8-2019

Antecedents and Consequences of Leaders' Security Orientation

Joseph J. Simpson
The University of Texas Rio Grande Valley

ANTECEDENTS AND CONSEQUENCES OF LEADERS' SECURITY ORIENTATION

A Dissertation

by

JOSEPH J. SIMPSON

Submitted to the Graduate School of
The University of Texas – Rio Grande Valley
In partial fulfillment of the requirement for the degree of

DOCTOR OF PHILOSOPHY

August 2019

Major Subject: Management

ANTECEDENTS AND CONSEQUENCES OF LEADERS' SECURITY ORIENTATION

A Dissertation
by
JOSEPH J. SIMPSON

COMMITTEE MEMBERS

Dr. Michael Abebe
Co-Chair of Committee

Dr. Jorge Gonzalez
Co-Chair of Committee

Dr. Pingshu Li
Committee Member

Dr. Mark Kroll
Committee Member

August 2019

ABSTRACT

Simpson, Joseph J., Antecedents and Consequences of Leaders' Security Orientation. Doctor of Business Administration, August 2019, 206 pp., 20 tables, 3 figures, references, 435 titles.

Organizations' leaders are responsible for ensuring that firms' proprietary assets are protected from expropriation. Firms are increasingly targets of large-scale proprietary assets breaches that jeopardize their ability to financially benefit from their innovation activities. Some firms have proactively built capabilities that allow them to protect their proprietary assets, while leaders are more security oriented and therefore do more to protect their organizations from proprietary assets breaches? Current research on leaders' role in the protection of proprietary assets is lacking at the strategic level because most studies on organizational security have emphasized employee-level behaviors (e.g., da Veiga & Eloff, 2010, Lee, Lee & Lee, 2002; Straub & Nance, 1990). Exploring leaders' role in proprietary asset protection is important given their role in strategic decision-making. Accordingly, research should examine leaders' security orientation influence on firm outcomes, including the drivers of orientations and consequences for strategic choice and organizational performance.

This dissertation examines the concept of leaders' security orientation (LSO) and its influence on choice of strategic alliance and innovation strategies, as well as on firm performance. I sought to achieve three objectives with this dissertation. First, I aimed to conceptualize LSO and measure it using a comprehensive, multi-dimension scale. Second, I explored the firm, managerial, and industry level drivers of LSO. Third, I examined the link

between LSO and firms' choices of equity and non-equity strategic alliances, exploitative and exploratory innovation, as well as firm performance. I drew insights from upper echelons, institutional, strategic sensemaking, and prospect theories.

I explored the above relationships using customized datasets drawn from different sources. I found several predictors and consequences of LSO at the managerial, firm, and industry levels, including executive technological interpretation as a threat, knowledge intensity and global presence, among others. The consequences of LSO included equity-based strategic alliances, exploitative innovation, and firm performance. I also tested and found evidence to support a mediating effect of LSO on firm performance through equity-based strategic alliances as well as a mediating effect of LSO on firm performance through exploitative innovation.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

CHAPTER I

INTRODUCTION

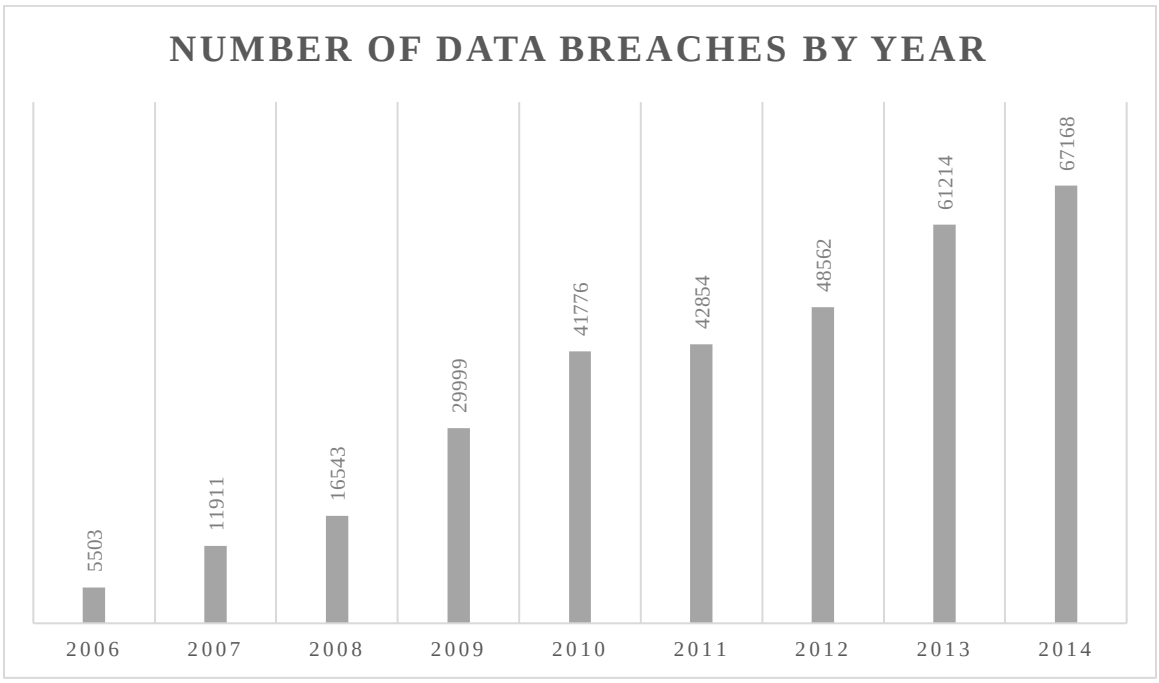
1.1 Security Issues in Contemporary Organizations

In 1997, Volkswagen A.G. was forced to pay General Motors Corporation $100 million following a corporate espionage case alleging that it stole General Motors trade secrets (Meredith, 1997). Following the revelation that more than 41 million customers' financial data was stolen, Target Inc., lost more than $200 million, which led to the departure of its CEO and Chief Information Officer (CIO). In addition, seven directors on the company's board were targeted for removal for failing to manage security risk at the company (Ziobro & Lublin, 2014). Similarly, a 2017 data breach of Equifax, a credit-monitoring agency, resulted in the dismissal of the CEO, the CIO, and the Chief Security Officer (Lecher, 2017).

Increasingly, organizations face multiple and significant threats to the security of their knowledge and information resources. Theft of proprietary assets can result in financial strain, inefficiency, lost productivity, and reputational damage to the affected firm (Hale, Landry, & Wood, 2004; Qusa & Abudalfa, 2013). The challenges that organizations face to the security of their proprietary assets are widespread. Competitors seek to illegally obtain proprietary information (Liebeskind, 1996; 1997; Teece, 1986). Similarly, in some instances, employees

might steal proprietary assets (Greenberg & Barling, 1996) including trade-secret information, among other security issues. Although these threats to organizations are well known, they occur at a growing rate. The figure below shows the number of data breaches reported to U.S. government agencies from 2006-2014 (Government Accountability Office, 2015).

Figure 1: Number of Data Breaches in the United States by Year



(source: Government Accountability Office, 2015)

As shown in the examples above, organizations face grave consequences should they fail to protect their vital proprietary assets. The protection of proprietary assets has important implications for firms' competitiveness. Liebeskind (1996) suggests that protecting one's knowledge is essential for achieving or sustaining competitive advantage. Competitors often aim to steal or acquire information about firms' innovations (Liebeskind, 1996; 1997; Teece, 1986), resulting in the loss of appropriability. The threats to an organization's proprietary resources are so pervasive that in the United States, trade secret theft alone costs an estimated $300 billion annually (Reuters, 2016). As another example, Epic Systems experienced trade secret theft so

severe that the offender, India's Tata Consultancy Services, was fined $940 million by a U.S. federal court (Kondalamahanty, 2016). Thus, the direct financial consequences of security breaches can be severe. In addition, firms frequently face reputational damage resulting from failing to secure assets, people, and information. For example, repeated data breaches result in reputational losses and erosion of the public's trust in the firm (Acquisti, Friedman, & Telang, 2006).

As the former director of the Federal Bureau of Investigation, Robert Mueller said, "there are only two types of companies: those that have been hacked, and those that will be hacked again" (2012). Organizations across various industries face the threat of hacking and other threats to their proprietary assets. Although these threats are likely to vary depending upon the industry, all organizations face threats to the safety and security of their resources. For example, a retail store is likely to be more concerned with inventory theft than a consulting firm. Similarly, an information systems firm is likely to be more concerned about a competitor stealing proprietary information than a convenience store.

Organizations develop strategies to protect their proprietary resources. The best approaches are often holistic in nature and are likely to address multiple facets of security, including planning, response, and learning as suggested in crisis management research (Pearson & Mitroff, 1993). For example, Google often protects its intellectual property using patents, but also through employee screening, non-disclosure agreements, limiting access to certain information and areas, and cybersecurity systems. Other mechanisms for protection of proprietary assets include secrecy (Bos, Broekhuizen, & de Faria, 2016; Robertson, Hannah, & Lautsch, 2015), information systems (Posthumus & Von Solms, 2004), and supply-chain security

(Williams, Lueg, & LeMay, 2008), among others. However, no known studies have taken a holistic approach to examining the protection of organizations' proprietary assets.

1.2 Statement of the Problem

Despite the consequences for firms in terms of loss of revenue and loss of competitive advantage, we still know little about the strategic approaches that firms should take in protecting their proprietary assets. Moreover, there remain many unanswered questions regarding how and why organizations take certain approaches to protecting resources such as information. If knowledge sharing is so important for fostering innovation (Spencer, 2003), then why do firms engage in efforts to limit knowledge flows within their organization, such as limited access to information between alliance partners, departments and employees (Jarvenpaa & Majchrzak, 2016)? This is particularly confusing in light of some scholars' suggestion that over-emphasizing protection can reduce innovative capacity, as the firm concentrates its efforts on activities related to control or secrecy of innovation and neglects exploration (March, 1991; Teece, 1986). In addition, there is a need for more research on the outcomes of security decisions in organizations. For example, what effect do leaders' security orientations have on firm performance, if any? Given that security breaches reduce firm value (Cavusoglu, Mishra, & Raghunathan, 2004), it should be expected that firms whose leaders actively address security issues capture more value from their activities, including innovation and strategic alliances.

Numerous studies about security in organizations have emerged (e.g., Bos et al., 2016; Liebeskind, 1997; Posthumus & Von Solms, 2004; Zohar, 2010). Scholarly research has long asserted that the protection of proprietary resources is critical for firms to reduce imitability (Manhart & Thalmann, 2015; Teece, 1986) and protect against loss (Barney, 1991; Grant, 1996). Similarly, management research addressing the protection of innovations from replication (e.g.

Teece, 1986) has largely ignored the role of security for information systems (e.g., Hong, Chi, Chao, & Tang, 2003). This "silo" approach provides useful information about respective areas of research but fails to provide a comprehensive perspective of leaders' security orientations. This is particularly important as senior leaders play a significant role in planning, developing, and implementing an organization's strategies, systems, and initiatives (Boal & Schultz, 2007; Doz & Kosonen, 2010; Kaplan & Norton, 2006).

Currently, there is little research on the role organizations' senior leaders play in preventing and managing security breaches. Specifically, not much is known about whether and how leaders' security orientations influence organizational strategy in protecting proprietary assets and whether these orientations affect organizational outcomes. Such a measure of leaders' security orientations is important for our understanding of how firms systematically approach the security of proprietary assets overall, instead of focusing on a single component of an organization's security strategy (e.g., patent enforcement) as is the current approach to the study of organizational security. Moreover, leaders already develop and maintain systems of security to protect firms' various proprietary assets (Bos et al., 2016; Hannah, 2005), which will be described later. However, we do not know why some leaders choose certain strategies, what influences them to do so, and what the outcomes of the chosen strategies are.

The prevailing narrow perspective is problematic because it ignores the complexities of safeguarding proprietary assets and the challenges organizations face in implementing enterprise security programs and initiatives. Moreover, this limited approach might mean that findings from past research might not fully explore the relationship between various firm-level constructs, such as the protection of knowledge and firm performance. Leaders' security orientations are also important for integrating diverse literatures, such as crisis management, information systems, and

accounting, to name a few. Thus, we can gain a more complete picture of security in organizations and examine its effects on various firm-level outcomes that have implications for strategic competitiveness.

Although numerous studies have examined how organizations protect their critical resources and deal with mounting security challenges, the current literature in this area is fragmented and does not present a systematic and coherent framework for understanding organizational security challenges. Past studies that have examined security in organizations have taken a piecemeal approach, only focusing on specific security threats (e.g., appropriation, theft) and not organizational approaches or orientations towards security. For example, studies have examined organizations' information security culture (Von Solms & Von Solms, 2004) and secrecy management (Bos et al., 2016) independently, but not as an interrelated organization-wide orientation of the firm.

Scholars have long studied organizations' climate and culture. Organizations' climates and culture have been described as "two alternative constructs for conceptualizing the way people experience and describe their work settings" (Schneider, Ehrhart, and Marcey, 2013, p. 362). The literature lacks consensus on definitions of climate, culture, and orientation. For example, two decades ago, there were more than 50 definitions of organizational culture (Verbeke, Volgering & Hessels, 1998). Despite lacking unified terminology, scholars generally view cultures as shared norms, beliefs, and values that guide actions (Verbeke et al., 1998; Zohar & Hofman, 2012). In contrast, climate is described as "socially shared perceptions of organizational members regarding key characteristics of their organization" (Verbeke et al., 1998; cf. Zohar & Hofman, 2012, p.3).

In contrast with cultures, orientations predominantly consist of top management efforts, behaviors and perceptions (e.g., Calantone, Cavusgil & Zhao, 2002; Jaworski & Kohli, 1993; Kohli & Jaworski, 1990). A common theme present in various conceptualizations of organizational orientations is that it involves an activity directed towards a particular focus or goal. Thus, whereas cultures and climates are often interpretations of organizational values, beliefs, or characteristics, orientations are generally actions, activities, or at least perceptions of these actions or activities that arise from top management. For example, measures of market orientation include items related to acting on information or competitor actions (Jaworski & Kohli, 1993) and learning orientation includes trying new processes and knowledge sharing (Calantone et al., 2002). These orientations have a number of important antecedents and consequences for firms (Jaworski & Kohli, 1993; Siguaw, Simpson, & Enz, 2006). Because the emphasis of this dissertation is primarily on top executives, I opt to focus on orientation as it relates to leaders' emphasis on security. The following section details the purpose of this dissertation.

1.3 Purpose of the Dissertation

In developing this dissertation, my purpose is three-fold. First, I develop a comprehensive measurement scale for Leaders' Security Orientation (LSO). The dimensions of the scale include security preparation for proprietary asset breaches, management of proprietary asset breaches, and post-breach learning and resilience. As mentioned previously, this scale is important for developing our understanding of firms' leaders' orientations towards protecting resources from loss. Second, I explore the antecedents of LSO in organizations, giving particular emphasis to managerial, firm and industry level predictors. Finally, I study the link between the LSO scale

and firm outcomes. Specifically, the outcomes of interest in this study include cooperative strategies, innovation strategies, and firm performance.

To achieve the first objective of this dissertation, I draw from research on crisis management and other scholarly works to establish the elements that comprise LSO. Specifically, I focus on awareness, prevention and preparedness, management of proprietary asset breaches, and post-breach learning and resilience phases developed by crisis management scholars (Bundy, Pfarrer, Short & Coombs, 2016; Mitroff, Pearson & Harrington, 1996). The preparedness of an organization to deal with a security issue can create synergy with the learning and resilience components of a leader's security orientation, helping to effectively resolve the issue. Similarly, improving efforts in one area of security can help the organization in other areas. For example, organizations conduct training and exercises to prepare for security breaches. During the course of these preparation efforts, the organization can enhance its learning and resilience. Lessons learned during these efforts can be applied to recovery efforts, which enhance the organization's ability to respond to, or recover from a breach. More specifically, if an organization conducts a mock security breach exercise and discovers a deficiency in response during the exercise, the organization can change the way it responds to that type of breach. This change in response could help the organization's management of proprietary asset breaches.

To achieve the second objective of this dissertation, I examine the influence of managerial, firm, and industry level antecedents on the development of LSO. These antecedents are most likely to influence LSO as suggested in past crisis management research (e.g., Desai, 2011; D'Aveni & MacMillan, 1990; Gittell, Cameron & Lim, 2006) and theory developed in the later sections of this dissertation. Past research suggests that an organization's environment (e.g., industry), management, and firm characteristics all work together to influence a its strategies and

its leaders' decisions (Finkelstein, Hambrick, & Cannella, 2009). For example, leaders with experience in specific areas, such as finance, are more likely to apply a financial perspective on that firm's issues and strategies (Carpenter, Geletkanycz & Sanders, 2004; Hambrick & Mason, 1984). If an organization's leaders have more security experience, they are more likely to develop a holistic security strategy that protects its proprietary assets than firms without such security experience. I explore whether elements of each of these three antecedents significantly predict LSO. The model I present in this dissertation suggests that both external factors (e.g., the industry environment) and internal factors (e.g., organizational and managerial characteristics serve as important drivers of LSO.

The third objective of this dissertation is to empirically test the relationship between LSO and firm strategic actions and performance. Scholarly research in strategic management has suggested that firms often engage in strategies to improve the appropriability of their valuable resources and capabilities (Cohen et al., 2002; Hsieh, Lee, & Ho, 2012; Liebeskind, 1996). For example, a firm often seeks patent protections to prevent competitors from imitating an innovation. The effects of such strategies have substantial impact on the firm's innovation capability and competitive advantage. For example, a firm's management of knowledge and knowledge resources, such as intellectual property, has a substantial impact on a firm's innovation (Ritala, Olander, Michailova, & Husted, 2015).

I also examined how and why organizations protect their resources from various actors. In doing so, I explored how such protection efforts affect various behaviors and outcomes, including firm performance. I expected that organizations' LSO would have a significant, but complex, relationship with the formation of strategic alliances and innovation strategies. That is, organizations with greater emphasis on securing their proprietary resources would be more likely

to accrue substantial benefits from their choices, but also face some consequences as well. In the following section, I advance the dissertation's research questions.

1.4 Research Questions

Using the organization as a unit of analysis, I sought to identify the multilevel drivers of LSO as well as its strategic and performance implications. Past research suggests that firms utilize strategies, such as secrecy and knowledge management, to reduce imitation from competitors and improve their competitive advantage (Liebeskind, 1996, 1997; Teece, 1986). I wanted to understand how firms' security orientation influences their behaviors in inter-organizational arrangements, their innovation strategies, and firm performance. Orientation towards security is important because of its potential impact on firms' competitive advantage. As such, I examine management, firm, and industry contexts that are expected to influence or alter their orientations towards security and, consequently, outcomes. The following research questions guide this study:

1. What is leaders' security orientation (LSO)? What are the conceptual dimensions of an LSO scale?
2. What are the managerial, organizational, and industry-level drivers of LSO? Specifically,
    a. Which specific managerial characteristics influence the development of LSO?
    b. Which specific organizational factors affect the development of LSO?
    c. What are some industry-level determinants of LSO?
3. What are the consequences of LSO on firms' strategies and performance?
    a. Does the presence of LSO significantly influence firms' strategic alliance activities? If so, why?

b. Does the presence of LSO significantly influence firms' innovation activities? If so, why? Is LSO significantly related with firm performance? If so, how does LSO influence firm performance?

1.5 Contributions of the Dissertation

Organizations must protect their proprietary resources to compete in today's hyper-competitive environment. One of the ways that organizations protect their competitive advantage is to institute security mechanisms to prevent the loss of proprietary information and even prevent employees from accidentally giving away confidential information to competitors. Consistent with this perspective, this dissertation offers a number of contributions for on-going conversations in both the scholarly and practitioner communities. Its scholarly contribution is to integrate disparate streams of research in the domain of protecting proprietary resources. And its practical contributions are to help organizations manage security to prevent loss.

1.5.1 Contributions to research

Understanding how and why organizations protect proprietary resources is incredibly important, as evidenced by the consequences of their losses and attention in recent scholarly research (Manhart & Thalmann, 2015). Within the domain of protecting organizational proprietary resources, competitive advantage is preserved, in part, by restricting competitors' imitation and maximizing appropriation of rents from innovations (Liebeskind, 1996; 1997; Teece, 1986). By providing a framework for the study of LSO, developing a scale for leaders' security orientation for firms, and testing LSO's effect on firm strategies and performance, we can better understand the ways in which organizations strategically protect their proprietary resources and the outcomes of doing so.

Developing an LSO scale is important for a number of reasons. First, it parsimoniously and holistically conceptualizes various organizational efforts to protect proprietary assets. Unlike the piecemeal approach common in extant literature, this dissertation proposes a new, comprehensive construct that explains the role organizational leaders play in the protection of proprietary assets. Further, the development of this scale sheds some light on how firms vary in their orientations towards the protection of proprietary assets and tests whether these differences have any effect on various strategic choices and firm performance. Second, the development of the LSO scale helps integrate desperate streams of research regarding the security of firm knowledge and information resources. Third, the development of a scale helps scholars understand how and why firms differ in their orientations towards security. Although previous research found that certain protection mechanisms (e.g., secrecy) are extremely effective in protecting organizational resources (Cohen et al., 2002; Somaya, 2003), this dissertation examines how such protection mechanisms influence strategic behavior and firm performance.

In addition to the aforementioned contributions to scholarly research, this study also seeks to explore the outcomes of security orientation on strategic alliance and innovation strategies. Considerable research has examined how managing alliances is a source of competitive advantage for firms (Ireland, Hitt, & Vaidyanath, 2002). Firms seek to minimize unwanted knowledge leakage to their partners while also achieving the goals of the partnership. Consequently, firms often institute numerous safeguarding mechanisms to minimize knowledge leakage to competitors. Scholarly research has long examined the need to protect resources in alliances (Jarvenpaa & Machrzak, 2016) but seldom explores the outcomes of such protection. With this dissertation, I identified factors that influence these protection mechanisms in organizations and whether such mechanisms have any effect on a firm's choice to engage in

strategic alliances. Organizations often choose innovation strategies based on expected outcomes. This dissertation seeks to determine how security orientations influence the choice of innovation strategies, knowing that organizations often choose between different types of alliances given their concerns about security (Oxley & Sampson, 2004). Part of this dissertation addresses whether security orientation influences firms' alliance and innovation practices and whether those practices translate into improved firm performance.

1.5.2 Contributions to practice

In addition to its scholarly contributions, this dissertation contributes to practice in several meaningful ways. First, by using the newly developed LSO scale, organizations can benchmark their orientations against other firms in similar industries. This could be beneficial for examining whether a firm has an underdeveloped security orientation among leaders and consequently may be more susceptible to knowledge loss or leakage to competitors. Likewise, the scale could be a useful tool for understanding the necessary elements of protecting proprietary assets from imitation. These dimensions likely include preparedness, management of proprietary asset breaches, and post-breach learning and resilience.

Second, this study explores the drivers of firms' security orientation as they attempt to improve appropriability. Innovation appropriability refers to a firm's ability to generate profits from its innovations. Understanding the drivers of security orientation could be useful in establishing mechanisms through which organizations can monitor and adapt to threats in a particular industry. Moreover, firms can examine whether their executive team has the needed expertise to prevent threats emanating from within and outside the organization. For example, an executive team without adequate knowledge of information technology could unknowingly be

placing its firm at risk of cyber-attacks or social engineering, which could cause it to lose valuable resources needed to remain competitive.

Third, the effects of leaders' security efforts on firm outcomes is important to organizations. Firms will be interested to know whether they have invested enough in protecting their proprietary resources or have invested too much. Consequently, the results of this research should help firms understand whether their leaders have the appropriate level of security orientation to minimize threats while maximizing performance. Moreover, firms need to know whether their alliances strike an ideal balance of security and sharing such that outsourcing innovations will not result in losses. Thus, this dissertation seeks to understand how differing security orientations affect strategic behavior and firm performance.

1.6 Key Terms and Definitions

This section provides a brief definition of major variables and concepts in the dissertation:

- *Cooperative Strategies*: Cooperative strategies are "structured cooperative agreements between firms" (Steensma, Marino, & Weaver, 2000, p. 960). Cooperative strategies are used to achieve various goals of organizations, including resource procurement (Galaskiewicz, 1985). In addition, cooperative strategies are important for some firms because they are more efficient than developing internal capabilities (Shan, 1990). These strategies include partnerships such as joint ventures and strategic alliances.
- *Equity strategic alliances:* Equity strategic alliances, or equity-based alliances, are alliances "in which two or more firms own different percentages of the company they have formed by combining some of their resources to create a competitive advantage"

(Hitt, Irelane, Hoskisson, 2015, p. 280). An example of an equity-based strategic alliance is a joint venture.

- *Non-equity-based alliances:* Non-equity strategic alliances, or non-equity-based alliances, are alliances "in which two or more firms develop a contractual relationship to share some of their resources to create a competitive advantage" (Hitt et al., 2015, p. 280). Examples of non-equity-based alliances include licensing agreements, distribution agreements, and supply contracts.
- *Crises and Crisis Management:* A crisis can be defined as "an event perceived by managers and stakeholders as highly salient, unexpected, and potentially disruptive" (Bundy et al., 2017, p. 1). Pearson and Clair (1998) define crisis management as "a systematic attempt by organizational members with external stakeholders to avert crises or to effectively manage those that do occur" (p. 61).
- *Data Breach:* Data breaches occur when unauthorized personnel, including employees, visitors, or criminals, receive or have access to information for which they are not authorized. Examples include hackers accessing information on company networks, maintenance staff seeing confidential production designs, and personal information, such as an employee's social security information inadvertently given to an applicant.
- *Industrial Espionage:* Industrial espionage, also referred to as corporate espionage, refers to attempts to gain access to a corporation's information for commercial purposes.
- *Innovation and Innovation Strategies:* Innovation refers to "technology, strategy, or management practices that a firm is using for the first time…" (Nord & Tucker, 1987, p. 6). Innovation strategy can be defined as the set of strategic decisions and actions that managers require to transform input to output, with the objective of achieving

competitive advantage (Malekzadeh, Bickford, & Spital, 1989). For example, innovation strategies are usually conceptualized as make versus buy decisions, a mix of the two (Cassiman & Veugelers, 2006), or internal versus external sourcing (Veugelers, 1997).

- *Knowledge Intensity:* Knowledge intensity refers to "the extent to which a firm depends on the knowledge inherent in its activities and outputs as a source of competitive advantage" (Autio, Sapienz, & Almeida, 2000, p. 913). Knowledge intensity is important for firms' financial performance (Autio et al., 2000). As such, organizations that are high in knowledge intensity must act to ensure that they protect their innovations from misappropriation.
- *Knowledge Management:* Knowledge management refers to a process that creates or locates knowledge and manages the dissemination and use of knowledge within or between organizations (Bennett & Gabriel, 1999).
- *Leaders/Top Leaders:* Leaders refer to the senior members of a firm who participate in decision-making at the firm level. Depending upon the company, this may include the Chief Executive Officer, Chief Marketing Officer, Vice President, among others.
- *Leaders' Security Orientation (LSO):* LSO is defined as the degree to which an organization's senior leaders prepare, manage, and learn from security issues related to the protection of proprietary asset breaches. LSO includes all efforts to protect the organization from security issues including planning and preparedness for proprietary assets, management of proprietary asset breaches, and learning and resilience following breaches involving proprietary assets. For example, firms often utilize intellectual property protection mechanisms, including patenting, to protect against competitor imitation. Utilization or emphasis on such mechanisms would be a component of LSO.

Resources are not limited to concepts or ideas but also to physical documents containing critical information.

- *Proprietary Assets:* Proprietary assets include all knowledge and information that a firm possesses that are not readily known or replicable to the public, competitors, and even unauthorized employees. I conceptualize proprietary assets as consisting of two categories: 1) sensitive customer and vendor information, and 2) secret products, service methods, and production techniques. Some of these proprietary assets include lists of customer names (Campbell, Gordon, Loeb & Zhou, 2003), or specialized production methods. They also include customers' social security information, banking information, pricing lists, distribution schedules, product design information, service processes, software configurations, and product production techniques.
- *Proprietary Asset Breaches:* Proprietary asset breaches include any instance in which an organization's proprietary assets are compromised or potentially compromised by a malicious actor or event. Such events can include attempted, yet unsuccessful, hacks, an inadvertent release of information to the public, or the leakage of information to a competitor from a former employee, to name a few.
- *Security Issues:* Security issues represent all stressors to an organization's ability to protect proprietary assets. Such stressors include security threats and actual instances of attempted or successful security breaches. Just as strategic issues can be labelled as threats or opportunities, so too can security issues.
- *Security Threat:* A security threat represents a potential risk to protect the organization's proprietary assets. Such security threats can include any risk of loss to the organization's

knowledge or information, such as the potential risk of an employee stealing information or potential cyber-attacks, among others.

1.7 Scope of the Dissertation

In this dissertation, I focus on security threats to organizations' proprietary assets how they protect against them. These threats include theft, hacking, information leakages, reverse engineering products, corporate espionage, news releases, tampering, and destruction, among others. Examples of theft include extortion and trade secret theft. Examples of corporate espionage include competitor hacking and theft of intellectual property. I do not focus on the responses to security outside of the organization. For example, I do not cover lawsuits or prosecution of crimes through courts. In addition, I only detail security breaches as they relate to proprietary assets.

The rest of the dissertation is organized as follows. In the next chapter, I present a systematic review of important conceptual and empirical literature related to Crisis Management. This literature review highlights key concepts in developing the concept of crisis management while also fleshing out approaches that firms take in protecting their valuable resources. Following the literature review, I present the theory and hypotheses in Chapter III. It is here I also develop the concept of leaders' security orientation (LSO). In Chapter IV, I describe the research design, including scale development, target sample and data sources, variable operationalization, and analytical techniques. Chapter V presents the results of my analysis. Chapter VI concludes with discussion, implications, and conclusion.

CHAPTER II

LITERATURE REVIEW

The purpose of this chapter is to provide a detailed overview of the theoretical and empirical research findings in the areas of interest for this dissertation. The literature review draws primarily from research in crisis management because findings in this body of work are applicable to the management of security events. In many ways, managing crises is similar to managing security issues, including security of proprietary assets. More specifically, the management of a security breach requires preparation, management of breaches, learning and resilience, as is the case with crises.

This chapter is comprised of three major sections. In the first section, I examine the literature on security issues in contemporary organizations. These security issues can be viewed as crisis events and should be addressed in a manner consistent with crises management best practices. In the second section, I provide a brief overview of the crisis management literature with particular emphasis on describing what a crisis is, the manner in which organizations handle crises, and the outcomes of crisis management efforts. In the third section, I examine the literature on crisis management using a three-pronged approach that includes preparedness, management of crises, and organizational learning and resilience. This approach serves as a foundation for conceptualizing leaders' security orientation, described in the following chapter.

2.1 Conceptualization of Proprietary Asset, Protection Mechanisms and Proprietary Asset Breaches

Proprietary assets include all knowledge and information that a firm possesses that are not readily known to the public, competitors, and even unauthorized employees. I conceptualize proprietary assets as consisting of two categories: 1) sensitive customer and vendor information and 2) secret products, service methods, and production techniques. Some of these proprietary assets include lists of customer names (Campbell, Gordon, Loeb & Zhou, 2003), and specialized production methods (Gershon, 1993). They also include customers' social security information, banking information, pricing lists, distribution schedules, product design information and knowledge, service processes, software configurations, and product production techniques. These proprietary assets are protected by various mechanisms including trade secrets, patents, access restrictions, facilities, and non-disclosure agreements, among others. Protection mechanisms for proprietary asset breaches are all methods that an organization uses to protect its proprietary assets.

2.1.1 Definition of proprietary asset breaches

I define proprietary asset breaches as breaches involving the loss of, unauthorized access to, or attempt to gain unauthorized access to a firm's proprietary assets. Specifically, proprietary asset breaches include employees accidentally leaving confidential documents in the open, intentional hacks of a company, and alliance partners viewing secret company processes involving product production. In the alliance partner example, this would include the partner having unauthorized or unintended access to secret documents or actual locations.

Table 1 below shows the categories of proprietary assets, examples of proprietary assets, their protection mechanisms, proprietary asset breaches, and some examples of proprietary asset breaches.

Table 1: Proprietary Assets, Protection Mechanisms, and Breaches

Category of Proprietary Assets	Types of Proprietary Assets	Protection Mechanisms	Proprietary Asset Breaches	Examples of Proprietary Asset Breaches
Sensitive customer & vendor information	Customer lists, Customer Social Security Information, Customer Banking Information, Vendor information, Pricing lists, Distribution schedules	Trade Secrets, Secrecy, Access Restrictions, Compartmentalization, Specialized facilities, Doors, Locks, Walls, Employee monitoring, Procedures and Rules, Non-disclosure Agreements, Non-compete agreements, Assignment provisions	Theft, Espionage, Fraud, Destruction, Unauthorized access, Attempted unauthorized access, Disasters, Accidents	Hacking of a bank's list of customers' accounts and information. Former employee stealing customer list to start his or her own business.
Secret products, intellectual assets, service methods, & production techniques	Product design information and knowledge, Service processes, Software configurations, Product production techniques, Brand name	Trade Secrets, Patents, Copyrights, Patent litigation and enforcement, Trademarks, Employee monitoring, Secrecy, Access Restrictions, Compartmentalization, Specialized facilities, Doors, Locks, Walls, Procedures and Rules, Non-disclosure Agreements, Non-compete agreements, Assignment provisions, Design complexity, Lead time	Theft, Espionage, Fraud, Patent infringement, Attempted unauthorized access, Destruction, Unauthorized access, Disasters, Accidents, Trade secret theft, Tampering, Counterfeiting, Terrorism, Recall, Defect	Corporate espionage of a competitor. Hacking of design information. Destruction of facility containing secret information.

2.1.2 Sensitive customer and vendor information

Recent high-profile data breaches show just how important information about people can be. Equifax's 2017 data breach led the company to fire its CEO, CIO, and CSO, and the expected cost of the breach could reach billions of dollars (Janofsky, 2017). Customer and vendor information can include social security numbers, phone numbers, credit card information, and shopping habits. With this information, competitors can steal customers, and malicious actors can harm customers. For example, a data breach can reduce trust and increase the perceived risks of shopping with a firm (Chakraborty, Lee, Bagchi-Sen, Upadhyaya, & Rao, 2016). Vendor information, such as pricing, is also valuable to gain a competitive edge over a firm's

competitors. Such information can be stored electronically on computers, in the "cloud" (online information storage), or in physical documents or files. Depending upon the medium, organizations utilize different methods for protecting customer and vendor information. For example, information systems protect electronically stored vendor and customer lists, while locks, doors, vaults, and fences are used to secure physical documents.

2.1.3 Intellectual assets, service methods, & production techniques

This category of proprietary assets includes all firm information related to production processes, service methods, and products. Examples include prototypes under development, service methods using proprietary technology or knowledge, and production processes needed to develop products. It includes all knowledge and know-how, both codified and tacit. necessary to perform an operation, protect, produce a product, or perform a service. Moreover, it includes all information related to intellectual property, trademarks, copyrights, and trade secrets. A somewhat famous example of leaked products occurred in 2010 when an Apple employee accidentally left an unreleased version of the iPhone at a pub (Diaz, 2010). An example of a secret production process is the mixing of Kentucky Fried Chicken's recipes at two different facilities that used two different producers (Chan, 2014). Proprietary service methods include Lexis/Nexis, Blackboard, and Skype (Borgman,1999). Organizations frequently protect these secret processes and methods by limiting unauthorized access from alliance partners, competitors, and other malicious actors. Despite a high-profile incident where an Apple employee lost a secret iPhone prototype, Apple is still renowned for its efforts to protect its proprietary assets (Diaz, 2010). In addition, many firms use non-disclosure agreements and non-compete agreements to prevent current and former employees from discussing proprietary information.

2.2 Review of Extant Literature on Proprietary Asset Protection

Three areas of literature are relevant to this dissertation. Research in management, information systems, and finance/accounting has all touched on protection of proprietary information to varying degrees. The literature in management is the most extensive, with studies that cover a broad range of issues including patents (e.g., Somaya, 2012) and interorganizational arrangements (e.g., Jarvenpaa & Majchrzak, 2016). Research in information systems is almost entirely concerned with protecting proprietary assets via electronic information and systems (e.g., Dhillon & Backhouse, 2000; Whitman, 2003). Finally, protection of proprietary assets in the areas of finance and accounting focuses on risk management (e.g., Stulz, 1996) and enterprise risk management (e.g., Beasley, Clune, & Hermanson, 2005).

2.2.1 Management research

Many studies in management research examine how firms protect their proprietary assets. These studies focus on how firms protect against threats, including trade secret theft (Hannah, 2007), patent infringement (Somaya, 2012), and trademark violations (Flikkema, Castaldi, de Man, & Seip, 2017). Protection measures include reliance on intellectual property protection mechanisms (IPPM) that take the form of trade secret protections, patents, copyrights, and trademarks (Hannah, 2005; Hertzfeld, Link, & Vonortas, 2006; James, Leiblein, & Lu, 2013; Manhart & Thalmann, 2015). Firms will often utilize IPPM to reduce the risk that their innovation activity will leak into the public domain and be used by other firms.

Secrecy refers to "the intentional withholding of a piece of knowledge, information, or behavior by one or more persons from the view of others" (Bos, Broekhuizen, & de Faria, 2015, p. 2620). Organizations approach secrecy through comprehensive policies and procedures as well as physical protection measures such as vaults or safes. Secrecy plays a significant role in

protecting innovations (Bos et al., 2015), and it is the most effective mechanism for protecting product innovation in the United States (Cohen et al., 2002). However, secrecy is generally more effective for services than for goods (Delerue & Lejuene, 2010) because goods can easily be reverse-engineered, and thus, imitable. Indeed, secrecy is rated more valuable than patents for many firms (Arundel, 2001), but industry leaders often use a combination of patents and secrecy tactics to preserve market leadership (Arora, 1997) in addition to the other methods, including copyrights and trademarks.

Moreover, organizations often utilize complex strategies to improve their own appropriation of innovations, such as designing features in products that prevent them from being replicated (Bos et al., 2015). For example, according to Bos and colleagues (2015), organizations frequently develop processes to protect knowledge from theft and inappropriate use, provide incentives to encourage protection, utilize technology to restrict access, foster values to protect knowledge, and communicate the importance of protecting knowledge.

If organizations can effectively eliminate the leakage of information to other organizations, then said organizations should be rewarded with greater appropriation from their innovations and developments. Organizations often develop and implement complex security programs to protect against the loss of key resources. For products, organizations can make replication more difficult through increasing a product's complexity (McEvily & Chakravathy, 2002; Thomä & Bizer, 2013). Such designs are important in limiting imitability, but also for reducing competitors' ability to gain useful intelligence about a firm's capabilities. If a firm can understand how a competitor produces a product, then it has access to the technology and costs used to produce that product. Such information can be useful to competing firms in developing pricing strategies and benchmarking production methods.

Oftentimes, organizations are incapable of relying solely on secrecy alone to reduce knowledge leakage to the public or competitors. Consequently, organizations will often implement intellectual property protection mechanisms (IPPMs) as a legal conduit to protect against imitation, including trade secrets, copyrights, trademarks, and patents (Hannah, 2005). However, implementing IPPM often comes at a cost. Applying for legal protections, such as patenting, allows competitors to gain crucial information about an organization's intellectual property, possible future product strategy, and, often, the capabilities of the organization to develop such products. Moreover, IPPM measures are often more financially costly to develop and maintain than secrecy (Arundel, 2001; Bos et al., 2015).

Although many entities might be interested in stealing proprietary assets from a company, competitors represent a major threat to the focal firm. Organizations often engage in competitive intelligence, or the collection of information from various entities (Reinmoeller & Ansari, 2016), in order to reduce uncertainty. Some of the information that a competitor acquires can be used to gain competitive advantage over another firm. This can be done by giving the competitor knowledge about the focal firm's operations and predict its future actions, potentially undercutting the focal firm's capabilities and strategies. Indeed, scholars have long argued that corporations would become "Corporate Central Intelligence Agencies" (Fair, 1966) and use information gained through business and competitive intelligence to inform key decision-makers about the challenges they face from their rivals (Cassady, 1964). As such, it is less surprising that corporate espionage has become a major issue for businesses (Chan, 2003). As a result, many countries have enacted legislation aimed at punishing offenders. In addition, corporations often intensely monitor employees as one way of reducing corporate espionage (Chan, 2003).

Equally important in the protection of proprietary assets is that organizations that have invested heavily in technology and research will be more likely to protect their technological innovations to reduce knowledge leakage. Thus, firms' knowledge intensity, or their reliance on technological innovation, plays a role in their need for more protection (Hashai, Asmussen, Benito, & Petersen, 2010). Thus, especially in inter-organizational arrangements, knowledge-intensive firms must act to ensure that opportunism is limited (Coff, 2003; Hashai & Almor, 2008) through intellectual property protection so it can maximize appropriation of innovations. Hashai and Almor (2008) argue that knowledge intensity can protect innovation by accumulating resources, which may protect against imitation. For example, investment in proprietary production techniques can create barriers to imitation because competitors lack the knowledge of such techniques.

Table 2 below summarizes the major studies that have examined the protection of proprietary assets, management of proprietary asset breaches, and learning and resilience. According to the table, studies have included both categories of proprietary assets and protection methods. However, none of these empirical studies have examined leaders' roles in protecting proprietary assets, managing proprietary asset breaches, or learning and resilience following a proprietary asset breach. A broad range of theories have been used to examine strategies for protection, including transaction cost economics, agency theory, self-categorization theory, and social embeddedness theory. Study samples of this line of research have primarily utilized research and development firms, ranging in size from 67 firms to 18,748 licensing projects. The protection of proprietary assets has served as the central focus of these studies, with relatively few examining management of proprietary asset breaches or learning and resilience. Finally, the major findings from these studies can be summarized as: firms use different strategies to protect

their proprietary assets depending upon firm size and industry, and these strategies have differential impacts on strategic choices and outcomes.

Table 2: Management Research on Proprietary Assets

Author(s) & Year	Category of Proprietary Asset Involved	Protection Method	Theory	Sample	Emphasis	Key Findings
Cassady (1964)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	N/A	N/A	N/A	Not Applicable	N/A
Fair (1966)	Secret products, service methods, & production techniques	N/A	N/A	N/A	Protection of proprietary assets	N/A
Teece (1986)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Patent, Copyright, Trade secret, Appropriation regime	N/A	N/A	Protection of Proprietary Assets; Management of proprietary asset breaches	N/A
Liebeskind (1996)	Secret products, service methods, & production techniques	Employee rules, Job design	N/A	N/A	Protection of Proprietary Assets	N/A
Arora (1997)	Secret products, service methods, & production techniques	Patents, Secrecy	N/A	18,748 Licensing projects between 1980-1990	Protection of Proprietary Assets	Whether firms use patents and/or secrecy depends upon the industry structure.
Liebeskind (1997)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Employee rules, Job design, compartmenta-lization of information, access restrictions	N/A	N/A	Protection of Proprietary Assets; Management of proprietary asset breaches	N/A
Cohen (2000)	Secret products, service methods, & production techniques	Patents, secrecy, lead tome, complementary marketing and manufacturing capabilities	N/A	1,478 R&D labs 18 interviews of R&D managers and intellectual	Protection of Proprietary Assets	Firms use a variety of mechanisms to protect innovations. The importance and effectiveness of a

Author(s) & Year	Category of Proprietary Asset Involved	Protection Method	Theory	Sample	Emphasis	Key Findings
				property officers		protection method depends on the industry. Secrecy is viewed as the most effective mechanism for protecting innovations.
Arundel (2001)	Secret products, service methods, & production techniques	Secrecy, Patents	N/A	2,849 R&D firms	Protection of Proprietary Assets; Management of proprietary asset breaches	Secrecy is more important than patents.
Cohen, Goto Nagata & Walsh (2002)	Secret products, service methods, & production techniques	Secrecy, Patents, Other legal, Lead Time, Complementary sales/service, Complementary manufacturing	N/A	1,478 U.S. R&D manufacturing firms 643 Japanese R&D manufacturing firms	Protection of Proprietary Assets	Patenting influences intra-industry knowledge flows. These flows differ between the U.S. and Japan.
McEvily & Chakravathy (2002)	Secret products, service methods, & production techniques	Complexity, Tacitness	Resource Based View	416 adhesive firms	Protection of Proprietary Assets	Complexity and tacitness protect major product innovations, but not minor innovations The specificity of a design for technological knowledge delayed imitation for minor innovations.
Chan (2003)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Employee monitoring	Agency Theory, Social Exchange Theory	N/A	Protection of Proprietary Assets; Management of Proprietary Asset Breaches	N/A

Author(s) & Year	Category of Proprietary Asset Involved	Protection Method	Theory	Sample	Emphasis	Key Findings
Somaya (2003)	Secret products, service methods, & production techniques	Patent Litigation	Divergent expectations, Asymmetric Information, Asymmetric stakes, Strategic Stakes	FJC Lawsuits 1983-1993 700 firms in the computers industry and 366 firms in the research medicines industry	Protection of Proprietary Assets; Management of Proprietary Asset Breaches	The decision to settle a patent lawsuit varies largely by industry. Firms use patents as a corporate strategy and are an effective isolating mechanism.
Hannah (2005)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Trade Secret, Patents, Copyrights, Trademarks, Non-disclosure agreements, trade secret protection procedures, access restrictions	Trust	111 employees of two high-tech firms	Protection of Proprietary Assets	Familiarity with access restriction procedures negatively influenced felt obligation to protect trade secrets. Familiarity with trade secret handling procedures were positively related with felt obligation to protect trade secrets.
Hertzfeld, Link & Vonortas (2006)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Patents, copyrights, trademarks, and trade secrets	Transaction Cost Economics, Industrial organization theory	288 research joint ventures from 2,120 organizations	Protection of Proprietary Assets	Patents are used most frequently to protect knowledge in partnerships. Copyrights, trademarks, and trade secrets are used in the early stages of a partnerships.
Hannah (2007)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Trade secrets, Non-disclosure agreements, assignment provisions, Noncompete agreements	Self-categorization, Norms of reciprocity	111 employees of two high-tech firms	Protection of Proprietary Assets	New employees classify a previous employer's trade secret information based on the following considerations: whether the information existed previously, whether the information is publicly

Author(s) & Year	Category of Proprietary Asset Involved	Protection Method	Theory	Sample	Emphasis	Key Findings
						available, general, and negative. These employees will protect this information if they feel obligated to their former or new employer and if they identify strongly with their former or new employers.
Hashai & Almor (2008)	Secret products, service methods, & production techniques	Activity integration	Transaction Cost Economics, Resource Based View	98 Israel firms	Protection of Proprietary Assets	There is a curvilinear relationship between R&D intensity and activity integration. Firms that follow this pattern experience higher performance.
Delerue & Lejuene (2010)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Job mobility restrictions, Secrecy, Lead Time	Resource Based View	250 employees of a biotechnology company	Protection of Proprietary Assets	Mobility restrictions affect firms' ability to appropriate rent through their influence on secrecy and lead time.
Hashai, Asmussen, Benito, & Petersen (2010)	Secret products, service methods, & production techniques	Knowledge transfer, Control and Monitoring	International-ization theory, Knowledge transfer efficiency Organization-al Learning	67 Israeli firms between 1995-1999	Protection of Proprietary Assets; Learning & Resilience	Firms' technological intensity affects their entry mode diversity.
Somaya (2012)	Secret products, service methods, & production techniques	Patenting, Licensing, Enforcement	N/A	N/A	Protection of Proprietary Assets; Management of Proprietary Asset Breaches;	N/A

Author(s) & Year	Category of Proprietary Asset Involved	Protection Method	Theory	Sample	Emphasis	Key Findings
					Learning & Resilience	
James, Leiblein & Lu (2013)	Secret products, service methods, & production techniques	Patents, Secrecy, Lead time, Complementary Assets	N/A	N/A	Protection of Proprietary Assets; Management of Proprietary Asset Breaches; Learning & Resilience	N/A
Thoma & Bizer (2013)	Secret products, service methods, & production techniques	Patent, Utility model, Industrial design, Trademark, Copyright, Secrecy, Design complexity, Lead time	N/A	1,624 small businesses in Germany	Protection of Proprietary Assets	Small businesses often do not protect innovations. Those that do, use secrecy and lead time, combined with other IPRs. The type of IPR depends upon the characteristics of the innovation, the type of innovator, and the market environment.
Bos, Broekhuien & de Faria (2015)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Secrecy, Trade secrets, Patents, Monitoring, Patent enforcement	N/A	N/A	Protection of Proprietary Assets; Management of Proprietary Asset Breaches; Learning & Resilience	N/A
Manhart & Thalmann (2015)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Secrecy, Trade secrets, Patents, Monitoring, Patent enforcement, Knowledge protection, Legal, Organizational, Technical	N/A	N/A	Protection of Proprietary Assets; Management of Proprietary Asset Breaches; Learning & Resilience	N/A

Author(s) & Year	Category of Proprietary Asset Involved	Protection Method	Theory	Sample	Emphasis	Key Findings
Reinmoeller & Ansari (2016)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Competitive intelligence, espionage	Social Embeddedne-ss	Ten Fortune 500 companies between 1985-2012	Protection of Proprietary Assets	Firms use competitive intelligence despite its negative stigma when they use opaque practices, justify its use through accepted beliefs and fear of abandonment, and adopt it by developing multiple versions.

The next section reviews existing research related to proprietary asset protection in the information systems literature.

2.2.2 Information systems

Although empirical research on data breaches was previously scant, scholars have begun to explore them. For example, Garrison and Ncube (2011) examined the characteristics of data breaches and found that: educational institutions are most likely to experience a breach, insider events are rarer than outside breaches, and that the number of records exposed in a breach depends on the industry and type of breach. Other studies have shown that data breaches have negative and significant effects on a firm's market value (Acquisti, Friedman & Telang, 2006) and shareholder wealth (Gatzlaff & McCullough, 2010).

Considerable attention has been given to the topic of information security in the information systems literature, with the majority of research in this area focused on the effect of data breaches and information systems vulnerabilities on firm value (e.g., Acquisti, Freidman, & Telang, 2006; Cavusoglu, Mishra, & Raghunathan, 2004; Telang & Wattal, 2007) and employee misuse of information systems (e.g., D'Arcy & Hovav, 2007; D'Arcy, Hovav, & Galletta, 2009). In particular, many studies have sought to understand why employees engage in computer abuse (e.g., Lowry, Posey, Bennett, & Roberts, 2015) and how to reduce instances of employee misuse or abuse of information systems through computer monitoring, security policies, SETA (security education, training, and awareness) programs (Chen, Ramamurthy & Kuang-Wei, 2015; D'Arcy & Hovav, 2009) and motivating employees to comply with information security rules (Herath & Rao, 2009). In particular, SETA programs are believed to improve compliance with security rules and assist in fostering a security culture (Chen et al., 2015). Developing an awareness of

rules, understanding how to comply with rules, and knowledge and fear of sanctions are thought to help achieve these goals.

Similarly, considerable research has focused on improving compliance with information systems policies (Bulgurcu, Cavusoglu, & Benbasat, 2010; Safa, Von Solms, & Furnell, 2016; Siponen, Pahnila, & Mahmood, 2010; Vance, Siponen, & Pahnila, 2012; Vroom & Von Solms, 2004) and encouraging better information security behaviors from computer users (Herath & Rao, 2009; Posey, Roberts, Lowry, Bennett, & Courtney, 2013). Among the many factors identified as important to improving information security include: auditing, policies, improving awareness, training and top management support for security (Von Solms & Von Solms, 2004). More recent scholarly attention in this field has focused on organization-wide efforts to improve information security (Dhillon, Syed, & Pedron, 2016; Safa et al., 2016). For example, Safa, Von Solms, and Furnell (2016) suggest that organizations integrate and consider all aspects of securing information, including physical assets, instead of solely focusing on information systems. Others have suggested that organizations treat an information system as a complex, adaptive system (Burns, Posey, Courtney, Roberts & Nanayakkara, 2017).

Table 3 below summarizes the major studies related to proprietary assets in the information systems literature. While management research related to proprietary assets primarily focuses on the firm level, information systems research examines events at both the firm and employee levels. Consistent with this approach, most of the theories in this area of research emphasize individual behavior (e.g., General Deterrence Theory) over organizational theories (e.g., Transaction Cost Economics). However, there is a lack of research on learning and resilience in information systems just as is the case in management research.

Table 3: Information Systems Research of Proprietary Assets

Author(s) & Year	Proprietary Asset Involved	Protection Method	Theory	Sample	Emphasis	Findings/Key Arguments
Straub & Welke (1998)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information Systems Security	General Deterrence Theory	1,211 members of the Data Processing Management Association	Protection of Proprietary Assets; Management of Security Breaches	Security countermeasures that can lower computer abuse by employees.
Gold, Malhotra, & Segars (2001)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information Systems Security	N/A	1,000 senior executives	Protection of Proprietary Assets	Security processes positively affect organizational effectiveness.
Cavusoglu, Mishra, & Raghunathan (2004)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information Systems Security	Efficient Market Hypothesis	66 security breaches between 1996-2001	N/A	An internet security breach is associated with a 2.1 percent decline in market value with an average loss in market capitalization of $1.65 billion per breach. The impact of a breach varies based on the firm type, size and year.
Von Solms & Von Solms (2004)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information Systems Security	N/A	N/A	Protection of Proprietary Assets; Management of Security Breaches; Learning & Resilience	N/A
Acquisti, Friedman & Telang (2006)	Sensitive customer & vendor information	Information Systems Security	N/A	79 data breaches	N/A	Data breaches have a negative and significant effect on market value, but that decreases over time.

Author(s) & Year	Proprietary Asset Involved	Protection Method	Theory	Sample	Emphasis	Findings/Key Arguments
D'Arcy & Hovav (2007)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information Systems Security, Policies, Education, Training	N/A	N/A	Protection of Proprietary Assets; Management of Security Breaches; Learning & Resilience	N/A
Telang & Wattal (2007)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information Systems Security	N/A	147 software vulnerability announc-ements from 18 firms	N/A	Software vulnerability announcements have a significant and negative effect on firm market value.
D'Arcy, Hovav, & Galletta (2009)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information System Security countermeasures, User awareness, computer monitoring, SETA programs,	General Deterrence Theory	269 computer users from eight companies	Protection of Proprietary Assets; Management of Security Breaches; Learning & Resilience	Three practices deter information systems misuse: SETA programs, computer monitoring, and awareness of policies
Herath & Rao (2009)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information System Security, Information Security System Policies	General Deterrence Theory, Protection Motivation Theory, Theory of Planned Behavior Organization-al Commitment, Decomposed Theory of Planned Behavior	312 employees from 78 companies	Protection of Proprietary Assets; Management of Security Breaches; Learning & Resilience	Threat perceptions about the severity of breaches and response perceptions of response efficacy, self-efficacy, and response costs are likely to affect policy attitudes; Organizational commitment and social influence have a significant impact on compliance intentions; Resource availability is a significant factor in enhancing self-efficacy, which in turn, is a significant predictor of policy compliance intentions

Author(s) & Year	Proprietary Asset Involved	Protection Method	Theory	Sample	Emphasis	Findings/Key Arguments
Bulgurcu, Cavusoglu, & Benbasat (2010)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information System Security, Information Security System Policies	Theory of Planned Behavior, Rational Choice Theory	110 panel members from a research panel	Protection of Proprietary Assets; Management of Security Breaches	Employee beliefs about information security vary based on the cost of compliance, cost of noncompliance, intrinsic benefits, and safety of resources and rewards.
Gatzlaff & McCullough (2010)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information System Security	N/A	77 data breaches between 2004 and 2006	Management of Security Breaches	Firms that aren't forthcoming about the breach experience worse market reactions. Firm size and subsidiary status mitigate the negative effects on firm stock price.
Siponen, Pahnila, & Mahmood (2010)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information System Security, Information System Security Policies	Deterrence theory, Protection Motivation Theory, Theory of Reasoned Action, Coping appraisal, Innovation Diffusion Theory	3,130 IT professionals	Protection of Proprietary Assets; Management of Security Breaches	Normative beliefs, Threat appraisal, self-efficacy, response efficacy, and visibility are significantly related to intention to comply with security policies Deterrence and rewards are significantly related to actual compliance
Garrison & Ncube (2011)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information System Security	N/A	947 data breaches	Management of Security Breaches	Educational institutions are most likely to experience a data breach. Data are most often stolen as opposed to hacked. Insider breaches are less frequent than outsider breaches.

Author(s) & Year	Proprietary Asset Involved	Protection Method	Theory	Sample	Emphasis	Findings/Key Arguments
						The number of records affected depends on the institution and breach type.
Vance, Siponen, & Pahnila (2012)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information System Security Policy	Protection Motivation Theory	210 employees	Protection of Proprietary Assets; Management of Security Breaches	Nearly all components of PMT significantly influence employees' intention to comply with IS security policies.
Chen, Ramamurthy & Kuang-Wei (2015)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	SETA, Comprehensive Information Security Program	Social Control Theory, General Deterrence Theory	100 respondents	Protection of Proprietary Assets; Management of Security Breaches	SETA programs awareness has a significant impact on security culture, and awareness of security programs.
Lowry, Posey, Bennett, & Roberts (2015)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information System Security Policy	Fairness Theory, Reactance Theory	553 employees	Protection of Proprietary Assets; Management of Security Breaches	Organizational trust reduces computer abuse. SETA decreases computer abuse
Safa, Von Solms, & Furnell (2016)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information System Security Policy	Social Bond Theory, Involvement Theory	416 employees	Protection of Proprietary Assets; Management of Security Breaches	Information security knowledge sharing, collaboration intervention and experience influence compliance with information security policies
Burns, Posey, Courtney, Roberts & Nanayakkara (2017)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Information Security	Protection Motivation Theory, General Deterrence Theory	Modeling	Protection of Proprietary Assets; Management of Security Breaches	Organizations should manage information security as a complex, adaptive system Targeting specific users with training is more efficient than widespread training. Increasing the strength of the deterrence appeals decreases

Author(s) & Year	Proprietary Asset Involved	Protection Method	Theory	Sample	Emphasis	Findings/Key Arguments
						the security vulnerability of a firm.

The next section reviews the auditing and financial risk management literatures related to proprietary assets.

2.2.3 Auditing/Financial risk management

Another relevant area of research in protecting firms' knowledge and information resources appears in financial risk management research. Risk management is concerned with all risks to an organization, including those outside of security, knowledge, and information. The concept of risk management primarily emphasizes financial and accounting issues (e.g., Dreze, 1981), but also includes operational risks associated with engineering (Dionne, 2013, p. 13). Thus, some of the literature in risk management is highly relevant to the protection of proprietary assets while other studies are not. Risk management is conceptualized as "a set of financial or operational activities that maximize the value of a company or a portfolio by reducing the costs associated with cash flow volatility" (Dionne, 2013). Financial executives rank risk management as a top objective (Froot, Scharfstein, & Stein, 1993), and it has been widely studied during the late 20th century (Dreze, 1981; Gatev & Strahan, 2006; Smith & Stulz, 1985). The core argument involving risk management suggests that corporations can reduce risk and increase shareholder value by reducing costs from taxes, bankruptcy, agency, information asymmetry, and payments to undiversified stakeholders (Adam, Fernando, & Golubeva, 2015). These risks can arise from operations (e.g., fraud, IT system breakdown), liquidity (e.g., lack of funds to meet financial obligations), default (e.g., recovery rate), market (e.g., exchange rates), and pure risk. The majority of research of traditional risk management has focused on pure risk and financial risk (Dionne, 2013) while largely ignoring operational risk (McShane, Nair, & Rustambekov, 2011).

Risk management researchers have identified two main activities for risk management (Dionne, 2013): hedging and diversification. Hedging involves investing in an offsetting

investment to reduce risk. Diversification refers to investing in various assets. These two activities include derivatives, structured products, market insurance, self-insurance, and self-protection. Increasingly, researchers have focused on indicators of firms' risk management activities. For example, Liebenberg and Hoyt (2003) suggested that the appointment of a Chief Risk Officer indicated that a firm prioritizes risk management. But the results of risk management activities are mixed. Some scholars have found positive relationships between risk management and firm value (e.g., Carter, Rogers, & Simkins, 2006; Bartram, Brown, & Conrad, 2009; Graham & Rogers, 2002), while others have argued that risk management techniques, such as derivatives, are too small in nonfinancial companies to influence firm value (Guay & Kothari, 2003). Despite the positive findings, risk management approaches were heavily criticized for failing to prevent the 2007 financial crisis (Fraser, Fraser, & Simkins, 2010).

Related to integrated risk management, recent research has focused on Enterprise Risk Management (ERM), which provides equal emphasis on all risks to a firm (Mcshane et al., 2011). Enterprise risk management is "the process by which organizations in all industries assess, control, exploit, finance and monitor risks from all sources for the purpose of increasing the organization's short and long-term value to its stakeholders" (Casualty Actuarial Society, 2017; c.f. D'Arcy & Brogan, 2001). Whereas previous risk management research heavily emphasized financial costs, ERM research focuses on all risk exposures (D'Arcy & Brogan, 2001; Harrington et al., 2002) including both traditional risks (e.g., product liability) and strategic risks (e.g., product obsolesce) that firms face (Bromiley, McShane, Nair, & Rustambekov, 2015). In their study of ERM adoption, Beasley and colleagues (2005) found that firms were more likely to adopt ERM depending upon a number of factors, including whether a firm had a Chief Risk Officer, the board was more independent, the CEO and CFO supported

ERM, and the firm was in the banking, education, or insurance industries. The success of these efforts is generally positive, with some studies finding a positive relationship between ERM and firm performance (Beasley et al., 2008; McShane et al., 2011).

For clarity, Table 4 below summarizes the literature on auditing and financial risk management while omitting studies with little-to-no emphasis on proprietary assets (e.g., Dreze, 1981). In the table, most of the works lack a theoretical basis or do not directly invoke theory, and most emphasize protection of proprietary assets with no emphasis on management of breaches or learning and resilience.

Table 4: Auditing/Financial Management Research of Proprietary Assets

Author(s) & Year	Proprietary Asset Involved	Protection Method	Theory Used	Sample	Emphasis	Findings/Key Arguments
D'arcy & Brogan (2001)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Enterprise Risk Management	N/A	N/A	Proprietary Asset Protection	N/A
Liebenberg & Hoyt (2003)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Appointment of Chief Risk Officer, Enterprise Risk Management	N/A	26 CRO appointments between 1997 and 2001	Proprietary Asset Protection	Firms with greater financial leverage are more likely to appoint a CRO.
Beasley, Clune, & Hermanson (2005)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Enterprise Risk Management	N/A	175 Chief audit executives	Proprietary Asset Protection	ERM implementation is positively correlated to the presence of a chief risk officer, board independence, CEO and CFO support, presence of Big Four auditor, and entity size.
McShane, Nair, & Rustambekov (2011)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Enterprise Risk Management	N/A	82 publicly traded insurers	Proprietary Asset Protection	Higher ERM ratings improve firm performance
Dionne (2013)	Secret products, service methods, & production techniques	Risk Management	N/A	N/A	Proprietary Asset Protection	N/A
Bromiley, McShane, Nair, & Rustambekov (2015)	Sensitive customer & vendor information; Secret products, service methods, & production techniques	Enterprise Risk Management	N/A	N/A	Proprietary Asset Protection	N/A

The next section discusses proprietary asset breaches as organizational crises.

2.2.4 Proprietary Asset Breaches as organizational crises

Proprietary asset breaches, when severe, can represent major crises for firms and even jeopardize a firm's survival. For example, the theft of critical trade secret information can compromise competitive advantage for a firm forever (Campbell et al., 2003), costs hundreds of billions annually in the United States (Reuters, 2016), and harms firms' reputations. Given these potential tremendous costs, organizational leaders must act quickly to resolve proprietary asset breaches and ensure future breaches do not occur. While not all security breaches are crises, many crises originate from failures in an organization's security apparatus. In this dissertation, I pay considerable attention to the literature on crisis management as a means of informing the discussion of protecting proprietary assets and dealing with their losses in organizations. Given that proprietary asset breaches can often become crises for organizations when they are severe or mismanaged, it should not be surprising that the two concepts are related. For example, Target's data breach that affected 41 million customers could unquestionably be described as a crisis for the firm even though it was inherently a proprietary asset breach. In contrast, if a firm had 20 records exposed in a data breach, it would be unlikely to be considered a crisis.

The concepts of security and crisis are conceptually distinct but exhibit some similarities. The actions taken for security breaches are often the same as those for crises unrelated to security. Research in crisis management is somewhat analogous to security issues in that organizations must prepare for, respond to, and learn from organizational crises (Bundy et al., 2016) and security issues alike. For example, organizations prepare for disasters, such as hurricanes and terrorist attacks. Terrorist attacks would be an obvious security breach, but hurricanes would not. Thus, many of the approaches to addressing security events are similar to those taken in other types of crises, such as executive misconduct that originates from financial

reporting. However, security breaches often are minimal and do not meet the crisis threshold. The distinction as to what constitutes a crisis is open to interpretation and likely varies based on individual perceptions. For example, a copyright lawsuit might not rise to the level of crisis for a firm's leaders if the amount of money involved is small or the likelihood of winning the suit is high; but a lawsuit for a small firm with little funds to fight a copyright infringement case might be considered a crisis. As such, a security breach (or security incidents) can be defined as *any instance in which the organization's resources are compromised or potentially compromised by a malicious actor or incident*.

Pearson and Clair (1998) define an organizational crisis as "a low-probability, high-impact event that threatens the viability of an organization and is characterized by ambiguity of cause, effect, and means of resolution, as well as by a belief that decisions must be made swiftly" (Pearson & Clair, 1998, p. 60). Such crises involve a triggering event, damage to organizational resources, and severe economic and/or social costs (Shrivastava, Mitroff, Miller, & Miglani, 1988). Crises can include a range of events including boycotts, loss of key employees, workplace violence, and many others (Mitroff & Apaslan, 2003). Pearson and Clair (1998) also define crisis management as "a systematic attempt by organizational members with external stakeholders to avert crises or to effectively manage those that do occur" (p. 61). Finally, they define crisis management effectiveness as "evidenced when potential crises are averted or when key stakeholders believe that the success outcomes of short- and long-range impacts of crises outweigh the failure outcomes" (Pearson & Clair, 1998, p. 61). Others, such as Bundy and colleagues (2016), have defined a crisis as "an event perceived by managers and stakeholders as highly salient, unexpected, and potentially disruptive" (p. 1).

Despite widespread acceptance and use of Pearson and Clair's (1998) definition in management literature, I opt for Bundy and colleagues' (2016) definition because the former suggests that crises are low probability, and perhaps they were at one time. But recent technological advances have accelerated the frequency of organizational crises, such that they are no longer low-probability events. These definitions guide this discussion of crises and the crisis management literature.

Over the years, scholars have attempted to better understand the nature and dimensions of organizational crises and how they are classified. Table 5 below summarizes the various conceptualizations of crises. For example, Miller (1988) described crises along financial, human, and environmental dimensions. Alternatively, Miller (1988) suggests there are five types of organizations (compulsive, dramatic, depressive, detached, and suspicious), and each type can contribute to the three types of crises. Similarly, Gundel (2005) classifies crises along two dimensions: predictability and influenceability. These dimensions refer to whether the crisis was predictable and whether the organization had a chance to influence damages before or during its occurrence.

In addition to broad categorizations of crises types, organizational crises span a myriad of events, including terrorism, extortion, loss of information, product recalls/defects, poor security, and sexual harassment (Pearson & Mitroff, 1993), to name a few. The vast range of incidents can be either large or small, depending on their impact on the firm. For example, a minor miscommunication can snowball into a much larger issue. However, generally speaking, much larger issues (e.g., a disaster) are more likely to be a crisis for a firm than smaller issues such as a miscommunication. According to Pauchant and Douville (1993), crisis management consists of

six major themes: technological issues, structural issues, strategic issues, subjective and cultural issues, stakeholder management, and social criticism.

Table 5: Conceptualizations of Crises

Author & Year	Conceptualization/Dimensions	Types of Crises (examples)	Relation to Proprietary Assets (examples)
Miller (1988)	Financial, Human, and Environment	Accidents, disasters	Hurricane destruction of production equipment or facilities
Mitroff, Pauchant, & Shrivastava (1988)	Technical/Economic, People/Social/Organizational, internal external	Product/service defects, computer breakdowns, failure to adapt, miscommunication, sabotage, product tampering, counterfeiting, illegal activities, terrorism, labor strikes, boycotts, governmental disasters, natural disasters	Intentional sabotage of a product by competitors
Pauchant & Douville (1993)	Technological issues, structural issues, strategic issues, subjective and cultural issues, stakeholder management, and social criticism	Accidents, bankruptcy, conflict, death, decline, disaster, product harm, strikes, safety recalls	Product harms customers
Pearson & Mitroff (1993)	Technical/economic, severe, normal	Bribery, accidents, terrorism, sabotage, kidnapping, recalls, defects, poor security, copyright infringement, rumors, reputation damage	Competitor in another country infringes on copyright
Gundel (2005)	Predictability and Influencability	Tunnel blaze in Kaprun, Mann Gulch Disaster, Bhopal, 1984, 9/11, Heysel Stadium disaster	Disaster destroys nuclear reactor
James, Wooten, & Dushek (2011)	Harmful or threatening	Financial collapse, pandemics, labor strikes, class action lawsuits, oil spill, financial scandals, product recalls	Recall forces shutdown of production processes
Bundy & Pfarrer (2015)	Uncertainty, disruption, change, social evaluations	Natural disasters, executive scandals, industrial accidents	Earthquake destroys all information

Several works suggest that there are multiple crisis phases or stages in an organization, ranging from pre-crisis to organizational learning (e.g., Bundy et al., 2016; James & Wooten, 2005; Mitroff, 1988; Pearson & Mitroff, 1993), which influence how an organization, its leaders, and employees should act in a crisis. This perspective emphasizes the temporal nature of crises, whereby organizations act or respond differently at each phase. During each phase, organizations

perform different actions to prevent or respond to a crisis. In the pre-crisis phase, organizations can organize by changing their structures or cultures (Bigley & Roberts, 2001; Weick & Sutcliffe, 2001). Then, during the management phase, organizations can act to resolve the crisis quickly and appease key stakeholders (Bundy & Pfarrer, 2015; Clair & Waddock, 2007; Pearson & Mitroff, 1993; Pearson & Clair, 1998; Pfarrer, DeCelles, Smith, & Taylor, 2008). Such actions can include communications (Coombs, 1995; 2007), technical responses, such as recalls (Bundy et al., 2016; Rhee & Haunschild, 2006), and CEO succession (Connelly, Ketchen, Gangloff, & Shook, 2015), among others.

Importantly, how an organization responds can influence the effectiveness or perceived effectiveness of a firm's handling of a crisis. Some communications strategies, for example, are more effective than others based on stakeholder attributions (Coombs & Holladay, 1996; Coombs, 2007; Huang, 2006). Other crisis management strategies, such as CEO succession, are more visible, but their effectiveness depends on attributions of responsibility as well (Connelly et al., 2016). Although some of these actions and communications can be more symbolic than sincere, many actions can be effective in mitigating concerns of stakeholders and provide an opportunity to become better or stronger as an organization (Dean, 2004; James et al., 2011). The ability of an organization to turn catastrophe into an advantage, however, depends largely upon an organization's resilience (Vogus & Sutcliffe, 2007) and learning (Lampel, Shamsie, & Shapira, 2009; Marcus & Nichols, 1999).

There are a few repeating themes within crisis management research that can be applied to security research. In many instances, security incidents do not rise to the level of crisis and organizations should be able to apply the findings from research in crisis management. The distinction between security breaches and crises, however, is often subjective. Both require a

swift reaction (Pearson & Clair, 1998) and preparedness plans (Mitroff & Pearson, 1993). The majority of research in crisis management addresses Johansen, Aggerholm, and Frandsen's (2012) three stages of crisis: pre-crisis, during-crisis, and post-crisis (see also Heide & Simonsson, 2014). This section covers pre-crisis efforts (e.g., awareness, preparedness, and prevention), efforts directed at resolving a crisis (e.g., crisis management), and post-crisis efforts that I refer to as learning and resilience. These three stages should have important implications for addressing security issues in organizations and later form the basis of my leaders' security orientation (LSO) conceptualization. The three stages also extend minor security issues, such as the theft of petty cash or damage to property, but do not rise to the level of a crisis.

2.2.3.1 Preparedness

2.2.3.1.1 ***Awareness.*** If an organization and its leaders are not aware of the threats it faces, they may fail to prevent a crisis (Pearson & Mitroff, 1993). Thus, organizations' leaders must ensure that the firm has a comprehensive system for understanding threats and the consequences of failing to protect against them. For example, organizations' leaders may monitor news reports, industry reports, or other media to determine whether new threats emerge. Media coverage of organizational crises has been found to have a significant negative spillover effect on the performance of all firms in an industry (Zavyalova, Pfarrer, Reger, & Shapiro, 2012). Knowing this, organizations will likely monitor breaches of other firms in an industry. Similarly, part of awareness is the idea of signal detection, or whether an organization recognizes the signs and symptoms of a crisis (Pearson & Clair, 1998). This way, organizations scan for and attempt to detect threats from potential crises.

In their examination of crisis management preparation, Elsubbaugh, Fildes, and Rose (2004) argue that there are four components of an organization's early warning signal detection:

assessment of weaknesses, anticipation of potential crises, environmental scanning, and auditing important functions. Such signal detection is important in achieving effective crisis management (Probst & Raisch, 2005; Wang & Belardo, 2009). As Mitroff and Pearson (1993) note, almost all crises leave signs or warning signals; ignoring them often leads to negative crisis management outcomes (Alpaslan, Green, & Mitroff, 2009). These crises occur whenever there is a gap between expectations and what actually happens in the environment (Egelhoff & Sen, 1992). However, researchers also suggest that organizations frequently ignore or block these signals for various reasons, such as a lack of urgency among organizations' leaders (Alpaslan et al., 2009; Mitroff & Pearson, 1993).

2.2.3.1.2 ***Prevention (Pre-Crisis).*** Organizations' leaders make efforts to prevent crises, often integrating crises prevention into their strategic management processes (Preble, 1997). Organizations and their leaders save themselves from crises more through effective prevention than through effective responses. For example, an organization can easily avoid a discrimination or harassment lawsuit by ensuring that its members do not discriminate or harass by instituting rules on harassment, training employees, and punishing offenders. However, some actions that organizations take increase the likelihood of crises. For example, researchers have found that some types of executive compensation promote risk-taking and increase the chance of experiencing a crisis (Bundy et al., 2016; Harris & Bromiley, 2007; Wowak, Mannor & Wowak, 2015), so organizations might limit some specific compensation types to minimize such risk-taking behaviors. Moreover, organizations can prepare for crises to reduce their consequences should they occur. Such actions can include changes in a firm's culture or structure (Bundy et al., 2016). Kash and Darling (1998) suggest that organizations should utilize information systems, planning procedures, and decision-making techniques to help prevent crises from occurring.

Other actions include developing administrative processes or procedures and physical barriers to prevent a crisis. For example, a firm might help prevent specific types of crises, such as terrorist attacks, by designing and building a facility that can resist an explosion, thus reducing or eliminating deaths or damage to proprietary assets.

Considering that crises can trigger a wide array of emotional and behavioral responses among victims, employees, and top managers (James et al., 2011), the decision-making processes of individuals and leaders can vary based on these responses and influence an organization's actions and outcomes. In one of the earliest works on crises to appearing in the sociology literature that had implications for management research, Hamblin (1958) found that leaders had more influence during crises, but groups were more likely to replace their leader if he or she did not have a solution to the crisis. As noted by Greening and Johnson (1996), organizations with top management teams (TMTs) high in functional heterogeneity, high in educational attainment, shorter tenures, and more tenure heterogeneity are better able to avoid crises. The authors suggest these characteristics are conducive to preventing crises as they represent cognitive processes, such as complex thinking and quality decision making. Thus, characteristics of an organization's executives can help a firm avoid crises, such as product tampering incidents. This highlights the importance of TMT, who work to detect threats on the horizon and avoid them altogether.

Some scholars have suggested that preparedness is a component of prevention (e.g., Bundy et al., 2016), and I view them as overlapping concepts that can be combined, but for this review I consider them as distinct for the purpose of clarity. Specifically, preparedness can be viewed as a component of prevention because preparedness efforts can help an organization prevent a crisis (Pearson & Mitroff, 1993). For example, people trained to react to a crisis can

accurately identify the signs of an impending crisis. As Pearson and Mitroff (1993) note, many crises can be prevented through crisis preparation efforts, but not all. For example, preparedness efforts with stakeholders, such as response strategies, are unlikely to have much of an effect on actual or realized crises events.

2.2.3.1.3 ***Preparedness.*** Crisis preparedness refers to a state of readiness to deal with the onset of a crisis. Companies differ in their preparedness (Mitroff, Pauchant, Finney, & Pearson, 1989; Pauchant & Mitroff, 1988). Elements of crisis preparedness include possessing a crisis plan, a crisis team, training on crises, procedures for handling a crisis, a crisis communicator, management training, among others (Johansen, Aggerholm, & Frandsen, 2012; Pearson & Mitroff, 1993). Similarly, Sadiq and Graham (2015) developed a list of preparedness activities at both the employer level and employee level, which include plans, agreements, insurance, contact lists, communications systems, and others that were positively related to an organization's preparedness. The development of coping strategies prior to a crisis can also help limit a crisis's damage to the organization (Darling, Hannu, & Raimo, 1996; c.f. Ritchie, 2004). As Health (1995; Ritchie, 2004) notes, proactive planning helps minimize damage through the reduction of risk, time in response, and poor resource management. Despite this, firms frequently avoid developing and practicing plans for crises. Surprisingly, only 49% of firms had a crisis management plan, even after the September 11, 2001 terrorist attacks (American Management Association, 2005). Even though organizations face a growing risk of potential crises, they are largely underprepared for them.

Despite past suggestions that crisis preparedness leads to more effective crisis management (Pearson & Mitroff, 1993), few studies have empirically tested whether this is indeed the case. Among these few studies, Tavitiyaman, Leong, Dunn, Njite, and Neal (2008)

examined the effectiveness of crisis management plans on organizational effectiveness. These authors found that crisis management preparedness was, in fact, associated with organizational effectiveness in the hotel industry. In the tourism literature, Topaloglu, Koseoglu, and Ondracek (2013) found that organizational readiness was positively related to firm financial and non-financial performance. Other preparedness efforts, such as organizing for reliability, have been associated with higher firm performance (Vogus & Welbourne, 2003).

2.2.3.2 ***Crisis management (During Crisis).*** In crisis management, organizations will activate their crisis management plans and respond in accordance with those plans (Pearson & Mitroff, 1993). Moreover, organizations utilize a number of crisis response strategies to help mitigate various stakeholder concerns (Bundy & Pfarrer, 2015). These crisis response strategies can be defined as a "set of coordinated communication and actions used to influence evaluators' crises perceptions" (Bundy & Pfarrer, 2015, p. 346). Such strategies can be effective or ineffective. For example, Firestone's response to the deaths of 150 people involving their tires was widely viewed as highly ineffective due to their communications and actions (Alpaslan et al., 2009). Moreover, dealing with crises can help to prevent future issues through learning as well as gaining knowledge to apply to future issues or incidents. These same approaches from crisis management can be applied to proprietary asset protection in organizations.

In contrast with the external perspective of crisis management presented earlier, the internal perspective focuses on the actions taken by organizations to handle technology, risk, and complexity (Bundy et al., 2016; Gephart, Van Maanen, & Oberlechner, 2009; Perrow, 1984; Starbuck & Milliken, 1988). A common theme in the crisis management literature is that organizations and their leaders must act quickly to ensure that a crisis is resolved (Bundy et al., 2016). Such actions can include communicating to stakeholders (Coombs, 2007), impression

management (Coombs, 1998; Rhee & Kim, 2012) and reorganizing personnel, structures, and culture (Fombrun, 1996; Rhee & Kim, 2012), among others. As mentioned previously, other actions can include technical responses such as recalls (Rhee & Haunschild, 2006; Bundy et al., 2016) and CEO succession (Connelly, Ketchen, Gangloff, & Shook, 2016), among others. For example, stakeholders will often react positively to replacing executives during a crisis, such as a bankruptcy (Bonnier & Bruner, 1989; Davidson, Worrell & Dutia, 1993).

Leadership has long been studied in crisis management, with attention directed towards leaders' and leadership team characteristics in predicting performance during or after a crisis. Similar to Greening and Johnson's (1996) study of TMTs and the likelihood of experiencing a crisis, Greening and Johnson (1997) also found that several TMT characteristics had curvilinear relationships with crisis severity. Thus, the structure of a TMT plays an important role in both the likelihood of experiencing a crisis and its severity. Moreover, a leader's crisis efficacy is an important predictor of motivation to lead in a crisis, leader role-taking, and performance in leadership roles (Hadley, Pittinsky, Sommer, & Zhu, 2011). The role of corporate governance also plays an important role (Daily, Dalton, & Cannella, 2003), especially as it relates to director exits during crises (e.g., Withers, Corley, & Hillman, 2012). According to Dowell, Shackell, and Stuart (2011), having more independent directors helps firms survive because they are able to provide firms with sufficient monitoring during a crisis and help resolve the situation. Their independence makes them less biased, able to challenge the CEO and top management, and better equipped to evaluate the company's strategy.

Also important in the crisis management literature is the focus on leader characteristics and leadership styles in predicting various outcomes. Considering that leadership has important implications for motivation and perceptions of crisis management (Van Wart & Kapucu, 2011),

it is not surprising to find that considerable attention is paid to the role of leaders in crises and their effects on others. For example, different leadership styles, such as charismatic leadership, are a known factor in emergent leaders during crises (Conger & Kanungo, 1987). Other approaches to understanding crisis leadership emphasize competencies of leaders that are needed to resolve crises. For example, Wooten and James (2008) argue that signal detection, preparation and prevention, damage control and containment, business recovery, and reflection and learning are important competencies for leaders to exhibit before, during, and after crises. Additionally, in his three-study dissertation on leadership and crisis management, Jungbauer (2016) examined the role of leadership on performance, leader evaluation, and incident reporting. It highlighted the importance of leadership not only on performance outcomes but also on follower behaviors. Other scholars have suggested that leaders often lack formal training and experience necessary to lead during a crisis (Wooten & James, 2008).

Other research in the area of crisis management leadership focuses on the process of strategy formation, strategy selection, and strategy effectiveness in crises. For example, Sinha's (2011) dissertation on crisis management in organizations examined how firms respond to crises. In addition, the dissertation explored the importance of various factors on crisis management strategy selection. Some of these factors include uncertainty in the external environment, impact of the crisis (e.g., severity), top management characteristics, formalization of processes, financial performance, and politicization. Other scholars have examined how organizational crises influence perceived strategic decision effectiveness (Hurt & Abebe, 2015). For example, Hurt and Abebe (2015) found that crises have a tendency to reduce conflict in strategic teams and improve collaboration, which help facilitate crisis resolution.

According to Staw and colleagues' (1981) threat rigidity theory, organizational crises can limit information processing and information search while causing executives to focus on issues that they believe are within their control, leading to centralization of authority (Greening & Johnson, 1997). This perspective suggests that the onset of a crisis can hamper effective decision making among executives. Because of this, the firm's performance could be harmed. For example, a firm, in response to a crisis could focus so intently on preventing another crisis that it fails to focus on future performance, and its innovation and creativity decline. However, others have argued that centralization is an important and beneficial component of resolving a crisis (Dowell et al., 2011). Specifically, Dowell and colleagues (2011) found support for the argument that a crisis helps to centralize power, thus allowing the firm to respond quickly and resolve it.

2.2.3.3 ***Post-Crisis Learning and Resilience.*** Organizational learning and resilience, in the context of organizational crises, refers to an organization's ability to learn, and bounce back, from a crisis. Although learning and resilience are likely to be more important following major crises as opposed to small events, organizations should still use any security-related breach as a learning opportunity to improve their responses in the future. By using the same learning and resilience approaches described in this section towards non-crises security issues, organizations should be able to avoid security issues in the future. As it pertains to crises, organizational learning can be viewed as an organization's ability to understand key lessons from events to prevent their occurrence or respond more effectively in future crises. Specifically, organizational resilience can be defined as "a function of an organization's overall situation awareness, management of keystone vulnerabilities and adaptive capacity in a complex, dynamic and interconnected environment" (McManus, Seville, Vargo, & Brunsdon, 2008, p. 82). Resilience is

important to firms because of its role in protecting firm performance (van der Vegt, Essens, Wahlstrom, & George, 2015). The crisis management literature is replete with examples of how organizations have used crises to help the organization perform better. For example, the leadership team of Hyundai Motors used a crisis to help shift its focus from imitation to innovation (Kim, 1998).

Several factors are known to influence organizational learning and resilience. An organization's structure, forms, and processes are means to improve reliability (Bigley & Roberts, 2001). More specifically, bureaucratic organizational structures hinder creativity and adaptability, reducing resilience in organizations (McManus, Seville, Vargo & Brunsdon, 2008). Similarly, having sufficient resources and relational reserves prior to a crisis improves firm performance (Gittell, Cameron, & Lim, 2006). Organizations that frequently experience crises respond better to crises due to their experience and ability to adapt based on prior knowledge (Bechky & Okhuysen, 2011). Relatedly, as organizations experience more crises, they are less likely to experience disasters in the future (Madsen, 2009). These factors, and others, are important for ensuring resilience in an organization.

Following a crisis, it is important for a firm to be able to understand what caused the crisis and to determine whether responses were effective. Within the crisis management literature, a major emphasis is placed on sensemaking both during and after a crisis (e.g., Maitlis & Sonenshein, 2010; Weick, 1988; Weick, Sutcliff, & Obstfeld, 2008). Sensemaking, or "turning circumstances into a situation that is comprehended explicitly in words and that serves as a springboard into action" (Weick, Sutcliffe, & Obstfeld, 2005, p. 409) is important because following a crisis, an organization must fully determine a crisis's cause to prevent its recurrence

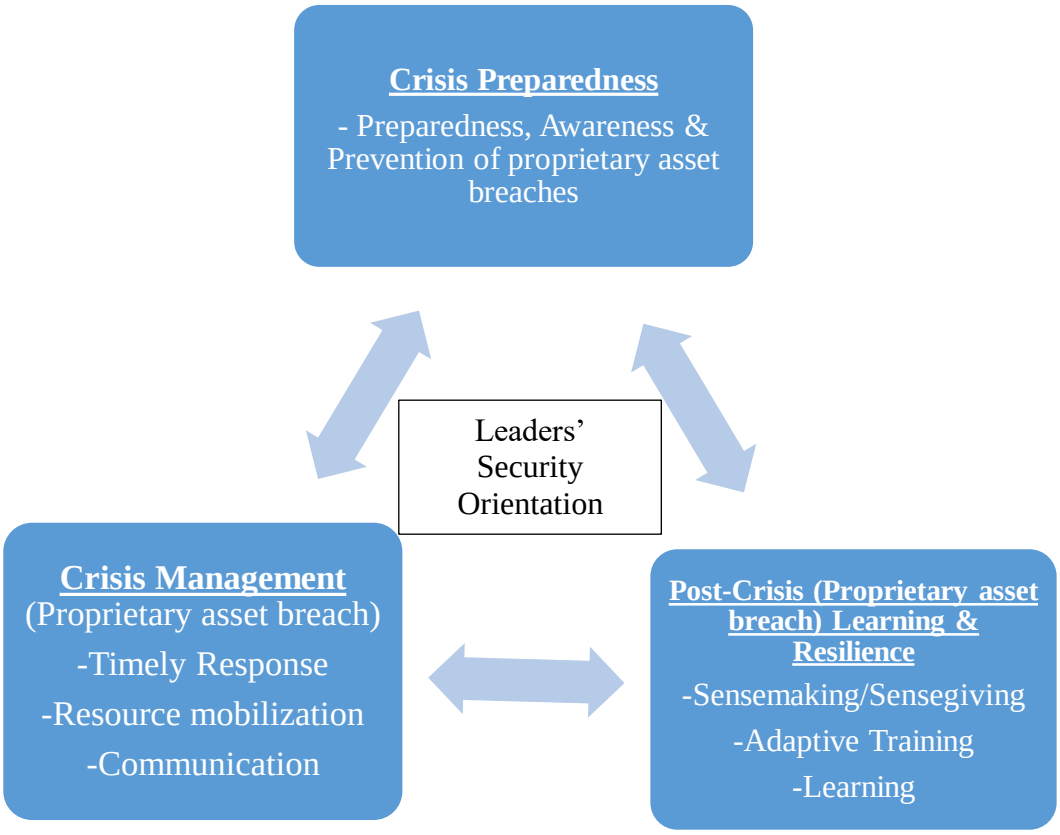
(Boudes & Laroche, 2009). However, if the causes are poorly or misunderstood, then learning from them will likely be unsuccessful (Carley & Harrald, 1997).

The importance of firms learning from their experiences cannot be understated. Crises can evoke pronounced changes in organizations and their employees, often to the point of redefining how these entities understand their meaning and purpose (Kahn, Barton, & Fellows, 2013). Crisis management literature also prioritizes organizational learning prior to and following crises (e.g., Lampel, Shamsie, & Shapira, 2009). For example, Sheaffer and Mano-Negrin's (2003) study of executive orientations and crisis preparedness found a significant relationship between their "unlearning" capabilities and crisis management preparedness. Rare events, such as crises, can foster or trigger organizational learning (Lampel et al., 2009). According to James, Wooten, and Dushek (2011), organizations can utilize crises as competitive opportunities through learning (Christianson, Farkas, Stucliffe & Weick, 2009; Wan & Yiu, 2009). Such learning is important for renewal and growth in firms (Ulmer, Sellnow, & Seeger, 2011), as they can create new priorities or foster innovative thinking to address challenges. Specifically, when firms emphasize learning, they focus on what went wrong and how to address and improve those issues rather than assigning blame and improving (Ulmer et al., 2011). As organizations make these improvements, they are able to renew their approaches and grow. There are a number of ways that organizations can utilize learning from crises to improve the firm and its outcomes. For example, when firms develop mindful cultures, they can improve learning by emphasizing attention to warning signals and drawing attention to system weaknesses (Veil, 2010). Firms can also improve learning by removing barriers, such as relying on past successes and trivializing mindlessness that may prevent learning from mistakes (Veil, 2010).

In what is probably the most comprehensive approach to organizational learning in crises, Brockner and James (2008) developed a framework for understanding executive perceptions of crises as opportunities. In their framework, various factors work to influence how and when an executive will view a crisis as an opportunity, including the individual's learning orientation, reflection upon the crisis, perceived value of the opportunity, and perceived attainability of the opportunity. Such a process, the authors argue, can lead to opportunities such as innovation, change, and opportunities to enhance the organization's reputation.

Figure 2 illustrates how I integrate security of proprietary assets and crisis management literatures to conceptualize comprise Leaders' Security Orientation. They are related in that firms that are more prepared for proprietary asset breaches, manage proprietary asset breaches, and have high learning and resilience are more likely to have leaders who are security oriented.

Figure 2: Link between Dimensions of Crisis Management and LSO



2.3 Cost, Impact, and Response to Proprietary Asset breaches

The cost of a security breach varies widely based on its type (e.g., information or personnel), magnitude (e.g., a single document versus thousands), and severity (e.g., trade secret information versus a training form). For example, a large data breach that affects millions of consumers' credit card information will cost considerably more than a small data breach about consumers' shopping habits. Conversely, the theft of a single document, such as the design information for a nuclear weapon, can have significant and grave consequences whereas the theft of thousands of design documents for a retired technology would have virtually no impact at all.

Given their potential significance, the cost of a proprietary asset breach can be severe for finances, personnel, assets, competitive advantage, or reputations. As mentioned previously, some studies have examined the impact of particular types of breaches. For example, scholars have investigated the impact of data breaches on a firm's finances (Acquisti, Friedman, & Teland, 2006; Gatzlaff & McCullough, 2010; Layton & Watters, 2014), finding that they have a significant and negative impact on outcomes, including market capitalization. Moreover, industry research suggests that data breaches cost more than $3 million per incident (Ponemon Institute, 2016). Finally, Campbell and colleagues (2003) suggest that after confidential information has been accessed by an unauthorized entity, the value of a strategic asset can be compromised permanently, like when a list of customers and their information is stolen and used by a competitor.

Other security breaches of proprietary assets can have direct financial costs or harm firms in indirect ways. As mentioned in the introduction of this dissertation, the cost of trade secret theft costs U.S. companies billions annually (Reuters, 2016). In addition to these financial costs, security breaches can cause firms to lose value from their innovations (Liebeskind, 1996). For

example, a security breach revealing the design or production methods of an invention allows a firm's competitors to imitate its secret processes or innovations. Moreover, employees leaving a firm can share their previous employers' secrets (Hannah, 2007), transferring valuable knowledge to the new employer and possibly reducing the former employer's competitiveness through knowledge transfer.

2.4 Leaders' Roles in Preventing and Managing Proprietary Asset Breaches

Leaders play several roles in preventing and managing proprietary asset breaches. The first role that an organization's senior leaders play is in prevention and preparedness. They are responsible for ensuring that the organization has plans in place to both prevent and mitigate potential security breaches once they occur. This responsibility partly emanates from external stakeholder expectations. For example, the Securities and Exchange Commission reaffirms this requirement by suggesting that boards of directors be proactive in planning for security breaches (Securities and Exchange Commission, 2014). Similarly, among the requirements of Sarbanes-Oxley regulation was the requirement that the CFO or CEO sign financial statements to ensure their accuracy. In addition, senior leaders are expected to proactively mitigate potential threats. Thus, they must develop and implement systems to prevent breaches from occurring (Pearson & Mitroff, 1993). When senior leaders fail in this regard, they are likely to be held accountable. For example, following Target Inc.'s 2014 data breach, the CEO and Chief Information Officer were dismissed and seven members of the board of directors were targeted for removal by shareholders who were unhappy with the company's failure to protect against security threats (Ziobro & Lublin, 2014). Unfortunately, however, most executives are unprepared for easily predictable crises (Starbuck, Greve, & Hedberg, 1978).

During a proprietary asset breach, as with any crisis, senior leaders are charged with taking responsibility (James & Wooten, 2008) and returning the firm to normalcy as quickly as possible. This requires that senior leaders urgently respond to a security breach to bring about its resolution by utilizing their knowledge, skills, and abilities (James & Wooten, 2008). Scholars suggest that certain leadership (Bundy et al., 2016) and organizational structures (Lin et al., 2006) may facilitate speedy and effective management of crises or security breaches. For example, boards of directors with fewer members are more likely to succeed in crises (Dowell, Shackell, & Stuart, 2011). Conversely, firms' age and size can retard leaders' efforts (Lange & Washburn, 2012). Moreover, senior leaders are responsible for communicating with various stakeholders to manage and mitigate concerns associated with an incident (Bundy et al., 2016). These factors likely play a similar role in security breaches where the means of resolution are the same.

After a security breach, organizations' leaders often focus on learning (Carmeli & Schaubroeck, 2008) and resilience (Sutcliffe & Vogus, 2003; Vogus & Sutcliffe, 2007). By doing so, leaders can help the organization prevent future security breaches, mitigate damage from a breach, and return to normalcy. Leaders accomplish learning and resilience by deliberately focusing on the event and developing prevention capabilities (Boin & McConnell, 2007; Bundy et al., 2016). In addition, because some people are resistant to learning from failure (Lampel, et al., 2009), leaders must emphasize learning from a proprietary asset breach and take appropriate action. As Kahn and colleagues (2013) note, learning only occurs when it is managed at multiple levels.

2.5 Chapter Summary

Proprietary asset breaches are significant and destructive events that can significantly affect the ways organizations, their leaders, and employees act. The cost of proprietary asset breaches often reaches hundreds of millions of dollars per incident and incidents can escalate into the thousands each year (Identity Theft Resource Center, 2017). During each phase of a crisis, an organization will focus its efforts in different ways. During the pre-crisis stage, organizations identify threats, prepare for potential crises, and respond quickly to ensure that key stakeholders are satisfied (Bundy et al., 2016). However, not all response strategies will be successful. Increasingly, more attention has been given to security threats in organizations. As with crises, the existence of these security threats influence organizations' actions to reduce the potential for information and knowledge loss. Organizations often adopt complex security systems, including wide-ranging policies and procedures, to prevent or mitigate the potential for harm. There are striking similarities between how organizations approach crises and how their leaders approach security. Consequently, it is intuitive to frame the approaches to the protection of proprietary assets based on a "tripod" model of crisis management. Drawing from this model, several themes in crisis management and leaders' security orientation emerge. These themes include awareness, preparedness, prevention, management of security breaches, as well as learning and resilience.

CHAPTER III

THEORY AND HYPOTHESES DEVELOPMENT

The purpose of this chapter is to detail the theory and hypotheses of this dissertation. First, I review the theoretical framework for the dissertation. Second, I describe the research model. Third, I provide an overview of LSO. Fourth, I detail the proposed antecedents of LSO, and fifth, I explain the relationship between LSO, strategic alliances, innovation, and firm performance. I conclude the chapter with a summary.

3.1 Theoretical Framework

The theoretical framework for this dissertation is grounded in upper echelons, strategic sensemaking, prospect, and institutional theories. In this section, I briefly describe the core tenets of each theory and how the predictions of each theory might apply to leaders' security orientation in organizations.

In 1984, Hambrick and Mason argued that managers' backgrounds could serve as useful proxies for their cognition and mental processes. The authors argue that researchers can predict outcomes, such as strategic decisions, based on managerial backgrounds (Hambrick & Mason, 1984). More specifically, upper echelon's theory (UET) suggests that characteristics such as age, functional background, and educational experiences are proxies for psychological constructs (Carpenter, Geletkanycz, & Sanders, 2004). In many management studies, these experiences are

operationalized through a variety of measures including education, age, and functional experience and influence a range of outcomes, including strategy choice, strategic change, and performance (Datta, Rajagopalan, & Zhang, 2003; Hambrick, 2007; Zhang & Rajagopalan, 2010). These studies also often focus on team composition, such as top management team functional heterogeneity (e.g., Alexiev, Jansen, Van den Bosch, & Volberda, 2010; Carpenter & Fredrickson, 2001). For example, Bantel and Jackson (1989) found support for the idea that more educated and functionally diverse management teams are more likely to lead innovative banks. Similarly, Herrmann and Datta (2005) found that firms have greater international diversification when their top management teams are more educated, have shorter tenures with the organization, are younger, and possess more international experience.

The theory rests on the assumption that organizational leaders have a tendency to rely on their education, experiences, and expertise to inform their decision-making (Hambrick, 2007; Hambrick & Mason, 1984). For example, in their original work on upper echelon's theory, Hambrick and Mason (1984) argued that a person with an MBA is less innovative or risk-prone than a person without an MBA. Similarly, executives with particular types of expertise are suggested to value different business processes. For example, a marketing executive would be more likely to value growth more than someone in production, who might prioritize efficiency (Hambrick & Mason, 1984).

Considering the arguments and findings above, someone with a background or experience in organizational security is more likely to perceive certain issues as a potential threat to the organization's proprietary assets than someone without similar experience. As such, we should expect their decisions to focus primarily, or significantly, on securing proprietary assets.

In addition, they would also likely place greater emphasis on examining their external environment and internal organization for threats to proprietary assets.

Prospect theory is primarily concerned with an individual's decision-making under risk (Kahneman & Tversky, 1979). Risk, in this sense, refers to conditions where a person knows the outcomes of all available options and the probabilities associated with each respective outcome (Knight, 1921). Prospect theory assumes people accrue utility from gains and losses in comparison to a reference point as opposed to total levels of wealth. Barberis (2013) describes four elements of prospect theory: "1) reference dependence, 2) loss aversion, 3) diminishing sensitivity, and 4) probability waiting" (p. 175). As an example, people will generally choose a definite gain of $1,000 to a 50 percent chance of $2,000 while they will generally take a 50 percent chance of losing $2,000 over losing $1,000 for sure. This example shows people are generally risk averse over gains while risk seeking over loss. In another example, golfers are much more likely to make a putt for par than for any other score (Pope & Schweitzer, 2011), which implies performance and loss aversion are related. Specifically, the authors argue that when golfers are under par, they are less focused on loss aversion than when they are at or over par (Pope & Schweitzer, 2011). Kahneman and Tversky (1979) originally expressed this sentiment, noting "a salient characteristic of attitudes to changes in welfare is that losses loom larger than gains. The aggravation that one experiences in losing a sum of money appears to be greater than the pleasure associated with gaining the same amount" (p. 279). This sentiment suggests that people are generally more prone to minimizing loss.

Although prospect theory is primarily aimed at the individual level, it has received some focus at the organizational level as well (Holmes, Bromiley, Devers, Holcomb, & McGuire, 2011). One of the ways this theory has been used among organizations is to explain

organizational risk and return. Specifically, scholars have suggested that whenever firm performance is below industry average, firms will take more risks (Holmes et al., 2011). This perspective indicates that firms and their leaders act similarly to individuals in that they all attempt to maximize value.

The perspective of maximizing expected value and loss aversion is useful for informing research on a number of issues, including security. Research in insurance suggests that people take proactive action to minimize loss through purchasing insurance with higher monthly premiums and a lower deductible despite the low probability of filing a claim (Sydnor, 2010). This finding suggests that people will often make decisions that cost more if they believe the expected loss to be high. Using insurance research to inform the discussion here, if a security breach becomes more likely and more devastating, the firm will be more likely to protect against it or avoid taking risks that might open itself up to a security breach. Thus, a firm is likely to spend more on security despite the relatively low probability of a proprietary asset breach. Conversely, as a security breach becomes less likely, the organization takes more risks to achieve maximum positive value. Such risks may include engaging in alliances with less reputable companies.

Executives are expected to know and understand their environments. How executives perform this process of information gathering, interpretation, and action has long been studied by management scholars (e.g., Daft & Weick, 1984; Dutton & Jackson, 1987; Jackson & Dutton, 1988; Thomas & McDaniel, 1990). This process of understanding the environment is predicated upon assumptions about the environment made by the executive or organization but ultimately starts with scanning (Daft & Weick, 1984). Scanning emphasizes organizations' information search and gathering process, which includes combing through the external and internal

environments (Thomas et al., 1993). Scanning is a critical component of understanding one's environment because the pieces of information that are found, or not found, can provide important clues about the environment and events that could occur.

Next in the process, executives translate information or data into knowledge and understanding about the organization's environment (Daft & Weick, 1984). Translation primarily involves making meaning from information that is gathered. Importantly, data can be straightforward, such as a major security breach of a competitor indicating a security threat, or the data can require more interpretation such as multiple probing attempts of a company's security software by external actors. Interpretation also depends upon whether the issue (e.g., technological change) is perceived or labeled as a threat or as an opportunity (Dutton & Jackson, 1987; Thomas et al., 1993) as such labeling tends to generate different actions (Dutton, Fahey, & Narayanan, 1983). In particular, viewing an issue as a threat may restrict information processing and search (Staw, Sandelands, & Dutton, 1981), while viewing issues as an opportunity is associated with opening information search and appraisal (Kiesler & Sproull, 1982; Nutt, 1984).

Finally, executives and organizations act on collected information and their interpretations of that information (Daft & Weick, 1984; Lant & Milliken, 1992; Thomas et al., 1993). Given that executives have restricted information and become more mechanistic when faced with threats (Shimizu, 2007), they will consider fewer options when they perceive security issues as threats as opposed to opportunities. In contrast, when an executive sees a security issue as an opportunity, the range of options explored and information search expands, allowing the organization to exploit a security weakness as a gain for the company. As mentioned earlier, organizations can exploit security weaknesses in a product or service by offering better protection against security threats, which can then be passed on as a benefit to consumers.

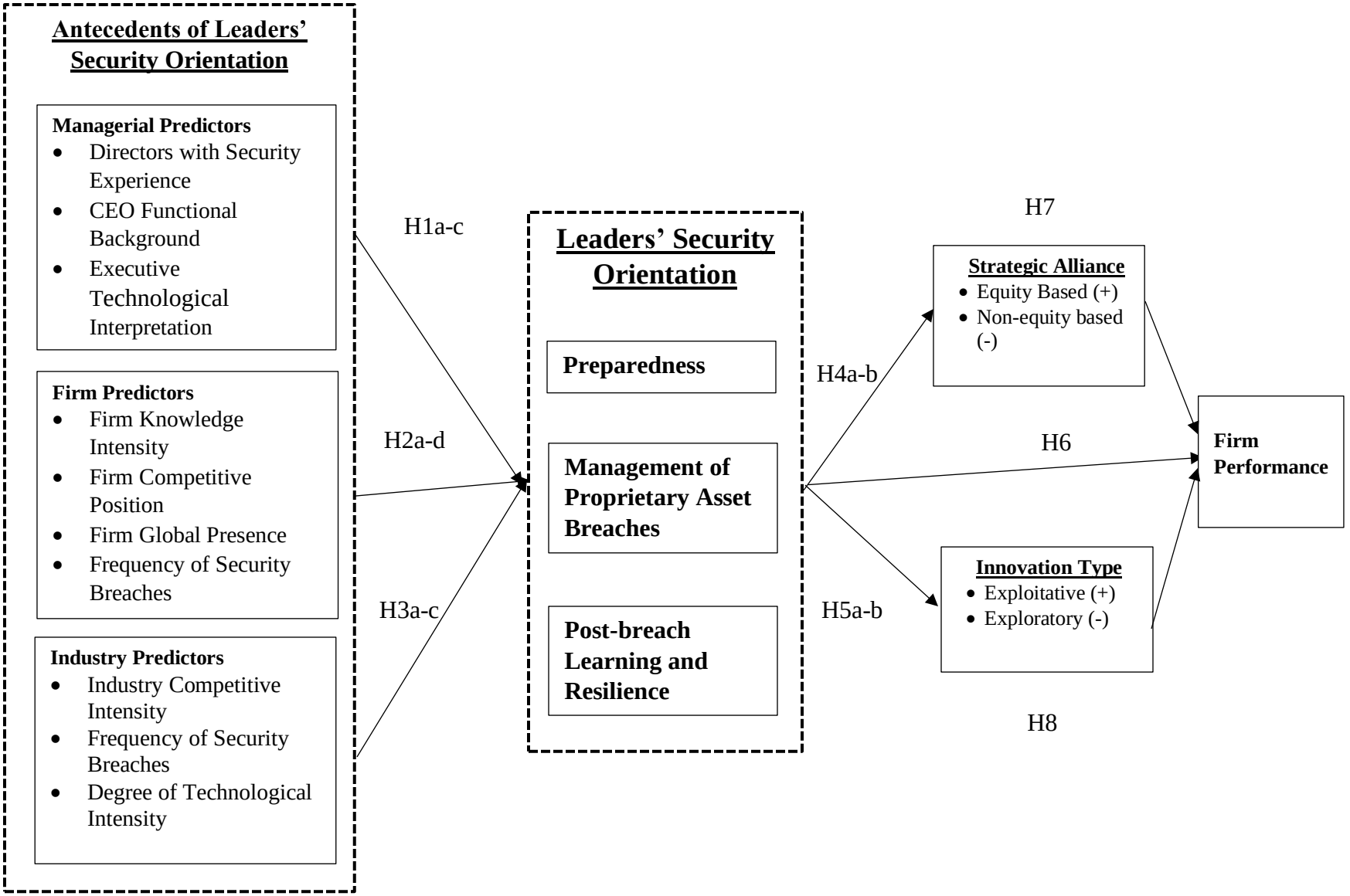
Neo-institutional theory explains why organizations look similar over time and the process of isomorphism (Meyer & Rowan, 1977). From an institutional perspective, organizations depend on external stakeholders for resource support and adopt their norms, practices, and structures in order to obtain and maintain legitimacy (DiMaggio & Powell, 1983; Scott & Davis, 2007). Over time, organizations in an industry become increasingly similar in their practices and structures, causing them to become isomorphic (DiMaggio & Powell, 1983). This isomorphism is important for establishing legitimacy for firms, which consequently drives performance (Suchman, 1995). Firms that deviate from industry norms face the potential of losing legitimacy and, subsequently, withdrawal of resource support from external stakeholders. Research on institutional theory has provided some support for this model, and scholars have argued that isomorphism legitimates (e.g., Deephouse, 1996; Pollock & Rindova, 2003), not adopting normative practices can hinder legitimacy (McKee, Mills, & Weatherbee, 2005), and adopting laws is faster when laws are forced rather than voluntary (Tolbert & Zucker, 1983), among others.

With regard to LSO, industry-wide practices create isomorphic pressure among organizational leaders to become more security oriented over time. Recent large-scale data breaches, especially in retail and healthcare sectors, have created external pressure on organizations to pursue such actions as the creation of industry standards for data protection. There have also been calls from the U.S. Securities and Exchange Commission for boards of directors to be more proactive in planning for data breaches (Securities and Exchange Commission, 2014) and lawsuits from consumers. Thus, government can force practices with regard to security breaches, or they can occur from voluntary participation in industry best practices.

3.2 Dissertation Research Model

The research model for this dissertation is presented in Figure 3 below. In the model, I argue three types of predictors influence the development of LSO: managerial, firm, and industry. Managerial predictors include the number of members on the board of directors with security experience, the CEO's functional background, and executive environmental interpretations. Firm level predictors include knowledge intensity, competitive position, global presence, and the frequency of security breaches. LSO, as represented in the research model, consists of three dimensions: preparedness, management of security breaches, and post-breach learning and resilience. Finally, I focus on three categories of strategic LSO outcomes: strategic alliances, innovation type, and firm performance.

Figure 3: Antecedents and Consequences of Leaders' Security Orientation



3.3 Leaders' Security Orientation Overview

Organizations inevitably face security threats that require them to take action to protect their valuable resources. Management scholars have focused on organizations' efforts to protect against various external threats such as those that emanate from competitors (Dutton & Jackson, 1987; Thomas, Clark, & Gioia, 1993). These threats to organizations influence executives' sensemaking processes and strategic actions in response to these threats (Thomas et al., 1993). There are three components of the strategic sensemaking process: scanning, interpretation, and action (Daft & Weick, 1984). In the context of security threats, organizations gather information about threats through various sources, attach meaning to them, and take actions in order to neutralize these threats. They can also gather information about security threats from a variety of sources including its directors, past experiences, and competitors. As Morgeson, Mitchell, and Liu (2015) note, "events occur over time, playing a major role in shaping thoughts, feelings and actions" (p. 515). For example, the Target and Home Depot data breaches of 2014-2015 should have led retailers to reexamine their security measures protecting consumer information. Similarly, organizations in industries that face frequent corporate espionage attempts from competitors are expected to have more mechanisms in place to prevent the trade secret theft. In addition to the substantive changes they make following security breaches, organizational leaders also engage in a collective sensemaking and sense giving processes in an attempt to explain why these incidents happen and what they mean for their firm going forward. Sensemaking, sense giving, and post-crisis learning all enable firms to develop a more robust security orientation and take actions aimed at protecting their proprietary resources from future security threats.

In response to external threats, organizational leaders make changes to address these threats, including interpreting them as positive learning opportunities (Thomas et al., 1993). In

this dissertation, I argue that greater security orientation among organizations address three components: preparedness, management of security breaches, and post-breach learning and resilience.

The preparedness dimension of LSO is concerned with top management's awareness and understanding of security threats related to proprietary assets, proactiveness in addressing emerging potential security threats, and training for these events. Similar to the general crisis perspective of preparedness whereby organizations prepare for or prevent crises, the preparedness component of LSO refers to a state of readiness to deal with the onset of a security breach or threat related to proprietary assets. Moreover, preparedness involves developing plans, instituting security measures, creating coping strategies, purchasing insurance, utilizing communication systems, collecting information, hiring staff, developing organization-wide training programs, and many other security related activities. Similar to the response function of organizational crisis management, the management dimension of LSO focuses on organizational responses. Management of proprietary asset breaches includes taking disciplinary actions against offenders, implementing speedy response to the event, communicating the event, prioritizing a response, as well as devoting resources to deal with security threats.

Finally, the post-breach learning and resilience dimension of LSO, analogous to learning and resilience in organizational crisis management, primarily involves organizational leaders' ability to allocate resources quickly and effectively to a security breach as well as being able to develop organization-wide learning. This function of LSO is comprised of leaders' adaptation to threats, comprehensive assessment of further security vulnerabilities, speedy implementation of security plans, continuous training programs, and remedial action when security related deficiencies are observed.

Specific to leaders' security orientation, I focus on managerial, firm, and industry antecedents. Managerial predictors are primarily situated at the managerial level of the firm. These predictors are focused on top managers and the board of directors who develop and approve the strategies of the firm while also prioritizing impending threats, shaping how the organization acts (Finkelstein et al., 2009). Firm-level antecedents are focused on the experiences of the firm, how the firm is situated in terms of its focus, and its relative position in the market. These predictors should shape the firm's focus. For example, frequently experiencing security breaches should focus the firm's attention on that issue. Similarly, a competitive position should direct the firm's attention towards minimizing risk and avoiding loss by focusing on organizational security. Last, industry predictors should also shape leaders' focus on security. Strong institutional forces can shape the adoption of norms and practices (Scott & Davis, 2007). As such, industry factors such as experiences with particular issues (e.g., security incidents), more technology in an industry, and competition represent institutional factors that influence a firm's orientations.

Drawing insights from the upper echelons and other theories, I hypothesize that managerial predictors such as director experience, CEO functional background, and executive environmental interpretation are associated with the development of LSO. I also argue that firm predictors, including knowledge intensity, competitive position, global presence, and frequency of security breaches are related to the development of LSO. Finally, industry variables such as competitive intensity, frequency of security breaches, and technological intensity serve as important antecedents to a firm's LSO. In this study, I suggest that managerial predictors, such as experiences of the firm, its managers and directors, and executive interpretations of the environment positively relate to a firm's LSO. More specifically, I argue that firms with directors

or CEOs with more security experience will be more likely to develop higher levels of LSO. At the firm level, I argue that firms more focused on knowledge and competition are more likely to have security oriented leaders. Firms that are globally situated will be higher in LSO. Firms that experience more frequent proprietary asset breaches will also be more security oriented. Finally, I propose that firms in industries with certain characteristics will be more likely to develop higher levels of LSO. For example, industries that are more competitive, experience frequent security breaches, and have more technological intensity will most likely have leaders with higher levels of LSO.

In this dissertation, I propose that leaders' security orientation has an influence on a firm's strategic choices, including strategic alliance activity, innovation, as well as firm performance. These arguments are rooted in dynamic capabilities (Teece et al., 1997), which suggest that leaders' security orientation offers a unique capability for firms and influences their behaviors. Organizational leaders with greater security orientation are more likely to develop capabilities to mitigate the negative consequences of knowledge sharing in inter-organizational collaborations. Given their superior capability in establishing contractual and behavioral safeguards, I argue that firms will be more likely to engage in equity strategic alliance activities since equity strategic alliances are more likely to include contractual safeguards (Manhart & Thalmann, 2015; Oxley, 1997; Quintas, Lefrere, & Jones, 1997). In addition, the more security oriented a firm's leaders are, the more likely that firm will commit resources in innovation activities that are less prone to expropriation. An orientation in security helps firms understand how to exploit incomplete factor markets by offering superior security protection in their products and services, while also maximizing appropriability of firm innovations. Finally, I argue that LSO is positively related to firm performance. These arguments are based on the idea

that security oriented firms take an active approach to protecting their resources against various threats. Because of this protection, these security oriented firms have confidence in their strategies and choose to engage more freely in innovation and strategic alliance. In addition, this focus on protection benefits firm performance by assisting with appropriation of innovation and reducing expropriation. Appropriation is defined as "the degree to which firms capture the profits associated with their innovative activity and are often considered to reflect the degree to which valuable knowledge spills out into the public domain" (Cohen and Leventhal, 1990, p. 138). Expropriation is the extent to which firms' property, including patents, are stolen or lost to external actors, such as thieves or competitors.

3.4 Antecedents of Leaders' Security Orientation

In this section, I make arguments regarding the relationship between the antecedents of LSO and LSO itself. The managerial antecedents of LSO are grounded in upper echelons theory (Hambrick, 2007; Hambrick & Mason, 1984), strategic sensemaking (Dutton & Jackson, 1987; Thomas et al., 1993), and prospect theory (Kahneman & Tversky, 1979). I also use strategic sensemaking, institutional theory (Meyer & Rowan, 1977; Dimaggio & Powell, 1983), and prospect theory (Kahneman & Tversky, 1979) to argue that firm, and industry characteristics are related to LSO. Finally, I argue that institutional pressures force firms to adopt norms and practices to gain and maintain legitimacy (Dimaggio & Powell, 1983; Suchman, 1995; Meyer & Rowan, 1977). A result of these institutional pressures is that firms in an industry with such norms become more security oriented over time.

3.4.1 Managerial characteristics and LSO

The firm's board of directors often serves as an important source of direction and guidance (Finkelstein et al., 2009; Hillman & Dalziel, 2003). Often, the board is useful in

identifying opportunities for firms (Cho & Hambrick, 2006). For example, a board's functional heterogeneity can influence focus on particular topics such as entrepreneurial issues (Tuggle, Schnatterly, & Johnson, 2010). Thus, stronger representation of a particular group, in the form of functional expertise, on a board of directors can push the board into longer, more impactful discussions on a particular issue of interest to the board.

If a firm faces security incidents, the board of directors must focus on security issues and, consequently, become more security oriented. As a 2016 Harvard Global Board of Directors Survey observed, over a third of directors cite cybersecurity as a top priority (Daum, Stuart, & Stautberg, 2016), highlighting the importance of this issue for board of directors. Thus, a board comprised of directors with security experience will be more likely to focus on ensuring security in the organization. Directors gain security experience by virtue of their positions (e.g., Chief Information Officer, Chief Technology Officer, Chief Security Officer, Chief Risk Officer). These directors will be more likely to know the full range of threats posed to the organization. They will also have a greater understanding of how these threats can be mitigated and emphasize security in board meetings to ensure the firm is protected against them. Given their experience and understanding, firms with a higher proportion of directors with security experience should have a greater orientation towards security.

H1a: The presence of directors with security experience will be positively related to leaders' security orientation.

As mentioned previously, executives' experiences heavily influence their interpretations and decisions. Experience in output functions such as marketing, sales, and product development generally makes an individual more attuned to issues outside the firm, like growth and searching for opportunities (Hambrick & Mason, 1984). In contrast, throughput functions, such as

production and accounting, tend to focus individuals more inwardly, towards issues such as operations. For example, Rajagopalan and Datta (1996) found that CEOs with more throughput experience were associated with higher industry concentration and capital intensity and negatively associated with product differentiation, industry growth, and demand instability. As such, throughput functional expertise can be viewed as emphasizing stability and minimizing uncertainty. This perspective is also reflected in Musteen, Barker, and Baeten's (2006) study, which found that CEOs with throughput functional expertise were less likely to accept change than CEOs with output functional expertise.

An executive, such as a Chief Operations Officer, who is usually responsible for daily operations and is below the CEO, would likely be focused heavily on issues affecting the operation of the firm and more oriented towards security. Given this inward focus, a COO functional background should prioritize threats directly facing the firm over opportunities for growth. Thus, CEO functional background as COO or in operations should be positively related to LSO and ensuring stability of operations through security of the organization.

H1b: CEO experience in the operations area will be positively related to leaders' security orientation.

Executive technological interpretation refers to executives' interpretation of strategic threats from technological changes. Technological changes in an organization's environment require that the organization adapt or fall behind (Anderson & Tushman, 1990). Given that swift technological changes can disrupt stability; organizations may view these changes as threats that must be protected against. Technological change also presents challenges in the sense that new and innovative security threats can potentially harm an organization. For example, the growing market for connected products and driverless vehicles is vulnerable to the threat of hacking.

Consequently, organizations that protect against these new threats offer a benefit, and they can advertise their product's safety over competitors who cannot.

Past research suggests that when executives perceive an issue as a threat, they will become more risk averse (Staw et al., 1981). Thus, when an organization's executives interpret technological change as a threat, they are more likely to become security oriented, viewing security as a threat and implementing security as a way of helping the organization avert loss. In addition, they should expand their security information search, drawing more attention to security issues and becoming more proactive in their approach to organizational security. Consequently, organizations poised to exploit security challenges as threats will be more security oriented.

H1c: Executive technological interpretation as a threat will be positively related to leaders' security orientation.

3.4.2 Firm characteristics

Firm knowledge intensity is "the extent to which a firm depends on the knowledge inherent in its activities and outputs as a source of competitive advantage" (Autio et al., 2000, p. 913). Knowledge intense firms depend upon effective utilization of knowledge for survival (Alvesson, 1995; Robertson et al., 2003). Past studies have linked knowledge intensity to firm financial performance (e.g., Autio et al., 2000), such that knowledge creation leads to better financial performance, which can be particularly valuable in international markets. Knowledge intense firms also employ enhancements in all of their knowledge processes, including knowledge creation, knowledge sharing, knowledge acquisition, and knowledge storage and documentation (Andreeva & Kianto, 2011). Frequently, knowledge intensity is measured as R&D spending or number of patents from corporate data (Autio et al., 2000; Haahti, Madupu,

Yavas, & Babakus, 2005), but it has also been assessed through direct questions to survey respondents (Haahti, Madupu, Yavas, & Babakus, 2005).

Having more knowledge and understanding of a specific technology inevitably helps understand its weaknesses. In turn, a greater understanding of a technology's weaknesses helps identify what security threats, if any, are present in a particular technology or product. Thus, knowledge intense firms should benefit from a greater understanding of the threats an organization faces. Given that past research finds that knowledge intensity assists in all knowledge processes (Andreeva & Kianto, 2011), it should then be likely that this includes knowledge processes related to security threats. Moreover, gains through intense knowledge development should facilitate the processes of sensemaking, described earlier.

During the scanning portion of sensemaking, firms with greater knowledge developed through their prioritization of it should have a better understanding of the information they find and the threats they face. This information should be helpful in identifying ambiguous security threats, which would go unnoticed by less knowledgeable firms. Moreover, the additional knowledge such firms possess should help them correctly interpret the threat and take effective action to either mitigate it or exploit it as an opportunity.

Considering that knowledge intense firms' survival is based on their knowledge, it is in these organizations' best interest to ensure that their knowledge is protected. As noted in Chapter II, knowledge intensity plays a role in organizations' need for more protection (Hashai, Asmussen, Benito, & Petersen, 2010), often forcing firms to focus on threats to appropriation that arise from opportunistic actors (Coff, 2003; Hashai & Almor, 2008). Leaks from employees, former employees, hacks, and others can provide competitors with valuable information, which can threaten a firm's competitiveness. This competitive interest from companies in securing their

resources from harm should focus organizations' efforts on protecting against expropriation. Such efforts include employee non-disclosure agreements, non-compete agreements, or requirements to protect information from loss or theft.

Firm knowledge intensity should be positively related to LSO. Knowledge intensity should assist a firm in environmental scanning for security threats, help with correctly identifying and interpreting relevant security threat information, and facilitate appropriate action to protect against the threat or exploit information for market benefits. Knowledge intensity helps firms decode highly complex knowledge (Autio et al., 2000), leading to better interpretation of information. Information about security threats can be highly complex. Some threats require specialized knowledge as to how they can harm a company. As such, knowledge-intense firms should be able to find this information, interpret the threat, and take action to mitigate it. Conversely, less knowledge intense firms should be less capable in these areas, in part, because of their inability to discern security threats appropriately and their inability to capitalize on them. According to Mudambi (2002), firms in R&D intense industries must make investments that contribute to scanning and identification (or in this case interpretation). Given these investments, knowledge-intense firms are more likely to search for and discover security related issues that pose a threat to the firm. Accordingly, we should expect that knowledge-intense firms will be more security oriented.

H2a: A firm's perceived knowledge intensity is positively related to leaders' security orientation.

A firm's market share serves as a proxy for its competitive position, relative to its competitors. A higher market share represents a higher standing in the market over its competitors. As noted in past research, either sustaining or gaining industry leadership is often a

key objective for organizations (Ferrier, Smith, & Grimm, 1999). There are benefits for these industry leaders. They often enjoy greater profits through economies of scale, market power, and reputational benefits (Armstrong & Collopy, 1996; Lieberman & Montgomery, 1988).

Despite the benefits of better competitive positioning, past research has shown that market leadership is seldom sustainable, with market leadership quickly eroding for many market leaders (Ferrier et al., 1999; Weiss & Pascoe, 1983). This is especially true for firms that fail to correctly understand their competitive environment and either take incorrect or no action to prevent erosion (Ferrier et al., 1999). It is important, then, for an industry leader to be on top of evolving threats related to security and the market. Tversky and Kahneman (1992) suggest that executives will become risk averse related to losses of low probability. This argument explains why so many people buy insurance for catastrophic events (Kahneman & Tversky, 1979).

The threat of losing market share is a significant consideration for industry leaders (Ferrier, Smith, & Grimm, 1999). As such, this threat is likely to dominate their attention, especially in hypercompetitive environments. In consideration of these arguments, firms' leaders with better competitive positioning should be more focused on issues in the environment and organization and take action to mitigate potential losses associated with proprietary asset breaches.

H2b: A firm's perceived competitive position is positively related to leaders' security orientation.

A firm's global presence represents the size or number of international operations. A firm with a greater proportion of sales from international operations has a more global presence than firms with a lower proportion of sales from international operations. Expansion of global

presence creates value opportunities for firms. These opportunities include economies of global scale, economies of global scope, tapping optimal locations for activities and resources, and maximization of knowledge transfer (Gupta & Govindarajan, 2001). Exploitation of these opportunities can lead to global competitive advantage (Gupta & Govindarajan 2001). A large volume of work has examined the value of knowledge flows garnered from multinational operations (e.g., Athanassiou & Nigh, 2000; Awate, Larsen, & Mudambi, 2015; Gupta & Govindarajan, 1991; Johanson & Vahlne, 1977; Kogut & Zander, 1993).

Consistent with the notion that global presence provides opportunities to create value, firms' global presence should be positively related to LSO. International operations allow for wider breadth of scanning for threats, a broader base for interpretation, and, as a consequence, more accurate action. Logically, the threats a company faces in one foreign country may be greater than the threats in its domestic operations. For example, kidnapping executives is of little concern in the United States but poses more risk in Mexico or India. By extension, expanding operations globally exposes the firm to a wider range of security threats that it must find, understand, and protect against. Moreover, laws differ significantly by country, with some countries often offering little formal protection of proprietary knowledge. Consequently, firms in such countries must find other mechanisms to protect their valuable resources.

Scholars have long understood the problems of internationalization and security. Oviatt and McDougall (1994), for example, suggest that software firms that quickly internationalize must develop protection mechanisms for their products to prevent expropriation. Internationalization raises challenges for firms as they must protect their proprietary knowledge on a global scale. This challenge also offers valuable opportunities for firms. Knowledge gained about security threats and the appropriate prevention mechanisms can be transferred to an office

in another country. For example, lessons learned from U.S. combat operations in Afghanistan are often applied to combat operations in Iraq (Hajjar, 2014), and vice versa. International firms rely on both formal measures, such as patent protection, as well as informal measures, such as secrecy (de Faria & Sofka, 2010) just as non-international firms do. However, the scope and type of approaches to security differ between international and domestic firms. For example, de Faria and Sofka (2010) examined the difference in breadth of knowledge protection strategies of international and host country firms. They found that multinational corporations differ in their protection strategies from domestic firms because the former chose from a wider breadth of options than their domestic counterparts.

H2c: Firm's global presence is positively related to leaders' security orientation.

Frequency of security breaches refers to the number of recent security breaches that a firm has faced. Security breaches are a significant threat to organizations, impacting market value (Cavusoglu, Mishra & Raghunathan, 2004; Goel & Shawky, 2009; Kannan, Reese, & Sridhar, 2007), reputation (Berezina, Cobanoglu, Miller & Kwansa, 2012), downtime and recovery costs (Garg, Curtis, & Halper, 2003), and perceptions of fear and safety (Ryan, 1993; Sonmez, Apostolopoulos, & Tarlow, 1999). The more these significant events occur, the more likely they are to have an impact on the organization. I anticipate that the frequency of security breaches that an organization faces is positively related to a leader's security orientation. Firms that frequently face or experience security threats should be better poised to understand the threat and take action to prevent future recurrence.

Awareness of events and threats plays a significant role in the actions he or she takes. This is especially true in the realm of security. For example, farmers have been found to be more likely to adopt security measures against bioterrorism if they frequently had unauthorized people

on their farms (Buttars, Young, & Baily, 2006). In addition, the perceived severity of the breach and vulnerability to it is significantly related to one's intention to adopt security measures (Lee & Larsen, 2009). Because of this, organizations that frequently experience these events will be more likely to view themselves as more vulnerable to security incidents and adopt protection mechanisms accordingly.

Negative events motivate organizations to actively prevent their return. For example, in the wake of the September 11, 2001, terrorist attacks, the United States adopted numerous security measures to prevent another major attack. Conversely, past studies suggest that the adoption of protective behaviors reduces security incidents (e.g., Safa, Von Solms, & Futcher, 2016; White, 2015). Thus, in the face of security incidents, especially as they grow more frequent over time, organizations should be more likely to adopt security measures to protect against security threats.

H2d: Leaders of organizations with frequent experience with proprietary asset breaches exhibit a high level of security orientation.

3.4.3 Industry characteristics

Industry competitive intensity is usually measured as a perception by firms' executives of how intense competition is in an industry (e.g. O'Cass & Weeraardena, 2010) or simply by the industry concentration ratio. Industry competitive intensity research has gleaned valuable insights into the benefits of intense competition but has also highlighted the drawbacks of intense competition as well. Studies have shown that competition is beneficial in that it helps firms to develop capabilities (Barnett et al., 1994; Levinthal & Myatt, 1994). Additionally, industry competitive intensity helps firms to develop learning capabilities (Weerawardena et al., 2006;

O'Cass & Weeraardena, 2010). However, research also suggests that competitive intensity is associated with unethical behavior (Schwepker, 1999).

Competitive industries are more likely to have aggressive competitors that engage in unethical actions such as espionage or trade secret theft (Mezias & Boyle, 2005; Sahaf, 2002). These actions targeting proprietary assets should be expected to prompt firms to adopt industry security norms to protect against loss. According to Shahaf (2002), competitive intensity hastens the use of proprietary asset protection functions such as intelligence. Considering this, we can expect that over time, all organizations will develop and implement similar protective functions in competitive industries.

H3a: Perceived industry competitive intensity is positively related to leaders' security orientation.

The frequency of security breaches in an industry refers to the number of recent security breaches in an industry. Frequent security breaches in an industry can send a signal to other firms in an industry that a threat is growing or is of sufficient significance that it should be addressed by those firms.

The more frequently an industry faces security threats such as breaches, the more likely it is firms will be more security oriented. Frequent attempts or incidents signal that an attacker is interested in a particular asset of firms in an industry. Consequently, firms should react by protecting the assets of interest. For example, an increase in the number of thefts at department stores could lead all companies in that industry to look for new methods of protection against theft. As organizations scan their environment for threats and opportunities, it is likely that they will uncover these frequent attacks, interpret the threat of security breaches as increasing, and act accordingly to mitigate harm to the organization's resources. Although threats such as security

breaches can and do narrow the range of options chosen by a particular organization, frequent security breaches are unambiguous, are likely to be easy to interpret, and offer obvious choices of resolution.

H3b: Leaders of organizations operating in industries with frequent proprietary asset breaches exhibit high security orientation.

Degree of technological intensity refers to an industry's reliance on technology. More specific to firms themselves, firms with a higher degree of technological intensity are those with more transformability in their processes and infrastructure (Meyer & Scott, 1992; Lepak, Takeuchi, & Snell, 2003; Thompson, 1965). More importantly at the industry level, technological intensity "determines the opportunities of a firm to acquire new technologies, assimilate them, and apply them to commercial ends" (Wu, 2012, p. 491). Moreover, high-tech sectors require rapid adaptation to remain viable (Wu, 2012). Technological intensity, due to the nature of products and services, require proprietary knowledge that is critical to firm survival (Osborn & Baughn, 1990).

Firms in high technological intensity settings require more and different types of protection against security threats in order to survive than those in low technological intensity settings. As security and protection of proprietary knowledge becomes more of a prerequisite to survival, these firms are more likely to be security oriented. For example, a firm that is required to or dedicated to developing new technology must protect against a multitude of threats ranging from external competitors, to internal leaks, to hackers and other malicious actors. Given that the breadth of threats is so vast in comparison with non-technologically intense industries, firms in technologically intense industries will be more focused on the security of their respective industries. Another benefit of industry technological intensity with regard to security is the

common knowledge of security threats, and resolutions to them, that are frequently discussed at tradeshows and industry conferences. Overall, industry technological intensity should be related to LSO.

H3c: An industry's degree of perceived technological intensity is positively related to leaders' security orientation.

3.5 Outcomes of Leaders' Security Orientation

Consistent with prospect theory, I argue that as firms become more security oriented, they understand more about security threats and are less likely to engage in risky behavior that would increase the probability of a negative outcome. As such, we can expect that organizations will choose alliance and innovation strategies that put the firm at less risk of a negative outcome.

3.5.1 LSO and cooperative strategies

Cooperative strategies, such as strategic alliances and joint ventures, have long been identified as effective mechanisms through which to acquire or pass on knowledge and information (Simonin, 1999). Although their effectiveness in transferring knowledge has often been questioned (Attewell, 1992; Kogut & Zander, 1992; Tiemessen et al., 1997), organizations still engage in cooperative agreements to acquire knowledge and achieve project goals. However, these interorganizational arrangements create issues for knowledge sharing and protection (Jarvenpaa & Majchrzak, 2016). I expect that the issues surrounding knowledge sharing and protection will induce firms to engage in equity strategic alliances due to their ability to minimize risk exposure (Das & Teng, 2000).

Engaging in cooperative agreements raises challenges for firms. Companies must balance their own needs for information accrual against the potential that they lose information to their partners and possibly competitors (Oxley & Sampson, 2004). Cooperative strategies pose

a risk for firms where expected gains and losses are often unclear. In the face of these uncertain decisions, prospect theory would suggest that organizations select strategies that are more risk averse than those that are more risk seeking (Holmes et al., 2011). Equity strategic alliances represent a way of lowering the probability of loss through contractual controls while non-equity strategic alliances have less ability to control the probability of loss through opportunism. Thus, firms higher in LSO will be more risk averse and choose equity strategic alliances that are less prone to expropriation than non-equity strategic alliances.

Scholars have identified several challenges related to information transfer in alliances including providing a partner with information about strategic directions, benchmarking data, potential to identify and recruit talent away from a firm, access to codified knowledge, and access to tacit knowledge (Oxley & Sampson, 2004). Thus, the protection of knowledge is extremely difficult (Liebeskind, 1996; 1997), especially in arrangements where partners can exploit the other's information or knowledge. As Oxley and Sampson (2004) note, "successful completion of alliance objectives often requires a firm to put valuable knowledge at risk of appropriation by alliance partners. Firms must therefore find the right balance between maintaining open knowledge exchanges…. and controlling knowledge flows to avoid unintended leakage of valuable technology" (p. 723). This balance of exploring knowledge from partners while also facing the potential of losing their own knowledge is referred to as a boundary paradox (Quintas, Lefrere, & Jones, 1997), which many scholars have discussed (Manhart & Thalman, 2015; Olander, Vanhala, & Humelinna-Laukkanen, 2015).

According to a number of studies, organizations often structure cooperative strategies based on concerns of imitation and reduced appropriation (e.g., Inkpen, 2000; Oxley & Sampson, 2004). Thus, organizations will engage in knowledge protection efforts to mitigate the potential

of opportunism in alliances and other inter-organizational agreements. Such knowledge protection has been identified a "precondition" of effective knowledge management (Gold & Arvind Malhotra, 2001). Norman (2001) identified three categories of knowledge protection in strategic alliances: human resources, legal structure of agreements and contracts, and alliance processes. The human resources category of knowledge protection involves governance of employees' protection of knowledge (Norman, 2001), including training, compliance programs, and monitoring and surveillance. The legal structure of agreements and contracts includes patenting or contracts, such as identification of proprietary information. The final category, alliance processes, includes governing information flows. For example, an organization might compartmentalize knowledge by only allowing certain aspects of a project to be revealed to a limited number of people.

Organizations that are more aware, or at least more concerned, with the spillover of knowledge to their partners are more likely to take action to mitigate these concerns actively using various protection measures, such as non-disclosure agreements as well as the creation of norms of sharing information in strategic agreements (Jarvenpaa & Majchrzak, 2016). Specifically, organizations that view or recognize that cooperative strategies can be a threat to their security are likely to believe their best interests are protected by structuring their agreements such that it is more difficult for a partner to gain proprietary information from the focal firm.

Concern for knowledge protection among organizations is an important predictor of their choice of cooperative strategy (Pisano, 1988). Indeed, selecting a governance structure of alliances is important to knowledge creation, knowledge sharing, and knowledge protection (Kale, Singh, & Perlmuter, 2000; Oxley, 1997). Research grounded in transaction cost

economics suggests that firms will engage in particular types of cooperative strategies to reduce transaction costs associated with spillover or leakage (Oxley & Sampson, 2004; Pisano, Russo, & Teece, 1988). Specifically, equity-based joint ventures are believed to enhance knowledge protection (Das & Teng, 2000; Pisano, 1988). The reason for this is that equity-based alliances allow a partner to gain control of assets developed during the partnership should another partner terminate the contract (Pisano, 1988). Moreover, contract provisions help reduce opportunism and enhance monitoring.

In the face of a gamble such as a strategic alliance, firms higher in LSO are more likely to view strategic alliances as a way of mitigating risks to proprietary assets associated with knowledge and resource sharing. This perspective suggests that firms' risk aversion influences their decisions, consistent with prospect theory. Given these findings from past research, it is likely that organizations that are aware of the threats posed to their proprietary knowledge will select equity-based alliances in an effort to protect against expropriation, affording firms the opportunity to minimize the potential for loss. Moreover, such equity-based alliances give firms the ability to enforce action against alliance partners who violate the terms of an agreement. Finally, it is also likely that equity-based alliances and firms' experiences with them will allow the firm to develop superior contracts that help protect against future security violations by a partner. These contracts should be superior due to a unique focus on reducing opportunities to exploit knowledge sharing during or after the contract. Thus, there is less chance that a partner can take advantage of another member of the partnership.

H4a: Leaders' Security Orientation is positively related to equity strategic alliances.

In contrast with equity-based alliances, firms higher in LSO will avoid non-equity-based alliances more than firms lower in LSO. The rationale for this argument is the parallel opposite

of Hypothesis 4a, which predicts that LSO is positively related to equity strategic alliances. Specifically, firms that are more concerned with expropriation will avoid non-equity-based alliances, which allow access to proprietary assets in a less restrictive and controlled manner. The inability of a firm to adequately control the partner firm's opportunism through non-equity alliances is likely to deter a firm from engaging in non-equity alliances (Das & Teng, 1999), especially in the context of expropriation where the probability of loss can be expected to increase. This lack of control exposes the firm to risks that are likely to result in lower expected value, increased uncertainty, and higher risk of expropriation. Moreover, firms' leaders engaging in non-equity strategic alliances are likely to expect greater losses under them and avoid them altogether to avoid performance loss. Considering the aforementioned arguments related to prospect theory, organizations will avoid these non-equity strategic alliances in favor of equity strategic alliances

H4b: Leaders' Security Orientation is negatively related to non-equity strategic alliances.

3.5.2 LSO and innovation strategies

Organizations' concerns for protecting innovations and maximizing appropriability should serve as an important driver of innovation strategies (Cassiman & Veugelers, 2006). Thus, an organization's security orientation should be related to their strategic choices regarding innovations. In the strategy literature, two approaches have received considerable attention: exploratory and exploitative innovation (March, 1991). Exploratory innovation refers to the pursuit and development of new knowledge, products, and services for nascent customers and markets (Benner & Tushman, 2003). Exploitative innovation emphasizes development of existing knowledge and existing products and services for current customers and markets

(Benner & Tushman, 2003). Firms higher in LSO should be more conservative in their strategies hoping to minimize expected loss and, thus, more likely to pursue exploitative innovation.

Similar to the arguments made in the section on LSO and cooperative strategies, I argue that innovation strategies, in the form of exploratory or exploitative innovations, represent decisions involving risk and uncertainty. Predicting firm innovation strategy under prospect theory arguments should be predicated upon deciding which strategy affords the most protection from loss. With a higher LSO, organizations will favor safer exploitative innovations over exploratory innovations due to the higher probability of loss from exploratory innovation. With low LSO, firms' leaders will favor riskier exploratory innovations over exploitative innovations due to the lack of risk aversion.

Past research suggests that an organization's characteristics influence the two approaches to innovation. For example, an organization's centralization, connectedness among members, and the formality of its rules influences innovation decisions (Jansen, Van den Bosch, & Volberda, 2006). In their study of exploration and exploitation in financial service firms, Jansen and colleagues (2006) argued that centralization, formalization, and lack of connectedness among members is positively related to exploitative innovation because it inhibits access to new knowledge and deviation from norms. In this way, people will stick to what they know and not try new things.

Jansen and colleagues' (2006) study is particularly relevant to LSO for a few reasons. First, centralization and formality are important for security in organizations. LSO is concerned with minimizing the risk of loss to its resources. As such, firms higher in LSO will focus more on implementing measures to prevent security breaches. Second, LSO will often influence leaders to adopt rules that prevent employees from connecting with one another. For example,

many security controls prevent employees from speaking to one another about company projects (Liebeskind, 1997). Inevitably, those measures will reduce communication between employees and prevent them from seeking knowledge from other employees (Hannah & Robertson, 2015).

Consistent with these past empirical findings, a firm's overall security orientation should be negatively related to exploratory innovation and positively related to exploitative innovation. Considering this perspective, firms that have adequately protected their resources and are high in LSO are more likely to minimize opportunities to find and use new knowledge and, as a result, be more likely to use exploitative innovation. Stated differently, firms more concerned with the protection of their resources are more likely to develop security measures to prevent expropriation and, consequently, be more risk averse in their innovation strategies.

H5a: Leaders' security orientation is positively related to exploitative innovation.

Leaders' security orientation should also be negatively related to exploratory innovation. In contrast with the arguments related to Hypothesis 5b, exploratory innovation requires that firms be open and connected with members and external actors. For example, to be more exploratory with innovation, a firm might encourage open exchange of information. This open exchange reduces the organization's ability to appropriate rents from innovations if proprietary information is leaked to competitors (Jansen et al., 2006). Thus, exploratory innovation is likely viewed as a direct threat to appropriation by firms scoring higher in LSO, resulting in a lower expected value from exploratory innovation activity. Considering these arguments, firms higher in LSO are unlikely to engage in such efforts as they might expose, or needlessly endanger, firms' proprietary assets.

H5b: Leaders' security orientation is negatively related to exploratory innovation.

3.5.3 LSO and firm performance

A firm's LSO and financial performance should be positively related. The benefits derived from protecting resources, avoiding expropriation, and minimizing loss from security events should help a firm by protecting or gaining competitive advantage. Scholars have long asserted this perspective, believing that protection of an organization's technological core is of utmost importance (Thompson, 1967). Thus, organizations that are better prepared for, respond to, and learn from security events should be able to avoid severe negative financial consequences of security failures. Considering the examples listed in the introduction and literature review of this work, organizations have lost hundreds of millions of dollars following security events.

Firms with an emphasis on security should be able to reduce their costs, resulting in improved firm financial performance. Regarding supply chains alone, firms that emphasize supply chain security were able to reduce theft by 38%, limit cargo delays by 49%, and experienced a 29% reduction in transit time, among other benefits, which should have a direct impact on firm performance (Peleg-Gillai, Bhat, & Sept, 2006). Similarly, firms that implemented U.S. government security programs were often able to increase their competitive advantage (Ritchie & Melnyk, 2012). Given that an estimated 75% of employees steal from their employers and an estimated 5% of annual revenue is lost to theft (Russakoff & Goodman, 2012), it would not be surprising to find that LSO improves firm financial performance.

H6: Leaders' security orientation is positively related to firm performance.

3.5.4 Equity alliances and firm performance

Equity strategic alliances create value by incorporating contractual and behavioral (e.g., trust) safeguards (Gulati, 1995; Inkpen, 2000). Equity partnerships should mediate the relationship between LSO and firm performance. When firms' leaders become more security

oriented, they will understand the risks associated with strategic alliances, develop appropriate safeguards to protect against expropriation in equity strategic alliances, and extract more value from their use in an equity strategic alliance. This value process suggests that equity strategic alliances are a mechanism through which LSO and firm performance are linked. Firms led by leaders with high LSO are expected to incorporate more safeguards in equity strategic alliances. When these safeguards are in place, there will be more information and knowledge sharing (Norman, 2002; Oxley, 2004). These safeguards minimize the probability of loss, allowing firms to maximize gains from strategic alliances (Inkpen, 2000). In addition, these safeguards should reduce expropriation from alliance partners to increase gains from alliance activities. For example, an executive higher in LSO would likely analyze the risks of expropriation in an equity-based strategic alliance, institute protection mechanisms such as regulating employee behavior in the alliance (Jarvenpaa & Majchrzak, 2016) that minimize opportunism, theft, or expropriation from potential alliance partners, and extract more value from the alliance by protecting the focal firm's proprietary assets while simultaneously actively participating in the alliance. In this way, LSO represents a dynamic capability for risk avoidance and improved ability to extract value from equity-based strategic alliance activities.

Firms are likely to share their resources to the extent that they believe their resources will not be stolen. Firms higher in LSO are likely to positively view the expected value from engaging in equity strategic alliances and extract more value from the relationship by designing and implementing appropriate controls to minimize risk of expropriation and opportunism, leading to higher firm performance.

H7: Equity strategic alliances mediate the relationship between LSO and firm performance.

3.5.5 Exploitative innovation and firm performance

Similar to the arguments above, I expect that exploitative innovation strategies mediate the relationship between LSO and firm performance. Firms choose innovation strategies based on the maximum expected value and minimize loss through choosing strategies that improve risk avoidance (Kahneman & Tversky, 1979). Firms higher in LSO are more likely to develop and implement effective safeguards that allow them to extract the most value from exploitative innovations, leading to higher performance. This process allows firms to emphasize protection of innovations and reduce expropriation to improve their performance.

Scholars have suggested that risk taking and exploitative innovation are negatively related (Hughes, Ireland, & Morgan, 2007). Moreover, exploitative innovation has been argued to negatively mediate the relationship between risk taking and firm performance (Kollmann & Stockmann, 2014), but was found to be insignificant. Kollmann and Stockmann suggested that risk taking reduces exploratory innovation, which positively influences firm performance. I argue one possible reason for this insignificant effect is that risk-taking alone does not explain how firms extract value from exploitative innovations.

Risk-taking is inversely related to LSO in that LSO is a means of mitigating risk of expropriation to a firm. In this way, LSO can positively affect firm performance through exploitative innovation. To conclude, LSO is expected to have a positive impact on exploitation, which, in turn, will have a positive effect on firm performance.

H8: Exploitative innovation mediates the relationship between LSO and firm performance.

Table 6: Summary of Hypotheses

Hypotheses
H1a: Directors with security experience are positively related to leaders' security orientation.
H1b: CEO functional background is positively related to leaders' security orientation.
H1c: Executive technological interpretation as a threat is positively related to leaders' security orientation.

H2a: Firm knowledge intensity is positively related to leaders' security orientation. *H2b: Firm competitive position is positively related to leaders' security orientation.* *H2c: Firm global presence is positively related to leaders' security orientation.*
H3a: Industry competitive intensity is positively related to leaders' security orientation. *H3b: Frequency of security breaches is positively related to leaders' security orientation.* *H3c: Degree of technological intensity is positively related to leaders' security orientation.*
H4a: Leaders' security orientation is positively related to equity-based alliances. *H4b: Leaders' security orientation is negatively related to non-equity-based alliances.*
H5a: Leaders' security orientation is positively related to exploitative innovation. *H5b: Leaders' security orientation is negatively related to exploratory innovation.*
H6: LSO is positively related to firm performance.
H7: Equity strategic alliances mediate the relationship between LSO and firm performance.
H8: Exploitative innovation mediates the relationship between LSO and firm performance.

3.6 Chapter Summary

In this chapter, I identified potential antecedents and consequences of leaders' security orientation (LSO). These included industry, managerial, and firm level predictors, expecting that these relationships are grounded in upper echelon's theory, sensemaking theory, institutional theory, and prospect theory. I hypothesize that specific executive and director characteristics positively influence LSO, as well as firm characteristics such as past security breaches, knowledge intensity and global presence, firm competitive position, and industry characteristics such as past security breach experiences, competitive intensity, and technological intensity. With regard to the consequences of LSO, I predict that LSO influences firm decisions about strategic alliances and innovation types as well as firm performance. I also argue that equity alliances and exploitative innovation have a mediating relationship between LSO and firm performance. These arguments are grounded in prospect theory, suggesting that as firms become more security oriented, they choose particular strategies, which then influence performance.

CHAPTER IV

METHODOLOGY

In this chapter, I discuss the methodological approaches of this dissertation. I begin by outlining the process of LSO scale development, which uses quantitative pretesting (Anderson & Gerbing, 1991; Howard & Melloy, 2016) for initial item reduction. For the scale development process, I follow Hinkin's (1998) guide for scale development and validation, followed by a detailed explanation of data sources. Next, I describe the measures and operationalizations used for the variables of interest. Then, I discuss the data analysis strategies, which includes multiple regressions to test the hypotheses with mediation analysis (Preacher & Hayes, 2004) for H7 and H8. I conclude with a chapter summary.

4.1 Scale Development

Scale development is a subject of great interest in scholarly research. Many best practices have been recommended, and perhaps the most widely used was created by Hinkin (1995). In his review of 277 measures, Hinkin (1995) follows Schwab's (1980) three-stage process of scale development: item generation, scale development, and scale evaluation. Later, Hinkin (1998) provided a six-step process of scale development consisting of item generation, questionnaire administration, initial item reduction, confirmatory factor analysis, convergent/discriminant validity, and replication. For this study, I follow Hinkin's (1998) six-step process, which I describe in greater detail below, with the exception of the sixth step, replication.

In the first stage of scale development, the researcher generates items for the scale. In this stage, the researcher develops items that sufficiently tap the domain of interest to ensure that the items represent the construct (Hinkin, 1998). In developing items, the researcher can choose an inductive approach, a deductive approach, or a combination of the two. In the inductive approach, the researcher relies entirely on experts or a sample of respondents to describe their feelings or behaviors related to a concept. An example of the inductive approach is Butler's (1991) examination of conditions of trust. In contrast, the researcher may choose a deductive approach to develop scale items. Using this approach, the researcher employs theory to guide the development of scale items. Deductive approaches to scale development require a strong theoretical understanding and basis for item generation (Hinkin, 1998). Alternatively, a researcher may choose a mix of inductive and deductive approaches in which the researcher utilizes both theory and experts to develop items, as noted by Kapuscinski and Masters (2010). I opted to follow this approach because of clear parallels between the well-established crisis management literature and the nascent organizational security literature. As the organizational security literature is underdeveloped, it is important to ensure that the theoretical and practical perspectives regarding security orientation align.

In the development of the domains, I utilized the three constructs presented previously to establish the elements of leaders' security orientation based on the crisis management literature. Those domains are threat awareness, planning, and protection, which comprise preparedness; security management of proprietary asset breaches; and learning and resilience related to proprietary assets. Following this, I developed a large pool of items which I believe sufficiently tap the constructs of interest using a Likert-type scale. This item pool is shown in the Table 8. Often, the number of items that are produced are over-representative, which allows the

researcher to later reduce them (Stanton, Sinar, Balzer, & Smith, 2002). Although researchers may conduct either an exploratory factor analysis or a confirmatory factor analysis to reduce the number of items, both methods are plagued by issues that sometimes make qualitative pretest methods preferable (Howard & Melloy, 2016). One such qualitative pretest method is an item-sort task in which participants are presented with scale items and constructs and instructed to assign the items to constructs (Anderson & Gerbing, 1991). Items that are frequently assigned to the correct constructs are retained, and items that are assigned incorrectly are dropped using a statistical test. Anderson and Gerbing's (1991) original test, based on a 95% statistical significance level, falls short in that the test is only accurate for assignment with two constructs (Howard & Melloy, 2016). To rectify this issue, Howard and Melloy (2016) developed an alternative method, which can accommodate more than two constructs in the item-sort task. As such, I use Howard and Melloy's (2016) method because my scale consists of more than two constructs. To reduce the number of items for the scale, I conducted an item-sort study by contacting 20 experts with experience in organizational security (Howard & Melloy, 2016). A full list of items is provided in Table 8 and reports whether the items matched the intended dimension of LSO.

The second stage of the scale development process is questionnaire administration. In this stage, I administered the items produced during the item development stage to the respondent pool. This pool is later described in the Sample and Data Sources and Sample Size sections of this chapter. Next, the researcher performs initial item reduction using an exploratory factor analysis (EFA) to refine a new scale further. In this stage, it is important for the researcher to ensure reliability, examine eigenvalues (if applicable), and determine the percentage of variance accounted for, among other evaluations. In addition, researchers should use scales that are

similar in nature to assess discriminate validity. Given the parallels to safety and security, the security education training and awareness scale developed by D'Arcy, Hovav, and Galletta (2009) would be an ideal candidate to assess discriminate validity of the LSO scale. Following item reduction, the researcher performs a confirmatory factor analysis (CFA) on a different sample, or a split sample. The assessments that the researcher performs during this stage include goodness-of-fit tests, chi-square, and other goodness-of-fit indices such as Comparative Fit Index (CFI). In the next stage, the researcher assesses convergent and discriminant validity of the scale. To assess discriminant validity in a CFA, scholars typically use the Fornell-Larker criterion (Fornell & Larker, 1981). For convergent validity, researchers use average variance extracted (Fornell & Larker, 1981; Hulland, 1999). Finally, the researcher performs replication and includes an assessment of reliability, convergent validity, discriminant validity, and criterion-related validity (Hinkin, 1995).

4.2 Sample and Data Sources

I use multiple sources for collecting data during each phase of the project. To assist in the development of items and to categorize items into factors, I contacted experts in the security field. The experts I use for this sample included senior security officials from the Department of Energy, a private security firm with more than 20,000 employees, former military special operations personnel, and the security director of a computer company with more than 100,000 employees.

For the respondent pool, I utilized Dynata (formerly Research Now) to recruit two panels of respondents. The first panel consisted of 225 respondents for the exploratory factor analysis. Research Now recruited a panel of managers from U.S. firms to complete the survey for the EFA. The second panel consisted of 295 respondents to perform the rest of the analysis. Online

recruitment panels and internet freelancing are becoming increasingly popular for survey recruitment in researching or examining social and behavioral topics (e.g., Martinez, White, Shapiro, & Hebl, 2016), particularly in marketing research (e.g., Evangelidis, & Levav, 2013; Luo & Toubia, 2015; Ward & Broniarczy, 2011). Recently, such panel methods have appeared in prominent management journals (e.g., Archak, Ghose, & Ipeirotis, 2011; Burbano, 2016; Castille, Buckner, & Thoroughgood, 2016; Crilly, Ni, & Jiang, 2015; Long, Bendersky, & Morrill, 2011; Steffens, Haslam, & Reicher, 2014; Steffens, Peters, Haslam, & van Dick, 2016).

To address potential issues arising from various sources of bias, I utilized multiple sources for data collection to minimize the likelihood of errors and bias. Specifically, I used a pool of experts for the item-sort task, a panel of managers for the EFA, and a panel of top managers for the CFA and regression analysis. Moreover, during the survey administration and analysis, I attempted to minimize common method bias or common method variance (CMV) as set forth in previous practice (Williams et al., 2010).

More specifically, I provided general, rather than specific, information on the study's objectives and offered anonymity and confidentiality to the respondents to reduce the chance of social desirability or consistent responses (Podsakoff, MacKenzie, Lee & Podsakoff, 2003). In addition to these steps, I added attentional checks utilized in past research. For example, I added three attention checks (Howard & Melloy, 2016). These items consisted of questions including variations of "Please verify where you are in the survey by marking a '2' for this item" (Miller & Baker-Prewitt, 2009), "For quality assurance purposes, please select 'strongly agree'" (Guin et al., 2012), and "As a validation check, please answer 'strongly disagree' for this question" (Gao, House, and Xie, 2015). Also, two motivation checks were added "Do you believe your data should be included for analysis" and "Using the slider below, how much effort did you put into

completing this survey." Participants that failed two out of the three checks were removed from the analysis.

The above listed procedures, although intended to minimize CMV, cannot eliminate it altogether. To address this limitation, I utilized methods intended to detect and control for CMV. Scholars suggest utilizing a marker variable that is expected to be unrelated to the other variables in the study to "tap into sources of method variance… [the] tendencies that impact the measurement of substantive variables" (Williams & McGonagle, 2016). According to Williams and McGonagle (2016), community satisfaction may tap into such sources of method variance related to affect-driven response tendencies in a survey related to job satisfaction. Given that LSO responses are likely affect driven towards the organizations' preparation, management, and learning and resilience of security breaches, a similar variable should serve as an ideal marker variable in the case of this dissertation. Patriotism has been identified as an ideal marker in affect related studies (e.g., Haynie, Svyantek, Mazzei, & Varma, 2016). In this study, I used Kosterman and Feshbach's (1989) patriotism scale, which represents love for one's country.

4.3 Sample Size

The sample sizes needed for exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) were based upon existing literature on scale development. According to Hinkin (1995) and others (e.g., Hoelter, 1983; Rummel, 1970; Schwab, 1980), recommended sample sizes for EFA and CFA vary. Rummel (1970), for example, recommends a 4:1 ratio of items to responses. Similarly, Schwab (1980) argues for a more conservative 10:1 item to response ratio. Nearly 40% of studies utilize a ratio of less than 5:1 (Costello & Osborne, 2003). Using simulations, some scholars have shown that as long as communalities are high, there are few factors, and model error is low, samples as low as 20 can still produce adequate factor structures

(Preacher & MacCallum, 2002). Using a basis of 4:1 ratio of respondents to items, the minimum sample for the EFA would be 188 given the 47-item scale.

Specific to CFA, Hoetler (1983) suggests a sample size of 200 for CFA. However, more recent research suggests that scholars should rely on calculating degrees of freedom to perform confirmatory factor analysis, structural equation modeling, or path analysis (e.g., Goodboy & Kline, 2017). Central to the concept of determining an adequate sample size is finding the degrees of freedom. Degrees of freedom show the difference between the information provided in the data the researcher is using (knowns) and the number of parameters (unknowns) in the data (Cortina, Green, Keeler, & Vandenberg, 2016; Rigdon, 1994). The calculation of degrees of freedom varies slightly depending upon the type of model and analysis but essentially involves subtracting the knowns and unknowns. A more detailed discussion regarding calculating degrees of freedom can be found in other works (Cortina et al., 2016; Kline, 2017).

I calculated degrees of freedom using a program that interfaces with RStudio (Cortina et al., 2016). Here, I calculated degrees of freedom for the lowest possible number of items for the LSO scale as a conservative estimation for sample size because increasing the number of indicators increases the degrees of freedom and reduces the required sample size (Kline, 2017). Given 20 indicators with three latent exogenous variables, this program determined there should be 210 knowns and 43 unknowns. The program subtracted 210 knowns from 43 unknowns, resulting in a final value of 167 degrees of freedom. When I increased the number of indicators to 30, the program calculated 402 degrees of freedom. Based on the online degrees of freedom calculator, and in comparison with MacCallum and colleagues' (1996) Table 2, the minimum sample size needed for the CFA was approximately 100 respondents. To confirm this number, I submitted the following information to Preacher and Coffman's (2006) online tool for computing

sample size for RMSEA: Alpha (.05), degrees of freedom (167), desired power (.80), null RMSEA (.05), alternative RMSEA (.08) as suggested by MacCallum and colleagues (1996) and others (e.g., Kline, 2017). The results of this analysis suggest a minimum sample size of 94. When the degrees of freedom were increased to 402, the results suggested a sample size of 55.

For regression, suggested sample size requirements vary as well. Hair and colleagues (2014) suggest a minimum of five responses for each variable in a regression. Given this requirement, and the research model with 14 variables, the minimum sample size needed for analysis would be 70. Others, however, offer a more nuanced view of estimating sample size requirements for regression, suggesting that a power analysis should be performed (Cohen, 1988).

To estimate the necessary sample size for the research model, I utilized Stata 13's powerreg function. Using this function requires several knowns, including the number of tests (1), alpha (.05), number of variables (14), power (.80) combined with unknowns for r-squared (coefficient of determination, or R^2), and effect size of the variable or variables of interest. The estimated r-squared is based on r-squared in past research given similar models. A review of a number of studies with similar control variables suggests an R^2 ranging from .01 (Morgan, Vorhies, & Mason, 2009), .09 (Wiklund & Shepherd, 2003) to greater than .60 (Autio, Sapienza, & Almeida, 2000). Given such a large difference in the R^2 values, I opted to use a conservative estimate of .06 for the model with controls and independent variables. Given that no previous research has examined the effect of security on the outcomes described in this study, I opted to utilize a conservative estimation of an effect of .03 for all independent variables in the analysis, which is between a small effect (.01) and medium (.06) according to Cohen (1988).

The resulting Stata function was as follows:

powerreg, r2f(.09) r2r(.06) nvar(14) ntest(1) alpha(.05) power(.80)

The results of this analysis suggested a sample size of 240. In addition, I performed some supplementary analysis by raising the R^2 to .30 and .60, reducing the required sample sizes to 184 and 108, respectively. When raising the number of variables (*nvar*) to 20, which would undoubtedly raise the model's R^2 (represented as *r2f* above), the required sample rose from 240 to 242.

In conclusion, the minimum sample size needed for each analysis differed. For the item sort task, sample sizes as low as five are acceptable, but 20 were used for this study (Howard & Melloy, 2016). For the EFA, I used a sample ratio of 4:1 with extra respondents included in case some of the data may be unusable. Thus, the sample for the EFA was 225. For the CFA, a minimum of 94 is needed, but because I will perform regression analysis on the same data, I sought to acquire a sample of 240 based on Stata's powerreg results to perform the regression analysis but ended up with 295 usable responses.

4.4 Measures and Variable Operationalization

Dependent and Independent Variables.

Leaders' security orientation. This construct measures leaders' orientation towards security. It is a seven-point Likert scale with 47 items, which are presented in Table 8. It covers an organization's security preparedness, management of security violations, and learning and resilience. More security oriented firms will score higher on the items whereas less security oriented firms will score lower and should be less capable of protecting against security threats. This item was collected using a self-report survey.

Directors with security experience. This measure was used to capture the amount of experience the board of directors has with security. It is measured as the proportion of directors

on the board with security experience. Executives rely on their experiences and education to make decisions (Hambrick, 2007; Hambrick & Mason, 1984). Consequently, boards of directors with more experience dealing with security issues will handle those issues differently than boards without such experience. This item was collected through self-report on survey items by asking respondents to indicate the proportion of directors with security experience.

CEO functional background. A CEO's functional background is a proxy for their perspective on particular issues. Output oriented functional backgrounds are associated with more external opportunity, whereas throughput functional backgrounds are associated with more internal processes (Hambrick & Mason, 1984). Of particular interest in this dissertation is protection of internal functions from various sources. Chief Executive Officers with past experience as Chief Operations Officers are likely to have considerable experience and understanding of security issues for a firm. This variable is operationalized as a dummy variable coded 1 if the CEO has an operations and/or COO background and 0, if otherwise. This item was collected through self-report on survey items by asking respondents whether the CEO has a background in operations or was previously a COO.

Executive technological interpretations. This variable represents an executive's interpretation of technological changes as a threat or opportunity in the face of technological change. It is operationalized as a four-item, five-point Likert scale consisting of the following statements: "Technological changes in our industry bring a lot of opportunities for our firm," "Our company is well-positioned to exploit technological changes in our industry," "Our company is concerned about security challenges that come with using new technologies," and "Technological changes would allow us to expand our product and service offerings." This was

collected through self-report on survey items and was adapted from Thomas and McDaniel (1990).

Firm knowledge intensity. Firm knowledge intensity is a composite measure of the number of intellectual properties the firm owns (e.g., patents, copyrights etc.) and a firm's R&D Intensity as measured by R&D divided by sales. Firm knowledge intensity is representative of a firm's focus on developing or acquiring new knowledge for market purposes (Autio et al., 2000), including information about how to exploit security vulnerabilities. This item was also collected through self-report on survey items.

Firm competitive position. This variable is measured as the firm's current market share (as a percentage) relative to its competitors and represents a firm's standing in the market in comparison to its competitors. A higher market share represents a higher standing in the market over its competitors. Gaining industry leadership is often a key objective for organizations (Ferrier, Smith, & Grimm, 1999). This item was collected through self-report on survey items.

Firm global presence. This item represents a firm's presence globally. A firm with a higher proportion of sales from international operations has a greater global presence than firms with a lower proportion of sales from international operations and allows more opportunities to create value for the firm. It was measured as a self-report from respondents about the proportion of sales from international operations and was adopted from past research (Fatemi, Desai, & Katz, 2003). In addition, I added one item related to how many countries the company currently operates in.

Frequency of security breaches (firm level). This item represents how often a firm is targeted by malicious attacks or accidental lapses in security. More frequent security breaches and more experience with them draws attention to the issue for a firm's executives as well as a

greater understanding of the means of resolution. It is measured as the number of security breaches in recent years. This item was collected through self-report on survey items and was developed for this survey.

Frequency of security breaches (industry level). This item represents how often an industry is targeted by malicious attacks or accidental lapses in security for the industry. Frequent security breaches in an industry helps firms to understand the assets under threat of loss or damage. It is measured as the number of recent security breaches in recent years the industry experiences. This item was collected through self-report on survey items and was created for this survey.

Industry competitive intensity. This variable is a measure of competitive intensity in an industry. It is measured with a six-item perceptual measure of the intensity of competition in an industry (Auh & Menguc, 2005). This item was collected through self-report on the survey.

Degree of technological intensity. This is a perceptual measure regarding the degree of technological intensity in an industry. The degree of technological intensity of an industry, as it relates to security, is important for firms to protect their innovations from expropriation from competitors, among other threats to their assets. This item appeared on the survey as a categorical choice that asked respondents to indicate if their firm operates in "high technology sectors." This item was collected through self-report on the survey as a five-point Likert scale, ranging from definitely not to definitely yes.

Equity based alliances. Equity based alliances is a three-item composite measure indicating the desirability of equity-based alliances for a firm. It is measured using a seven-point Likert scale designed for this study. This item was collected through self-report on the survey by asking respondents to indicate the degree to which they participate in equity-based alliances.

Non-equity-based alliances. Non-equity-based alliances is a three-item measure indicating the desirability of non-equity-based alliances for a firm. It is measured using a seven-point Likert scale designed for this study. This item was collected through self-report on the survey by asking respondents to indicate the degree to which they participate in non-equity strategic alliances.

Exploitative innovation. Exploitative innovation represents the extent to which a firm builds upon existing knowledge to meet current customer needs. It is a six-item Likert type measure adopted from Lubatkin, Simsek, Ling, and Veiga (2006).

Exploratory innovation. Exploratory innovation represents the extent to which a firm developed new knowledge for nascent customers. It is a six-item Likert type measure adopted from Lubatkin and colleagues (2006).

Firm performance. In this dissertation, firm performance is measured as an eight-item composite measure related to performance compared with major competitors over the last three years. This item will be collected through self-report on survey items and measured on a seven-point Likert scale. These questions ask respondents to evaluate the performance of their major line of business over the past year relative to their major competitors. The items used for this scale were adopted from Morgan, Vorhies, and Mason (2009). More specifically, these items cover performance in market share growth, acquiring new customers, increasing sales to current customers, growth in sales revenue, business unit profitability, return on investment, return on sales, and reaching financial goals.

Control Variables.

Firm size. Firm size represents a firm's resources and ability to perform certain actions, such as implement sizeable security systems for reasons not directly related to caring about

security or being more security oriented. Generally, firm size is measured in one of a few ways. The first way that firm size is measured is by revenue or sales in a given year (Gulati, 1999). Another way is by total assets (Hansen & Wernerfelt, 1989). Firm size can also be measured as the number of employees (Morgan, Vorhies, & Mason, 2009). Given these measures (and others), I opted for firm size represented as the number of employees for the primary reason that sample respondents are most likely to know this number, and respondents might be sensitive about providing firm financial data.

Board size. This measure is operationalized as the number of people on the board of directors. Firms with larger boards have a greater range of experience to draw from when addressing security issues, which may be directly relevant to the issue of security orientation of a firm's leaders.

Industry. This item indicates the industry of the respondent's company. Respondents were instructed to denote their respective industry. Industry, as argued throughout this dissertation, should have an effect on the security orientation of a firm's leaders as well as on its outcomes.

Patriotism. This item is a five-point Likert scale developed by Kosterman and Feshbach (1989). It measures one's affinity towards their own country. This scale is used as a marker variable in this study and should be unrelated to the variables of interest.

SETA. Five-item measure of security education, training, and awareness (D'arcy et al., 2009). It is measured using a five-point, Likert scale and was used to help assess discriminate validity of LSO and other existing constructs.

All variables and their operationalizations are presented in Table 7.

Table 7: Variable Descriptions and Operationalization

Variable	Measure
Leaders' security orientation (LSO)	47-item measure of LSO
Directors with security experience	The proportion of directors on the board with security experience
CEO functional background	Dummy variable as to whether the CEO has an operations and/or COO background
Executive technological interpretations	Four-item measure adapted from Thomas & McDaniel (1990): -Technological changes in our industry bring a lot of opportunities for our firm -Our company is well-positioned to exploit opportunities related to technological changes in our industry -Our company is concerned about security challenges that come with using new technologies -Our company is ready to adapt to security challenges associated with using new technologies.
Firm knowledge intensity	The number of intellectual properties the firm owns (e.g., patents, copyrights etc.) R&D Intensity (R&D/Sales)
Firm competitive position	Firm current market share (as a percentage) relative to its competitors
Firm global presence	The proportion of sales from international operations The number of countries the company operates in
Frequency of security breaches (firm)	Number of recent security breaches experienced by a firm in recent years
Frequency of security breaches (industry)	Number of recent security breaches experienced by an industry in recent years
Industry competitive intensity	Six-item measure from Auh & Menguc (2005): -Competition in our industry is cut-throat -There are many promotion wars in our industry -Anything that one competitor can offer, others can match easily -Price competition is a hallmark of our industry -One hears of a new competitive move almost every day -Our competitors are relatively weak
Degree of technological intensity	Categorical choice on survey asking respondents to indicate if their firm operates in "high technology sectors"
Patriotism	Three-item measure adapted from Kosterman and Feshbach (1989): -I am proud to be from my country. -I am emotional attached to my country and affected by its actions

	-Although at times I may not agree with the government, my commitment to my country always remains the same
Equity based alliances	Three-item measure asking respondents to indicate the desirability of equity alliances: - Our company is involved in equity based strategic alliances with our business partners -Our company plans on forming an equity based strategic alliance with our business partner -Our company plans to maintain the equity-based strategic alliances we have with our business partners
Non-equity-based alliances	Three-item measure asking respondents to indicate the desirability of non-equity alliances: - Our company is involved in non-equity based strategic alliances with our business partners -Our company plans on forming non-equity based strategic alliance with our business partners -Our company plans to maintain the non-equity based strategic alliances we have with our business partners
Exploitative innovation	Six-item measure adopted from Lubatkin et al (2006) asking respondents to assess their firm's orientation during the past three years using a 5-point scale: - Our company looks for novel technological ideas by thinking "outside the box" -Our company bases its success on its ability to explore new technologies -Our company creates products and services that are innovative to the firm -Our company looks for creative ways to satisfy its customers' needs -Our company aggressively ventures into new segments -Our company actively targets new customer groups
Exploratory innovation	Six-item measure adopted from Lubatkin et al. (2006) asking respondents to assess their firm's orientation during the past three years using a 5-point scale: -Our company commits to improve quality and lower cost -Our company continuously improves the reliability of its products and services -Our company increases the levels of automation in its operations -Our company constantly surveys existing customers' satisfaction -Our company fine-tunes what it offers to keep its current customers satisfied -Our company penetrates more deeply into its existing customer base

Firm performance	Eight-item measure of related to a firm's performance compared with major competitors over the last three years -Market share growth relative to competition -Acquiring new customers -Increasing sales to current customers -Growth in sales revenue -Business unit profitability -Return on investment -Return on sales -Reaching financial goals
Firm size	Number of employees of the firm
Board size	Number of members on the board of directors
Industry	Industry of the respondent
SETA	Five-item measure of security education, training, and awareness: -My organization provides training to help employees improve their awareness of computer and information security issues. -My organization provides employees with education on computer software copyright laws -In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way -My organization educates employees on their computer security responsibilities -In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.

Table 8: Leaders' Security Orientation Scale

	Item	Predicted Dimension of LSO	Actual Dimension of LSO
1	Our top management is quick to detect threats to our organization's proprietary assets.	Preparedness	
2	Our top management collects information about security threats to proprietary assets.	Preparedness	
3	Our top management actively monitors threats to our organization's proprietary assets.	Preparedness	
4	Threats to the security of our knowledge resources are our top management's concern.	Preparedness	
5	Our top management is aware of the threats to its proprietary assets.	Preparedness	
6	Our top management has a process for identifying threats to proprietary assets.	Preparedness	
7	Our top management is aware of the threats posed to the proprietary assets of the organization.	Preparedness	
8	Our top management is aware of the potential consequences of a failure in protecting proprietary assets.	Preparedness	
9	Our top management is aware of the likelihood of a security incident involving proprietary assets.	Preparedness	
10	Overall, our top management is aware of the potential security threats to proprietary assets.	Preparedness	
11	Overall, our top management is aware of the potential negative consequences of a security incident of an incident involving proprietary assets.	Preparedness	
12	Our top management understands the risk of security incidents to proprietary assets.	Preparedness	
13	Our top managers have developed strategies for security involving proprietary assets.	Preparedness	
14	Top management ensures that employees are required to sign documents preventing the disclosure of confidential information.	Preparedness	
15	Top managers ensure there are policies for screening employees' access to proprietary assets.	Preparedness	

16	Top managers ensure that all employees receive training and education on security threats and protection related to proprietary assets.	Preparedness	
17	Top management ensures all employees are trained on security policy related to proprietary assets.	Preparedness	
18	Our top management meets frequently to discuss security of proprietary assets.	Preparedness	
19	Top managers disseminate information about security threats to proprietary assets to all levels in the organization.	Preparedness	
20	Our top managers communicate with law enforcement to identify threats to security to proprietary assets.	Preparedness	
21	Our top management meets frequently to discuss security threats to proprietary assets.	Preparedness	
22	Top managers ensure our security department spends time discussing security threats to proprietary assets to proprietary assets to other departments.	Preparedness	
23	Top managers periodically disseminate information on security threats and potential prevention to all employees.	Preparedness	
24	Top managers reprimand employees if they do not comply with security policies related to proprietary assets.	Management of Proprietary Asset Breaches	
25	Top managers ensure that employees will incur penalties if they do not comply with security policies related to proprietary assets.	Management of Proprietary Asset Breaches	
26	Our top management communicates information about security events quickly to our employees.	Management of Proprietary Asset Breaches	
27	Top management systematically informs employees when a security event involving proprietary assets has occurred.	Management of Proprietary Asset Breaches	
28	When a security threat involving proprietary assets is discovered, top management quickly relays that information to our employees.	Management of Proprietary Asset Breaches	
29	Responding quickly to a security threat involving proprietary assets is a significant priority of our top managers.	Management of Proprietary Asset Breaches	

30	Top management ensures the management of security incidents involving proprietary assets of different departments are well coordinated.	Management of Proprietary Asset Breaches	
31	Top management ensures that our organization has a security department devoted to responding to security incidents involving proprietary assets.	Management of Proprietary Asset Breaches	
32	Top management will respond immediately to handle a security incident involving proprietary assets.	Management of Proprietary Asset Breaches	
33	Top management has adequate resources to allocate to a security incident involving proprietary assets if one were to occur.	Management of Proprietary Asset Breaches	
34	Top management ensures our organization adapts rapidly to major security events involving proprietary assets based on prior incidents.	Management of Proprietary Asset Breaches	
35	Top management ensures that our organization can recover quickly if a major security event involving proprietary assets were to occur.	Management of Proprietary Asset Breaches	
36	Top management resolves security threats involving proprietary assets quickly.	Management of Proprietary Asset Breaches	
37	If our organization came up with a great security plan involving proprietary assets, top management would implement it in a timely manner.	Learning & Resilience	
38	Top management uses information from past security incidents if a security threat involving proprietary assets arises.	Learning & Resilience	
39	If our organization finds a weakness in our security system involving proprietary assets, top management takes corrective action immediately.	Learning & Resilience	
40	When our organization finds a new threat related to proprietary assets, top management makes concerted action to adapt our security to respond to the threat in the future.	Learning & Resilience	
41	Our organization evaluates our security systems involving proprietary assets including all policies, procedures and devices frequently enough.	Learning & Resilience	
42	Top management ensures there are routine audits of our security system.	Learning & Resilience	

43	Top management utilizes statistical information of security incidents involving proprietary assets to evaluate security policy.	Learning & Resilience	
44	Top management evaluates employees' compliance with security policies related to proprietary assets.	Learning & Resilience	
45	Top management is able to learn from our failures related to security of proprietary assets.	Learning & Resilience	
46	Top management conducts drills or exercises to test our management of security threats involving proprietary assets.	Learning & Resilience	
47	Top management documents security incidents involving proprietary assets and reviews them periodically.	Learning & Resilience	

4.5 Analytical Strategies

To perform this research, I employed multiple methods to address this dissertation's research questions. For scale development, I used an item-sort task following Howard and Melloy's (2016) design to develop and test a scale of Leaders' security orientation using a sample of managers obtained from contacting security experts and an EFA. I also performed a CFA from data obtained from a respondent panel. To test my hypotheses related to antecedents and consequences of leaders' security orientation, I performed multiple regressions based on data obtained from a respondent panel. An item-sort and EFA were performed. The regression analysis with mediation (Preacher and Hayes, 2004) was performed as part of the dissertation defense.

4.5.1 Item sort task

For the item-sort task, I contacted a pool of 20 security experts via LinkedIn and a large university in south Texas. These experts included the director of security at a computer software and electronics company with more than 100,000 employees, Department of Energy security specialists, former military special operations personnel, faculty with information security knowledge at a research university, and the general manager of a security company with more than 40,000 employees. These experts were asked to complete an item-sort task where they selected one of four columns labeled: Proprietary Asset Protection Preparedness, Management of Proprietary Asset Breaches, Post-Breach Learning & Resilience, and none.

Following data collection, responses were analyzed using Howard and Melloy's (2016) proposed process. Items that were not correctly assigned to the correct column and failed to achieve significance ($p<.05$) were rejected and dropped from the survey pool, reducing the number of items for the survey.

4.5.2 Pilot study

225 respondents were contacted via the respondent panel company Dynata, formerly Research Now. Their responses were analyzed using an Exploratory Factor Analysis. In addition, the SETA scale was used to assess discriminate validity of the LSO scale. For the EFA, I utilized the process outlined by Hair, Black, Babin and Anderson (2014). Varimax rotation was initially selected due to its wide acceptance and use in management research (Hair et al., 2014). Factors with eigenvalues less than 1 were disregarded. Factor loadings greater than .50 were retained (Hair et al., 2014). Items with high cross-loadings were eliminated. Items with communalities less than .50 were eliminated. This process was performed until no significant cross-loadings were present and all items have factor loadings higher than .50.

Given the previous discussion of the three dimensions of LSO, I expected the EFA would result in three separate factors, which would be labeled preparedness, management of proprietary asset breaches, and post-breach learning and resilience. In addition, I anticipated that the EFA would result in a further reduction of items.

4.6 Chapter Summary

This chapter documented the steps I took to develop and test a Leaders' Security Orientation scale. First, I developed a list of items based on existing research in crisis management and in concert with experts in security. Second, I followed pretest procedures developed by Anderson and Gerbing (1991) and later refined by Howard and Melloy (2016). I then administered the survey to a test group and used an item-sort task to analyze the scale. Following this, I performed an EFA based on data collected from a respondent panel. Finally, I administered another survey to a different group of respondents to perform a CFA and tested my overall research model using a mediation model regression analysis.

CHAPTER V

RESULTS

In this chapter, I present the results of the data analysis. This chapter is organized into five sections. In the first section, I provide a summary of data collection and item-sort activities. The second section provides details on the exploratory factor analysis (EFA). The third section reports the results of the confirmatory factor analysis (CFA). The fourth section presents the results of hypotheses tests. The fifth and final section of this chapter concludes with a summary.

5.1 Data Collection

To develop the Leader Security Orientation (LSO) scale, I relied on a combination of inductive and deductive approaches to scale development used in past research (e.g., Kapuscinski & Masters, 2010). The data collection process consisted of three stages. First, consistent with standard scale development protocol, I began by contacting individuals with expertise in security to help with the item-sort task. The item-sort task is used to improve items in a scale by exposing items to experts for categorization and feedback, especially in newly developed scales (Howard & Melloy, 2016). In addition, an item-sort helps with item reduction and refinement. I then contacted a firm to collect data from a sample of managers, followed by a sample of firm executives with the minimum title of Vice President.

I contacted more than 20 experts to complete the item-sort task. A total of 24 respondents completed the survey. Four surveys were removed due to careless responding or failed attention

checks, resulting in 20 complete survey responses. All respondents were male with an average age of 45. Respondents were in their current position, on average, for five years. Professional titles included Senior Director Security Operations, Vice President, Associate Professor, and Executive Vice President, among others. Ten percent (2 of 20) held the title security specialist, another 10% held the title Associate Professor (2 of 20), while the remaining 80% were Senior Director Security Operations, General Manager, Business Development Manager, Chief Operations Officer, Executive Vice President, Department Chair, Senior Associate Performance Assurance, Facility Security Officer, Senior Protection Services Consultant, Security Manager, Vice President, Senior Engineer, Cyber Security Manager, Director of Search, Supervisory Special Agent, and Security Consultant. For the item-sort, each item in the survey must meet a minimum of 15 of 20 correctly categorized responses to be retained (Howard & Melloy, 2016). The original scale consisted of 47 items. A total of 19 items passed the minimum threshold for the analysis, with most categorized as Preparedness (15 items); four items were categorized as Management of Proprietary Asset Breaches, and one item was categorized as Learning and Resilience. Two items were categorized under Preparedness but were anticipated to fall under Management of Proprietary Asset Breaches or Learning and Resilience in the exploratory factor analysis (EFA) and confirmatory factor analysis (CFA). The complete list of items, along with the number of items correctly categorized as well as their predicted and actual dimensions are listed in Table 9 below. According to the table, 53% (25 of 47) of the items did not fall within a dimension of LSO. Thirty-six percent of the items (17 of 47) were categorized as preparedness. Management of Proprietary Asset Breaches accounted for 9% (4 of 47) of categorizations and Learning and Resilience comprised the final 2% (1 of 47).

Table 9: Item-sort task

	Item	Number Categorized as predicted	Predicted Dimension of LSO	Actual Dimension of LSO
1	Our top management is quick to detect threats to our organization's proprietary assets.	6	Preparedness	N/A
2	Our top management collects information about security threats to proprietary assets.	11	Preparedness	N/A
3	Our top management actively monitors threats to our organization's proprietary assets.	15	Preparedness	Preparedness
4	Threats to the security of our knowledge resources are our top management's concern.	12	Preparedness	N/A
5	Our top management is aware of the threats to its proprietary assets.	16	Preparedness	Preparedness
6	Our top management has a process for identifying threats to proprietary assets.	18	Preparedness	Preparedness
7	Our top management is aware of the threats posed to the proprietary assets of the organization.	15	Preparedness	Preparedness
8	Our top management is aware of the potential consequences of a failure in protecting proprietary assets.	13	Preparedness	N/A
9	Our top management is aware of the likelihood of a security incident involving proprietary assets.	16	Preparedness	Preparedness
10	Overall, our top management is aware of the potential security threats to proprietary assets.	16	Preparedness	Preparedness
11	Overall, our top management is aware of the potential negative consequences of a security incident of an incident involving proprietary assets.	11	Preparedness	N/A
12	Our top management understands the risk of security incidents to proprietary assets.	18	Preparedness	Preparedness
13	Our top managers have developed strategies for security involving proprietary assets.	15	Preparedness	Preparedness

14	Top management ensures that employees are required to sign documents preventing the disclosure of confidential information.	17	Preparedness	Preparedness
15	Top managers ensure there are policies for screening employees' access to proprietary assets.	17	Preparedness	Preparedness
16	Top managers ensure that all employees receive training and education on security threats and protection related to proprietary assets.	16	Preparedness	Preparedness
17	Top management ensures all employees are trained on security policy related to proprietary assets.	17	Preparedness	Preparedness
18	Our top management meets frequently to discuss security of proprietary assets.	17	Preparedness	Preparedness
19	Top managers disseminate information about security threats to proprietary assets to all levels in the organization.	15	Preparedness	Preparedness
20	Our top managers communicate with law enforcement to identify threats to security to proprietary assets.	14	Preparedness	N/A
21	Our top management meets frequently to discuss security threats to proprietary assets.	14	Preparedness	N/A
22	Top managers ensure our security department spends time discussing security threats to proprietary assets to proprietary assets to other departments.	18	Preparedness	Preparedness
23	Top managers periodically disseminate information on security threats and potential prevention to all employees.	14	Preparedness	N/A
24	Top managers reprimand employees if they do not comply with security policies related to proprietary assets.	6	Management of Proprietary Asset Breaches	N/A
25	Top managers ensure that employees will incur penalties if they do not comply with security policies related to proprietary assets.	6	Management of Proprietary Asset Breaches	N/A
26	Our top management communicates information about security events quickly to our employees.	13	Management of Proprietary Asset Breaches	N/A
27	Top management systematically informs employees when a security event involving proprietary assets has occurred.	12	Management of Proprietary Asset Breaches	N/A

28	When a security threat involving proprietary assets is discovered, top management quickly relays that information to our employees.	15	Management of Proprietary Asset Breaches	Management of Proprietary Asset Breaches
29	Responding quickly to a security threat involving proprietary assets is a significant priority of our top managers.	12	Management of Proprietary Asset Breaches	N/A
30	Top management ensures the management of security incidents involving proprietary assets of different departments are well coordinated.	15	Management of Proprietary Asset Breaches	Management of Proprietary Asset Breaches
31	Top management ensures that our organization has a security department devoted to responding to security incidents involving proprietary assets.	4	Management of Proprietary Asset Breaches	Preparedness
32	Top management will respond immediately to handle a security incident involving proprietary assets.	17	Management of Proprietary Asset Breaches	Management of Proprietary Asset Breaches
33	Top management has adequate resources to allocate to a security incident involving proprietary assets if one were to occur.	6	Management of Proprietary Asset Breaches	N/A
34	Top management ensures our organization adapts rapidly to major security events involving proprietary assets based on prior incidents.	3	Management of Proprietary Asset Breaches	N/A
35	Top management ensures that our organization can recover quickly if a major security event involving proprietary assets were to occur.	5	Management of Proprietary Asset Breaches	N/A
36	Top management resolves security threats involving proprietary assets quickly.	15	Management of Proprietary Asset Breaches	Management of Proprietary

				Asset Breaches
37	If our organization came up with a great security plan involving proprietary assets, top management would implement it in a timely manner.	1	Learning & Resilience	N/A
38	Top management uses information from past security incidents if a security threat involving proprietary assets arises.	14	Learning & Resilience	N/A
39	If our organization finds a weakness in our security system involving proprietary assets, top management takes corrective action immediately.	5	Learning & Resilience	Preparedness
40	When our organization finds a new threat related to proprietary assets, top management makes concerted action to adapt our security to respond to the threat in the future.	6	Learning & Resilience	N/A
41	Our organization evaluates our security systems involving proprietary assets including all policies, procedures and devices frequently enough.	1	Learning & Resilience	N/A
42	Top management ensures there are routine audits of our security system.	0	Learning & Resilience	N/A
43	Top management utilizes statistical information of security incidents involving proprietary assets to evaluate security policy.	12	Learning & Resilience	N/A
44	Top management evaluates employees' compliance with security policies related to proprietary assets.	3	Learning & Resilience	N/A
45	Top management is able to learn from our failures related to security of proprietary assets.	18	Learning & Resilience	Learning & Resilience
46	Top management conducts drills or exercises to test our management of security threats involving proprietary assets.	1	Learning & Resilience	N/A
47	Top management documents security incidents involving proprietary assets and reviews them periodically.	13	Learning & Resilience	N/A

Before collecting responses for the exploratory factor analysis (EFA), I eliminated items that did not meet the 15 of 20 predicted response rule of thumb recommended by Howard and Melloy (2016). Respondents indicated that some of the items were redundant. I further eliminated items that were similar. Because most of the retained items fall under one dimension, and a few items under Learning and Resilience had a sizeable proportion of accurate classification, I opted to retain three items and improve their wording. In addition, I changed two Preparedness items to more closely align with the conceptualization of Management of Proprietary Asset Breaches. Finally, because all the Learning and Resilience items only tapped learning but not resilience, I followed the recommendation of one respondent and added an item on resilience, resulting in a total of 24 items for the updated survey. Table 10 below provides the updated list of items and their respective dimensions. The updated list of items in Table 10 was used for subsequent data collection.

Table 10: Revised LSO Scale

	Item	LSO Dimension
1	Our top management has a process for identifying threats to proprietary assets.	Preparedness
2	Our top management is aware of the likelihood of a security incident involving proprietary assets.	Preparedness
3	Overall, our top management is aware of the potential security threats to proprietary assets.	Preparedness
4	Our top management understands the risk of security incidents to proprietary assets.	Preparedness
5	Our top managers have developed strategies for security involving proprietary assets.	Preparedness
6	Top management ensures that employees are required to sign documents preventing the disclosure of confidential information.	Preparedness
7	Top managers ensure there are policies for screening employees' access to proprietary assets.	Preparedness
8	Top managers ensure that all employees receive training and education on security threats and protection related to proprietary assets.	Preparedness
9	Our top management meets frequently to discuss security of proprietary assets.	Preparedness

10	Top managers disseminate information about security threats to proprietary assets to all levels in the organization.	Preparedness
11	Top managers ensure our security department spends time discussing security threats to proprietary assets to other departments.	Preparedness
12	Our top management actively manages proprietary asset breaches.	Management of Proprietary Asset Breaches
13	Top management ensures all employees utilize their training during a proprietary asset breach.	Management of Proprietary Asset Breaches
14	When a security threat involving proprietary assets is discovered, top management quickly relays that information to our employees.	Management of Proprietary Asset Breaches
15	Top management ensures the management of security incidents involving proprietary assets of different departments are well coordinated.	Management of Proprietary Asset Breaches
16	Top management will respond immediately to handle a security incident involving proprietary assets.	Management of Proprietary Asset Breaches
17	Top management resolves security threats involving proprietary assets quickly.	Management of Proprietary Asset Breaches
18	Top management uses information from past security incidents if a security threat involving proprietary assets arises to learn.	Learning & Resilience
19	Top management learns from statistical information of security incidents involving proprietary assets to evaluate security policy.	Learning & Resilience
20	Top management is able to learn from our failures related to security of proprietary assets.	Learning & Resilience
21	Top management documents security incidents involving proprietary assets and reviews them periodically.	Learning & Resilience
22	Top management ensures our organization is resilient in the face of a security incident.	Learning & Resilience
23	Top management makes concerted action to learn from new threats to our proprietary assets and adapt our security.	Learning & Resilience
24	If a weakness in our security system in proprietary assets is found, top management is able to bounce back from such problem by taking corrective action.	Learning & Resilience

5.2 Exploratory Factor Analysis

225 respondents were recruited from Dynata, formerly Research Now, to respond to the survey. Dynata is a data collection and market research company that provides research panels for surveys. This company's services have previously been used by other scholars (Choudhary,

Pani, Papa & Vicentini, 2018; Redmiles, Kross & Mazurek 2016). Typically, researchers calculate response rates to help determine response quality because people who complete the survey may differ from those who do not (Singleton & Strait, 2010). Surveys conducted via third-party data collection services (such as the one I am using here) do not allow researchers to assess response rates because third-party data collection services do not provide an initial number of respondents that were contacted for the survey or a specific response rate. Consequently, it is difficult to ascertain the size of the larger pool of respondents they targeted, and what percent actually completed the survey. The initial response to the survey included 260 respondents. However, the number of respondents was reduced to 225 after checking for non-response, careless responding, and failed attention checks. The average age of respondents was 44, the average number of years that respondents worked was 9.8, and 42 percent of respondents were female.

I utilized SPSS version 25 to perform an exploratory factor analysis (EFA). The measures for the new LSO scale were included in an EFA along with the previously validated Security, Education, Training and Awareness (SETA) scale developed by D'Arcy, Hovav, and Galletta (2009). The SETA scale was included to assist with assessing discriminant validity. Recent literature indicates that principal axis factoring with oblique rotations (e.g., Promax rotations) are preferable in the early stages of scale development (Hair, Anderson & Tatham, 1987; El Akremi, Gond, Swaen, Roeck, & Igalens, 2015), so I employed principal axis factoring with oblique rotations. The Promax rotation resulted in four factors; three unique to this study and one unique to the SETA scale, suggesting adequate discriminant validity. After removing three items due to low loadings (<.50), three factors remained; the previously established SETA scale and two unique factors for the LSO scale. Eigenvalues for each of the three factors were 13.67, 1.37, and

1.04, respectively. One of the SETA items loaded higher on the second factor of the LSO scale and was retained under that factor. Table 11 below shows the results of the EFA from the pattern matrix. The Kaiser-Meyer-Olkin measure of sampling adequacy was .960. Bartlett's test of sphericity was significant ($p < .01$). Discriminant validity was assessed by evaluating the factor correlation matrix. The correlation between the first and third measure was above .70, suggesting that the measures are not distinct. However, the first and third factors were below the .70 cutoff when compared with the SETA scale. Consequently, there is evidence that the factors are distinct from the SETA measure, providing support for LSO as a new construct.

Table 11: Exploratory Factor Analysis (EFA) Results

	Factor 1 Management of proprietary asset breaches	Factor 2 SETA	Factor 3 Communication of proprietary asset breaches
Cronbach's Alpha	(.90)	(.87)	(.86)
Our top managers have developed strategies for security involving proprietary assets.	0.920		
Top management ensures our organization is resilient in the face of a security incident.	0.844		
Our top management has a process for identifying threats to proprietary assets.	0.779		
Our top management is aware of the likelihood of a security incident involving proprietary assets.	0.758		
Top management documents security incidents involving proprietary assets and reviews them periodically.	0.748		
Top management makes concerted action to learn from new threats to our proprietary assets and adapt our security.	0.743		
Top management learns from statistical information of security incidents involving proprietary assets to evaluate security policy.	0.741		
If a weakness in our security system in proprietary assets is found, top management is able to bounce back from such problem by taking corrective action.	0.708		
Our top management actively manages proprietary asset breaches.	0.699		
Top management resolves security threats involving proprietary assets quickly.	0.676		

Top management ensures the management of security incidents involving proprietary assets of different departments are well coordinated.	0.670		
Overall, our top management is aware of the potential security threats to proprietary assets.	0.661		
Our top management understands the risk of security incidents to proprietary assets.	0.647		
Top managers ensure there are policies for screening employees' access to proprietary assets.	0.592		
My organization educates employees on their computer security responsibilities		0.884	
My organization provides training to help employees improve their awareness of computer and information security issues.		0.704	
In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.		0.674	
In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way		0.560	
Top managers disseminate information about security threats to proprietary assets to all levels in the organization.			0.700
When a security threat involving proprietary assets is discovered, top management quickly relays that information to our employees.			0.673
Our top management meets frequently to discuss security of proprietary assets.			0.557
My organization provides employees with education on computer software copyright laws.			0.507

Internal consistency was assessed using Cronbach's alpha for each of the three identified factors. The first factor, which consisted of 14 items produced a Cronbach's alpha of .90, well above the minimum .70 cutoff for Cronbach's alpha established Nunnally and Bernstein (1994). The second factor, the SETA scale, produced an alpha of .87. The third factor, consisting of five items, produced an alpha of .859 with the one SETA scale item and an alpha of .857 without the SETA scale item. Upon further analysis of the two unique factors identified in this study, the first factor appears to consist of items related to planning, implementation, and response. The second factor appears to consist of items related to communications. Thus, two factors emerge: management of proprietary asset breaches and communication of proprietary asset breaches,

different than the anticipated factors of preparedness, management, and learning and resilience. The updated scale consists of two factors based on these EFA results.

5.3 Confirmatory Factor Analysis

Dynata also recruited the 242 respondents for the third sample of this study. I instructed Dynata to only contact executives of firms with 50 or more employees and who held the title of Vice President or higher. This differs from the previous sample of employees with the title of manager that Dynata collected for the EFA. A total of 410 respondents attempted the survey, but 115 were dropped due to failed attention checks, refusal to participate in the survey, or careless responding, which left 295 usable responses overall. Of these, 213 useable responses were available for the CFA based on the variables selected. This sample was subsequently used for hypothesis testing.

Upon collecting these data and prior to performing the CFA, I first tested for the presence of common method variance by performing a Harman's (1967) single-factor test with several of the study's variables. In addition to the steps recommended by Lindell and Whitney (2001), Richardson and colleagues (2009), and Williams and colleagues (2010), I used marker variables prior to data collection (varying response scale format, evaluating theoretical susceptibility to CMV relative to other study variables, and a priori selection of marker variable), I report the marker variable in the correlation matrix (shown later, in Table 13). The results of this test were below the 50 percent cutoff (48.8 percent), indicating that CMV was unlikely to be present. I then performed a test of common method variance with the following variables included in a CFA model: executive technological interpretations, exploratory innovation, exploitative innovation, LSO, firm performance, and the marker variable (patriotism). I performed the following steps consistent with past research on CFA marker technique for CMV (Richardson et

al., 2009; Williams et al., 2010): 1) creation of a CFA model 2) creation of a baseline model where the marker is not allowed to correlate with the variables and marker item factor loadings and errors terms are set to the unstandardized values in the CFA 3) identification of the method-C (equal constraints) and method-U (free varying or unconstrained) models, and 4) creation of the method-R model that constrains the factor correlations to unstandardized estimates in the baseline. Table 12, below, shows the results of these tests.

Table 12: Common Method Variance Results

CFA Marker Analysis			
Model	χ^2	***df***	**CFI**
1. CFA with Marker	2003.66	934	0.916
2. Baseline	1941.18	940	0.921
3. Method-C	1915.19	939	0.923
4. Method-U	1802.03	899	0.929
5. Method-R	1912.80	946	0.924
Chi-square model comparison tests			
Models	$\Delta\ \chi^2$	Δ ***df***	χ^2 critical value $\alpha = 0.05$ (p-value)
Baseline versus Method-C	21.01	1	(.00)
Method-C versus Method-U	118.80	40	(.00)
Method-C versus Method-R	0.28	7	(.99)

According to the table above, Method-C fits significantly better than the baseline model, so there is evidence of shared CMV between the indicators of the variables for analysis and the marker variable. Since Method-U fits significantly better than Method-C, then CMV congeneric method variance, meaning that its effects vary across the variables (Richardson et al., 2009), is present. However, since Method-R is not significantly different from Method-C, CMV is not likely to skew the relationships for analysis. Given that CMV is present, and to remain conservative, for all subsequent analysis in the dissertation, I retained the marker variable. I then performed a CFA testing a two-factor measure of LSO against a single-factor measure of LSO. The single-factor model was acceptable (χ^2 = 275.37, RMSEA = .06, CFI = .974, TLI = .971,

SRMR = .02), but slightly worse than the two-factor model (χ^2 = 274.92, RMSEA = .06, CFI = .974, TLI = .971, SRMR = .02). However, a chi-square difference test was insignificant (p = .55), indicating that there is no marked difference between a single-factor or two-factor model. Consequently, subsequent analysis will use the single-factor measure. I then tested a six-factor CFA model consisting of the variables in the CMV tests, which was acceptable across fit indices (χ^2 = 2003.66, CFI = .916, TLI = .911, SRMR = .04, RMSEA = .06) and performed better than five-factor, or four-factor models.

5.4 Results of Hypotheses Tests

I used the sample Dynata collected for the confirmatory factor analysis to conduct the main analysis and test all eight hypotheses using Stata 13.1. Table 13 below displays the descriptive statistics and correlations of all focal variables. Several correlations are interesting and warrant further discussion. Importantly, most of the main variables of the analysis hold significant bi-variate correlations with other variables in the study. Second, LSO is positively and significantly correlated with all the variables except for the directors with security experience, CEO functional background, frequency of security breaches, and board and firm size. Third, executive technological interpretation was positively and significantly correlated with all of the hypothesized predictors of LSO at the firm and industry levels, except for directors with security experience, CEO functional background, and firm size. Finally, frequency of security breaches – both across firms and industries – was positively correlated with most of the variables in the analysis.

Table 13: Descriptive Statistics and Correlations

Variable	Mean	S.D.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1. Directors with Security Experience	11.42	22.1	1																		
2. CEO Functional Background	0.38	0.487	0.02	1																	
3. Executive Technological Interpretation	3.75	0.84	0.02	-0.36*	1																
4. Firm Knowledge Intensity[1a]	87	956	0.02	-0.16*	0.32*	1															
5. Firm Competitive Position[2]	40.56	25.73	0.12	-0.18*	0.19*	0.19*	1														
6. Firm Global Presence[3a]	32.23	28.61	0.14*	-0.24*	0.23*	0.33*	0.39*	1													
7. Frequency of Security Breaches	2.66	1.46	0.00	-0.16*	0.18*	0.30*	0.30*	0.42*	1												
8. Industry Competitive Intensity	4.56	1.15	-0.01	-0.36*	0.51*	0.29*	0.15*	0.34*	0.39*	1											
9. Frequency of Security Breaches (Industry)	3.82	1.8	-0.06	-0.16*	0.19*	0.17*	0.10	0.27*	0.60*	0.44*	1										
10. Degree of Technological Intensity	3.08	1.45	0.06	-0.23*	0.41*	0.38*	0.23*	0.45*	0.35*	0.50*	0.30*	1									
11. LSO	5.17	1.31	0.08	-0.31*	0.66*	0.28*	0.19*	0.15*	0.10	0.39*	0.21*	0.42*	1								
12. Equity Alliances	4.3	1.93	0.08	-0.31*	0.48*	0.43*	0.16*	0.40*	0.40*	0.47*	0.36*	0.44*	0.50*	1							
13. Non-equity Alliances	4.35	1.8	0.06	-0.26*	0.46*	0.44*	0.21*	0.35*	0.37*	0.46*	0.34*	0.39*	0.47*	0.68*	1						
14. Exploitative Innovation	5.12	1.27	0.06	-0.38*	0.73*	0.30*	0.17*	0.17*	0.05	0.51*	0.15*	0.43*	0.72*	0.50*	0.49*	1					
15. Exploratory Innovation	4.91	1.32	0.08	-0.36*	0.71*	0.30*	0.20*	0.24*	0.16*	0.56*	0.21*	0.50*	0.77*	0.61*	0.51*	0.84*	1				

[1] I opted to use IP owned by the firm instead of a composite measure of IP owned and R&D intensity due to low coefficient alpha (.00).
[2] Firm competitive position was measured using market share.
[3] I opted to use a single-item measure of global presence (international sales) due to a lack of collected data.

16. Firm Performance	4.93	1.18	0.08	-0.40*	0.66*	0.27*	0.19*	0.22*	0.16*	0.52*	0.21*	0.41*	0.67*	0.48*	0.43*	0.73*	0.73*	1			
17. Board Size	7.61	4.37	-0.02	-0.09	0.13*	0.18*	-0.00	0.08	0.06	0.09	0.02	0.05	0.07	0.13*	0.16*	0.07	0.06	0.00	1		
18. Firm Size	12173	45664	-0.01	0.04	0.04	-0.09	-0.04	0.05	-0.05	-0.04	0.05	-0.07	0.03	0.01	-0.06	0.00	0.01	-0.05	0.25*	1	
19. Marker	4.23	0.73	-0.04	-0.06	0.32*	0.09	-0.03	-0.06	-0.07	0.17*	-0.01	0.03	0.22*	0.15*	0.08	0.27*	0.23*	0.23*	0.00	0.05	1

*p<.05, N=201, [a]log-transformed

Following the CFA, I used an ordinary least square (OLS) regression analysis for testing Hypotheses 1a through 3c with the marker variable included in the analysis. The results of the OLS regressions include Model 1, a model with the controls and the independent variables and Model 2, a model with the controls, marker variable, and independent variables. Both models are presented in Table 14. Industry as a control was excluded from this analysis due to a setup error in Qualtrics that corrupted the collected data. I opted to use robust standard errors for this analysis because a Breusch-Pagan test of heteroskedasticity was significant ($p<.05$). Multicollinearity was not a significant concern as Variance Inflation Factor (VIF) values were below 3, which is well below the recommended VIF cutoff of 10 (Hair et al., 2010).

Table 14: Sensitivity Analysis for CMV

	Model (1)	Model (2)
Firm Size[a]	0.018 (0.032)	0.015 (0.032)
Board Size	-0.005 (0.018)	-0.004 (0.018)
Directors with Security Experience (H1a)	0.001* (0.00)	0.001* (0.000)
CEO Functional Background (H1b)	-0.163 (0.136)	-0.166 (0.140)
Executive Technological Interpretation (H1c)	0.920** (0.134)	0.910** (0.149)
Firm Knowledge Intensity (H2a)[a]	0.007 (0.038)	0.006 (0.038)
Firm Competitive Position (H2b)	0.006* (0.003)	0.006* (0.003)
Firm Global Presence (H2c)[a]	-0.084 (0.059)	-0.082 (0.060)
Frequency of Security Breaches (Firm) (H2d)	-0.134* (0.064)	-0.133* (0.063)
Industry Competitive Intensity (H3a)	0.078 (0.100)	0.075 (0.098)
Frequency of Security Breaches (Industry) (H3b)	0.033 (0.048)	0.035 (0.048)
Degree of Technological Intensity (H3c)	0.155* (0.061)	0.155* (0.061)
Marker Variable		0.035 (0.114)
Constant	1.059**	0.963**

	(0.514)	(0.496)
Observations	202	202
R-squared	.56	.56
Adjusted R-squared	.50	.50

[a]Log-transformed with constant added
Robust Standard Errors in parentheses ** p<0.01, * p<0.05
Δ in R-squared from Control Only model (not shown)

Models 1 and 2 in Table 14 above were used as a sensitivity analysis for the results with and without the marker variable to evaluate whether CMV influences the results (Williams et al., 2010). In Model 1, the independent variables are added without the marker variable to predict LSO. In Model 2, the marker variable is added to the model and coefficients and significance are compared (Williams et al., 2010; Zhu, Chew, & Spangler, 2005). Statistical significance remained the same for all substantive variables in the analysis while the coefficients displayed only minor changes. Except for executive technological interpretations, coefficients only changed at the third decimal, indicating that CMV was not likely to influence the results of the analysis. Despite the evidence that CMV was unlikely to affect the results, the marker variable was retained for hypothesis testing to help correct for CMV by simply being added as a control (Siemens et al., 2010). In addition, the high correlations appearing among executive technological interpretations, firm global presence, firm competitive position, and industry competitive intensity could influence the results. Consequently, I opted to conduct hypothesis testing for each of the predictors of LSO in a separate model shown in Table 15, below.

Table 15: Hypothesis Testing for Predictors of LSO

	Model (1)	Model (2)	Model (3)	Model (4)	Model (5)	Model (6)	Model (7)	Model (8)	Model (9)	Model (10)	Model (11)	Model (12)
Firm Size[a]	-0.017 (0.041)	-0.024 (0.042)	-0.007 (0.038)	0.012 (0.029)	-0.038 (0.040)	-0.033 (0.042)	-0.014 (0.042)	-0.020 (0.041)	-0.002 (0.035)	-0.027 (0.040)	0.007 (0.038)	0.015 (0.032)
Board Size	0.025 (0.023)	0.032 (0.024)	0.014 (0.021)	-0.010 (0.017)	0.013 (0.022)	0.025 (0.023)	0.014 (0.024)	0.023 (0.023)	0.013 (0.020)	0.026 (0.022)	0.015 (0.021)	-0.004 (0.018)
Marker Variable	0.400** (0.117)	0.413** (0.118)	0.373** (0.113)	0.039 (0.116)	0.357** (0.120)	0.424** (0.117)	0.428** (0.118)	0.412** (0.114)	0.262* (0.113)	0.411** (0.118)	0.344** (0.115)	0.035 (0.114)
Directors with Security Experience (H1a)		0.002 (0.001)										0.001* (0.000)
CEO Functional Background (H1b)			-0.786** (0.168)									-0.166 (0.140)
Executive Technological Interpretation (H1c)				1.024** (0.107)								0.910** (0.149)
Firm Knowledge Intensity (H2a)[a]					0.207** (0.051)							0.006* (0.038)
Firm Competitive Position (H2b)						0.010* (0.004)						0.006* (0.003)
Firm Global Presence (H2c)[a]							0.130* (0.057)					-0.082 (0.060)
Frequency of Security Breaches (Firm) (H2d)								0.096 (0.058)				-0.133* (0.060)
Industry Competitive Intensity (H3a)									0.409** (0.088)			0.075 (0.098)
Frequency of Security Breaches (Industry) (H3b)										0.156** (0.049)		0.035 (0.048)
Degree of Technological Intensity (H3c)											0.370** (0.059)	0.155* (0.061)
Constant	3.40** (0.534)	3.30** (0.536)	3.84** (0.506)	1.19** (0.452)	3.44** (0.547)	2.99** (0.591)	3.07** (0.596)	2.13** (0.561)	2.13** (0.551)	2.81** (0.553)	2.42** (0.518)	.963* (0.469)
Observations	254	246	254	253	237	251	225	254	252	254	253	202
R-squared	0.05	0.07	0.14	0.44	0.12	0.09	0.09	0.06	0.18	0.10	0.22	0.56
Adj. R-squared	0.05	0.06	0.13	0.43	0.11	0.08	0.08	0.05	0.17	0.09	0.21	0.53
[a]Log-transformed with constant added												
Robust Standard errors are in parenthesis												
** p<0.01, * p<0.05												

Table 15 above presents the results of the OLS regression analysis testing hypotheses 1a through 3c. Hypothesis 1a predicted a positive and significant relationship between the proportion of directors with security experience and LSO. The relationship was tested in Model 2 and was not supported (β=0.002, $p>.05$). Interestingly, however, the variable becomes significant in Model 12 with the inclusion of all other variables in the analysis, suggesting that an interaction effect could be occurring between one or more of the variables in the analysis. The second hypothesis, H1b, predicted a positive relationship between CEO functional background, coded as 1 if the CEO had a background in operations and zero if otherwise, and LSO and was not supported in Model 3 (β=-0.786, $p<.01$) due to the negative relationship. The relationship between Executive Technological Interpretations was positive and significant (β=1.024, $p<.01$), supporting H1c in Model 4. Hypothesis 2a was tested in Model 5. This hypothesis predicted a positive relationship between firm knowledge intensity and LSO. The hypothesis was supported (β=0.207, $p<.01$). Hypothesis 2b predicted a positive relationship between firm competitive position and LSO and was supported in Model 6 (β=0.010, $p<.05$). Hypothesis 2c was tested in Model 7 and predicted a positive relationship between firm global presence and LSO. This hypothesis was supported (β=0.130, $p<.05$). Hypothesis 2d predicted a positive relationship between frequency of security breaches (firm) and LSO and was not supported in Model 8 (β=.096, $p>.05$). Model 9 tested the relationship between industry competitive intensity and LSO. This relationship was positive and significant (β=0.409, $p<.01$) supporting H3a. Hypothesis 3b predicted a positive and significant relationship between frequency of security breaches and LSO. This hypothesis was supported in Model 10 (β=0.156, $p<.01$). Finally, degree of technological intensity was predicted to be positively related to LSO according to hypothesis H3c. Model 11, supports this hypothesis (β=0.370, $p<.01$). Model 12, a model including

variables in the analysis, was included to probe the overall predictive power of the variables (in terms of R^2).

Overall, the full model from Table 15 is robust, with an adjusted R^2 of .56, indicating the model explains the majority of the variance in the dependent variable, LSO. Table 16 below presents a summary of the results of hypotheses tests on the predictors of LSO.

Table 16: Summary of Results on the Predictors of LSO

Hypotheses	Supported?
H1a: Directors with security experience are positively related to leaders' security orientation.	No
H1b: CEO functional background is positively related to leaders' security orientation.	No
H1c: Executive technological interpretation as a threat is positively related to leaders' security orientation.	Yes
H2a: Firm knowledge intensity is positively related to leaders' security orientation.	Yes
H2b: Firm competitive position is positively related to leaders' security orientation.	Yes
H2c: Firm global presence is positively related to leaders' security orientation.	Yes
H2d: Frequency of security breaches is positively related to leaders' security orientation.	No
H3a: Industry competitive intensity is positively related to leaders' security orientation.	Yes
H3b: Frequency of security breaches is positively related to leaders' security orientation.	Yes
H3c: Degree of technological intensity is positively related to leaders' security orientation.	Yes

As a next step, I performed a second analysis for the consequences of LSO in which I tested the relationship between LSO and alliances, innovation, and firm performance. Hypotheses 4a and 4b predicted positive and negative relationships between LSO and equity and non-equity-based alliances, respectively. Hypotheses 5a and 5b were concerned with the relationship between LSO and innovation. Specifically, Hypothesis 5a predicted a positive relationship between LSO and exploitative innovation while Hypothesis 5b predicted a negative

relationship between LSO and exploratory innovation. Hypothesis 6 predicted a positive and significant relationship between LSO and firm performance. To test hypotheses H4a through H6, I conducted a regression analysis. I then performed a mediation analysis for H7 and H8 using the procedures described by Hayes (2012) and described later. These results are displayed in Table 17. Model 1 includes control variables and the independent variable with equity strategic alliances as the dependent variable. Model 2 adds the marker variable to this analysis to ensure that the effects of CMV are accounted for in the analysis. The marker variable reduces the coefficient size of LSO on equity-based alliances. Model 3 includes control variables and LSO as the predictor variable with non-equity-based strategic alliances as the dependent variable. Model 4 includes the marker variable. In contrast with Model 2, the marker variable appears to have no effect on the results in Model 4. Models 5 and 6 use exploitative innovation as the dependent variable. Model 5 includes control variables along with LSO as the independent variable, while Model 6 adds the marker variable. In Model 6 the marker is significant while the coefficient for LSO is reduced by .02. Model 7 uses exploratory innovation as the dependent variable with controls and LSO as an independent variable. Model 8 adds the marker variable. When the marker is added, LSO's coefficient is again reduced by .02. Firm performance is used as the dependent variable in Models 9 and 10. In Model 9, the controls and independent variable are included. In Model 10 the marker variable is added to the model. When the marker variable is added to the model, the coefficient for LSO is again reduced by .02. As with previous hypothesis testing, I utilized Huber-White robust standard errors to correct for heteroskedasticity. VIFs in all models were below the established cutoff of 10.

Table 17: Outcomes of LSO

	Model (1)	Model (2)	Model (3)	Model (4)	Model (5)	Model (6)	Model (7)	Model (8)	Model (9)	Model (10)
Dependent Variable	Equity-alliances	Equity-alliances (H4a)	Non-equity alliances	Non-equity alliances (H4b)	Exploitative Innovation	Exploitative Innovation (H5a)	Exploratory Innovation	Exploratory Innovation (H5b)	Firm Performance	Firm Performance (H6)
Firm Size[a]	-0.01 (0.05)	-0.02 (0.05)	-0.06 (0.04)	-0.06 (0.04)	-0.05 (0.03)	-0.06* (0.03)	-0.05* (0.02)	-0.06* (0.02)	-0.05 (0.03)	-0.06* (0.03)
Board Size	0.05 (0.03)	0.05 (0.03)	0.06** (0.02)	0.06** (0.02)	0.02 (0.01)	0.02 (0.01)	0.01 (0.01)	0.02 (0.01)	0.00 (0.02)	0.00 (0.02)
Leaders' Security Orientation	0.72** (0.08)	0.70** (0.08)	0.64** (0.07)	0.64** (0.07)	0.70** (0.07)	0.68** (0.07)	0.77** (0.05)	0.75** (0.05)	0.60** (0.06)	0.58** (0.07)
Marker		0.15 (0.16)		0.01 (0.14)		0.21* (0.08)		0.18* (0.08)		0.16 (0.09)
Constant	0.31 (0.48)	-0.20 (0.65)	0.93* (0.44)	0.89 (0.60)	1.67** (0.40)	0.98* (0.46)	1.13** (0.32)	0.53 (0.43)	2.09** (0.38)	1.54** (0.40)
Observations	253	253	252	252	252	252	252	252	248	248
R-squared	0.26	0.26	0.24	0.24	0.53	0.54	0.59	0.60	0.45	0.46
Adjusted R-squared	0.23	0.24	0.22	0.21	0.51	0.52	0.59	0.60	0.45	0.46
Δ in R-squared		.24**		.21**		.52**		.60**		.46**

[a]Firm Size is log-transformed with constant added
Robust Standard Errors are in parentheses
** p<.01, *p<.05
Δ in R-squared is from control-only model (not shown)

Hypothesis 4a predicted a positive relationship between LSO and equity-based strategic alliances and was supported 4a (β =.70, p<.01). I predicted a negative and significant relationship between LSO and non-equity-based alliances for hypothesis 4b. The relationship was positive and significant (β =.64, p<.01), contrary to my theorizing and was rejected. Hypothesis 5a was supported (β =.68, p<.01) given the positive and significant relationship between LSO and exploitative innovation. I also predicted a negative relationship between LSO and exploratory innovation for hypothesis 5b. The relationship was negative and significant (β =.75, p<.01) and, thus, the relationship was not supported. Hypothesis 6 was supported (β =.58, p<.01) and predicted a positive relationship between LSO and firm performance. Overall, the results indicate that Leaders' Security Orientation (LSO) is a significant and positive predictor of equity-based strategic alliances, non-equity based strategic alliances, exploitative innovation, exploratory innovation, and firm performance. Consistent with the results from the predictors of LSO, these models had moderate to high R^2 values, indicating that the models with LSO explain 21 to 60 percent of the variance in the dependent variables in Table 17.

In order to test the mediation hypotheses (H7 and H8), I performed a mediation analysis using the PROCESS macro in SPSS developed by Hayes (2013) and selected Model 4 with 5,000 bootstrap samples. The marker variable was also added. Using this procedure, confidence intervals (CIs) are used to evaluate statistical significance with 95% confidence. If the CIs do not contain zero, the relationship is significant. For example, if the two values for the CI are both above .01 or if they are both below .01, then the relationship is significant at the 0.05-level. The results of the mediation analysis are presented in Table 18 and Table 19 below.

Table 18: Equity alliances as a mediator between LSO and firm performance

Hypothesis 7: Equity alliances as a mediator between LSO and firm performance					
Path		Coefficient	SE	t-value	*p*-value
1	IV (LSO) to Mediator (Equity Alliances)	.705	.646	9.08	.000
2	Direct Effect of Mediator (Equity Alliances) on DV (Firm Performance)	.127	.036	3.52	.000
3	Total Effect of IV (LSO) on DV (Firm Performance)	.595	.068	8.74	.000
4	Direct Effect of IV (LSO) on DV (Firm Performance)	.506	.074	6.83	.000
Model Summary	R^2=.45,	F =27.56,	*df* (4,240),	0.000	
Bootstrap Results for Indirect Effect (95% Bias-Corrected Confidence Interval-5000 Resample)					
Indirect Effect of IV (LSO) on DV (Firm Performance) through Mediator (Equity alliances)		Data .089	Boot .027	SE .028	Lower .036	Upper .14

Table 19: Exploitative innovation as a mediator between LSO and firm performance

Hypothesis 8: Exploitative innovation as a mediator between LSO and firm performance					
Path		Coefficient	SE	t-value	*p*-value
1	IV (LSO) to Mediator (Exploitative Innovation)	.796	.492	1.62	.000
2	Direct Effect of Mediator (Exploitative Innovation) on DV (Firm Performance)	.465	.749	6.20	.000
3	Total Effect of IV (LSO) on DV (Firm Performance)	.592	.068	8.71	.000
4	Direct Effect of IV (LSO) on DV (Firm Performance)	.273	.071	3.87	.000
Model Summary	R^2=.52,	F = 27.22,	*df* (4,239),	0.000	
Bootstrap Results for Indirect Effect (95% Bias-Corrected Confidence Interval-5000 Resample)					
Indirect Effect of IV (LSO) on DV (Firm Performance) through Mediator (Exploitative Innovation)		Data .32	Boot .056	SE .028	Lower .212	Upper .433

In the first mediation analysis I included the dependent variable (performance), the independent variable (LSO), and mediator variable (equity-based alliances), in addition to the controls. As can be seen in Table 18, this model resulted in an R^2 of .45. In this model, LSO had a significant and indirect relationship with firm performance (*ab* = .09; 95% CI = [.04, .14]).

Next, the direct effect (*c'* = .51; 95% CI = [.36, .65]) is added to the indirect effect to produce the total effect (*ab* + *c'* = .60; 95% CI = [.46, .73]). Taken together, these results indicate a significant and positive partially mediated relationship, partially supporting hypothesis 7. Finally, consistent with Wen and Fan (2015), I take the ratio of the indirect effect (.09) and the total effect (.60) to evaluate the meaningfulness of the effect size. The ratio, .15, indicates that approximately one-sixth of the total effect was accounted for by the indirect effect of equity alliances on firm performance via LSO. The ratio is low, suggesting that a small amount of the relationship is accounted for by the mediation. Stated differently, LSO is associated with slightly increased firm performance through equity alliances. In contrast, the direct relationship between LSO and firm performance accounts for a much greater portion of the relationship.

The second mediation analysis consisted of evaluating the relationship between LSO and firm performance as mediated by exploitative innovation. The same software and procedures were followed as the first mediation analysis. The second model resulted in an overall R^2 of .52 and is presented in Table 19. In this model, LSO had a significant indirect relationship on firm performance (*ab* = .32; 95% CI = [.21, .43]). Next, the direct effect (*c'* = .27; 95% CI = [.13, .41]) is added to the indirect effect (*ab* + *c'* = .59; 95% CI = [.46, .73]). Taken together, these results indicate a partially mediated relationship is present given that the indirect and complete effects are significant, partially supporting hypothesis 8. A summary of these results is provided in Table 20. Again, I take the ratio of the indirect effect (.32) and the total effect (.59) to evaluate the meaningfulness of the effect size of the model. This time, over half (.54) of the total effect was accounted for by the indirect effect via LSO, suggesting a strong partially mediated relationship between the variables in the analysis even after controlling for board size and firm performance and including the marker variable.

Table 20: Summary of Results for Outcomes of LSO

Hypothesis	Supported?
H4a: Leaders' security orientation is positively related to equity-based alliances.	Yes
H4b: Leaders' security orientation is negatively related to non-equity-based alliances.	No
H5a: Leaders' security orientation is positively related to exploitative innovation.	Yes
H5b: Leaders' security orientation is negatively related to exploratory innovation.	No
H6: Leaders' security orientation is positively related to firm performance.	Yes
H7: Equity strategic alliances mediate the relationship between leaders' security orientation and firm performance.	Partial
H8: Exploitative innovation mediates the relationship between leaders' security orientation and Firm Performance.	Partial

5.5 Supplementary Analysis

During the analysis of the dissertation, three problems arose: Data quality concerns, differences in coefficients and signs when testing individual relationships versus the full model effects (Table 15, Model 12) and a limited number of control variables. The first problem is that the quality of the data could be sub-optimal and should be validated. Some of the predicted relationships were not significant and others were in the opposite direction of the predicted hypothesis. One method of validating the quality of a dataset is to use multiple samples collected from different sources (Campbell & Fiske, 1959). Because most of the variables in the study were perceptual, it would be impossible to accurately match a sample from prior objective and subjective studies. For example, my measure of equity-based strategic alliances measures the perceived attractiveness of equity-based strategic alliances instead of the actual number of strategic alliances that the firm has pursued. Despite this limitation, I proceeded by performing propensity score matching using *teffects* test in Stata, version 13.1, consistent with previous research in strategic management (e.g. Haleblian, Pfarrer, & Kiley, 2017). To begin the analysis,

I collected data from COMPUSTAT on all firms for the variables employees (firm size) and revenue (performance) for the period between 2016 and 2019 and averaged each variable. I then standardized all variables from the COMPUSTAT data and survey data collected for the dissertation. Following this, I merged the two data sets using 1) employees from COMPUSTAT and firm size from the survey as one variable, *firm size* 2) firm performance survey item number four (growth in sales revenue) and firm revenue from COMPUSTAT as one variable, *firm performance* and 3) a group variable representing 1 if the data came from the survey and 0 if the data came from COMPUSTAT, *group,* for a total of three variables. *Group* was used as the treatment or matching variable, *firm size* was used as an independent variable, and *firm performance* was used as the dependent variable. The total number of observations for the analysis was 9195 when all data were merged. The test showed no significant differences between the survey data and the COMPUSTAT data (β=.222, p>.05). I followed this analysis by performing another propensity score analysis using psmatch2 in Stata. The results confirmed the first test (β=.097, p>.05), with the differences in coefficients between the two outputs likely due to differences in estimation between *teffects* and *psmatch2*. However, some caution should be used when evaluating this result because propensity score matching should be used on objective measures (Bettis, Gambardella, Helfat, & Mitchell, 2014) and my tests used standardized values of objective and perceptual measures.

The second concern comes from the changes in results shown in Table 15 where the size of many of the coefficients, their signs (e.g. positive and negative) and statistical significance change when comparing the individual hypothesis tests against the full model (Model 12). Changes in Model 12 could occur for two reasons. The first reason for these changes could be multicollinearity. Although variance inflation factors (VIFs) were below established cutoffs, high

correlations are present in Table 13, which is often indicative of multicollinearity (Paul, 2006). In addition, sign changes and significance can indicate multicollinearity (Williams, 2015). Consequently, there is some evidence that multicollinearity could be the cause of changes to coefficients and significance in Model 12. The second cause could be from interaction effects present in the full model that were not previously hypothesized or tested. To explore this possibility, interaction effects among variables whose hypotheses were not supported using robust standard errors. Results of this additional analysis are shown in Table 21.

Model 1 of Table 21 tests the moderating effect of CEO functional background as a COO on the relationship between directors with security experience and LSO. The relationship between directors with security experience and LSO is positive and significant (β=.006, p<.01), CEO functional background and LSO is negative and significant (β=-.762, p<.01) and the interaction between the directors with security experience and CEO functional background on LSO is negative and significant (β=-.004, p<.05), indicating that there is a significant interaction effect between the two variables such CEO functional background as a COO intensifies the negative relationship between directors with security experience and LSO. Model 2 tests the moderating effect of frequency of security breaches on the relationship between directors with security experience and LSO. The results indicate that there is a cross-over interaction in Model 2 given that neither the relationship between directors with security experience and LSO (β=-.001, p>.05) nor the relationship between security breaches and LSO (β=.006, p>.05) are significant, but the interaction between directors with security experience and security breaches (firm) on LSO (β=.002, p<.01) is significant. This result indicates that firm-level security breaches increases the negative effect of directors with security experience on LSO.

Table 21: Interaction effects for predictors of LSO

	Model 1 LSO	Model 2 LSO
Firm Size	-0.006 (0.039)	-0.022 (0.042)
Board Size	0.015 (0.022)	0.025 (0.024)
Marker	0.376** (0.114)	0.416** (0.117)
Directors with security experience	0.006** (0.002)	-0.001 (0.001)
CEO functional background	-0.762** (0.181)	
Directors with security experience x CEO functional background	-0.004* (0.002)	
Security breaches (firm)		0.061 (0.065)
Directors with security experience x security breaches (firm)		0.002** (0.001)
Constant	3.736** (0.507)	3.129** (0.570)
Observations	246	246
R-squared	0.162	0.088

Robust standard errors are in parenthesis
** p<0.01, * p<0.05

The third concern is related to having few control variables, especially in the hypothesis testing for the consequences of LSO. To alleviate concerns that the relationship between LSO and the outcomes discussed in this dissertation are because of other factors, I added the predictors of LSO as controls to Models 1 through 5 in Table 22 in addition to the original controls of Firm Size, Board Size, and the Marker variable, below.

Table 22: Outcomes of LSO supplementary analysis

	Model (1)	Model (2)	Model (3)	Model (4)	Model (5)
	Equity Alliances	Non-equity Alliances	Exploitative Innovation	Exploratory Innovation	Firm Performance
Firm Size	-0.04 (0.04)	-0.06 (0.04)	-0.06* (0.02)	-0.05* (0.02)	-0.05* (0.03)

Board Size	0.03 (0.02)	0.04 (0.02)	0.01 (0.01)	0.01 (0.01)	-0.01 (0.01)
Marker	0.25 (0.16)	0.05 (0.15)	0.08 (0.08)	0.10 (0.08)	0.17 (0.09)
LSO	0.43** (0.14)	0.34* (0.14)	0.45** (0.10)	0.49** (0.09)	0.37** (0.09)
Directors with security experience	0.00** (0.00)	0.00* (0.00)	0.00 (0.00)	0.00 (0.00)	0.00 (0.00)
CEO functional background	-0.34 (0.25)	-0.46* (0.23)	-0.24* (0.11)	-0.02 (0.12)	-0.18 (0.13)
Executive technological interpretation	0.16 (0.25)	0.03 (0.23)	0.36* (0.20)	0.29 (0.18)	0.39** (0.12)
Knowledge intensity	0.16* (0.06)	0.23** (0.07)	0.04 (0.02)	0.00 (0.04)	-0.01 (0.04)
Competitive intensity	-0.00 (0.00)	0.01 (0.00)	0.00 (0.00)	0.00 (0.00)	0.00 (0.00)
International presence	0.12 (0.09)	0.11 (0.09)	-0.05 (0.04)	-0.03 (0.04)	-0.00 (0.05)
Security breaches (firm)	0.27** (0.09)	0.14 (0.10)	-0.12* (0.05)	-0.03 (0.05)	0.00 (0.05)
Competitive intensity	0.03 (0.14)	0.19 (0.14)	0.21* (0.08)	0.30** (0.08)	0.12 (0.09)
Security breaches	0.10 (0.08)	0.12 (0.09)	0.00 (0.04)	-0.01 (0.04)	-0.01 (0.04)
Degree of technological intensity	0.13 (0.11)	-0.02 (0.10)	0.04 (0.05)	0.10 (0.05)	0.03 (0.05)
Constant	-1.19 (0.86)	0.28 (0.78)	0.93* (0.42)	-0.39 (0.42)	0.90 (0.50)
Observations	201	201	200	200	198
R-squared	0.51	0.48	0.72	0.75	0.63

Robust standard errors are in parenthesis
** p<0.01, * p<0.05

The results of these additional tests show that LSO remains significant across all dependent variables for H4a through H6. Compared with the results from Table 17, the coefficients for LSO as a predictor of each of the dependent variables are reduced across all models. Consequently, LSO appears to be robust to the addition of numerous control variables.

5.6 Chapter Summary

Overall, the results of the empirical analyses suggest that several of the antecedents I predicted were indeed significant drivers of LSO. Specifically, the results indicate that CEO functional background, executive technological interpretation as a threat, firm knowledge intensity, firm competitive position, firm global presence, industry competitive intensity, frequency of security breaches at the industry level and degree of technological intensity were significant predictors of LSO. Furthermore, the findings show that LSO was a significantly predictor of equity-based alliances, exploitative innovation, and firm performance. In addition to the direct relationships found, the results also provide support for a mediated relationship between LSO and firm performance through equity-based strategic alliances and a mediated relationship between LSO and firm performance through exploitative innovation. However, two of the relationships (non-equity-based alliances and exploratory innovation) were significant but in the opposite direction predicted. In the next chapter, I will discuss the scholarly and practical implications, limitations, and future research directions of these findings.

CHAPTER VI

DISCUSSION AND CONCLUSION

6.1 Discussion and Implications

In this final chapter of the dissertation, I reflect on the implications of the research questions posed in the first chapter and the corresponding findings. First, I answer the question: what influences the development of leaders' security orientation (LSO)? Second, I explore whether LSO affects firm performance, and if so, how? I also discuss whether LSO is associated with market-based strategies. Last, but not least, I conclude with the limitations of my dissertation and offer directions for future research.

Prior to answering these questions, some reflection upon the concept of LSO is warranted here. When originally conceptualizing LSO, past theorizing, research, and expert opinions suggested that LSO might be a three-dimensional construct consisting of preparedness, management and learning and resilience. The results of the item-sort, EFA, and CFA indicate that, at best, LSO maintains a two-factor structure, but only marginally so over a single-factor structure. Consequently, LSO can be re-conceptualized here as as the degree to which an organization's senior leaders manage and communicate security issues related to the protection of proprietary asset breaches.

6.1.1 What influences the development of leaders' security orientation (LSO)?

The empirical analysis in the previous chapter shows that several managerial, firm, and industry level factors predict LSO. First, the findings indicate that the strongest predictor of LSO is executive technological interpretations as a threat. The positive relationship between executive technological interpretations as a threat and LSO is likely due to the strong effect that technological changes have on firms' survival (Anderson & Tushman, 1990; Eggers & Park, 2018; Partridge, Rohlin, & Weinstein, 2019). Additionally, viewing technological changes as a strategic threat likely influences executives' orientation and actions. Regulatory focus theory (Higgins, 1998; Ahmadi et al., 2017) may provide some insights in this regard. The theory suggests that human motivation is predicated on seeking pleasure and avoiding pain (Higgins, 1998). Regulatory focus theory highlights two primary cognitive approaches among individuals that serve as motivational systems: promotion-focus and prevention-focus (Higgins, 1998). The focus relevant to my dissertation is prevention-focus. Prevention-focus emphasizes vigilance and taking actions to prevent harm or loss (Florack et al., 2013; Higgins, 1998) in addition to safety (Crowe & Higgins, 1997). The prevention focus, then, motivates individuals towards mistake-avoidance (Ahmadi et al., 2017; Crowe & Higgins, 1997). Previous research has found that managers' prevention focus affects their risk-taking and orientation toward exploration. Thus, when executives view the environment as a threat, they become more prevention-focused and, consequently, more security oriented. More specifically, as individuals perceive executive technological interpretations as a threat, executives will work to ensure that they do not make mistakes via prevention focus and become more security oriented.

In contrast, I found no evidence that the composition of boards of directors affects the security orientation of a firm's leaders. This finding is contrary to the upper echelon theory

prescription that the greater composition of executives in a specific area of expertise, the more the firm focuses resource allocation and action to that area (Tuggle, Schnatterly, & Johnson, 2010). While empirical research has found that board composition affects firms' strategic orientations (Ibrahim & Angelidis, 1994; Wang & Dewhirst, 1992), my findings suggest that board composition did not have a meaningful effect on the orientation of a firm's senior executives. This is interesting because the negative relationship discovered suggests that CEOs with operations backgrounds seem less security oriented. Thus, the negative relationship between CEO functional background and LSO may be explained by managerial hubris. Specifically, it is possible that CEOs with operations backgrounds may have increased overconfidence in their ability to manage risk (Galavotti, 2019). The relationship between expertise and overconfidence makes sense given that previous research has found a link between functional expertise and risk-taking (Minton et al., 2010). Additionally, operations managers may be less focused on risk to the firm than people with other types of experiences such as executives with experience as Chief Financial Officers (CFOs) (Minton et al., 2010; Minton et al., 2014). Therefore, executives with experience and education in managing different types of risks may be more security oriented than executives with experience in operations. Moreover, CEOs with operations backgrounds may be more focused on daily operations (e.g., managing the firm's supply chain) in lieu of strategic decisions and focus on strategic threats (e.g., strategic direction of the firm). The possible lack of strategic focus from CEOs with an operations background is important because the CEO sets priorities and objectives for the firm based on their previous experiences and preferences (Finkelstein & Hambrick, 1987; Lovelace, Bundy, & Hambrick, 2018; Zor, Linder & Endenich, 2019). Consequently, CEOs with operations backgrounds may be more prone to experience a security breach due to lower LSO. Despite this non-finding, my supplementary

analysis performed in Section 5.5 discovered two moderating effects. First, I found that having a CEO with a functional background in operations increases the negative effect between directors with security experience and LSO. This result could be due to the CEO's focus further directing the board's attention away from security issues and more towards operational ones. Second, I discovered that LSO was highest under conditions of high security breaches and higher proportions of directors of directors with security experience. This result could be due to increased focus on breaches due to their occurrence combined with increased ability to diagnose the cause and focus on prevention via greater expertise.

At the firm level, there are three important predictors of LSO. First, firm knowledge intensity is a significant predictor of LSO. Knowledge intensity, which is the extent to which a firm depends on knowledge in activities and outputs used for competitive advantage (Autio et al., 2000), is an important predictor of LSO because knowledge intensity increases the need for security (Hashai et al., 2010). In addition, knowledge intense firms must limit opportunism of partners (Hashai & Almor, 2008). Moreover, knowledge intensity plays a role in the scanning process by helping firms executives to know and understand threats to proprietary assets through improved understanding of threats via stronger knowledge processes (Andreeva & Kianto, 2011) Specifically, more knowledge intense firms should have an improved understanding of the weaknesses of the technology they possess and, as a consequence, be more focused on protecting their proprietary assets. Second, firm competitive position predicts LSO. A firm's market share, or competitive position, is an important predictor of LSO likely due to firms taking protective actions and attempting to reduce potential losses in the face of threats (Ferrier et al., 1999; Kahneman & Tversky, 1979; Oviatt & McDougall, 1994), especially when a firm is a market leader and focused on issues in the environment (Ferrier et al., 1999). Third, a firm's global

presence, or percent of international sales, predicts LSO. As organizations expand to other countries, they face a broader range of threats to proprietary assets (Sheffi, 2001). This finding is consistent with previous research that shows multinational corporations use a wider breadth of protection strategies for their firms than domestic firms (de Faria & Sofka, 2010).

Finally, I argued that industry level factors would be associated with increased LSO. Industry competitive intensity was significantly associated with LSO. Industry competitive intensity refers to perceptions of executives regarding the intensity of competition in an industry (O'Cass & Weeaardena, 2010). The finding that industry competitive intensity predicts LSO is consistent with previous research that suggests that firms in competitive industries adopt protection functions such as intelligence over time (Sahaf, 2002). The frequency of security breaches at the industry level is another predictor of LSO. As I argued previously, more frequent security breaches in an industry should be uncovered when organizations in an industry scan their environment and act to protect their proprietary assets upon discovery of these threats. Finally, the degree of technological intensity, or firms' reliance on technology in an industry, predicts LSO. Firms in technologically intense industries likely require added protections because technology is difficult to protect and easy to steal.

These findings support previous research in the areas of strategic sensemaking as well as institutional and prospect theories. For example, executives' perceived threats in an industry force firms' and their executives to engage in strategic sensemaking and act (Hoffman & Ocasio, 2000), eventually shaping the behavior and norms of an industry (Rao, Monin, & Duran, 2003) under the premise of minimizing potential losses.

Additionally, my findings have implications for research in knowledge management and knowledge protection. Previous research on knowledge management and knowledge protection

as it relates to protection of proprietary assets primarily focused on strategies such as secrecy (e.g., Earl, 2001; Bos, Broekhuizen, & de Faria, 2015). However, few studies have explored predictors of knowledge protection or orientations towards security (e.g., Leiponen & Byma, 2009; Gallié & Legros, 2012). My study extends this limited research by exploring predictors at the managerial, firm, and industry levels that are associated with increased focus on executives' protection of proprietary assets via their LSO. In this way, I extend previous research in knowledge protection by suggesting that several managerial, firm, and industry characteristics increase leaders' focus on protecting proprietary assets. In the next subsection, I discuss how LSO affects firm performance.

6.1.2 Does LSO affect firm performance? If so, how?

The findings of this dissertation indicate that LSO is associated with a direct increase in relative firm performance. This finding is consistent with previous research that security affects firm performance (Peleg-Gillai et al., 2006; Ritchie & Melnyk, 2012). Although past research has tied security initiatives to a firm's performance, my dissertation links executive orientations to firm performance. For example, Ritchie and Melnyk (2012) found that late adopters of a government security program had increased competitive advantage. Another study found that emphasizing security directly led to an improvement in performance (Peleg-Gillai et al., 2006). My study adds an important component of security orientation of firm's leaders, as opposed to the adoption of policies, to this prior research. As noted previously, protecting a firm's technological core is a critical component of firms' competitive advantage (Thompson, 1967), and the findings of this dissertation provide some evidence that leaders' security orientation helps enhance firm performance. Thus, past theorizing and research combined with this study continue to suggest that improving security and security orientations of firms and their leaders

improves firm performance. Moreover, because some firms lose a sizeable portion of their revenues to theft (Russakoff & Goodman, 2012), a greater orientation towards security from executives will likely result in reduced security-related losses through increased security efforts, which in turn will boost firm performance.

The findings also indicate that LSO is indirectly associated with improved firm performance through market-based strategies. Specifically, the partially mediated relationship between LSO and firm performance through equity-based strategic alliances suggests that leaders higher in LSO are able to extract higher firm performance through the use of more effective security controls in their alliances, a finding that supports the idea that LSO could be a dynamic capability for leaders. Organizations utilize safeguards in alliances to protect against expropriation, but researchers have questioned the effectiveness of safeguards for years (e.g., Norman, 2002; Reuer & Tong, 2010). Usually, firms in alliances are highly reliant on contracts (Reuer & Tong, 2010), relational strategies such as trust (Srivastava & Gnyawali, 2011), and regulating employee behavior, including segmenting knowledge and information sharing (Das & Teng, 1999; Jarvenpaa & Majchrzak, 2016) to reduce opportunism and expropriation from alliance partners. For example, firms in inter-organizational alliances use trust as a relational strategy in alliances to develop cooperation and reduce the threat of opportunism from alliance partners (Ybarra & Turk, 2009). Previously, researchers found that safeguards in strategic alliances improve gains from those alliances (Inkpen, 2000; Jiang, Li, Gao, Bao, & Jiang, 2013). However, no previous research has established a link between executives' orientations towards security and firm performance through equity-based strategic alliances. Taken together, my findings suggest that organizations with leaders higher in LSO can produce better results from

equity-based strategic alliances through improved capability in reducing security threats, which then influences performance.

I also discovered a partially mediating effect between LSO and firm performance through exploitative innovations. I argued that higher LSO would be associated with increased firm performance through exploitative innovation, whereby higher LSO increases the ability to institute effective controls to current products and services offered to existing customers and markets. A key problem with product innovations is that they are eventually reverse engineered, allowing competitors to replicate or imitate innovations (Jensen & Thursby 1986; Minagawa, Trott & Hoecht, 2007). The potential of expropriation and theft by competitors or other actors is especially problematic in countries where proprietary asset protections are weak (Fosfuri, 2000) because a competitor can reverse engineer, reproduce, and then sell the focal firm's product as their own with little or no legal consequences. Thus, it becomes important for firms to stay ahead by continually introducing new products and services. However, the mediating relationship of LSO and performance through exploitative innovation suggests that firms with leaders higher in LSO can extract more value from exploitative innovations by improving or simply focusing on the security of innovations, thereby reducing competitors' ability to replicate the focal firms' innovations. Another possible explanation is that security-oriented leaders will pursue more aggressive legal enforcement against competitors attempting to steal the focal firm's proprietary assets. This argument is similar to the idea that leaders higher in LSO institute more security in strategic alliances, and as a consequence, improve firm performance. Finally, firms that are superior at executing exploitative innovation are more likely to protect their market share rather than pursuing new customers.

6.1.3 Is LSO associated with market-based strategies?

In Chapter IV, I predicted a positive relationship between LSO and equity-based strategic alliances. Equity-based strategic alliances are long-term cooperative agreements that pose challenges for firms and their competitive advantage (de Man & Roijakkers, 2009; Lorange & Roos, 1991; Lunnan & Haugland, 2008). Companies that engage in these cooperative agreements face the possibility that their partners may partake in opportunistic behavior and steal information or other valuable proprietary assets (Das & Teng, 1999; Williamson, 1981). Alliances make for complex relationships because risks must be identified and controlled (de Man & Roijakkers, 2009). Thus, firms must engage in protective action to mitigate the risk of theft or knowledge loss in equity-based strategic alliances (Oxley & Sampson, 2004). Protections in alliances can range from using contracts to minimize opportunism from partners (Reuer & Tong, 2010; Williamson, 1991) to establishing governing entities to monitor performance and agreement violations (Hoetker & Mellewigt, 2009).

The results from Chapter V support my previous arguments that equity-based strategic alliances are attractive for leaders with high LSO because they provide superior protections against expropriation (taking another's property). Interestingly, however, I found a positive and significant relationship between LSO and non-equity based strategic alliances; possibly due to hubris or a perceived lack of risk with the strategies presented in this dissertation that affect leaders' decision-making.

Exploitative and exploratory innovation strategies are commonly explored innovation strategies in management research. Exploitative innovation involves the pursuit of existing knowledge and extension of current products and services for the firm's existing customers (Benner & Tushman, 2003). Exploitative innovation is generally viewed as safer than

exploratory innovation (Jansen et al., 2006). Exploratory innovation refers to emerging knowledge, products, and services for new customers and markets. Compared to exploitative innovation, exploratory innovation is usually viewed as riskier. Jansen and colleagues' (2006) study shows that increasing certainty and formality are important mechanisms that firms use to minimize risk when using risky innovation strategies. Consequently, I hypothesized and found significant relationships between LSO and the two innovation strategies.

My results show positive relationships between LSO and exploitative innovation. I also found a positive relationship between LSO and exploratory innovation. I argued that LSO serves as an important predictor of innovation strategy attractiveness due to the potential risks and benefits of different innovation strategies. Exploitative innovation, as opposed to exploratory innovation, has traditionally been viewed as providing superior protections for innovations (Jansen et al., 2006). This study finds that LSO was associated with increased exploratory innovation; it was interesting because it was contrary to my hypothesis. Although I hypothesized and found a positive relationship between LSO and exploitative innovation, I also hypothesized a negative relationship between LSO and exploratory innovation. The relationship between LSO and exploratory innovation was positive, despite my predictions. The result could be for two reasons. First, managerial hubris could lead executives higher in LSO to believe that they can adequately protect innovations despite exploratory innovation exposing proprietary assets to greater risk. Second, exploratory innovation may not be as risky as thought, especially when a firm has effective security in place. However, I found no studies that examined exploratory innovation and security in more depth.

Thus, my dissertation has implications for market-based strategies and firm performance research. The findings support prospect theory in that firms with leaders higher in LSO will

pursue less-risky cooperative and innovation strategies. Interestingly, however, I also found that firms' leaders higher in LSO also pursue both risky and less-risky cooperative and innovation strategies, which could be explained by two reasons. First, leaders with high LSO might be prone to hubris and incorrectly believe they would not experience proprietary asset breaches thinking they are more protected from security threats. Hubris, or ignorance, encourages these leaders to pursue riskier and safer strategies alike. The second possible explanation is that firms' leaders higher in LSO might view the strategies presented in this study as equally risky. Using cooperative and innovation strategies that are perceived as more risky than the ones presented in this study might result in different findings than those discovered here (e.g., external sourcing versus internal R&D). Past research supports the perspective that firms choose innovation strategies based on concerns associated with appropriability (Cassiman & Veugelers, 2006). For example, Cassiman and Veugelers (2006) found that the strength of intellectual property protections increased the decision to source innovations internally, explaining that when organizations produce effective protective measures, they will source innovations internally.

To summarize the findings of this study, I discovered that LSO is a standalone construct that is predicted by managerial, firm, and industry factors. The predictors of LSO (e.g., executive technological interpretation, knowledge intensity, global presence) suggest that UET, strategic sensemaking, and institutional theory affect LSO at different levels. The consequences of LSO – that leaders high in LSO will pursue safer cooperative and innovation strategies and extract more value from these strategies – are grounded in dynamic capabilities theory. This theory specifies that executives tend to pursue strategies that minimize risk in the face of security to protect performance and, as a consequence, perform better. Thus, LSO appears to be an important

dynamic capability that executives can utilize to extract more value from their alliance and innovation activities to improve firm performance.

6.1.4 Practical Implications

Beyond the scholarly implications, the findings of this dissertation have a number of practical implications. The positive relationship between LSO and equity-based strategic alliances suggests that firms wishing to pursue equity-based strategic alliances should find or develop executives high in LSO. Similarly, the positive relationship between LSO and exploitative and explorative innovation means that firms should also find or develop executives high in LSO if they wish to pursue exploitative innovations. Considering both findings, executives higher in LSO may be attractive for firms seeking to explore new strategies that those without this orientation may not find attractive.

Given the findings that both equity-based strategic alliances and exploitative innovation served as intermediary mechanisms linking LSO to firm performance, security orientation should lead executives to consider risks associated with expropriation in alliances and innovation strategies and take more protective actions to prevent proprietary assets from being compromised or lost. Increased protective actions, in turn, should lead to firms extracting more value from their performance. Thus, all organizations might want to reevaluate whether they have adequate protections for their proprietary assets when they are involved in alliances or innovating, regardless of their leaders' security orientations. However, the findings of my dissertation suggest that high LSO leaders may be better equipped to extract more value from alliances and innovations than leaders who are lower in LSO. Finally, the findings provide evidence that firms with leaders higher in LSO experience increased firm performance. Thus, firms could possibly

hire executives higher in LSO to improve firm performance, likely because these leaders are more focused on reducing profit-minimizing factors (e.g., shrinkage, fraud, IP theft).

Given the important link between LSO and firm performance, developing top management teams with people high in LSO should be a high priority. Hiring top managers with LSO should produce alliance and innovation-seeking behavior as well as better firm performance. Moreover, firms may decide that training current and rising executives in LSO may be a desirable option to improve firm performance. Thus, an important component of hiring executives should be to assess individuals' LSO and train top managers to be more security oriented. Although no training on LSO currently exists, firms and their boards of directors interested in training executives on LSO should learn about preparedness, management, and learning and resilience related to proprietary assets. Moreover, emphasis should be given to explaining threats that competitors and other malicious actors pose, as well as how firms can help prevent theft or expropriation.

In addition, my theorizing and findings suggest that a mechanism exists between LSO, equity-based strategic alliances, and firm performance due to an improved understanding of risks to proprietary assets and proactive capabilities in managing such risks. The results of this study provide some support for this theory. The relationship between LSO and firm performance through equity-based strategic alliances suggests that managers should 1) focus on protecting proprietary assets during alliances, 2) work to prevent expropriation from alliance partners by focusing on or instituting security measures, and 3) become more oriented towards security if the organization engages in equity-based strategic alliances. Consequently, firms with leaders who are higher in LSO are more likely to be able to achieve greater firm performance through safer equity-based strategic alliances. I found similar results for a mediation effect of LSO,

exploitative innovation strategies, and firm performance. The mediated relationship between LSO and firm performance through exploitative innovation suggests that managers should 1) become more security-oriented when engaging in exploitative innovation, 2) institute proprietary protection measures with exploitative innovations, and 3) work to prevent expropriation from entities that seek to steal proprietary innovations from the firm. Taken together, these findings suggest that firms that focus more on LSO can better extract value in their cooperative and innovation strategies and, consequently, improve firm performance.

6.2 Limitations and Future Research Directions

All studies have limitations that should be addressed, and this dissertation is no different. Specific to this study, there are several issues with research design that limit this study's validity and generalizability. The first limitation is associated with data collection and common method variance issues. Because the variables were all collected at one time and collected by the same source, there is a chance that common method bias could influence the results. To counteract the chance that common method bias could influence the statistical results, I conducted tests for CMV and found that congeneric CMV was present in the data and took steps to mitigate its effect by using a marker variable in all subsequent analysis. However, I did not examine or include better marker variables that could reduce the potential influence of CMV more effectively.

In addition, I did not collect objective measures of firm performance, alliances strategies, and innovation strategies. Top managers (Vice President and above) rated items collected for this study, and these executives might be biased towards their firms or even lie about performance or attractiveness of alternatives. Nevertheless, I believe the measures selected for this study are

better than objective measures because it is unlikely that firms' executives would share these measures in a survey.

The findings and implications of this research point to several important future research directions. First, given the importance of security and firm level strategies and outcomes, it is important for future researchers to explore other determinants of LSO. The models used to predict performance only accounted for approximately half of relative firm performance. Consequently, there may be other important predictors of LSO, including firm-level factors. For example, perhaps the severity of a proprietary asset breach could affect LSO. In exploring these predictors, scholars may also wish to further reduce the number of items on the scale for more widespread adoption.

Given that all of the antecedents of LSO at the industry level were supported, more research is needed to explore more nuanced issues related to LSO and industry. For example, can firms hire executives from technologically intense industries to gain executives higher in LSO? Another interesting line of research would be to examine the transference of LSO across industries and whether or not LSO is more important in various industries. Scholars could also examine if LSO helps facilitate adoption of industry norms related to security at a faster rate than firms lead by leaders who are not as security oriented. Importantly, future research in this area could examine whether there exists a curvilinear relationship between the antecedents and consequences of LSO and LSO itself. More specifically, perhaps having leaders who are too security-oriented hamper productivity and limit their focus on growth strategies while leaders too low in LSO pursue too many risky opportunities. The findings related to industry seem to suggest that important differential effects may exist based on industry, thus many moderating conditions should be explored in future research.

A second important area for future research is the implications of hiring security-oriented firm executives and members of the board of directors. Directors serve an important role in setting the direction and approving strategies of the firm (Finkelstein, Hambrick, & Cannella, 2009), and hiring more directors with security experience could improve focus on security issues. As mentioned earlier in this dissertation, boards of directors increasingly view security as a top strategic concern (Lending, Minnick, & Schorno, 2018; Ziobro & Lublin, 2014). Thus, hiring more individuals to senior executive ranks or the boards of directors that possess high LSO or security experience may help firms to prevent or reduce the consequences of proprietary asset breaches. Do firms with CIOs or CISOs that are paid more or have higher representation on the board of directors become more security oriented? Representation and pay are two important indicators of importance of issues (Finkelstein et al., 2009).

Next, future research should explore whether LSO affects executives' decisions regarding risks in other types of strategic alliances. More specifically, future research should address whether LSO affects the propensity to engage in vertical partnerships over horizontal ones. This is important given that horizontal partnerships are more prone to risks associated with expropriation (Rindfleisch, 2000). In contrast, vertical partnerships pose fewer risks to firms given they pose much less risk of opportunism from alliance partners. Future research should also examine whether partners in an alliance are more security oriented based on seniority (senior versus junior and vice versa). In conjunction with this line of inquiry, researchers should examine whether more security-oriented firms are able to extract more value in their alliances from the perspective of the less or more senior partner.

Although this study provides important implications for scholarly research and practitioners, it does suffer from several shortfalls mentioned previously that future research

should address. First, the cross-sectional design of my dissertation is a significant flaw that limits the implications of the study. Consequently, my research does not answer whether or not LSO is associated with risk-aversion, an area for future research. Another study could examine whether LSO increases or reduces the propensity of executives to engage in alliances or innovation activity and whether the decision to engage (or not) in such activities affects long-term performance. Also importantly, this study does not answer the question: How do firms reconcile or balance the need for protection versus the need to innovate? Answering this question is especially important given that firms need to innovate to remain competitive. This study also did not examine the long-term firm performance implications of choosing exploitative innovation over exploratory innovation. These questions, and many other have important implications for competitive advantage and firm survival. Additional studies should pursuing this line of research should incorporate mixed methods (e.g. qualitative and quantitative) and policy capturing methods.

Additionally, I believe it is important to evaluate and understand the effect of LSO on a firms' employees. Scholars in information systems have long been interested in understanding operational-level factors, such as information security governance and its impact on employee security behaviors (e.g., Veiga & Eloff, 2007; Hu, Diney, Hart & Cooke, 2012). These behaviors are important because they can affect firm performance should the firm experience a breach because of employee failures or malicious actions. Consequently, it would be interesting to evaluate whether LSO affects employee-level security behavior, as top management commitment to initiatives is an important determinant of employees' adherence to those initiatives (Niehoff, Enz, & Grover, 1990). More specifically, related to this study, past researchers have argued that

top management is one of, if not the most, important component of information security (Hu et al., 2012; Von Solms & Von Solms, 2004).

Finally, LSO and other security-related studies may produce valuable insights into reducing both the frequency and severity of proprietary asset breaches, data breaches, and other security threats. Scholars and managers are already increasingly concerned with the effect of security incidents (e.g., Kashmiri, Nichol, & Hsu, 2017) given their impact on firm performance (Martin, Borah, & Palmatier, 2017). For example, Zafar and colleagues (2016) argue that the presence of a Chief Information Officer on a top management team improves firm performance following a security breach and helps them recover more quickly than firms that do not have CIOs. Thus, future research should directly measure the effect of security-related investments on firms' performance.

6.3 Conclusion

This dissertation explored the various predictors and consequences of Leader Security Orientation (LSO). The findings reveal several predictors and consequences of LSO. Specifically, several managerial and industry level predictors emerged as important, such as executives' interpretation of the environment as a threat and a firm's global presence, among many others. The findings of this dissertation also point to important organizational outcomes of LSO, particularly in the area of strategic alliance, organizational innovation, and firm performance. They indicate that LSO is an important determinant of strategic behavior and, consequently, firm performance. In a world where organizations face increasing threats to their proprietary assets, improving leaders' security orientations may be a means by which firms gain and sustain competitive advantage. I extend previous research in two important ways. First, I developed a new scale of Leader Security Orientation (LSO) for use in strategic alliance and

innovation research. Second, I link organizational leaders' orientations towards protection of proprietary assets and strategic outcomes, a finding not previously explored in research.

REFERENCES

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 1563-1580.

Adam, T. R., Fernando, C. S., & Golubeva, E. (2015). Managerial overconfidence and corporate risk management. *Journal of Banking & Finance*, *60*, 195-208.

Ahmadi, S., Khanagha, S., Berchicci, L., & Jansen, J. J. (2017). Are managers motivated to explore in the face of a new technological change? The role of regulatory focus, fit, and complexity of decision-making. *Journal of Management Studies*, *54*(2), 209-237.

Alexiev, A. S., Jansen, J. J., Van den Bosch, F. A., & Volberda, H. W. (2010). Top management team advice seeking and exploratory innovation: The moderating role of TMT heterogeneity. *Journal of Management Studies*, *47*(7), 1343-1364.

Alpaslan, C. M., Green, S. E., & Mitroff, I. I. (2009). Corporate governance in the context of crises: Towards a stakeholder theory of crisis management. *Journal of Contingencies and Crisis Management*, *17*(1), 38-49.

Alvesson, M. (1995). *Management of knowledge-intensive companies* (Vol. 61). Berlin: de Gruyter.

American Management Association. (2004). *2004 AMA survey: Crisis management and security issues.* New York: Author.

Anderson, J. C., & Gerbing, D. W. (1991). Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities. *Journal of Applied Psychology*, *76*(5), 732.

Anderson, P., & Tushman, M. L. (1990). Technological discontinuities and dominant designs: A cyclical model of technological change. *Administrative Science Quarterly*, 604-633.

Andreeva, T., & Kianto, A. (2011). Knowledge processes, knowledge-intensity and innovation: a moderated mediation analysis. *Journal of Knowledge Management*, *15*(6), 1016-1034.

Archak, N., Ghose, A., & Ipeirotis, P. G. (2011). Deriving the pricing power of product features by mining consumer reviews. *Management Science*, *57*(8), 1485-1509.

Armstrong, J. S., & Collopy, F. (1996). Competitor orientation: Effects of objectives and information on managerial decisions and profitability. *Journal of Marketing Research, 33*(2),188-199.

Arora, A. (1997). Patents, licensing, and market structure in the chemical industry. *Research Policy*, *26*(4), 391-403.

Arundel, A. (2001). The relative effectiveness of patents and secrecy for appropriation. *Research Policy*, *30*(4), 611-624.

Athanassiou, N., & Nigh, D. (2000). Internationalization, tacit knowledge and the top management teams of MNCs. *Journal of International Business Studies*, *31*(3), 471-487.

Attewell, P. (1992). Technology diffusion and organizational learning: The case of business computing. *Organization Science*, *3*(1), 1-19.

Auh, S., & Menguc, B. (2005). Balancing exploration and exploitation: The moderating role of competitive intensity. *Journal of Business Research*, *58*(12), 1652-1661.

Autio, E., Sapienza, H. J., & Almeida, J. G. (2000). Effects of age at entry, knowledge intensity, and imitability on international growth. *Academy of Management Journal*, *43*(5), 909-924.

Bantel, K. A., & Jackson, S. E. (1989). Top management and innovations in banking: does the composition of the top team make a difference?. *Strategic Management Journal*, *10*(S1), 107-124.

Barberis, N. C. (2013). Thirty years of prospect theory in economics: A review and assessment. *Journal of Economic Perspectives*, *27*(1), 173-96.

Barnett, C. K., & Pratt, M. G. (2000). From threat-rigidity to flexibility-Toward a learning model of autogenic crisis in organizations. *Journal of Organizational Change Management*, 13(1), 74-88.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99-120.

Bartram, S. M., Brown, G. W., & Conrad, J. (2009). The effects of derivatives on firm risk and value (Working paper). *Chapel Hill: University of North Carolina*.

Beasley, M. S., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, *24*(6), 521-531.

Bechky, B. A., & Okhuysen, G. A. (2011). Expecting the unexpected? How SWAT officers and film crews handle surprises. *Academy of Management Journal*, *54*(2), 239-261.

Benner, M. J., & Tushman, M. L. (2003). Exploitation, exploration, and process management: The productivity dilemma revisited. *Academy of Management Review, 28*(2), 238-256.

Bennett, R., & Gabriel, H. (1999). Organisational factors and knowledge management within large marketing departments: an empirical study. *Journal of Knowledge Management*, *3*(3), 212-225.

Berezina, K., Cobanoglu, C., Miller, B. L., & Kwansa, F. A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management*, *24*(7), 991-1010.

Bigley, G. A., & Roberts, K. H. (2001). The incident command system: High-reliability organizing for complex and volatile task environments. *Academy of Management Journal, 44*(6), 1281-1299.

Boal, K. B., & Schultz, P. L. (2007). Storytelling, time, and evolution: The role of strategic leadership in complex adaptive systems. *The Leadership Quarterly*, *18*(4), 411-428.

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management, 15*(1), 50-59.

Bonnier, K. A., & Bruner, R. F. (1989). An analysis of stock price reaction to management change in distressed firms. *Journal of Accounting and Economics, 11*(1), 95-106.

Borgman, C. L. (1999). What are digital libraries? Competing visions. Information Processing & Management, *35*, 227-243

Bos, B., Broekhuizen, T. L., & de Faria, P. (2016). A dynamic view on secrecy management. *Journal of Business Research*, *68*(12), 2619-2627.

Boudes, T., & Laroche, H. (2009). Taking off the heat: Narrative sensemaking in post-crisis inquiry reports. *Organization Studies, 30*(4), 377-396.

Brockner, J., & James, E. H. (2008). Toward an understanding of when executives see crisis as opportunity. *The Journal of Applied Behavioral Science*, *44*(1), 94-115.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning, 48*(4), 265-276.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Bundy, J., & Pfarrer, M. D. (2015). A burden of responsibility: The role of social approval at the onset of a crisis. *Academy of Management Review*, *40*(3), 345-369.

Bundy, J., Pfarrer, M. D., Short, C. E., & Coombs, W. T. (2016). Crises and Crisis Management Integration, Interpretation, and Research Development. *Journal of Management*, 43(6), 1661-1692.

Burbano, V. C. (2016). Social responsibility messages and worker wage requirements: Field experimental evidence from online labor marketplaces. *Organization Science*, *27*(4), 1010-1028.

Burns, A. J., Posey, C., Courtney, J. F., Roberts, T. L., & Nanayakkara, P. (2017). Organizational information security as a complex adaptive system: insights from three agent-based models. *Information Systems Frontiers*, *19*(3), 509-524.

Butler Jr, J. K. (1991). Toward understanding and measuring conditions of trust: Evolution of a conditions of trust inventory. *Journal of Management*, *17*(3), 643-663.

Buttars, N. K., Young, A. J., & Bailey, D. (2006). Adoption of security systems by dairy farms to address bioterrorist threats in the intermountain United States. *Journal of Dairy Science*, *89*(5), 1822-1829.

Calantone, R. J., Cavusgil, S. T., & Zhao, Y. (2002). Learning orientation, firm innovation capability, and firm performance. *Industrial Marketing Management*, *31*(6), 515-524.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431-448.

Carley, K. M., & Harrald, J. R. (1997). Organizational learning under fire. *The American Behavioral Scientist*, *40*(3), 310-332.

Carmeli, A., & Schaubroeck, J. (2008). Organisational crisis-preparedness: the importance of learning from failures. *Long Range Planning*, *41*(2), 177-196.

Carpenter, M. A., & Fredrickson, J. W. (2001). Top management teams, global strategic posture, and the moderating role of uncertainty. *Academy of Management Journal*, *44*(3), 533-545.

Carpenter, M. A., Geletkanycz, M. A., & Sanders, W. G. (2004). Upper echelons research revisited: Antecedents, elements, and consequences of top management team composition. *Journal of Management*, *30*(6), 749-778.

Carter, D. A., Rogers, D. A., & Simkins, B. J. (2006). Does hedging affect firm value? Evidence from the US airline industry. *Financial Management*, *35*(1), 53-86.

Cassady, R. (1964). The Intelligence Function and Business Competition. *California Management Review, 6*(3), 85-92.

Cassiman, B., & Veugelers, R. (2006). In search of complementarity in innovation strategy: Internal R&D and external knowledge acquisition. *Management Science, 52*(1), 68-82.

Castille, C. M., Buckner, J. E., & Thoroughgood, C. N. (2018). Prosocial citizens without a moral compass? Examining the relationship between Machiavellianism and unethical pro-organizational behavior. *Journal of Business Ethics, 149*(4), 919-930.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 70-104.

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Rao, H. R. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems, 83*, 47-56.

Chan, C. (2014). This is the vault where KFC guards the Colonel's secret original recipe. Retrieved from http://sploid.gizmodo.com/this-is-the-vault-where-kfc-guards-the-colonels-secret-1650566046.

Chan, M. (2003). Corporate espionage and workplace trust/distrust. *Journal of Business Ethics, 42*(1), 45-58.

Chen, Y. A. N., Ramamurthy, K. R. A. M., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems, 55*(3), 11-19.

Cho, T. S., & Hambrick, D. C. (2006). Attention as the mediator between top management team characteristics and strategic change: The case of airline deregulation. *Organization Science, 17*(4), 453-469.

Choudhary, P., Mital, M., Pani, A. K., Papa, A., & Vicentini, F. (2018). Impact of enterprise mobile system implementation on organizational ambidexterity mediated through BPM customizability. *Business Process Management Journal, 24*(5), 1235-1254.

Christianson, M. K., Farkas, M. T., Sutcliffe, K. M., & Weick, K. E. (2009). Learning through rare events: Significant interruptions at the Baltimore & Ohio Railroad Museum. *Organization Science, 20*(5), 846-860.

Clair, J. A., & Waddock, S. (2007). A ''total'' responsibility management approach to crisis management and signal detection in organizations. *International Handbook of Organizational Crisis Management,* 299-314.

Coff, R. (2003). Bidding wars over R&D-intensive firms: Knowledge, opportunism, and the market for corporate control. *Academy of Management Journal, 46*(1), 74-85.

Cohen, W. M., & Levinthal, D. A. (1990). Absorptive capacity: A new perspective on learning and innovation. *Administrative Science Quarterly, 35*(1), 128-152.

Cohen, W. M., Goto, A., Nagata, A., Nelson, R. R., & Walsh, J. P. (2002). R&D spillovers, patents and the incentives to innovate in Japan and the United States. *Research Policy, 31*(8), 1349-1367.

Conger, J. A., & Kanungo, R. N. (1987). Toward a behavioral theory of charismatic leadership in organizational settings. *Academy of Management Review, 12*(4), 637-647.

Connelly, B. L., Ketchen, D. J., Gangloff, K. A., & Shook, C. L. (2015). Investor perceptions of CEO successor selection in the wake of integrity and competence failures: A policy capturing study. *Strategic Management Journal, 37*(10), 2135-2150.

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

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

Coombs, W. T., & Holladay, S. J. (1996). Communication and attributions in a crisis: An experimental study in crisis communication. *Journal of Public Relations Research, 8*(4), 279-295.

Cortina, J. M., Green, J. P., Keeler, K. R., & Vandenberg, R. J. (2017). Degrees of freedom in SEM: Are we testing the models that we claim to test?. *Organizational Research Methods, 20*(3), 350-378.

Costello, A. B., & Osborne, J. W. (2003, April). Exploring best practices in factor analysis: Four mistakes applied researchers make. In *Trabajo presentado en la Annual Meeting of the American Educational Research Association (AERA), Chicago, IL*.

Crilly, D., Ni, N., & Jiang, Y. (2015). Do-no-harm versus do-good social responsibility: Attributional thinking and the liability of foreignness. *Strategic Management Journal*. *37*(7), 1316-1329.

Crowe, E., & Higgins, E. T. (1997). Regulatory focus and strategic inclinations: Promotion and prevention in decision-making. *Organizational Behavior and Human Decision Processes, 69*(2), 117-132.

Daft, R. L., & Weick, K. E. (1984). Toward a model of organizations as interpretation systems. *Academy of Management Review, 9*(2), 284-295.

Daily, C. M., Dalton, D. R., & Cannella, A. A. (2003). Corporate governance: Decades of dialogue and data. *Academy of Management Review, 28*(3), 371-382.

D'Arcy, S. P., & Brogan, J. C. (2001). Enterprise risk management. *Journal of Risk Management of Korea, 12*(1), 207-228.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117.

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics, 89*(1), 59-71.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20*, 79-98.

Darling, J., Hannu, O., & Raimo, N. (1996). Crisis management in international business: A case situation in decision making concerning trade with Russia. *The Finnish Journal of Business Economics, 4*, 12–25.

Das, T. K., & Teng, B. S. (1999). Managing risks in strategic alliances. *Academy of Management Perspectives, 13*(4), 50-62.

Das, T. K., & Teng, B. S. (2000). A resource-based theory of strategic alliances. *Journal of Management, 26*(1), 31-61.

Das, T. K., & Teng, B. S. (2000). Instabilities of strategic alliances: An internal tensions perspective. *Organization Science, 11*(1), 77-101.

Datta, D. K., Rajagopalan, N., & Zhang, Y. (2003). New CEO openness to change and strategic persistence: The moderating role of industry characteristics. *British Journal of Management, 14*(2), 101-114.

Daum, J. H. Stuart, S. & Stautberg, S. (2016). 2016 Global Board of Directors Survey. Harvard Law School Forum on Corporate Governance and Financial Regulation.

D'Aveni, R. A., & MacMillan, I. C. (1990). Crisis and the content of managerial communications: A study of the focus of attention of top managers in surviving and failing firms. *Administrative Science Quarterly*, 634-657.

Davidson, W. N., Worrell, D. L., & Dutia, D. (1993). The stock market effects of CEO succession in bankrupt firms. *Journal of Management, 19*(3), 517-533.

Dean, D. H. (2004). Consumer reaction to negative publicity effects of corporate reputation, response, and responsibility for a crisis event. *Journal of Business Communication*, *41*(2), 192-211.

Deephouse, D. L. (1996). Does isomorphism legitimate?. *Academy of Management Journal*, *39*(4), 1024-1039.

Delerue, H., & Lejeune, A. (2010). Job mobility restriction mechanisms and appropriability in organizations: The mediating role of secrecy and lead time. *Technovation*, *30*(5), 359-366.

de Faria, P., & Sofka, W. (2010). Knowledge protection strategies of multinational firms—A cross-country comparison. *Research Policy*, *39*(7), 956-968.

De Man, A. P., & Roijakkers, N. (2009). Alliance governance: balancing control and trust in dealing with risk. *Long Range Planning, 42*(1), 75-95.

Desai, V. M. (2011). Mass media and massive failures: Determining organizational efforts to defend field legitimacy following crises. *Academy of Management Journal, 54*, 263–278

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Commun. ACM*, *43*(7), 125-128.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: an organizational transformation case study. *Computers & Security, 56*, 63-69.

Diaz, J. 2010. How Apple lost the iPhone 4. ***Gizmodo.com.*** December 10, 2016. http://gizmodo.com/5520438/how-apple-lost-the-next-iphone.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, *48*, 147-160.

Dionne, G. (2013). Risk management: History, definition, and critique. *Risk Management and Insurance Review*, *16*(2), 147-166.

Dowell, G. W., Shackell, M. B., & Stuart, N. V. (2011). Boards, CEOs, and surviving a financial crisis: Evidence from the internet shakeout. *Strategic Management Journal, 32*(10), 1025-1045.

Doz, Y. L., & Kosonen, M. (2010). Embedding strategic agility: A leadership agenda for accelerating business model renewal. *Long Range Planning*, *43*(2-3), 370-382.

Dreze, J. H. (1981). Inferring risk tolerance from deductibles in insurance contracts. *Geneva Papers on Risk and Insurance*, 48-52.

Dutton, J. E., Fahey, L., & Narayanan, V. K. (1983). Toward understanding strategic issue diagnosis. *Strategic Management Journal*, *4*(4), 307-323.

Dutton, J. E., & Jackson, S. E. (1987). Categorizing strategic issues: Links to organizational action. *Academy of Management Review*, *12*(1), 76-90.

Earl, M. (2001). Knowledge management strategies: Toward a taxonomy. *Journal of Management Information Systems*, *18*(1), 215-233.

Egelhoff, W. G., & Sen, F. (1992). An information-processing model of crisis management. *Management Communication Quarterly*, *5*(4), 443-484.

Eggers, J. P., & Park, K. F. (2018). Incumbent adaptation to technological change: The past, present, and future of research on heterogeneous incumbent response. *Academy of Management Annals*, *12*(1), 357-389.

El Akremi, A., Gond, J. P., Swaen, V., De Roeck, K., & Igalens, J. (2015). Do employees perceive corporate social responsibility? Development and validation of a multidimensional corporate social responsibility scale. *J. Manag. doi*, *10*(0149206315569311).

Elsubbaugh, S., Fildes, R., & Rose, M. B. (2004). Preparation for crisis management: A proposed model and empirical evidence. *Journal of Contingencies and Crisis Management*, *12*(3), 112-127.

Evangelidis, I., & Levav, J. (2013). Prominence versus dominance: How relationships between alternatives drive decision strategy and choice. *Journal of Marketing Research*, *50*(6), 753-766.

Fair, W. R. (1966). The corporate CIA-a prediction of things to come. *Management Science*, *12*(10), B-489.

Fatemi, A., Desai, A. S., & Katz, J. P. (2003). Wealth creation and managerial pay: MVA and EVA as determinants of executive compensation. *Global Finance Journal*, *14*(2), 159-179.

Ferrier, W. J., Smith, K. G., & Grimm, C. M. (1999). The role of competitive action in market share erosion and industry dethronement: A study of industry leaders and challengers. *Academy of Management Journal*, *42*(4), 372-388.

Finkelstein, S., Hambrick, D. C., & Cannella, A. A. (2009). *Strategic leadership: Theory and research on executives, top management teams, and boards*. Oxford University Press, USA.

Florack, A., Keller, J., & Palcu, J. (2013). Regulatory focus in economic contexts. *Journal of Economic Psychology*, *38*, 127-137.

Flikkema, M. J., Castaldi, C., de Man, A. P., & Seip, M. (2017). Trademark scope and similarity as predictors of the trademark-innovation linkage. *EPIP Conference 2017*.

Fombrun, C. (1996). *Reputation.* John Wiley & Sons, Ltd.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research, 18*, https://doi.org/10.1177/002224378101800313

Fosfuri, A. (2000). Patent protection, imitation and the mode of technology transfer. *International Journal of Industrial Organization*, *18*(7), 1129-1149.

Finkelstein, S., Hambrick, D. C., & Cannella, A. A. (2009). *Strategic leadership: Theory and research on executives, top management teams, and boards.* Oxford University Press, USA.

Fraser, J. R., Fraser, J., & Simkins, B. (2010). *Enterprise risk management: Today's leading research and best practices for tomorrow's executives* (Vol. 3). John Wiley & Sons.

Froot, K. A., Scharfstein, D. S., & Stein, J. C. (1993). Risk management: Coordinating corporate investment and financing policies. *Journal of Finance*, *48*(5), 1629-1658.

Galaskiewicz, J. (1985). Interorganizational relations. *Annual Review of Sociology, 11*(1), 281-304.

Galavotti, I. (2019). Systematic Literature Review on Experience and Learning in Acquisitions: Search Strategy and Data Synthesis. In *Experience and Learning in Corporate Acquisitions* (pp. 125-137). Palgrave Macmillan, Cham.

Gallié, E. P., & Legros, D. (2012). French firms' strategies for protecting their intellectual property. *Research Policy*, *41*(4), 780-794.

Garrison, C., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security*, *19*(4), 216-230.

Gatev, E., & Strahan, P. E. (2006). Banks' advantage in hedging liquidity risk: Theory and evidence from the commercial paper market. *The Journal of Finance*, *61*(2), 867-892.

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, *13*(1), 61-83.

Gao, Z., House, L. A., & Xie, J. (2016). Online survey data quality and its implication for willingness-to-pay: A cross-country comparison. *Canadian Journal of Agricultural Economics/Revue canadienne d'agroeconomie*, *64*(2), 199-221.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, *11*(2), 74-83.

Gephart, R. P., Van Maanen, J., & Oberlechner, T. (2009). Organizations and risk in late modernity. *Organization Studies*, *30*(2-3), 141-155.

Gittell, J. H., Cameron, K., Lim, S., & Rivas, V. (2006). Relationships, layoffs, and organizational resilience airline industry responses to September 11. *The Journal of Applied Behavioral Science*, *42*(3), 300-329.

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

Gold, A. H., & Arvind Malhotra, A. H. S. (2001). Knowledge management: An organizational capabilities perspective. *Journal of Management Information Systems*, *18*(1), 185-214.

Goodboy, A. K., & Kline, R. B. (2017). Statistical and practical concerns with published communication research featuring structural equation modeling. *Communication Research Reports*, *34*(1), 68-77.

Government Accountability Office. (2015). Cybersecurity: Actions needed to address challenges facing federal systems. GAO-15-573T.

Graham, J. R., & Rogers, D. A. (2002). Do firms hedge in response to tax incentives?. *The Journal of Finance*, *57*(2), 815-839.

Grant, R. M. (1996). Toward a knowledge-based theory of the firm. *Strategic Management Journal*, *17*(S2), 109-122.

Greenberg, L., & Barling, J. (1996). Employee theft. *Journal of Organizational Behavior*, *3*, *49-64*.

Greening, D. W., & Johnson, R. A. (1996). Do managers and strategies matter? A study in crisis. *Journal of Management Studies*, *33*(1), 25-51.

Greening, D. W., & Johnson, R. A. (1997). Managing Industrial and Environmental Crises The Role of Heterogeneous Top Management Teams. *Business & Society*, *36*(4), 334-361.

Guay, W., & Kothari, S. P. (2003). How much do firms hedge with derivatives?. *Journal of Financial Economics*, *70*(3), 423-461

Guin, T. D. L., Baker, R., Mechling, J., & Ruyle, E. (2012). Myths and realities of respondent engagement in online surveys. *International Journal of Market Research*, *54*(5), 613-633.

Gulati, R. (1995). Social structure and alliance formation patterns: A longitudinal analysis. *Administrative Science Quarterly*, 619-652.

Gundel, S. (2005). Towards a new typology of crises. *Journal of Contingencies and Crisis Management*, *13*(3), 106-115.

Gupta, A. K., & Govindarajan, V. (1991). Knowledge flows and the structure of control within multinational corporations. *Academy of Management Review*, *16*(4), 768-792.

Haahti, A., Madupu, V., Yavas, U., & Babakus, E. (2005). Cooperative strategy, knowledge intensity and export performance of small and medium sized enterprises. *Journal of World Business*, *40*(2), 124-138.

Hadley, C. N., Pittinsky, T. L., Sommer, S. A., & Zhu, W. (2011). Measuring the efficacy of leaders to assess information and make decisions in a crisis: The C-LEAD scale. *The Leadership Quarterly*, *22*(4), 633-648.

Hair, J., Anderson, R. O., & Tatham, R. (1987). *Multidimensional Data Analysis.* New York.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). Multivariate data analysis: Pearson new international edition. *Essex: Pearson Education Limited*.

Hale, J. C., Landry, T. D., & Wood, C. M. (2004). Susceptibility audits: A tool for safeguarding information assets. *Business Horizons*, *47*(3), 59-66.

Hajjar, R. (2014). What Lessons Did We Learn (or Re-Learn) About Military Advising After 9/11?. *Military Review*, *94*(6), 63.

Hamblin, R. L. (1958). Leadership and crises. *Sociometry*, *21*(4), 322-335.

Hambrick, D. C. (2007). Upper echelons theory: An update. *Academy of Management Review*, *32*(2), 334-343.

Hambrick, D. C., & Mason, P. A. (1984). Upper echelons: The organization as a reflection of its top managers. *Academy of Management Review*, *9*(2), 193-206.

Hannah, D. R. (2005). Should I keep a secret? The effects of trade secret protection procedures on employees' obligations to protect trade secrets. *Organization Science*, *16*(1), 71-84.

Hannah, D. R. (2007). An examination of the factors that influence whether newcomers protect or share secrets of their former employers. *Journal of Management Studies*, *44*(4), 465-487.

Hannah, D. R., & Robertson, K. (2015). Why and how do employees break and bend confidential information protection rules?. *Journal of Management Studies*, *52*(3), 381-413.

Hansen, G. S., & Wernerfelt, B. (1989). Determinants of firm performance: The relative importance of economic and organizational factors. *Strategic management journal*, *10*(5), 399-411.

Harman, H. H.(1967). ***Modern Factor Analysis*** (2nd ed.). Chicago: University of Chicago Press.

Harrington, S. E., Niehaus, G., & Risko, K. J. (2002). Enterprise risk management: the case of united grain growers. *Journal of Applied Corporate Finance*, *14*(4), 71-81.

Harris, J., & Bromiley, P. (2007). Incentives to cheat: The influence of executive compensation and firm performance on financial misrepresentation. *Organization Science*, *18*(3), 350-367.

Hashai, N., & Almor, T. (2008). R&D intensity, value appropriation and integration patterns within organizational boundaries. *Research Policy*, *37*(6), 1022-1034.

Hashai, N., Asmussen, C. G., Benito, G. R., & Petersen, B. (2010). Technological knowledge intensity and entry mode diversity. *Management International Review*, *50*(6), 659-681.

Hayes, A. F. (2012). PROCESS: A versatile computational tool for observed variable mediation, moderation, and conditional process modeling [White paper]. Retrieved from http://www.afhayes.com/public/process2012.pdf

Hayes, A. F. (2013). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach.* Guilford. New York.

Haynie, J. J., Svyantek, D. J., Mazzei, M. J., & Varma, V. (2016). Job insecurity and compensation evaluations: the role of overall justice. *Management Decision*, *54*(3), 630-645.

Heide, M., & Simonsson, C. (2014). Developing internal crisis communication: New roles and practices of communication professionals. *Corporate Communications: An International Journal*, *19*(2), 128-146.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Herrmann, P., & Datta, D. K. (2005). Relationships between top management team characteristics and international diversification: An empirical investigation. *British Journal of Management*, *16*(1), 69-78.

Hertzfeld, H. R., Link, A. N., & Vonortas, N. S. (2006). Intellectual property protection mechanisms in research partnerships. *Research Policy, 35*(6), 825-838.

Higgins, E. T. (1998). Promotion and prevention: Regulatory focus as a motivational principle. In *Advances in Experimental Social Psychology* (Vol. 30, pp. 1-46). Academic Press.

Hillman, A. J., & Dalziel, T. (2003). Boards of directors and firm performance: Integrating agency and resource dependence perspectives. *Academy of Management Review*, *28*(3), 383-396.

Hinkin, T. R. (1995). A review of scale development practices in the study of organizations. *Journal of Management*, *21*(5), 967-988.

Hinkin, T. R. (1998). A brief tutorial on the development of measures for use in survey questionnaires. *Organizational Research Methods, 1*(1), 104-121.

Hitt, M.A., Ireland, R.D. and Hoskisson, R.E. (2015). *Strategic Management: Competitiveness and Globalization Concepts,* 6th ed., Thomson, South-Western, Mason, OH

Hoetker, G., & Mellewigt, T. (2009). Choice and performance of governance mechanisms: matching alliance governance to asset type. *Strategic Management Journal*, *30*(10), 1025-1044.

Hoffman, A. J., & Ocasio, W. (2001). Not all events are attended equally: Toward a middle-range theory of industry attention to external events. *Organization Science*, *12*(4), 414-434.

Holmes Jr, R. M., Bromiley, P., Devers, C. E., Holcomb, T. R., & McGuire, J. B. (2011). Management theory applications of prospect theory: Accomplishments, challenges, and opportunities. *Journal of Management*, *37*(4), 1069-1107.

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, *11*(5), 243-248.

Howard, M. C., & Melloy, R. C. (2016). Evaluating Item-Sort Task Methods: The presentation of a new statistical significance formula and methodological best practices. *Journal of Business and Psychology*, *31*(1), 173-186.

Hoelter, J. W. (1983). The analysis of covariance structures: Goodness-of-fit indices. *Sociological Methods & Research*, *11*(3), 325-344.

Hsieh, P. F., Lee, C. S., & Ho, J. C. (2012). Strategy and process of value creation and appropriation in service clusters. *Technovation*, *32*(7-8), 430-439.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policy: The critical role of top management and organizational culture. *Decision Sciences*,*43*(4), 615-659.

Huang, Y. H. (2006). Crisis situations, communication strategies, and media coverage a multicase study revisiting the communicative response model. *Communication Research*, *33*(3), 180-205.

Hughes, M., Ireland, R. D., & Morgan, R. E. (2007). Stimulating dynamic value: Social capital and business incubation as a pathway to competitive success. *Long Range Planning*, *40*(2), 154-177.

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: a review of four recent studies. *Strategic Management Journal*, *20*(2), 195-204.

Hurt, K. J., & Abebe, M. A. (2015). The effect of conflict type and organizational crisis on perceived strategic decision effectiveness an empirical investigation. *Journal of Leadership & Organizational Studies*, *22*(3), 340-354.

Ibrahim, N. A., & Angelidis, J. P. (1994). Effect of board members' gender on corporate social responsiveness orientation. *Journal of Applied Business Research*, *10*, 35-35.

Identity Theft Resource Center. (2017). At mid-year, U.S. data breaches increase at record pace. Retrieved on November 21, 2017 from http://www.idtheftcenter.org/Press-Releases/2017-mid-year-data-breach-report-press-release.

Inkpen, A. C. (2000). Learning through joint ventures: a framework of knowledge acquisition. *Journal of Management Studies*, *37*(7), 1019-1044.

Ireland, R. D., Hitt, M. A., & Vaidyanath, D. (2002). Alliance management as a source of competitive advantage. *Journal of Management*, *28*(3), 413-446.

Jackson, S. E., & Dutton, J. E. (1988). Discerning threats and opportunities. *Administrative Science Quarterly*, *33*(3) 370-387.

James, E. H., & Wooten, L. P. (2005). Leadership as (Un) usual: How to Display Competence in Times of Crisis. *Organizational Dynamics*, *34*(2), 141-152.

James, E. H., Wooten, L. P., & Dushek, K. (2011). Crisis management: Informing a new leadership research agenda. *The Academy of Management Annals*, *5*(1), 455-493.

James, S. D., Leiblein, M. J., & Lu, S. (2013). How firms capture value from their innovations. *Journal of Management*, *39*(5), 1123-1155.

Janofsky, A. (2017). Equifax breach could cost billions. Retrieved from https://www.wsj.com/articles/equifax-breach-could-cost-billions-1505474692

Jansen, J. J., Van Den Bosch, F. A., & Volberda, H. W. (2006). Exploratory innovation, exploitative innovation, and performance: Effects of organizational antecedents and environmental moderators. *Management Science*, *52*(11), 1661-1674.

Jarvenpaa, S. L., & Majchrzak, A. (2016). Interactive self-regulatory theory for sharing and protecting in interorganizational collaborations. *Academy of Management Review*, *41*(1), 9-27.

Jaworski, B. J., & Kohli, A. K. (1993). Market orientation: antecedents and consequences. *The Journal of Marketing*, 53-70.

Jensen, R., & Thursby, M. (1986). A strategic approach to the product life cycle. *Journal of International Economics*, *21*(3-4), 269-284.

Jiang, X., Li, M., Gao, S., Bao, Y., & Jiang, F. (2013). Managing knowledge leakage in strategic alliances: The effects of trust and formal contracts. *Industrial Marketing Management*, *42*(6), 983-991.

Johansen, W., Aggerholm, H. K., & Frandsen, F. (2012). Entering new territory: A study of internal crisis management and crisis communication in organizations. *Public Relations Review, 38(*2), 270-279.

Johanson, J., & Vahlne, J. E. (1977). The internationalization process of the firm—a model of knowledge development and increasing foreign market commitments. *Journal of International Business Studies*, *8*(1), 23-32

Jungbauer, D. K. K. L. (2016). Leading in times of crisis: Examining the effectiveness of different leadership styles across stages of the crisis lifecycle (Doctoral dissertation, Department of Organizational and Business Psychology, TU Chemnitz).

Kahn, W. A., Barton, M. A., & Fellows, S. (2013). Organizational crises and the disturbance of relational systems. *Academy of Management Review*, *38*, 377-396.

Kahneman, D., & Tversky, A. 1979. Prospect theory: An analysis of decisions under risk. *Econometrica, 47*, 263-291.

Kale, P., Singh, H., & Perlmutter, H. (2000). Learning and protection of proprietary assets in strategic alliances: Building relational capital. *Strategic Management Journal*, *21*(3), 217-237.

Kannan, K., Reese, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce, 12*(1), 69-91.

Kaplan, R. S., & Norton, D. P. (2006). How to implement a new strategy without disrupting your organization. *Harvard Business Review*, *84*(3), 100.

Kapuscinski, A. N., & Masters, K. S. (2010). The current status of measures of spirituality: A critical review of scale development. *Psychology of Religion and Spirituality*, *2*(4), 191-205.

Kash, T. J., & Darling, J. R. (1998). Crisis management: prevention, diagnosis and intervention. *Leadership & Organization Development Journal*, *19*(4), 179-186.

Kashmiri, S., Nicol, C. D., & Hsu, L. (2017). Birds of a feather: intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science, 45*(2), 208-228.

Kiesler, S., & Sproull, L. (1982). Managerial response to changing environments: Perspectives on problem sensing from social cognition. *Administrative Science Quarterly*, 548-570.

Kim, L. (1998). Crisis construction and organizational learning: Capability building in catching-up at Hyundai Motor. *Organization Science, 9*(4), 506-521.

Kline, R. B. (2017). ***Principles and Practice of Structural Equation Modeling***. 4th ed. Boston: Guilford publications.

Knight, F. H. (1921). Cost of production and price over long and short periods. *Journal of Political Economy, 29*(4), 304-335.

Kogut, B., & Zander, U. (1993). Knowledge of the firm and the evolutionary theory of the multinational corporation. *Journal of International Business Studies*, *24*(4), 625-645.

Kollman, T., & Stockman, C. (2014). Filling the entrepreneurial orientation-performance gap: the mediating effects of exploratory and exploitative innovations. *Entrepreneurship: Theory & Practice, 38*(5), 1001-1026.

Kohli, A. K., & Jaworski, B. J. (1990). Market orientation: the construct, research propositions, and managerial implications. *The Journal of Marketing, 54*(2), 1-18.

Kondalamahanty, A. (2016). India's TCS fined $940 million in US trade secrets lawsuit. IBtimes.com. Retrieved on April 27, 2016 from http://www.ibtimes.com/indias-tcs-fined-940-million-us-trade-secrets-lawsuit-2355025.

Kosterman, R., & Feshbach, S. (1989). Toward a measure of patriotic and nationalistic attitudes. *Political Psychology, 10*(2), 257-274.

Lampel, J., Shamsie, J., & Shapira, Z. (2009). Experiencing the improbable: Rare events and organizational learning. *Organization Science, 20*(5), 835-845.

Lange, D., & Washburn, N. T. (2012). Understanding attributions of corporate social irresponsibility. *Academy of Management Review, 37*(2), 300-326.

Lant, T. K., & Milliken, F. J. (1992). The role of managerial learning and interpretation in strategic persistence and reorientation: An empirical exploration. *Strategic Management Journal, 13*(8), 585-608.

Layton, R., & Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications*, *19*(6), 321-330.

Lecher, C. (2017). Equifax's CEO is stepping down in the wave of the massive data breach. The Verge. Retrieved from https://www.theverge.com/2017/9/26/16365946/equifax-ceo-data-breach-stepping-down.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177-187.

Lee, Y., Lee, J., & Lee, Z. (2002). Integrating software lifecycle process standards with security engineering. *Computers & Security*, *21*(4), 345-355.

Leiponen, A., & Byma, J. (2009). If you cannot block, you better run: Small firms, cooperative innovation, and appropriation strategies. *Research Policy*, *38*(9), 1478-1488.

Lepak, D. P., Takeuchi, R., & Snell, S. A. (2003). Employment flexibility and firm performance: Examining the interaction effects of employment mode, environmental dynamism, and technological intensity. *Journal of Management, 29*(5), 681-703.

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate Governance, Social Responsibility, and Data Breaches. *Financial Review, 53*(2), 413-455.

Levinthal, D., & Myatt, J. (1994). Co-evolution of capabilities and industry: the evolution of mutual fund processing. *Strategic Management Journal, 15*(S1), 45-62.

Liebenberg, A. P., & Hoyt, R. E. (2003). The determinants of enterprise risk management: vidence from the appointment of chief risk officers. *Risk Management and Insurance Review, 6*(1), 37-52.

Lieberman, M. B., & Montgomery, D. B. (1988). First-mover advantages. *Strategic Management Journal, 9*(S1), 41-58.

Liebeskind, J. P. (1996). Knowledge, strategy, and the theory of the firm. *Strategic Management Journal*, *17*(S2), 93-107.

Liebeskind, J. P. (1997). Keeping organizational secrets: Protective institutional mechanisms and their costs. *Industrial and Corporate Change*, *6*(3), 623-663.

Lin, Z., Zhao, X., Ismail, K, & Carley, K. M. 2006. Organizational design and restructuring in response to crises: Lessons from computational modeling and real-world cases. *Organization Science,* 17: 598-618.

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, *86*(1), 114.

Long, C. P., Bendersky, C., & Morrill, C. (2011). Fairness monitoring: Linking managerial controls and fairness judgments in organizations. *Academy of Management Journal*, *54*(5), 1045-1068.

Lorange, P., & Roos, J. (1991). Why some strategic alliances succeed and others fail. *Journal of Business Strategy*, *12*(1), 25-30.

Lovelace, J. B., Bundy, J., Hambrick, D. C., & Pollock, T. G. (2018). The shackles of CEO celebrity: Sociocognitive and behavioral role constraints on "star" leaders. *Academy of Management Review*, *43*(3), 419-444.

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, *25*(3), 193-273.

Lubatkin, M. H., Simsek, Z., Ling, Y., & Veiga, J. F. (2006). Ambidexterity and performance in small-to medium-sized firms: The pivotal role of top management team behavioral integration. *Journal of Management*, *32*(5), 646-672.

Lunnan, R., & Haugland, S. A. (2008). Predicting and measuring alliance performance: A multidimensional analysis. *Strategic Management Journal*, *29*(5), 545-556.

Luo, L., & Toubia, O. (2015). Improving online idea generation platforms and customizing the task structure on the basis of consumers' domain-specific knowledge. *Journal of Marketing*, *79*(5), 100-114.

MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological Methods*, *1*(2), 130.

Madsen, P. M. (2009). These lives will not be lost in vain: Organizational learning from disaster in US coal mining. *Organization Science*, *20*(5), 861-875.

Maitlis, S., & Sonenshein, S. (2010). Sensemaking in crisis and change: Inspiration and insights from Weick (1988). *Journal of Management Studies, 47*(3), 551-580.

Malekzadeh, A. R., Bickford, D. J., & Spital, F. C. (1989, August). Integrating Environment, Competitive Strategy, and Structure with Technology Strategy: The Strategic Configurations. In *Academy of Management Proceedings* (Vol. 1989, No. 1, pp. 27-31). Briarcliff Manor, NY 10510: Academy of Management.

Manhart, M., & Thalmann, S. (2015). Protecting organizational knowledge: a structured literature review. *Journal of Knowledge Management, 19*(2), 190-211.

March, J. G. (1991). Exploration and exploitation in organizational learning. *Organization Science, 2*(1), 71-87.

Marcus, A. A., & Nichols, M. L. (1999). On the edge: Heeding the warnings of unusual events. *Organization Science, 10*(4), 482-499.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36-58.

Martinez, L. R., White, C. D., Shapiro, J. R., & Hebl, M. R. (2016). Selection BIAS: Stereotypes and discrimination related to having a history of cancer. *Journal of Applied Psychology, 101*(1), 122.

McEvily, S. K., & Chakravarthy, B. (2002). The persistence of knowledge-based advantage: an empirical test for product performance and technological knowledge. *Strategic Management Journal, 23*(4), 285-305.

McKee, M. C., Mills, A. J., & Weatherbee, T. (2005). Institutional field of dreams: Exploring the AACSB and the new legitimacy of Canadian business schools. *Canadian Journal of Administrative Sciences, 22*(4), 288-301.

McManus, S., Seville, E., Vargo, J., & Brunsdon, D. (2008). Facilitated process for improving organizational resilience. *Natural Hazards Review, 9*(2), 81-90.

McShane, M. K., Nair, A., & Rustambekov, E. (2011). Does enterprise risk management increase firm value?. *Journal of Accounting, Auditing & Finance, 26*(4), 641-658.

Meredith, R. (1997). VW agrees to pay G.M. $100 million in espionage suit. Retrieved from http://www.nytimes.com/1997/01/10/business/vw-agrees-to-pay-gm-100-million-in-espionage-suit.html.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology, 83*(2), 340-363.

Meyer, J. W., & Scott, W. R. (1992). ***Organizational environments: Ritual and Rationality*.** Sage Publications, Inc.

Mezias, S. J., & Boyle, E. (2005). Blind trust: Market control, legal environments, and the dynamics of competitive intensity in the early American film industry, 1893–1920. *Administrative Science Quarterly, 50*(1), 1-34.

Miller, D. (1988). Organizational pathology and industrial crisis. *Industrial Crisis Quarterly, 2*(1), 65-74.

Miller, J., & Baker-Prewitt, J. (2009). Beyond 'trapping'the undesirable panelist: The use of red herrings to reduce satisficing. In *CASRO Panel Quality Conference, New Orleans, LA, February*.

Minton, B., Taillard, J., & Williamson, R. (2010). Board composition, risk taking and value: Evidence from financial firms. *SSRN Electronic Journal*.

Minton, B. A., Taillard, J. P., & Williamson, R. (2014). Financial expertise of the board, risk taking, and performance: Evidence from bank holding companies. *Journal of Financial and Quantitative Analysis, 49*(2), 351-380.

Minagawa Jr, T., Trott, P., & Hoecht, A. (2007). Counterfeit, imitation, reverse engineering and learning: reflections from Chinese manufacturing firms. *R&D Management, 37*(5), 455-467.

Mitroff, I. I. (1988). Crisis management: Cutting through the confusion. *MIT Sloan Management Review, 29*(2), 15.

Mitroff, I. I., Pauchant, T. C., & Shrivastava, P. (1988). The structure of man-made organizational crises: Conceptual and empirical issues in the development of a general theory of crisis management. *Technological Forecasting and Social Change, 33*(2), 83-107.

Mitroff, I. I., Pauchant, T., Finney, M., & Pearson, C. (1989). Do (some) organizations cause their own crises? The cultural profiles of crisis-prone vs. crisis-prepared organizations. *Organization & Environment, 3*(4), 269-283.

Mitroff, I. I., Pearson, C. M., & Harrington, L. K. (1996). *The essential guide to managing corporate crises: A step-by-step handbook for surviving major catastrophes*. Oxford University Press.

Mitroff, I. I. (2001). ***Managing Crises before They Happen: What Every Executive and Manager Needs to Know About Crisis Management*.** New York: Amacom.

Mitroff, I. I., & Alpaslan, M. C. (2003). *Preparing for evil*. Harvard Business School.

Morgan, N. A., Vorhies, D. W., & Mason, C. H. (2009). Market orientation, marketing capabilities, and firm performance. *Strategic Management Journal*, *30*(8), 909-920.

Morgeson, F. P., Mitchell, T. R., & Liu, D. (2015). Event system theory: An event-oriented approach to the organizational sciences. *Academy of Management Review*, *40*(4), 515-537.

Mudambi, R. (2002). Knowledge management in multinational firms. *Journal of International Management*, *8*(1), 1-9.

Mueller, R. S. (2012). Speeches. Retrieved from https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

Musteen, M., Barker III, V. L., & Baeten, V. L. (2006). CEO attributes associated with attitude toward change: The direct and moderating effects of CEO tenure. *Journal of Business Research*, *59*(5), 604-612.

Niehoff, B. P., Enz, C. A., & Grover, R. A. (1990). The impact of top-management actions on employee attitudes and perceptions. *Group & Organization Studies*, *15*(3), 337-352.

Nord, W. R., & Tucker, S. (1987). *Implementing routine and radical innovations*. Free Press.

Norman, P. M. (2001). Are your secrets safe? Knowledge protection in strategic alliances. *Business Horizons*, *44*(6), 51-61.

Norman, P. M. (2002). Protecting knowledge in strategic alliances: Resource and relational characteristics. *The Journal of High Technology Management Research*, *13*(2), 177-202.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychological Theory***.** New York, NY: MacGraw-Hill, 131-147.

Nutt, P. C. (1984). Types of organizational decision processes. *Administrative Science Quarterly*, *29*(3), 414-450.

O'Cass, A., & Weerawardena, J. (2010). The effects of perceived industry competitive intensity and marketing-related capabilities: Drivers of superior brand performance. *Industrial Marketing Management*, *39*(4), 571-581.

Olander, H., & Hurmelinna-Laukkanen, P. (2015). Perceptions Of Employee Knowledge Risks In Multinational, Multilevel Organisations: Managing Knowledge Leaking And Leaving. *International Journal of Innovation Management*, *19*(3), 1540006.

Olander, H., Vanhala, M., Hurmelinna-Laukkanen, P., & Blomqvist, K. (2015). HR-related Knowledge Protection and Innovation Performance: The Moderating Effect of Trust. *Knowledge and Process Management*, *22*(3), 220-233.

Osborn, R. N., & Baughn, C. C. (1990). Forms of interorganizational governance for multinational alliances. *Academy of Management Journal, 33*(3), 503-519.

Oxley, J. E. (1997). Appropriability hazards and governance in strategic alliances: A transaction cost approach. *The Journal of Law, Economics, and Organization*, *13*(2), 387-409.

Oxley, J. E., & Sampson, R. C. (2004). The scope and governance of international R&D alliances. *Strategic Management Journal*, *25*(8-9), 723-749.

Oviatt, B. M., & McDougall, P. P. (1994). Toward a theory of international new ventures. *Journal of International Business Studies*, *25*(1), 45-64.

Partridge, M., Rohlin, S. M., & Weinstein, A. L. (2019). Firm formation and survival in the shale boom. *Small Business Economics*, 1-22.

Pauchant, T. C., & Douville, R. (1993). Recent research in crisis management: A study of 24 authors' publications from 1986 to 1991. *Industrial & Environmental Crisis Quarterly*, *7*(1), 43-66.

Pauchant, T. C., & Mitroff, I. I. (1988). Crisis Prone Versus Crisis Avoiding Organizations Is your company's culture its own worst enemy in creating crises?. *Organization & Environment*, *2*(1), 53-63.

Pearson, C. M., & Mitroff, I. I. (1993). From crisis prone to crisis prepared: A framework for crisis management. *The Academy of Management Executive, 7*(1), 48-59.

Pearson, C. M., & Clair, J. A. (1998). Reframing crisis management. *Academy of Management Review*, *23*(1), 59-76.

Peleg-Gillai, B., Bhat, G., & Sept, L. (2006). Innovators in supply chain security: better security drives business value. Manufacturing Institute.

Perrow, C. (1984). *Normal accidents: Living with high risk systems*. New York: Basic Books.

Pfarrer, M. D., Decelles, K. A., Smith, K. G., & Taylor, M. S. (2008). After the fall: Reintegrating the corrupt organization. *Academy of Management Review, 33*(3), 730-749.

Pisano, G. P., Russo, M., & Teece, D. (1988). Joint ventures and collaborative arrangements in the telecommunications equipment industry.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879.

Pollock, T. G., & Rindova, V. P. (2003). Media legitimation effects in the market for initial public offerings. *Academy of Management Journal, 46*(5), 631-642.

Ponemon Institute. (2016). 2016 Ponemon Institute cost of a data breach study. December 26, 2016. Securityintelligence.com. https://securityintelligence.com/media/2016-cost-data-breach-study/

Pope, D. G., & Schweitzer, M. E. (2011). Is Tiger Woods loss averse? Persistent bias in the face of experience, competition, and high stakes. *American Economic Review, 101*(1), 129-57.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly, 37(*4), *1189*-1210.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*(8), 638-646.

Preacher, K. J., & Hayes, A. F. (2004). SPSS and SAS procedures for estimating indirect effects in simple mediation models. *Behavior Research Methods, Instruments, & Computers*, *36*(4), 717-731.

Preacher, K. J., & MacCallum, R. C. (2002). Exploratory factor analysis in behavior genetics research: Factor recovery with small sample sizes. *Behavior Genetics*, *32*(2), 153-161.

Preble, J. F. (1997). Integrating the crisis management perspective into the strategic management process. *Journal of Management Studies, 34*(5), 769-791.

Probst, G., & Raisch, S. (2005). Organizational crisis: The logic of failure. *The Academy of Management Executive, 19*(1), 90-105.

Quintas, P., Lefrere, P., & Jones, G. (1997). Knowledge management: a strategic agenda. *Long Range Planning, 30*(3), 385-391.

Qusa, H., & Abudalfa, S. (2013). Secure collaborative processing architecture for mitb attack detection. *International Journal of Network Security & Its Applications, 5*(5), 83-93.

Rajagopalan, N., & Datta, D. K. (1996). CEO characteristics: does industry matter?. *Academy of Management Journal*, *39*(1), 197-215.

Rao, H., Monin, P., & Durand, R. (2005). Border crossing: Bricolage and the erosion of culinary categories in French gastronomy. *American Sociological Review,70,* 968–991.

Redmiles, E. M., Kross, S., & Mazurek, M. L. (2016, October). How i learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of*

the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 666-677). ACM.

Reinmoeller, P., & Ansari, S. (2016). The persistence of a stigmatized practice: A study of competitive intelligence. *British Journal of Management*, *27*(1), 116-142.

Reuer, J. J., & Tong, T. W. (2010). Discovering valuable growth opportunities: An analysis of equity alliances with IPO firms. *Organization Science*, *21*(1), 202-215.

Reuters. (2016). Congress just passed tough new trade secret protection legislation. Fortune.com. Accessed on October 20, 2016 from http://fortune.com/2016/04/28/congress-trade-secret-legislation/.

Rhee, M., & Haunschild, P. R. (2006). The liability of good reputation: A study of product recalls in the US automobile industry. *Organization Science, 17*(1), 101-117.

Rhee, M., & Kim, T. (2012). After the collapse: a behavioral theory of reputation repair. *The Oxford handbook of Corporate Reputation*, 446-465.

Rigdon, E. E. (2016). Choosing PLS path modeling as analytical method in European management research: A realist perspective. *European Management Journal*, *34*(6), 598-605.

Ritala, P., Olander, H., Michailova, S., & Husted, K. (2015). Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study. *Technovation*, *35*, 22-31.

Ritchie, B. W. (2004). Chaos, crises and disasters: a strategic approach to crisis management in the tourism industry. *Tourism Management*, *25*(6), 669-683.

Ritchie, W. J., & Melnyk, S. A. (2012). The impact of emerging institutional norms on adoption timing decisions: evidence from C-TPAT—A government antiterrorism initiative. *Strategic Management Journal*, *33*(7), 860-870.

Richardson, H. A., Simmering, M. J., & Sturman, M. C. (2009). A tale of three perspectives: Examining post hoc statistical techniques for detection and correction of common method variance. *Organizational Research Methods*, *12*(4), 762-800.

Robertson, K. M., Hannah, D. R., & Lautsch, B. A. (2015). The secret to protecting trade secrets: How to create positive secrecy climates in organizations. *Business Horizons*, *58*(6), 669-677.

Robertson, M., Scarbrough, H., & Swan, J. (2003). Knowledge creation in professional service firms: Institutional effects. *Organization Studies*, *24*(6), 831-857.

Rummel, R. J. (1970). ***Applied Factor Analysis.*** Evanston, IL: Northwestern University Press.

Russakoff, R. & Goodman, M. (2011). Employee theft: Are you blind to it? Retrieved from https://www.cbsnews.com/news/employee-theft-are-you-blind-to-it/.

Sadiq, A. A., & Graham, J. D. (2015). Exploring the predictors of organizational preparedness for natural disasters. *Risk Analysis, 36,* 1040-1053.

Sahaf, M. A. (2002). Competitive Intelligence: An Effective War-Game. *Paradigm*, *6*(1), 80-89.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56,* 70-82.

Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, *2016*(2), 15-18.

Schneider, B., Ehrhart, M. G., & Macey, W. H. (2013). Organizational climate and culture. *Annual Review of Psychology, 64,* 361-388.

Schwab, D,P, (1980). Construct validity in organization behavior, Pp, 3-43 in B,M, Staw & L,L, Cummings(Eds,), *Research in Organizational Behavior,* Vol, 2, Greenwich, CT: JAI Press

Schwepker, C. H. (1999). Understanding salespeople's intention to behave unethically: The effects of perceived competitive intensity, cognitive moral development and moral judgment. *Journal of Business Ethics*, *21*(4), 303-316.

Scott, W. R., & Davis, G. F. (2007). ***Organizations and Organizing. Rational, Natural, and Open System Perspectives.*** Upper Sadle River: Pearson.

Securities and Exchange Commission. (2014). Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the focus. Retrieved from http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#_edn4

Shan, W. (1990). An empirical analysis of organizational strategies by entrepreneurial high-technology firms. *Strategic Management Journal*, *11*(2), 129-139.

Sheaffer, Z., & Mano-Negrin, R. (2003). Executives' orientations as indicators of crisis management policies and practices. *Journal of Management Studies, 40*(2), 573-606.

Sheffi, Y. (2001). Supply chain management under the threat of international terrorism. *The International Journal of Logistics Management*, *12*(2), 1-11.

Shimizu, K. (2007). Prospect theory, behavioral theory, and the threat-rigidity thesis: Combinative effects on organizational decisions to divest formerly acquired units. *Academy of Management Journal, 50*(6), 1495-1514.

Srivastava, M. K., & Gnyawali, D. R. (2011). When do relational resources matter? Leveraging portfolio technological resources for breakthrough innovation. *Academy of Management Journal*, *54*(4), 797-810.

Shrivastava, P., Mitroff, I. I., Miller, D., & Miclani, A. (1988). Understanding industrial crises [1]. *Journal of Management Studies*, *25*(4), 285-303.

Singleton, R., & Strait, B. (2010). *Approaches to Social Research* (5th ed.). New York: Oxford University Press.

Sinha, T. (2011). *Crisis Management in Organizations: An Exploratory Study of Factors that Affect Strategy Formation and Selection* (Doctoral dissertation, Ohio University).

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: an empirical investigation. *Computer*, *43*, 64-71.

Smith, C.W. and Stulz, R. M. (1985). The determinants of firms' hedging policies", *Journal of Financial and Quantitative Analysis, 20*(4), 391-405

Somaya, D. (2003). Strategic determinants of decisions not to settle patent litigation. *Strategic Management Journal, 24*(1), 17-38.

Somaya, D. (2012). Patent strategy and management an integrative review and research agenda. *Journal of Management*, *38*(4), 1084-1114.

Spencer, J. W. (2003). Firms' knowledge-sharing strategies in the global innovation system: empirical evidence from the flat panel display industry. *Strategic Management Journal*, *24*(3), 217-233.

Siguaw, J. A., Simpson, P. M., & Enz, C. A. (2006). Conceptualizing innovation orientation: A framework for study and integration of innovation research. *Journal of Product Innovation Management*, *23*(6), 556-574.

Stanton, J. M., Sinar, E. F., Balzer, W. K., & Smith, P. C. (2002). Issues and strategies for reducing the length of self-report scales. *Personnel Psychology*, *55*(1), 167-194.

Starbuck, W. H., Greve, A., & Hedberg, B. (1978). Responding to crises. *Journal of Business Administration*, *9*(2), 111-137.

Starbuck, W. H., & Milliken, F. J. (1988). Challenger: fine-tuning the odds until something breaks. *Journal of Management Studies*, *25*(4), 319-340.

Staw, B. M., Sandelands, L. E., & Dutton, J. E. (1981). Threat rigidity effects in organizational behavior: A multilevel analysis. *Administrative Science Quarterly*, 501-524.

Steensma, H. K., Marino, L., Weaver, K. M., & Dickson, P. H. (2000). The influence of national culture on the formation of technology alliances by entrepreneurial firms. *Academy of Management Journal*, *43*(5), 951-973.

Steffens, N. K., Haslam, S. A., & Reicher, S. D. (2014). Up close and personal: Evidence that shared social identity is a basis for the 'special' relationship that binds followers to leaders. *The Leadership Quarterly*, *25*(2), 296-313.

Steffens, N. K., Peters, K., Haslam, S. A., & van Dick, R. (2016). Dying for charisma: Leaders' inspirational appeal increases post-mortem. *The Leadership Quarterly*, *28*(4), 530-542.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS quarterly*, 441-469.

Stulz, R. M. (1996). Rethinking risk management. *Journal of Applied Corporate Finance*, *9*(3), 8-25.

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review*, *20*(3), 571-610.

Sutcliffe, K. M., & Vogus, T. J. (2003). Organizing for resilience. *Positive organizational scholarship: Foundations of a New Discipline*, *94*, 110.

Sydnor, J. (2010). (Over) insuring modest risks. *American Economic Journal: Applied Economics*, *2*(4), 177-99.

Tavitiyaman, P., Leong, J. K., Dunn, G. E., Njite, D., & Neal, D. M. (2008). The effectiveness of lodging crisis management plans. *Journal of Quality Assurance in Hospitality & Tourism*, *8*(4), 24-60.

Teece, D. J. (1986). Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy. *Research Policy*, *15*(6), 285-305.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 509-533.

Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering*, *33*(8), 544-557.

Thomä, J., & Bizer, K. (2013). To protect or not to protect? Modes of appropriability in the small enterprise sector. *Research Policy*, *42*(1), 35-49.

Thomas, J., Clark, S., & Gioia, D. (1993). Strategic sense- making and organizational performance: Linkages among scanning, interpretation, action, and out- comes. *Academy of Management Journal*, *36*, 239-270.

Thomas, J. B., & McDaniel, R. R. (1990). Interpreting strategic issues: Effects of strategy and the information-processing structure of top management teams. *Academy of Management Journal, 33*(2), 286-306.

Tiemessen, I., Lane, H. W., Crossan, M. M., & Inkpen, A. C. (1997). Knowledge management in international joint ventures. *Cooperative Strategies: North American Perspectives*, 370-399.

Tolbert, P. S., & Zucker, L. G. (1983). Institutional sources of change in the formal structure of organizations: *The Diffusion of Civil Service Reform,* 1880-1935.

Topaloglu, C., Ali Koseoglu, M., & Ondracek, J. (2013). Crisis readiness, strategic orientation and performance: evidence from Turkey. *International Journal of Management and Enterprise Development*, *12*(3), 212-236.

Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty*, *5*(4), 297-323.

Tuggle, C. S., Schnatterly, K., & Johnson, R. A. (2010). Attention patterns in the boardroom: How board composition and processes affect discussion of entrepreneurial issues. *Academy of Management Journal*, *53*(3), 550-571.

Ulmer, R. R., Sellnow, T. L., & Seeger, M. W. (2011). ***Effective crisis communication: Moving from crisis to opportunity***. Sage Publications.

Van Der Vegt, G. S., Essens, P., Wahlström, M., & George, G. (2015). Managing risk and resilience. *Academy of Management Journal*, *58*(4), 971-980.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management, 49,* 190-198.

Van Wart, M., & Kapucu, N. (2011). Crisis management competencies: The case of emergency managers in the USA. *Public Management Review, 13*(4), 489-511.

Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. *Information Systems Management*, *24*(4), 361-372.

Veil, S. R. (2010). Mindful learning in crisis management. *Journal of Business Communication, 48(*2), 116-147. *0021943610382294.*

Verbeke, W., Volgering, M., & Hessels, M. (1998). Exploring the conceptual expansion within the field of organizational behaviour: Organizational climate and organizational culture. *Journal of Management Studies*, *35*(3), 303-329.

Veugelers, R. (1997). Internal R&D expenditures and external technology sourcing. *Research Policy, 26*(3), 303-315.

Vogus, T. J., & Welbourne, T. M. (2003). Structuring for high reliability: HR practices and mindful processes in reliability-seeking organizations. *Journal of Organizational Behavior, 24*(7), 877-903.

Vogus, T. J., & Sutcliffe, K. M. (2007, October). Organizational resilience: towards a theory and research agenda. In *2007 IEEE International Conference on Systems, Man and Cybernetics* (pp. 3418-3422). IEEE.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371-376.

Von Solms, S. B. (2005). Information Security Governance–compliance management vs operational management. *Computers & Security*, *24*(6), 443-447.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23,* 191-198.

Wan, W. P., & Yiu, D. W. (2009). From crisis to opportunity: Environmental jolt, corporate acquisitions, and firm performance. *Strategic Management Journal, 30*(7), 791-801.

Wang, J., & Dewhirst, H. D. (1992). Boards of directors and stakeholder orientation. *Journal of Business Ethics*, *11*(2), 115-123.

Wang, W. T., & Belardo, S. (2009). The role of knowledge management in achieving effective crisis management: a case study. *Journal of Information Science. 35*(6), 635-659.

Ward, M. K., & Broniarczyk, S. M. (2011). It's not me, it's you: How gift giving creates giver identity threat as a function of social closeness. *Journal of Consumer Research*, *38*(1), 164-181.

Weerawardena, J., O'Cass, A., & Julian, C. (2006). Does industry matter? Examining the role of industry structure and organizational learning in innovation and brand performance. *Journal of Business Research, 59*(1), 37-45.

Weick, K. E. (1988). Enacted sensemaking in crisis situations. *Journal of Management Studies, 25*(4), 305-317.

Weick, K., & Sutcliffe, K. (2001). Managing the unexpected: Assuring high performance in an age of uncertainty. *Wiley, 1*(3), 5.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the process of sensemaking. *Organization Science*, *16*(4), 409-421.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: Processes of collective mindfulness. *Crisis Management*, *3*(1), 81-123.

Weiss, L. W., Pascoe, G., & Martin, S. (1983). The size of selling costs. *Review of Economics and Statistics*, *65*(4), 668-672.

Wen, Z., & Fan, X. (2015). Monotonicity of effect sizes: Questioning kappa-squared as mediation effect size measure. *Psychological Methods*, *20*(2), 193.

White, G. L. (2015). Education and prevention relationships on security incidents for home computers. *Journal of Computer Information Systems*, *55*(3), 29-37.

Whitman, J. Q. (2003). The two western cultures of privacy: Dignity versus liberty. *Yale LJ*, *113*, 1151.

Wiklund, J., & Shepherd, D. (2003). Knowledge-based resources, entrepreneurial orientation, and the performance of small and medium-sized businesses. *Strategic Management Journal*, *24*(13), 1307-1314.

Williamson, O. E. (1981). The economics of organization: The transaction cost approach. *American Journal of Sociology*, *87*(3), 548-577.

Williamson, O. E. (1991). Comparative economic organization: The analysis of discrete structural alternatives. *Administrative Science Quarterly*, *36*(2), 269-296.

Williams, L. J., Hartman, N., & Cavazotte, F. (2010). Method variance and marker variables: A review and comprehensive CFA marker technique. *Organizational Research Methods*, *13*(3), 477-514.

Williams, Z., Lueg, J. E., & LeMay, S. A. (2008). Supply chain security: an overview and research agenda. *The International Journal of Logistics Management*, *19*(2), 254-281.

Williams, L. J., & McGonagle, A. K. (2016). Four research designs and a comprehensive analysis strategy for investigating common method variance with self-report measures using latent variables. *Journal of Business and Psychology*, *31*(3), 339-359.

Withers, M. C., Corley, K. G., & Hillman, A. J. (2012). Stay or leave: Director identities and voluntary exit from the board during organizational crisis. *Organization Science*, *23*(3), 835-850.

Wooten, L. P., & James, E. H. (2008). Linking crisis management and leadership competencies: The role of human resource development. *Advances in Developing Human Resources*, *10*(3), 352-379.

Wowak, A. J., Mannor, M. J., & Wowak, K. D. (2015). Throwing caution to the wind: The effect of CEO stock option pay on the incidence of product safety problems. *Strategic Management Journal*, *36*(7), 1082-1092.

Wu, J. (2012). Technological collaboration in product innovation: The role of market competition and sectoral technological intensity. *Research Policy, 41*(2), 489-496.

Ybarra, C. E., & Turk, T. A. (2009). The evolution of trust in information technology alliances. *The Journal of High Technology Management Research*, *20*(1), 62-74.

Zafar, H., Ko, M. S., & Osei-Bryson, K. M. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers*, *18*(6), 1205-1215

Zavyalova, A., Pfarrer, M. D., Reger, R. K., & Shapiro, D. L. (2012). Managing the message: The effects of firm actions and industry spillovers on media coverage following wrongdoing. *Academy of Management Journal*, *55*(5), 1079-1101.

Zhang, Y., & Rajagopalan, N. (2010). Once an outsider, always an outsider? CEO origin, strategic change, and firm performance. *Strategic Management Journal*, *31*(3), 334-346.

Zhu, W., Chew, I. K., & Spangler, W. D. (2005). CEO transformational leadership and organizational outcomes: The mediating role of human–capital-enhancing human resource management. *The Leadership Quarterly*, *16*(1), 39-52.

Ziobro, P. & Lublin J. (2014). ISS's view on Target directors is a signal on cybersecurity. Retrieved on August 26, 2016 from http://www.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278.

Zohar, D. (2010). Thirty years of safety climate research: Reflections and future directions. *Accident Analysis & Prevention*, *42*(5), 1517-1522.

Zohar, D. M., & Hofmann, D. A. (2012). Organizational culture and climate. In S. W. J. Kozlowski (Ed.), *Oxford library of psychology. The Oxford handbook of organizational psychology*, Vol. 1, pp. 643-666). New York, NY, US: Oxford University Press.

Zor, U., Linder, S., & Endenich, C. (2019). CEO characteristics and budgeting practices in emerging market SMEs. *Journal of Small Business Management*, *57*(2), 658-678.

BIOGRAPHICAL SKETCH

Joseph Simpson holds a Bachelor of Arts in Intelligence Studies at American Military University (2009), a Master of Science in Homeland Security Management at Long Island University – Riverhead (2011), a graduate certificate in International Security Studies from Stanford University (2011), and an MBA from the University of Texas Pan American (2014). He received his Ph.D. in Business Administration (Management) from the University of Texas – Rio Grande Valley (UTRGV) in August of 2019.

His experience includes a combined ten years of experience in nuclear weapons security and military special operations. He also owns multiple businesses and manages approximately 30 employees and several contractors. His real estate holding company manages multiple properties and is currently under negotiations for multiple other businesses. His research interests intersect at the areas of corporate governance, executive decision making, strategy and organizational security. His work has appeared in *Journal of Business Ethics, Tourism Management,* and *Journal of Travel Research.* He has also presented several papers at top management conferences including annual Academy of Management and Southern Management Association conferences. Joseph is now a Collegiate Professor of Management at Virginia Tech and the inaugural director of the Integrated Security Education and Research Center. He can be reached at jjsimpson@vt.edu.