporate reputation: Creating, protecting and repairing your most valuable asset*. London, England: Kogan Page Publishers.

Andoh-Baidoo, F. K., & Osei-Bryson, K. M. (2007). Exploring the characteristics of Internet security breaches that impact the market value of breached firms. *Expert Systems with Applications, 32*(3), 703-725.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management*, *6*(4), 279-314.

Barton, L. (1993). *Crisis in Organizations: Managing and Communicating in the Heat of Chaos. Cincinnati*. OH: South-Western Publishing Company.

Benoit, W. L. (1997). Image repair discourse and crisis communication. *Public Relations Review*, *23*, 177-186.

Benoit, W. L. (2015). *Accounts, excuses, and apologies: A theory of image restoration strategies* (2nd ed.). Albany, NY: State University of New York Press.

Benoit, W. L., & Drew, S. (1997). Appropriateness and effectiveness of image repair strategies. *Communication Reports*, *10*(2), 153-163.

Boyes, H. (2015). Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review*, *5*(4), 28-34.

Braaten, D. O., Cody, M. J., & DeTienne, K. B. (1993). Account episodes in organizations: Remedial work and impression management. *Management Communication Quarterly*, *6*(3), 219-250.

Coombs, W. T. (1995). Choosing the right words the development of guidelines for the selection of the "appropriate" crisis-response strategies. *Management Communication Quarterly*, *8*(4), 447-476.

Coombs, W. T. (2000). Designing post-crisis messages: Lessons for crisis response strategies. *Review of Business*, *21*(3/4), 37-41.

Coombs, W. T. (2007a). Crisis management and communications. *Institute for public relations*, *4*(5), 6.

Coombs, W. T. (2007b). 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. (2010). Parameters for crisis communication. In Coombs, W. T. & Holladay, S. J. (Eds.), *The handbook of crisis communication* (pp. 17-53). Hoboken, NJ: Wiley-Blackwell.

Coombs, W. T. (2012). *Ongoing crisis communication: Planning, managing, and responding* (3rd ed.). Thousand Oaks, CA: Sage.

Coombs, W. T., & Holladay, S. J. (2005), An Exploratory Study of Stakeholder Emotions: Affect and Crises. In Neal M. Ashkanasy, Wilfred J. Zerbe, Charmine E.J. Härtel (Eds.), *Research on Emotion in Organizations* (pp.263-280). Bingley, England: Emerald Group Publishing.

Coombs, W. T., & Holladay, S. J. (2008). Comparing apology to equivalent crisis response strategies: Clarifying apology's role and value in crisis communication. *Public Relations Review*, *34*(3), 252-257.

Davis, G., Garcia, A., & Zhang, W. (2009). Empirical analysis of the effects of cyber security incidents. *Risk analysis*, *29*(9), 1304-1316.

DiFonzo, N., & Bordia, P. (2000). How top PR professionals handle hearsay: Corporate rumors, their effects, and strategies to manage them. *Public Relations Review*, *26*(2), 173-190.

DiFonzo, N., & Bordia, P. (2007). Rumor, gossip and urban legends. *Diogenes*, *54*(1), 19-35.

Escalas, J. E., & Stern, B. B. (2003). Sympathy and empathy: Emotional responses to advertising dramas. *Journal of Consumer Research*, *29*(4), 566-578.

Fearn-Banks, K. (2017). *Crisis communications: A casebook approach* (5th ed.). New York, NY: Routledge.

Fingarette, H. (1985). Victimization: A legalist analysis of coercion, deception, undue influence, and excusable prison escape. *Washington & Lee Law Review*, *42*(1), 65-118.

Fink, S. (1986). *Crisis management: Planning for the inevitable*. New York, NY: American Management Association.

Folkman, S., Lazarus, R. S., Dunkel-Schetter, C., DeLongis, A., & Gruen, R. J. (1986). Dynamics of a stressful encounter: Cognitive appraisal, coping, and encounter outcomes. *Journal of personality and social psychology*, *50*(5), 992-1003.

Fuchs-Burnett, T. (2002). Mass public corporate apology. *Dispute Resolution Journal*, *57*(2), 26-32.

Gill, K. (2000). The moral functions of an apology. *The Philosophical Forum. 31*(1), 11-27.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, *46*(7), 404-410.

Gonodo-Madikizel, P. (2003). Remorse, forgiveness, and re-humanization: 53 Stories form South Africa. *Journal of Humanistic Psychology*, *42*, 7-32.

Gudykunst, W. B., & Nishida, T. (1986). Attributional confidence in low-and high-context cultures. *Human communication research*, *12*(4), 525-549.

Gudykunst, W. B., & Nishida, T. (1994). *Bridging Japanese/North American differences* (Vol. 1). Thousand Oaks, CA: Sage.

Gudykunst, W. B., Ting-Toomey, S., & Chua, E. (1988). *Culture & interpersonal communication*. Newbury Park, CA: Sage.

Hall, E. T. (1976). *Beyond culture*. Garden City, NY: Anchor Press, Doubleday.

Hall, E. T., & Hall, M. R. (1989). *Understanding cultural differences*. Yarmouth, ME: Intercultural press.

Hearit, K. M. (2006). *Crisis management by apology: Corporate response to allegations of wrongdoing*. Mahwah, NJ: Lawrence Erlbaum Associates Publishers.

Hermann, C. F. (1963). Some consequences of crisis which limit the viability of organizations. *Administrative science quarterly*, *8*(1), 61-82.

Hermann, C. F. (Ed.). (1972). *International crises; insights from behavioral research*. New York, NY: Free Press.

Hofstede, G. (1984). The cultural relativity of the quality of life concept. *Academy of Management review*, *9*(3), 389-398.

Hofstede, G. (1994). The business of international business is culture. *International business review*, *3*(1), 1-14.

Hofstede, G. H., & Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations* (2nd ed.). Thousand Oaks, CA: Sage.

Hofstede, G., & Hofstede, G. J. (2005). *Cultures and organizations: Software of the mind.* (Revised and expanded 2nd ed.). New York, NY: McGraw-Hill.

Identity Theft Resource Center. Data breach reports 2016 (2017). Retrieved from http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf

International Telecommunication Union (2016). Percentage of Individuals Using the Internet. Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2016/Individuals_Internet_2000-2015.xls

Janssens, M., Lambert, J., & Steyaert, C. (2004). Developing language strategies for international companies: The contribution of translation studies. *Journal of World Business*, *39*(4), 414-430.

Jin, Y. (2009). The effects of public's cognitive appraisal of emotions in crises on crisis coping and strategy assessment. *Public Relations Review*, *35*(3), 310-313.

Jin, Y., Pang, A., & Cameron, G. T. (2007). Integrated crisis mapping: Towards a publics-based, emotion-driven conceptualization in crisis communication. *Sphera Publica*, *7*(7), 81-96.

Ju, J., & Power, M. R. (1998). Cultural differences in the efficacy of apologies. *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies*, *3*(1), 56-66.

Kiambi, D. M., & Shafer, A. (2016). Corporate Crisis Communication: Examining the Interplay of Reputation and Crisis Response Strategies. *Mass Communication and Society*, *19*(2), 127-148.

Kim, D., Pan, Y., & Park, H. S. (1998). High-versus low-context culture: A comparison of Chinese, Korean, and American cultures. *Psychology and Marketing*, *15*(6), 507-521.

Kim, S., Avery, E. J., & Lariscy, R. W. (2009). Are crisis communicators practicing what we preach?: An evaluation of crisis response strategy analyzed in public relations research from 1991 to 2009. *Public Relations Review*, *35*, 446–448.

Kluckhohn, C., & Kelly, W. H. (1945). The concept of culture. In Ralph Linton (ed.), *The science of man in the world crisis* (pp. 78-106). New York, NY: Columbia University Press.

Kroeber, A. L., & Kluckhohn, C. (1952). *Culture: A critical review of concepts and definitions*. Cambridge, MA: The museum.

Lang, A. (2000). The limited capacity model of mediated message processing. *Journal of communication*, *50*(1), 46-70.

Lazare, A, (2005). *On apology*. New York, NY: Oxford University Press.

Lazarus, R. S. (1966). *Psychological stress and the coping process*. New York, NY: McGraw-Hill.

Leape, L. L. (2012). Apology for errors: whose responsibility?. *Frontiers of health services management*, *28*(3), 3-12.

Lee, B. K. (2004). Audience-oriented approach to crisis communication: A study of Hong Kong consumers' evaluation of an organizational crisis. *Communication Research*, *31*, 600-618.

Lee, S., & Chung, S. (2012). Corporate apology and crisis communication: The effect of responsibility admittance and sympathetic expression on public's anger relief. *Public Relations Review*, *38*(5), 932-934.

Lucero, M., Tan Teng Kwang, A., & Pang, A. (2009). Crisis leadership: when should the CEO step up?. *Corporate Communications: An International Journal*, *14*(3), 234-248.

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures*, *9*(1-2), 3-31.

Lyon, L., & Cameron, G. T. (2004). A relational approach examining the interplay of prior reputation and immediate response to a crisis. *Journal of Public Relations Research*, *16*(3), 213-241.

Maddux, W. W., Kim, P. H., Okumura, T., & Brett, J. M. (2011). Cultural differences in the function and meaning of apologies. *International Negotiation*, *16*(3), 405-425.

Men, L. R. (2012). CEO credibility, perceived organizational reputation, and employee engagement. *Public Relations Review*, *38*(1), 171-173.

Morris, M. W., Menon, T., & Ames, D. R. (2001). Culturally conferred conceptions of agency: A key to social perception of persons, groups, and other actors. *Personality and Social Psychology Review*, *5*(2), 169-182.

Murray, E., & Shohen, S. (1992). Lessons from the Tylenol tragedy on surviving a corporate crisis. *Medical Marketing and Media*, *27*(2), 14-19.

Nishimura, S., Nevgi, A., & Tella, S. (2008). Communication style and cultural features in high/low context communication cultures: a case study of Finland, Japan and India. In A. Kallioniemi (Ed.). *Renovating and developing subject didactics. Proceedings of a subject-didactic symposium in Helsinki on Feb. 2, 2008.* Part 2 (pp. 783-796). Helsinki, Finland: University of Helsinki (Research Report).

Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis*, *31*(3), 497-512.

Ohbuchi, K. I., Kameda, M., & Agarie, N. (1989). Apology as aggression control: its role in mediating appraisal of and response to harm. *Journal of personality and social psychology*, *56*(2), 219-227.

Patel, A., & Reinsch, L. (2003). Companies can apologize: Corporate apologies and legal liability. *Business Communication Quarterly*, *66*(1), 9-25.

Pearlin, L. I., & Schooler, C. (1978). The structure of coping. *Journal of health and social behavior*, *19*(1), 2-21.

Ponemon Institute. (2015). Global Analysis. Retrieved from http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03053WWEN&attachment=SEW0305WWEN.P*DF*

Prakash, M., & Singaravel, G. (2015). An approach for prevention of privacy breach and information leakage in sensitive data mining. *Computers & Electrical Engineering*, *45*, 134-140.

Regester, M. (1989). Crisis management: What to do when the unthinkable happens. London: Hutchinson Business.

Robbennolt, J. K. (2003). Apologies and legal settlement: An empirical examination. *Michigan Law Review, 102*, 460-516.

Scott, M. B., & Lyman, S. M. (1968). Accounts. *American sociological review*, *33*(1), 46-62.

Switankowsky, I. (2000). Sympathy and empathy. *Philosophy today*, *44*(1), 86-92.

Taylor, C. (1985). Human agency and language. New York, NY: Holt, Rinehart & Winston.

Thomas, R. L., & Millar, M. (2008). The impact of failing to give an apology and the need-for cognition on anger. *Current Psychology*, *27*, 126-134.

Ting-Toomey, S. (1985). Toward a theory of conflict and culture. In W. B. Gudykunst, L. Stewart, & S. Ting-Toomey (Eds.), *Communication, culture and organizational processes* (pp. 71-86). Beverly Hills, CA: Sage.

Triandis, H. C. (2001). Individualism-collectivism and personality. *Journal of personality*, *69*(6), 907-924.

TRUSTe (2015). Consumer confidence privacy index. Retrieved from https://www.truste.com/resources/privacy-research/us-consumer-confidence-index-2015/

Turk, J. V., Jin, Y., Stewart, S., Kim, J., & Hipple, J. R. (2012). Examining the interplay of an organization's prior reputation, CEO's visibility, and immediate response to a crisis. *Public Relations Review, 38*(4), 574-583.

Tyler, L. (1997). Liability means never being able to say you're sorry: Corporate guilt, legal constraints, and defensiveness in corporate communication. *Management Communication Quarterly*, *11*(1), 51-73.

Tylor, E. B. (1871). *Primitive culture: researches into the development of mythology, philosophy, religion, art, and custom* (Vols. 1-2). London, England: John Murray.

Ulmer, R. R., Sellnow, T. L., & Seeger, M. W. (2014). *Effective crisis communication: Moving from crisis to opportunity* (3rd ed.). Thousand Oaks, CA: Sage

Veltsos, J. R. (2012). An analysis of data breach notifications as negative news. *Business Communication Quarterly*, *75*(2), 192-207.

APPENDIX

APPENDIX A

BREACH LEVEL INDEX

Gemalto and SafeNet, the world's leading company with the specialty in data, transaction, and identity protection solutions, provides the Breach Level Index which is a publicly-available database of data breaches from more than 40 countries. The BLI includes the type of data, the number of records breached, the source of the breach incidents and so on, and is available since 2013. Refer to http://breachlevelindex.com/ for further information.

APPENDIX B

CODEBOOK FOR CONTENT ANALYSIS OF CORPORATE STATEMENTS

Variable	Conceptual definition	Operational definition	Example
ID	Unique four digit number assigned to each statement		
Country	The country in which the statement was issued	0 = America 1 = South Korea	
Industry	The type of industry in which the corporates belongs to	0 = Education 1 = Financial 2 = Government 3 = Healthcare 4 = Retail 5 = Technology 6 = Other	
Source of breach	The source of data breach incidents	0 = Accidental Loss 1 = Hacktivist 2 = Malicious Insider 3 = Malicious Outsider 5 = Others	
Type of breach	The type of data breached	0 = Nuisance 1 = Account Access 2 = Financial Access 3 = Identity Theft 4 = Existential data	
Responsibility	Taking responsibility for causing the crisis situation or not being able to prevent it.	0 = Absence 1 = Passive responsibility admittance 2 = Active responsibility admittance	1 = “We apologize for this incident”, “We regret to inform you that ~” etc. 2 = “We didn’t live up to that responsibility”, “We feel deeply responsible for this incident” etc.
Sympathy	Phrases that shows	0 = Absence	1 = “We apologize for

	concern for victim's feelings, pain, or frustration about personal data loss	1 = Low sympathetic expression 2 = High sympathetic expression	the frustration/inconvenience/concern this incident may have caused" 2 = "We join you in pain and concern", "I share those feelings"
Compensation	Any kind of offer provided to victims to offset the negative impact of personal information loss	0 = Absence 1 = Presence	1 = "We are offering you a year of complimentary identity protection services at no cost"
Reassurance	Reassurance for non-repetition of future data breach crisis	0 = Absence 1 = present	1 = "To prevent a similar event from happening in the future", "We are taking additional steps to strengthen and enhance the security on our servers" etc.
Use of excuse	Type of account that denies full responsibility.	0 = Absence 1 = Present	1 = "Despite our efforts", "Although we did our best to secure your data safely" etc., (Unavoidability), "We were the victim of" etc. (victimization).
Function of apology	What apology primarily deliver its message to the readers	0 = Providing analytic accounts 1 = Expressing concern/sympathy 2 = Others	
Organizational representation	A person whose point of view is taken to deliver the message	0 = CEO or President 1 = All members of organization 2 = Name of organization 3 = Other managers (PT, HR, or IT) 4 = Unknown	

APPENDIX C

EXAMPLES OF APOLOGY STATEMENTS

C1. Examples of apology statements from the United States (Source: Anthem Inc., Target, Premera Blue Cross)

Anthem BlueCross BlueShield

Anthem was the victim of a sophisticated cyber attack –

Important message from Joseph Swedish, President and CEO

To our valued provider partner:

Safeguarding your patients' personal, financial and medical information is one of our top priorities, and because of that, we have state-of-the-art information security systems to protect your data. However, despite our efforts, Anthem was the target of a very sophisticated external cyber attack. These attackers gained unauthorized access to Anthem's Information Technology (IT) system and have obtained personal information from our current and former members such as their names, birthdays, medical IDs/Social Security numbers, street addresses, email addresses and employment information, including income data. Based on what we know now, there is no evidence that credit card, provider or medical information, such as claims, test results, or diagnostic codes were targeted or compromised.

Once the attack was discovered, Anthem immediately made every effort to close the security vulnerability, contacted the Federal Bureau of Investigation (FBI) and began fully cooperating with their investigation. Anthem has also retained Mandiant, one of the world's leading cybersecurity firms, to evaluate our systems and identify solutions based on the evolving landscape.

Anthem's own associates' personal information – including my own – was accessed during this security breach. We join you in your concern and frustration, and I assure you that we are working around the clock to do everything we can to further secure your data.

Anthem will individually notify current and former members whose information has been accessed. We will provide credit monitoring and identity protection services free of charge so that those who have been affected can have peace of mind. We have created a dedicated website - www.AnthemFacts.com - where members can access information such as frequent questions and answers. We have also established a dedicated toll-free number that both current and former members can call if they have questions related to this incident. That number is: 1-877-263-7995. As we learn more, we will continually update this website.

We want to personally apologize to you and your patients for what has happened, as I know you expect us to protect their information. We will continue to do everything in our power to make our systems and security processes better and more secure, and hope that we can earn back your trust and confidence in Anthem.

Sincerely,

Joseph R. Swedish

Joseph Swedish
President and CEO
Anthem, Inc.

Anthem Blue Cross and Blue Shield is the trade name of: In Colorado: Rocky Mountain Hospital and Medical Service, Inc. In Connecticut: Anthem Health Plans, Inc. In Indiana: Anthem Insurance Companies, Inc. In Kentucky: Anthem Health Plans of Kentucky, Inc. In Maine: Anthem Health Plans of Maine, Inc. In Missouri (excluding 30 counties in the Kansas City area): RightCHOICE® Managed Care, Inc. (RIT), Healthy Alliance® Life Insurance Company (HALIC), and HMO Missouri, Inc. RIT and certain affiliates administer non-HMO benefits underwritten by HALIC and HMO benefits underwritten by HMO Missouri, Inc. RIT and certain affiliates only provide administrative services for self-funded plans and do not underwrite benefits. In Nevada: Rocky Mountain Hospital and Medical Service, Inc. In New Hampshire: Anthem Health Plans of New Hampshire, Inc. In Ohio: Community Insurance Company. In Virginia (serving Virginia excluding the city of Fairfax, the town of Vienna and the area east of State Route 123): Anthem Health Plans of Virginia, Inc. In Wisconsin: Blue Cross Blue Shield of Wisconsin ("BCBSWi") underwrites or administers the PPO and indemnity policies; Compcare Health Services Insurance Corporation ("Compcare") underwrites or administers the HMO policies; and Compcare and BCBSWi collectively underwrite or administer the POS policies. Independent licensees of the Blue Cross and Blue Shield Association. ® ANTHEM is a registered trademark of Anthem Insurance Companies, Inc. The Blue Cross and Blue Shield names and symbols are registered marks of the Blue Cross and Blue Shield Association.

Dear Target Guests,

As you have probably heard, Target learned in mid-December that criminals forced their way into our systems, gaining access to guest credit and debit card information. As a part of the ongoing forensic investigation, it was determined last week that certain guest information, including names, mailing addresses, phone numbers or email addresses, was also taken.

Our top priority is taking care of you and helping you feel confident about shopping at Target, and it is our responsibility to protect your information when you shop with us.

We didn't live up to that responsibility, and I am truly sorry.

Please know we moved as swiftly as we could to address the problem once it became known, and that we are actively taking steps to respond to your concerns and guard against something like this happening again. Specifically, we have:

1. Closed the access point that the criminals used and removed the malware they left behind.
2. Hired a team of data security experts to investigate how this happened. That effort is ongoing and we are working closely with law enforcement.
3. Communicated that our guests will have zero liability for any fraudulent charges arising from the breach.
4. Offered one year of free credit monitoring and identity theft protection to all Target guests so you can have peace of mind.

In the days ahead, Target will announce a coalition to help educate the public on the dangers of consumer scams. We will also accelerate the conversation–among customers, retailers, the financial community, regulators and others–on adopting newer, more secure technologies that protect consumers.

I know this breach has had a real impact on you, creating a great deal of confusion and frustration. I share those feelings. You expect more from us and deserve better.

We want to earn back your trust and confidence and ensure that we deliver the Target experience you know and love.

We are determined to make things right, and we will.

Sincerely,

Gregg Steinhafel

Gregg Steinhafel, chairman, president and chief executive officer, Target

As you may have heard in media reports, Premera Blue Cross ("Premera") publicly disclosed that cyber attackers gained unauthorized access to a data base that stores member information. Premera is taking this issue very seriously and is working with the FBI on investigating the attack. Blue Cross and Blue Shield of Oklahoma ("BCBSOK") is neither owned nor operated by Premera. Premera is a separate company that operates in Washington and Alaska. BCBSOK works with Premera to administer certain aspects of your health care benefit; you may have received health care services in one of these states which is why your information was in their system.

The privacy and security of our member's information is a top priority at BCBSOK. We continue to safeguard your personal information through robust privacy and security measures.

The following is a copy of the letter that the President and CEO of Premera will be sending to individuals associated with BCBSOK that were affected by this incident.

Dear Member:

I am writing to inform you that Premera Blue Cross ("Premera") was the target of a sophisticated cyberattack, and that some of your personal information may have been accessed by the attackers. As part of our investigation, we notified the FBI and are coordinating with their own investigation into this attack.

We are Premera take this issue seriously and regret the concern it may cause. I'm writing to provide you information on the steps we are taking to protect you and your information moving forward.

What happened?

On January 29, 2015, we discovered that cyberattackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on May 5, 2014. We worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remove the infection created by the attack on our IT systems.

Our investigation determined that the attackers may have gained unauthorized access to your information, which could include your name, address, telephone number, date of birth, member identification number, Social Security number if it is part of your member identification number or patient identifier, email address if you provided it to us, and claims information, including clinical information. The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately.

Why does Premera have your information?

We believe you have or had health plan coverage through another independent Blue Cross Blue Shield (BCBS) plan, and that you may have received services in Washington or Alaska at some point since 2002. Premera is a service provider in Washington and Alaska to BCBS plans across the country.

What is Premera doing to protect you?

We recognize this issue can be frustrating and we are taking steps to protect you. We are providing protection and assistance to those affected by this cyberattack, including two years of free credit monitoring and identity theft protection services.

Specifically, we are providing you a free, two-year membership in Experian's® ProtectMyID® Alert to help detect possible misuse of your personal information and provide you with identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. Due to privacy laws, we are not able to enroll you directly. For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your free, two-year membership, please see the additional information provided in this letter.

We also recommend that you regularly review the Explanation of Benefits (EOB) statements your health insurer sends you. If you identify medical services listed on your EOB that you did not receive, please contact your health insurer immediately.

What has Premera done to prevent this from happening in the future?

Along with steps we took to cleanse our IT system of issues raised by this cyberattack, Premera is taking additional actions to strengthen and enhance the security of our IT systems moving forward.

Where can you get more information on this issue?

You have two options to obtain more information, online or via phone. You can visit http://www.premeraupdate.com for more information. Or, call 1-800-768-5817, Monday through Friday, 5:00 a.m. to 8:00 p.m. Pacific Time (closed on U.S. observed holidays). TTY/TDD users should call 1-877-283-6562.

I want you to know that protecting your information is incredibly important to us at Premera, as is helping you through this situation with the information and support you need.

Sincerely,

Jeffrey Roe
President & CEO
Premera Blue Cross

Activate ProtectMyID Now in Two Easy Steps

1. ENSURE **That You Enroll By: September 30, 2015** (You will not be able to enroll after this date.)
2. VISIT the **ProtectMyID Web Site: www.protectmyid.com/premera**

If you have questions related to the product being offered or need an alternative to enrolling online, please call 888-451-6558 and provide engagement #: **PC92585.** A credit card is not required for enrollment.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH PROTECTMYID MEMBERSHIP:

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free Copy of your Experian credit report:** See what addresses, employers, public records and accounts are already associated with you.
- **Alerts for:**
  - 3-Bureau Credit Monitoring: Alerts you of new accounts appearing on your Experian, Equifax® and TransUnion® credit reports.
  - 3-Bureau Active Fraud Surveillance: Daily monitoring of 50 potential indicators of fraud appearing on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.*

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 888-451-6558.

INFORMATION ABOUT PREVENTING IDENTITY THEFT

Even if you choose not to take advantage of this free credit monitoring service, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

---

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Equifax	Experian	Transunion
PO Box 740241	PO Box 2002	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused:

You can contact the **Federal Trade Commission** immediately at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft
1-877-438-4338

If you are a resident of Maryland or North Carolina, you can also obtain information about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes from these sources:

Maryland:
Consumer Protection Division
Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us/idtheft/index.htm
1-410-528-8662

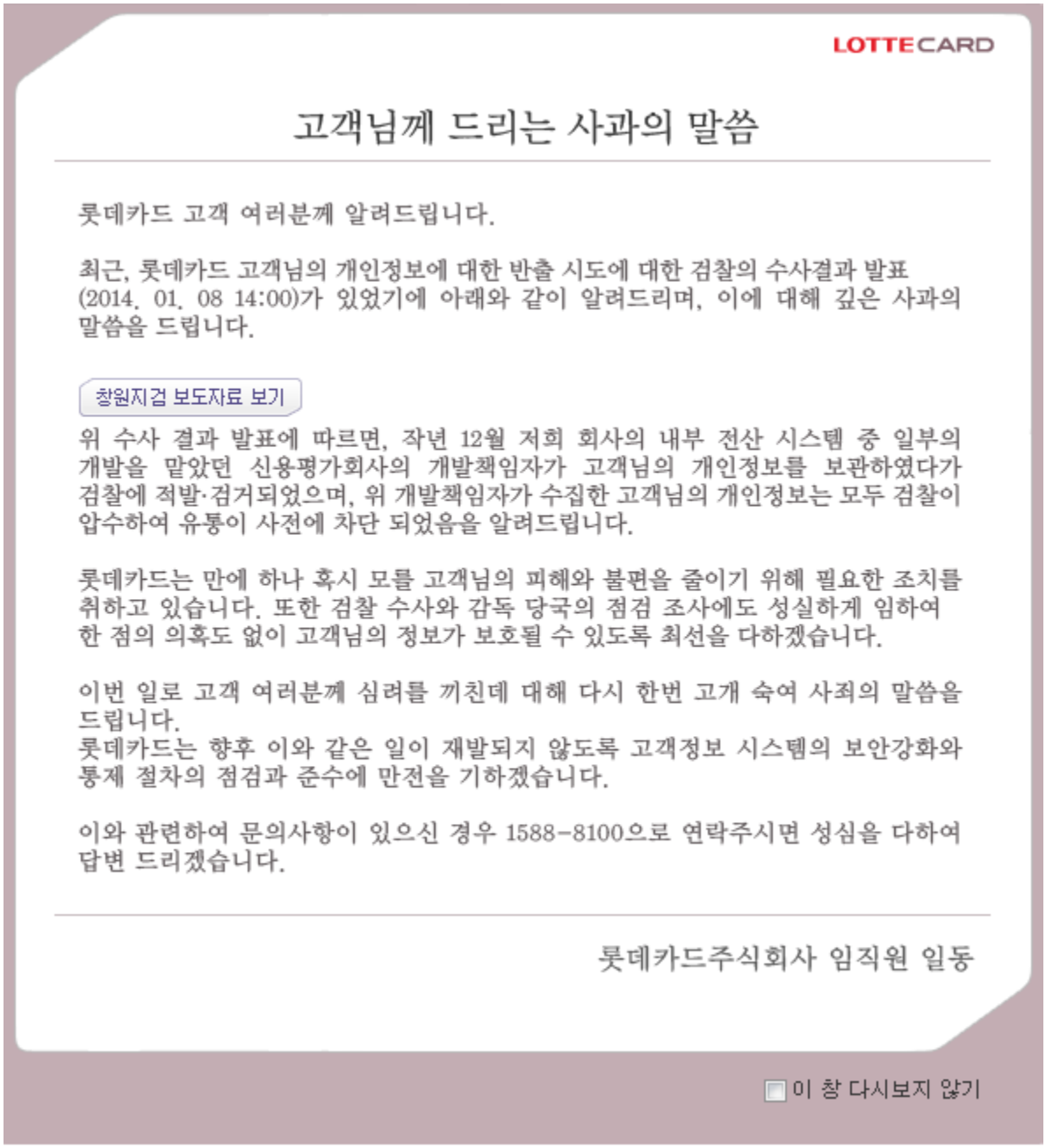
North Carolina:
Office of the Attorney General
9001 Mail Service Center
Raleigh, NC 27699
www.ncdoj.gov
1-919-716-6400

You can also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

We're happy to provide our letters, at no cost, in Spanish, Tagalog, Chinese, Navajo, or Braille.

- **Español:** Para asistencia en Español, por favor llame al numero ubicado en la parte posterior de su tarjeta de identificación.
- **Tagalog:** Upang humingi ng tulong sa Tagalog, paki tawagan ang numero na nakasulat sa inyong kard.
- 中文: 如果需要中文高助，請撥打您卡上的電話號碼。
- **Dine:** Dinék'ehjí áka'a'doowoo.ł biniiyé, t'áá shǫǫdi koji' hodíílnih béésh bee hane'í bi numbo bee néé ho'dólzinígíí biniiyé nanitinígíí bine'dęę' bikáá'

C2. Examples of apology statements from South Korea
(Source: Lotte Inc., Korean Telecom, The Blue Houese)



LOTTE CARD

고객님께 드리는 사과의 말씀

롯데카드 고객 여러분께 알려드립니다.

최근, 롯데카드 고객님의 개인정보에 대한 반출 시도에 대한 검찰의 수사결과 발표(2014. 01. 08 14:00)가 있었기에 아래와 같이 알려드리며, 이에 대해 깊은 사과의 말씀을 드립니다.

창원지검 보도자료 보기

위 수사 결과 발표에 따르면, 작년 12월 저희 회사의 내부 전산 시스템 중 일부의 개발을 맡았던 신용평가회사의 개발책임자가 고객님의 개인정보를 보관하였다가 검찰에 적발·검거되었으며, 위 개발책임자가 수집한 고객님의 개인정보는 모두 검찰이 압수하여 유통이 사전에 차단 되었음을 알려드립니다.

롯데카드는 만에 하나 혹시 모를 고객님의 피해와 불편을 줄이기 위해 필요한 조치를 취하고 있습니다. 또한 검찰 수사와 감독 당국의 점검 조사에도 성실하게 임하여 한 점의 의혹도 없이 고객님의 정보가 보호될 수 있도록 최선을 다하겠습니다.

이번 일로 고객 여러분께 심려를 끼친데 대해 다시 한번 고개 숙여 사죄의 말씀을 드립니다.
롯데카드는 향후 이와 같은 일이 재발되지 않도록 고객정보 시스템의 보안강화와 통제 절차의 점검과 준수에 만전을 기하겠습니다.

이와 관련하여 문의사항이 있으신 경우 1588-8100으로 연락주시면 성심을 다하여 답변 드리겠습니다.

롯데카드주식회사 임직원 일동

이 창 다시보지 않기

머리 숙여 사과드립니다.

고객님

고객님의 개인정보 보호에 최우선으로 노력해왔으나, 소중한 고객님의
개인정보가 침해되는 사고가 발생한 점에 대해 머리 숙여 진심으로 사과 드립니다.

경찰은 불법적인 목적으로 지난해 2월부터 최근까지 당사의 홈페이지에서 고객님의
개인정보(이름,주민등록번호,전화번호,카드결제번호,카드유효기간,주소,고객관리번호,
유심카드번호,서비스가입정보,요금제정보)를 유출시킨 범인을 검거했다고
발표(2014.3.6) 하였습니다.

kt는 침해사실 확인 후 불법접근 시도를 차단하는 등 보안을 한층 더 강화하는 한편,
지속적인 감시로 더 이상의 피해가 발생되지 않도록 조치를 완료하였습니다.

kt는 가장 최우선으로 고객님의 소중한 자산인 개인정보가 유통되거나 악용되지 않도록
모든 조치를 다할 것이며 다시는 불의의 사고가 재발하지 않도록 원점에서 다시 시작해
빠른 시간 내에 혁신하겠습니다.

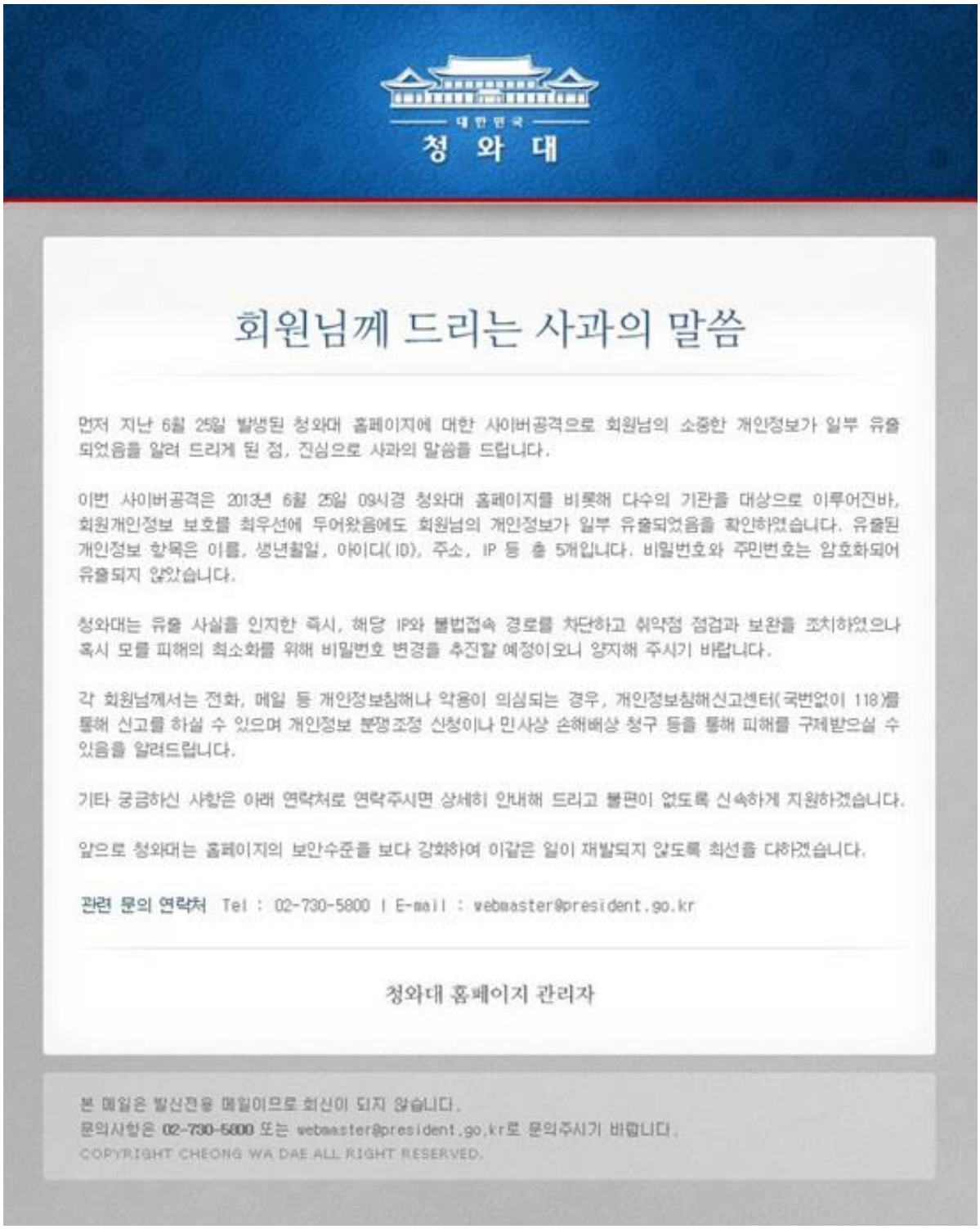
이 사건을 악용하여 개인정보를 묻거나 불법TM으로 의심되는 전화를 받으시는 경우 kt고객센터,
이동통신 서비스 불법TM 신고센터(1661-9558)로 연락 주시면 확인하실 수 있습니다.

항상 kt를 믿고 사랑해 주시는 고객님께 심려를 끼쳐 드리게 되어 다시 한번 진심으로
사과 드립니다.

- 개인정보유출 확인안내 : 올레닷컴 홈페이지 또는 고객센터(무선 114번, 유선 100번)

주식회사 케이티 임직원 일동

olleh



대한민국
청 와 대

회원님께 드리는 사과의 말씀

먼저 지난 6월 25일 발생된 청와대 홈페이지에 대한 사이버공격으로 회원님의 소중한 개인정보가 일부 유출되었음을 알려 드리게 된 점, 진심으로 사과의 말씀을 드립니다.

이번 사이버공격은 2013년 6월 25일 09시경 청와대 홈페이지를 비롯해 다수의 기관을 대상으로 이루어진바, 회원개인정보 보호를 최우선에 두어왔음에도 회원님의 개인정보가 일부 유출되었음을 확인하였습니다. 유출된 개인정보 항목은 이름, 생년월일, 아이디(ID), 주소, IP 등 총 5개입니다. 비밀번호와 주민번호는 암호화되어 유출되지 않았습니다.

청와대는 유출 사실을 인지한 즉시, 해당 IP와 불법접속 경로를 차단하고 취약점 점검과 보완을 조치하였으나 혹시 모를 피해의 최소화를 위해 비밀번호 변경을 추진할 예정이오니 양지해 주시기 바랍니다.

각 회원님께서는 전화, 메일 등 개인정보침해나 악용이 의심되는 경우, 개인정보침해신고센터(국번없이 118)를 통해 신고를 하실 수 있으며 개인정보 분쟁조정 신청이나 민사상 손해배상 청구 등을 통해 피해를 구제받으실 수 있음을 알려드립니다.

기타 궁금하신 사항은 아래 연락처로 연락주시면 상세히 안내해 드리고 불편이 없도록 신속하게 지원하겠습니다.

앞으로 청와대는 홈페이지의 보안수준을 보다 강화하여 이같은 일이 재발되지 않도록 최선을 다하겠습니다.

관련 문의 연락처 Tel : 02-730-5800 | E-mail : webmaster@president.go.kr

청와대 홈페이지 관리자

본 메일은 발신전용 메일이므로 회신이 되지 않습니다.
문의사항은 02-730-5800 또는 webmaster@president.go.kr로 문의주시기 바랍니다.
COPYRIGHT CHEONG WA DAE ALL RIGHT RESERVED.