10-7-2020

Cyber Supply Chain Risk Management: Toward an Understanding of the Antecedents to Demand for Assurance

Clark Hampton

Steve G. Sutton

Vicky Arnold

Deepak Khazanchi

Cyber Supply Chain Risk Management: Toward an Understanding of the Antecedents to Demand for Assurance

Clark Hampton University of South Carolina

Steve G. Sutton Norwegian School of Economics University of Central Florida

Vicky Arnold Norwegian School of Economics University of Central Florida

Deepak Khazanchi University of Nebraska at Omaha

ABSTRACT:

Recognizing the need for effective cyber risk management processes across the supply chain, the AICPA issued a new SOC in March 2020 for assuring cyber supply chain risk management (C-SCRM) processes. This study examines supply chain relationship factors and cyber risk issues to better understand the demand for CSCRM assurance. Resource-Advantage Theory of Competition provides the conceptual foundation for assessing the dual drivers of relationship building and cyber risk management on demand for assurance. We use a field survey to collect data from 205 professionals enabling evaluation of the complex relationships in the theoretical model. Results support all hypotheses, provide satisfactory model fit, and support the underlying theory. Trust and cyber supply chain risk both positively influence demand for assurance over C-SCRM processes. This study expands the literature on cyber assurance by auditors and elaborates on overall supply chain processes that help drive value from auditors providing such assurance.

Keywords: cyber risk management; supply chain risk management; cyber supply chain risk management; cyber assurance; voluntary assurance; SOC reports.

I. INTRODUCTION

Concern is rapidly growing among organizations as vulnerabilities to cyber threats increasingly arise through third party relationships where even the most secure systems become vulnerable through connections to third parties' less secure systems (Eaton, Grenier, and Layman 2019). As a response, cyber supply chain risk management (C-SCRM)1 has emerged as a focal risk management area evolving from the interactive risks arising from cybersecurity, information risk management, and supply chain management (Colicchia, Creazza, and Menachof 2019). The American Institute of Certified Public Accountants (AICPA 2020a) has responded to this developing demand

with a new System and Organization Controls (SOC) Report for Supply Chains.2 The SOC for Supply Chains focuses on management's control practices over systems involved in supply chain related activities, the operation and use of these systems, and the cyber controls over related technologies.

The ninth annual cost of cybercrime study conducted by the Ponemon Institute emphasizes the associated risk to core systems, such as industrial control systems, as cyberattackers shift their attack patterns to exploit supply chain partners' environments to gain entry into a more secure organization's system (Bissell, Lasalle, and Cin 2019). While a decade ago only one in four companies relied on the internet for their business operations, today it is 100 percent; indirect attacks through partners' systems are expected to grow to 23 percent of breaches over the next five years (Bissell et al. 2019). In the financial services industry, most organizations already consider partner cybersecurity risk when making key business decisions; yet, they lament the lack of consistent third party risk measurement and reporting (Bitsight 2019). Gartner posits that rapidly increasing concern is leading to greater use of cybersecurity ratings provided by independent bodies, and such cybersecurity ratings will become as important as credit ratings in assessing the viability of supply chain partners (Olyaei, Ambrose, and Wheatman 2018). Despite a perceived high demand for assurance on partners' C-SCRM, the accounting profession has had limited success in past forays into cyber-related assurance products with questions over their ability to provide desired comfort and trust to the marketplace (Gendron and Barrett 2004), ability to mobilize accounting firms' widespread development of services (Boulianne and Cho 2009), or to align services with traditional customer bases (Sutton and Hampton 2003).

The purpose of this study is to explore organizations' demand for C-SCRM assurance. Agile organizations require agile supply chain partners, and this necessitates the smooth sharing of information resources across supply chain partners, but such relationships also open organizations to supply chain interruptions from a single partner's processing failures and to cyberattacks through a partners' systems (AICPA 2020a; Colicchia et al. 2019; Duncan 2019). Research shows that organizations with strong enterprise risk management processes focus on reducing partners' cyber supply chain risk as a foundation for increased information sharing (Arnold, Benford, Hampton, and Sutton 2014). Reducing such risks in global supply chains is particularly critical (Arnold, Benford, Hampton, and Sutton 2010; Arnold, Benford, Hampton, and Sutton 2012), and maintaining effective enterprise risk management enables agile organizations to enhance flexibility and improve supply chain performance (Arnold, Benford, Canada, and Sutton 2015). Thus, risk management appears valued from a relational perspective as well as a risk reduction perspective, but whether assurance over such risk management processes is valued is unknown.

The Resource-Advantage Theory of Competition (R-A theory) is coupled with the conceptual framework for C-SCRM risk identification to garner a better theoretical understanding of the joint influences of relationship building and cyber supply chain risk

on the value of C-SCRM assurance. R-A theory (Arnett 2011; Ferrell 2011) provides perspectives on how dependencies and commitments develop in long-term relationships that lead to trust between supply chain partners. However, R-A theory also recognizes that supply chain partners may well be motivated to support the relationship even if it requires a loss of control due to imbalances in power and may require additional investments in trust building mechanisms such as C-SCRM assurance. The conceptualization of cyber supply chain risk (Khazanchi and Sutton 2001; Sutton, Hampton, Khazanchi, and Arnold 2008) aligns with the SOC for Supply Chains (AICPA 2020b) as supply chain risks exist at the process management and strategy level, the operational process level, and the technical level. Sutton et al. (2008) provide a detailed operationalization of the associated cyber supply chain risk assessment. Our R-A theory based model predicts trust, power, and cyber supply chain risk3 have a positive relationship with demand for C-SCRM assurance, a mechanism consistent with a direct signaling of trust and risk management intentions (Fan and Stevenson 2018).

The results provide strong support for our theoretical model. We collected data from 205 experienced supply chain and cyber risk professionals (i.e., Chief Information Officers [CIOs], Information Technology [IT] Auditors, IT Security Staff, and Supply Chain Managers), and asked respondents a series of questions related to their own organization, a key supply chain partner, and the trading relationship between the two. The results confirm that greater dependency of a supply chain partner allows an organization to increase power over the partner. However, consistent with the predictions of R-A theory, our results also indicate that this power imbalance is associated with higher perceived risk being inherited from the supply chain partner's system. This increased risk, in conjunction with organizational power over the supply chain partner, drives a demand for assurance over the supply chain partner's C-SCRM. While a supply chain partner's dependency creates power differentials favoring the organization, our results support the R-A theory prediction that this same dependency also triggers organizational behaviors that are beneficial to the partner. These organizational behaviors positively impact organizational trust of the partner by indicating a shared perception between the organization and its partner that the supply chain relationship is long-term, intended to be mutually beneficial, and that neither partner will take actions that are detrimental to the other party. While trust is critical to the development of supply chain partnerships capable of sustaining competitive advantage, our results confirm that ‘‘trust but verify’’ is the guiding principal of organizations engaged in supply chain partnerships (Johnson 2016). Organizations seek verification (i.e., direct signals) that their trust in their supply chain partner's operations and cybersecurity is not misplaced (Fan and Stevenson 2018; Olyaei et al. 2018; Bissell et al. 2019; Bitsight 2019; Duncan 2019).

This research contributes to the accounting information systems literature on multiple levels. Cyber security research lies at the intersection of accounting and information systems research placing it firmly in the AIS research domain (Janvrin and Wang 2019). However, Janvrin and Wang (2019) note that there is limited theoretical understanding

of how cyber security issues relate to reporting and decision making within organizations, and little is understood about the viability of various cybersecurity initiatives in practice. Our research contributes to the theoretical, methodological, and practical dimensions of the research challenges to moving related AIS research forward.

From a theory standpoint, this research contributes to the past debate as to the market's value placed on cyber assurance provided by auditors. In the business-to-business sphere, we see an expressed demand for assurance over supply chain partners' C-SCRM. Three key aspects of supply chain relationships drive this demand—established trust in a trading partner, developed imbalances in power within the relationship, and perceived cyber supply chain risk. These three factors are considered the greatest inhibitors to collaborative supply chain development (Soosay and Hyland 2015; Fan and Stevenson 2018).

From a research methods perspective, this study also contributes to the development of key constructs for research on CSCRM. In the course of the study, a comprehensive multi-dimensional construct is established for assessing the level of risk in a supply chain partner that captures the management level control and strategies, the operational level controls over use of systems and operations, and the technical level—all key elements of understanding inheritable cyber supply chain risk from a trading partner (AICPA 2020b; Colicchia et al. 2019; Sutton et al. 2008). We also develop a construct for assessing a priori demand for assurance that allows a researcher to capture the potential demand for new assurance services.

From a practice perspective, the research directly addresses demand for the new SOC for Supply Chains (AICPA 2020a). The results indicate that risks across all the components of the SOC are viewed as important components and in aggregate drive the demand for assurance over a supply chain partner's operations, systems, and C-SCRM. Our results also highlight the value of assurance in established supply chain partner relationships where trust is already high, consistent with arguments that cyber supply chain risks are likely to cause organizations to reassess risks even with established partners (Fan and Stevenson 2018; Olyaei et al. 2018; Colicchia et al. 2019; Duncan 2019).

II. AICPA'S SOC FOR SUPPLY CHAINS

In March 2020, the AICPA released its SOC for Supply Chains—an assurance service designed to help organizations assess the risks and associated controls in place among its trading partners both up and down the supply chain. When supply chains are disrupted, the risk of failing to meet production or delivery commitments to trading partners is significant. Supply chain members require visibility across complex networks to effectively assess their own supply chain risk and vulnerabilities, and to effectively implement appropriate controls to detect, prevent, and respond to such risks (Fan and Stevenson 2018; AICPA 2020a).

These risks can emanate in many ways from trading partner relationships, and organizations should be interested in assessing and monitoring such risks for a multitude of reasons. The core focus of the SOC for Supply Chains is on understanding the risks associated with trading partners' production, manufacturing, or distribution of goods. These risks include the partner's management objectives and planning as associated with supply chain activities, the core business processes, and systems that facilitate production, manufacturing, or distribution activities within the partner organization, and the risk that exudes from establishing IT connectivity with the trading partner to facilitate effective information flow across the supply chain—the backbone of contemporary, on-demand supply chains (AICPA 2020a).

As with all SOCs, the SOC for Supply Chain was developed based on principle system objectives specified in the trust services criteria: security, availability, processing integrity (i.e., over production, manufacturing, or delivery of goods), confidentiality, and privacy. An engagement is built around the trust services criteria that management selects to report upon, but the AICPA (2020b, 232) notes that ''because of the increased dependence on technology and concerns about cybersecurity risks, security is likely to be addressed in most examinations performed using the trust services criteria. Often, customers and business partners of an entity are also interested in the effectiveness of controls over availability because such controls may be integral to meeting their commitments.''

Despite demand for better understanding supply chain partners' cyber risk management practices, questions invariably linger as to the audit profession's realistic role in these processes and the degree to which organizations will demand assurance over partners' C-SCRM reports. Earlier attempts by the profession to establish a foothold in cybersecurity assurance services had limited success, and many questioned whether they could compete against IT firms in meeting the demand. Studies in the aftermath of these early cybersecurity assurance ventures suggest companies did not buy into the value of audit firms providing such services, particularly those related to consumer comfort and trust (Gendron and Barrett 2004). Other research found accounting firms were unwilling to invest in services considered of questionable marketability; thus, a supply problem also existed (Boulianne and Cho 2009). Alas, other researchers questioned whether targeting the consumer market rather than the business market seemed inconsistent with reputational advantages (Sutton and Hampton 2003). On the other hand, arguments were also put forth that there should be a market for cybersecurity services targeted toward supply chain partners given the reputational advantages in the business-to-business marketplace (Khazanchi and Sutton 2001; Sutton and Hampton 2003), and frameworks for related C-SCRM assurance were proposed (Khazanchi and Sutton 2001; Sutton et al. 2008). Ultimately, the research question lingers: is there market demand for accountant provided assurance over businesses' cybersecurity and technology-driven supply chains?

III. THEORY AND HYPOTHESES DEVELOPMENT

The theoretical foundations for understanding supply chain relationships are derived from R-A theory[4] (Hunt 1995, 1997b, 1997c, 2000; Hunt and Morgan 1995). R-A theory focuses on the judicial use of valuable resources to achieve superior financial performance. R-A theory falls within a class of theories derived from the social capital perspective and the view that organizations develop mutual benefit through the combination of unique and valuable resources that have maximum value through collaboration and the collaboration is considered a strategic asset within itself (Soosay and Hyland 2015). R-A theory has its foundations in neo-classical economics, such as transaction cost economics, but builds on this foundation to incorporate social and organizational perspectives with a specific focus on buyer-supplier interorganizational relationships. Much of this social and organizational perspective has its foundations in Hunt and Morgan's (1995) prior work on commitment and trust in such relationships.

R-A theory explicitly adopts a fundamental assumption that information about customers, competitors, suppliers, and production techniques is both imperfect and costly to obtain (Hunt 1997b). Successful organizations focus on developing comparative advantage through available resources that are unique. This, in turn, allows the organization to achieve superior financial performance through either more efficient or effective production—or ideally through more efficient production that leads also to more effective production (Hunt 1997c, 1999). The theory implicitly acknowledges the concept that competition is less between organizations and more supply chain versus supply chain (Sutton and Hampton 2003).

Leveraging Social Capital into Collaborative Supply Chains

In developing relationships with supply chain partners, this theoretical perspective has significant ramifications. Most notably, R-A theory posits that such behavior is often motivated by constrained self-interest seeking (Hunt 1997b, 1997c). This behavioral perspective is critical as organizations develop trading relationships. Trading relationships, like many other types of resources, must be carefully selected and groomed over time to develop a strategic portfolio of relationships. Development of strong, long-term relationships can be costly (Hunt 1997a). Given the high exit costs, such relationships should be restricted to those that provide a comparative advantage (Morgan and Hunt 1999) and those in which the partner behaves in a trustworthy manner (Morgan and Hunt 1994). The establishment of trust is critical, but the maintenance of that trust over time becomes even more important.

Developing a transaction based trading partner into a key relational partner is an evolutionary process that requires time (Hunt and Morgan 1994). Frequently in such trading relationships, one organization will be dominant and the other will be dependent, leading the supply chain partner to perceive that the dominant firm has power and control over the relationship (Morgan and Hunt 1999). Organizations have long been

[4] Also referred to as Comparative Advantage Theory of Competition in its early gestations (e.g., Hunt and Morgan 1995).

thought to view these relationships as a liability, and fear participating in them will require relinquishment of power.

Morgan and Hunt (1999, 282) posit on the other hand that supply chain partners enter such relationships ‘‘not reluctantly but optimistically.’’ They theorize that such relationships can make an organization more competitive, yield greater access to valuable resources, and offer the best means by which to access such resources. Treating such relationships as strategic assumes the available resources are used efficiently, are complex, and are maintained and protected to ensure ongoing availability (Bharadwaj, Varadarajan, and Fahy 1993; Hunt and Morgan 1995, Morgan and Hunt 1999). Access to these resources rarely, if ever, comes without a cost. The partner must provide a certain level of asset specificity in an efficient and effective manner for the relationships to survive; thus, the supply chain partner will also make investments, but only when such investments support and foster a long-term, strategic relationship (Chen, Paulraj, and Lado 2004; Hunt and Davis 2008). Supply chain partners often make short-term sacrifices to preserve profitable, long-term relationships with the more powerful firm (Hunt and Davis 2008). Nonetheless, such an interorganizational relationship creates a substantial dependence and transfer of power in the relationship (Emerson 1962; Son, Narasimhan, and Riggins 2005).

Power is arguably still important as it can be the most direct driver of a relationship and enables the more powerful partner to determine the agenda and protocols for the relationship (Dekker 2003; Seal, Berry, and Cullen 2004; Ca¨ker 2008). However, judicial use can foster and sustain a longer-term relationship with the partner when both parties view the relationship as a potential resource—a premise of R-A theory. But, R-A theory also posits that the development of a long-term relationship is premised on the partner maintaining constrained self-interest seeking behavior (Hunt 1997a). Given the premise that information on customers, suppliers, and alliance partners is imperfect and very costly to attain, the more powerful partner remains under a certain veil of ignorance as to the actual behavior of the weaker partner (Hunt 1997c).

Accentuating this void of information are the conditions under which such relationships are most valuable and most likely to be sustainable over the long-term. Organizations perceive long-term relationships generating a valuable resource advantage to be most sustainable when they arise from organizational, informational, or relational resources (Morgan and Hunt 1999). Organizational resources consist of proprietary technologies that are often gained through organizational learning. Informational resources on their face have a highly perishable life when considering the information itself; however, the systems that gather, use, and disseminate information have a much longer life. Such informational resources frequently include technologies that facilitate tight electronic coupling of the organization’s IT systems. While an organization may interact and benefit from a supply chain partner’s organizational and informational resources, the organization has little opportunity to aggregate information on the depth of integration and sustainability of such resources within the partner firm. The organization will also

likely lack sufficient information to reliably assess the security of the partner's systems and the associated cyber risks that may accrue from linking with the partner's systems (Johnson 2016; Colicchia et al. 2019; Duncan 2019).

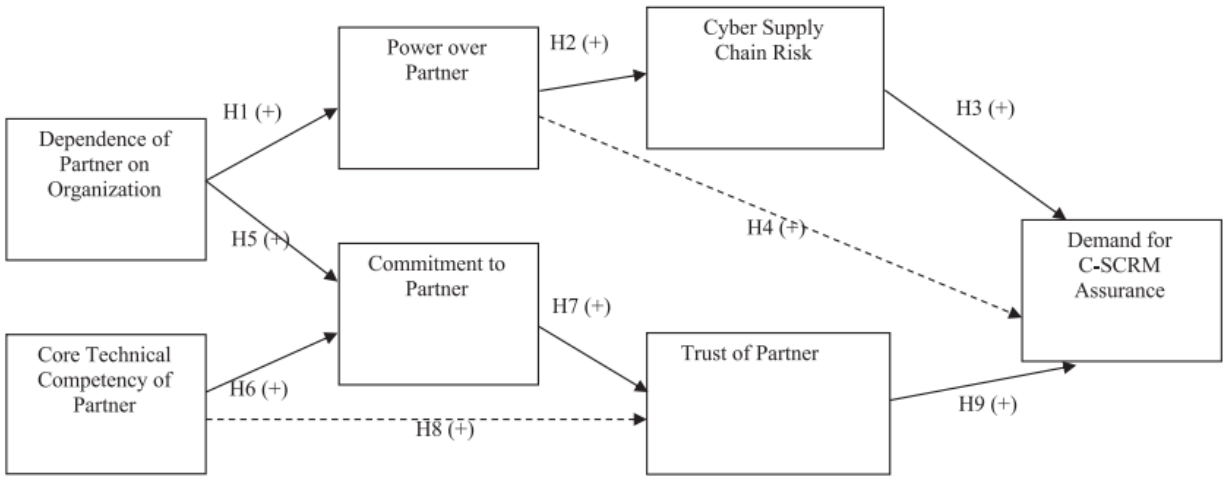
Relational resources are most valuable when associated with trust, commitment, and loyalty (Morgan and Hunt 1999). Trust and commitment do not evolve quickly but must be developed over time based on experience with the trading partner (Hunt and Morgan 1994). Both are critical to long-term relationships that are sustainable and generate a resource advantage. Relationship commitment arises when an organization believes a relationship warrants maximum effort to maintaining that relationship. Trust exists when an organization has confidence that a supply chain partner is reliable and participates in the relationship with integrity. Accordingly, trust is instrumental to commitment; and, in the presence of commitment, the existence of trust is the conduit through which an organization is willing to pursue stronger relationships with that partner (Morgan and Hunt 1994). However, in the absence of perfect information, the organization lacks certainty as to the justifiability of placing such trust in the trading partner and relying on that trust to minimize risk. Minimizing levels of risk are just as important as the potential resource advantage in allowing the relationship to build (Arnold et al. 2010; 2014; Colicchia et al. 2019).

A Signaling Theory Perspective on Verification

Fan and Stevenson (2018) propose that simply relying on social capital as often espoused in the supply chain risk management literature leaves organizations vulnerable. They apply signaling theory (Spence 1973) as a complement of social capital based theorizations. Using a field study of multiple organizations, Fan and Stevenson (2018) reveal that social capital is the primary driver of collaborative supply chains, but that social capital can erode over time and an organization cannot always see when a trading partner has reassessed the value of the supply chain relationship. The supply chain partner may no longer see the relationship as a strategic priority or choose to exhibit the same willingness to invest in a relationship controlled by the organization. This risk leads organizations to pursue signals that provide assurance over the continuity of the strategic relationship. Fan and Stevenson (2018) find that in collaborative relationships the preferred mechanism is direct signaling where there is voluntary and deliberate disclosure by the supply chain partner of information on the risk; while in more adversarial relationships, the organization must seek indirect signals of risk levels—often by ‘‘reading between the lines’’ on communications between the parties.

C-SCRM assurance is a direct signaling mechanism for alleviating risks that come from imperfect information in supply chain partner relationships (Khazanchi and Sutton 2001). Organizations can outsource processes; but they cannot outsource the risks associated with work stoppages and supply chain disruptions (Johnson 2016; Bissell et al. 2019). One of the assumptions inherent in C-SCRM assurance is a focus on supply chain partners that are more deeply integrated at the organizational and informational

FIGURE 1
Research Model



resource level (Colicchia et al. 2019)—the types of relationships perceived to be most sustainable over time in terms of providing a resource advantage (Morgan and Hunt 1999). Such assurance provides direct signaling of the reasonableness of trust placed in a supply chain partner and a clear understanding of the supply chain partner's on-going cyber supply chain risk mitigation efforts. The research model presented in Figure 1 reflects this relationship. In the following subsections, we look more specifically at individual hypotheses in the model. Key to the model is our focus on an organization's view of its relationship with a selected supply chain partner. Thus, we will use the terms ''organization'' and ''partner'' to refer to the two entities, respectively. Some of the relationships are well-established in the literature (e.g., H1 and H5), but we provide the hypothesis formulation for all relationships to develop a more comprehensive overall model reflective of the complexities of R-A theory.

Establishing and Using Power

Dependence is the extent to which one trading partner is reliant on the second partner, and the relationship generates rewards and benefits that cannot be easily garnered through alternative available relationships (Kumar, Scheer, and Steenkamp 1998; Morgan and Hunt 1999). Relative dependence is the primary determinant of power in an interorganizational relationship (Emerson 1962; Hart and Saunders 1997; Son et al. 2005). Such an imbalance in power is common in supply chain relationships (Ca¨ker 2008; Morgan and Hunt 1999). The first hypothesis is as follows:

> **H1:** As a supply chain partner's dependence increases, the organization's power in the trading relationship increases.

A power advantage position allows for greater influence in putting governance structures[5] in place (Emsley and Kidon 2007). However, if the supply chain partner sees the governance structure as necessary to maintaining the relationship, but not as having any personal efficiency gains attached, then the partner may behave in a manner counter to the intent of the structures (Ca¨ker 2008). The supply chain partner may view such governance structures as self-interested behavior on the part of the organization and be less inclined to act in a *constrained* self-interest seeking mode (Hunt 1997c). In such situations, greater exchange of information could put the more powerful organization at risk should the partner fail to have appropriate safeguards in place (Colicchia et al. 2019). The interconnectedness of partner company intranets that commonly occurs in collaborative supply chain relationships leaves an organization vulnerable to security intrusions and other cyber-attacks if the partner has inadequate security in place (Johnson 2016; Duncan 2019). Even in the presence of strict contracts intended to mitigate risks, partners can fail to live up to the requirements of those contracts (Arnold et al. 2010, 2015; Johnson 2016).

Alternatively, the supply chain partner may simply fail to integrate processes at a level expected that creates risks further down the line as to ability to perform as needed across the supply chain. Frequently, the supply chain partner faces significant investment requirements to place itself in the position of providing resource advantages in a relationship (Chen et al. 2004; Hunt and Davis 2008) and may even face short-term losses in order to achieve long-term comparative advantage (Hunt and Davis 2008). These costs can be a significant deterrent to the supply chain partner putting the resources in place to create a lasting long-term resource advantage. Khazanchi and Sutton (2001) found little integration among a large sample of small- and medium-sized enterprises that were connected electronically in supply chains, despite their often single trading partner exerting its power to contractually mandate electronic integration and communication. Rather, orders were received electronically and printed out; thus, the print-outs drove manual based processes. Anderson and Lanen (2002) similarly did not observe any evidence of widespread integration of EDI connections with back office activities. While partners might adhere to performance requirements in the short-term, the lack of integration could affect long-term interest in further cutting cycle times throughout the supply chain and likewise affect competitiveness (Khazanchi and Sutton 2001; Nicolaou 2008). While technology integration, even among small and medium-sized enterprises, has substantially increased over the past decade, the motivations to implement adequate cybersecurity plans lacking perceived benefit from such

[5]Vosselman and van der Meer-Kooistra (2009) define governance structures as the institutional framework within which transactions are executed, noting that in interorganizational relationships the most common governance structure traditionally has been contracts. Sutton et al. (2008) note for example that Walmart Inc., in the early 2000s, required all supply chain partners to sign a contract that said that any damage to Walmart's systems that occurred as a result of connection with the partner's systems would be the financial responsibility of the trading partner regardless of cause. Sutton et al. (2008) note the limited value of such contracts when there is an imbalance in power and the smaller supply chain partner will likely be unable to cover the costs and will simply go out of business, providing Walmart with no recourse.

investments remains low, so cybersecurity may still be weak (Gordon, Loeb, Lucyshyn, and Zhou 2015).

The use of power to force processes on a dependent supply chain partner may not always result in the desired outcome. The supply chain partner may see the more powerful organization as unrealistically enforcing technological requirements and find the requirements overly burdensome. Research has shown this relationship between dependence and risk to be prevalent in early electronic integration efforts associated with small supply chain partners under large powerful organizations' mandates (Khazanchi and Sutton 2001; Anderson and Lanen 2002). This suggests a high probability that cyber supply chain risk will increase in situations where there is a power imbalance and potentially a lack of expected collaboration on strategic deployments. This leads to the second hypothesis:

> **H2:** As an organization's power over a supply chain partner increases, the level of cyber supply chain risk for that partner increases.

If an organization perceives that substantial cyber supply chain risk evolves from a supply chain partner, then the organization is more likely to seek a governance structure to mitigate that risk. Such supplier uncertainty creates an unpredictability that can affect the organization's ongoing activities. An organization operating in a cyber supply chain environment should make a great effort to minimize the level of uncertainty that it faces in future supply chain activities (Son et al. 2005). This is consistent with R-A theory where information is imperfect and costly to obtain (Hunt 1997c). One form of governance structure that can help reduce uncertainty is assurance over the supply chain partner's C-SCRM processes.

The desire to minimize risk uncertainty with cyber supply chain partners is consistent with emerging research suggesting that traditional reliance on social capital relationships leave organizations vulnerable. Organizations should recognize this risk and seek signals that clarify the supply chain partner's efforts to meet the collaborative needs for uninterrupted processing activity, information sharing, and security in the supply chain (Fan and Stevenson 2018). The preferred signal is a direct signal that voluntarily and clearly communicates adherence, the type of direct signal that C-SCRM assurance is designed to provide. This leads to the third hypothesis:

> **H3:** An organization is more likely to demand assurance over a supply chain partner's C-SCRM processes if the relationship increases the level of perceived cyber supply chain risk.

Faced with the potential risks from entering into a cyber supply chain relationship with a partner, an organization in a power advantage position would be likely to push for some level of assurance of supply chain capability. Prior research indicates that the assurance process yields higher quality systems and processes, although it is uncertain whether the quality was derived from the assurance, or those pursuing assurance have quality (Jamal, Maier, and Sunder 2003). There are lower levels of comfort available

through indirect signals such as cybersecurity ratings (Olyaei et al. 2018), but monitoring and assurance are increasingly advocated by security researchers (Johnson 2016). Nonetheless, while a part of the demand for assurance is likely affected by the perceived level of risk, the potential for self-interest seeking behavior by the supply chain partner in reaction to processes implemented via the power advantage will also provide motivation to implement an assurance process. Thus, we predict that as the power of an organization increases within a supply chain relationship, the demand for assurance over a trading partner's C-SCRM will increase. However, we also anticipate that this effect will flow through increased levels of cyber supply chain risk. That leads to the fourth hypothesis:

> **H4:** The level of cyber supply chain risk mediates the impact of power over a supply chain partner on the demand for CSCRM assurance.

Such assurance can come from multiple sources. There are similar but different sources of assurance to that provided by the proposed AICPA SOC. Coletti, Sedatole, and Towry (2005) operationalize assurance in their experiment as an outside consultant while the Institute of Internal Auditors has also actively considered cyber risk review under internal audit risk management efforts (e.g., Arnold, Hampton, Khazanchi, and Sutton 2004; Sutton, Arnold, Benford, and Canada 2009). In summary, one source of the demand for assurance comes from the power advantage position and an organization's ability to push governance structures onto the partner. However, this demand for assurance is also influenced by how committed the organization is to the trading relationship and whether the nature of the relationship justifies a relatively high cost control measure.

Commit, Trust, but Verify

Commitment is the strong desire to maintain a valued relationship (Moorman, Zaltman, and Despande 1992) and is a central tenet to all relational exchanges between firms (Morgan and Hunt 1994). Committed relationships are based on confidence that the relationship will endure because of joint efforts and sacrifices (Boyle, Dwyer, Robicheaux, and Simpson 1992). As commitment develops, an organization must assess both the vulnerabilities and the dependency of the supply chain partner (Free 2008). Dependency provides a certain level of commitment by the supply chain partner as the relationship yields greater returns than any other available alternatives (Morgan and Hunt 1999). For the organization on the other side of the relationship, if the partner is viewed as supplying a resource that provides comparative advantage, the more powerful organization should leverage this dependency and commit to a longer-term relationship if it helps the partner anchor into the supply chain network (Hunt and Davis 2008). This leads to H5:

> **H5:** As the level of a supply chain partner's dependence increases, the organization is more likely to commit to the trading relationship.

The underlying potential for resource advantage that drives commitment is also based on the competency of the supply chain partner. Before committing to even the early stages of a trading relationship, an organization will assess the potential supply chain partner's ability to fulfill their end of the commitment (Hunt 1997c, 1999; Emsley and Kidon 2007; Hunt and Davis 2008; Lavastre, Gunasekaran, and Spalanzani 2012; Duncan 2019). If a potential partner is not perceived as likely to be competent and reliable, an organization is not likely to enter into a long-term relationship (Hunt and Morgan 1994; Morgan and Hunt 1999; Nicolaou and McKnight 2006). Core technical competence is a key precursor to commitment as the supply chain partner must bring valuable resources to the relationship that allow the supply chain as a whole to achieve superior comparative advantage—ideally through more efficient production that leads to more effective production (Hunt 1997c, 1999). This leads to the sixth hypothesis:

> **H6:** As the perception of core technical competence of the supply chain partner increases, the organization's commitment to the relationship increases.

Commitment is the foundation for a supply chain relationship to develop and become static. Long-term experiences impact the social construction of the relationship between the supply chain partner and the organization based on perceptions of fairness, professionalism, and appropriate behavior (Hunt and Morgan 1995; Morgan and Hunt 1999; Chua and Mahama 2007). A fundamental part of commitment is the long-term perspective, which is a precursor to developing trust (Hunt 1997a; Free 2008; Hunt and Davis 2008). The memories of past events and changes in the relationship will affect the stability and perceived fairness of the relationship (Morgan and Hunt 1994; Chua and Mahama 2007); and, ultimately these interactions during the commitment phase shape the form and nature of the trust (Hunt 1997a; Free 2008; Hunt and Davis 2008). This leads to the seventh hypothesis:

> **H7:** As an organization's commitment to a supply chain partner increases, trust in the partner increases.

As noted earlier, commitment arises when an organization believes the relationship warrants the effort required to strengthen it (Morgan and Hunt 1994). Similarly, trust develops when an organization has confidence that a supply chain partner is reliable, which in the initial development stages relates to competency (Hunt 1997c, 1999). Thus, as core technical competence of the partner increases, the willingness to trust will also increase. However, a supply chain partner's technical competence will only influence trust in the presence of an organization's decision to commit to a relationship with the partner. In the presence of commitment, trust will become the conduit through which an organization is willing to pursue stronger relationships with that partner and invest in appropriate control mechanisms (Morgan and Hunt 1994; Hunt and Davis 2008). Thus, we posit that as a supply chain partner's technical competency increases, trust will increase, but that this effect from technical competency will flow through commitment to the partner. This leads to the eighth hypothesis:

H8: Commitment to the supply chain partner mediates the impact of a partner's core technical competence on trust of the partner.

The trust-control relationship is fundamental to the concept of building alliances. This concept, termed ''trust but verify,'' has often been used in establishing political alliances between countries where the balance of power is skewed in a given direction, but the relationship is viewed as mutually beneficial. This development of mutual trust is important in the development of an interorganizational relationship (Morgan and Hunt 1999; Son et al. 2005; Johnson 2016). This is consistent also with Bedard, Jackson, and Graham's (2005) views on the role of systems reliability assurance as a vehicle for justifying trust.

Assurance helps reduce the asymmetries that arise in the presence of only imperfect information (e.g., Hunt 1997a). Assurance represents a direct signal confirming the supply chain partner's vision of the strategic importance of the supply chain relationship and their on-going efforts to build the social capital that increases the value of the relationship (Fan and Stevenson 2018). Such signals are considered increasingly important from a strategic management standpoint as they justify the investments of an organization from both capital and social investment perspectives (Bergh, Connelly, Ketchen, and Shannon 2014). Accordingly, we posit that as an organization's trust in a partner increases, the demand for assurance over the partner's C-SCRM processes increases. This leads to the ninth hypothesis:

H9: As trust in a supply chain partner increases, an organization's demand for assurance over that relationship increases.

The view that control needs trust, and trust needs control, suggests that the two are intertwined in terms of developing effective control systems in a solid interorganizational relationship. The rational approach views trust and control as having a common goal—the absorption of behavioral uncertainty (Vosselman and van der Meer-Kooistra 2009). In the current study, we are examining the demand for a new assurance service that did not previously exist. Thus, in our model where the data are collected before any such engagements have been completed, the directionality of the relationship must necessarily be from trust to assurance. Future research should recognize the likely recursive nature of this relationship once assurance has been previously attained.

We test each of the hypotheses individually while examining them in the overall context of a structural model. The support of the overall model is the most critical component in terms of assessing the viability of R-A theory in explaining the complex social relationships existing among partners in cyber supply chain relationships. Hence, we simultaneously examine the hypotheses within the overall context of the model.

IV. METHODS

Data Collection

To test the above hypotheses, a web based survey instrument was used and targeted to individuals with the knowledge, experience, and expertise to evaluate the potential risks as well as the ability to influence cyber risk interactions. To ensure that respondents had the requisite skills, CIOs, information systems security specialists, IT internal audit specialists with cyber experience, and cyber relationship development staff were invited to participate. The views of these individuals are instrumental in shaping and guiding organizational perceptions of the cyber supply chain relationship (Beugre´ and Acar 2008; Colicchia et al. 2019; Luo 2007; Yilmaz, Sezen, and Kabaday 2004). Prior to data collection, the survey instrument was pretested for ease of use, clarity, and time to complete by 42 individuals from the targeted groups. The responses were not used for hypotheses testing nor did these respondents participate in this research beyond the pretest phase.

- To reach the targeted sample, we employed a survey company who solicited potential respondents via e-mail based on their job titles.[6,7] Out of the e-mail solicitations, 1,021 respondents started the survey at the survey company's site. Each respondent was presented with the following pre-screening questions to evaluate their suitability for participation: Does your organization have experience in working with trading partners (e.g., suppliers, customers, outsourcers, etc.) in a B2B e-commerce relationship?
- Does your organization repeatedly transact with any such trading partners?
- Do you have a basic understanding of the technological and IT-driven components of B2B e-commerce?
- Do you have a reasonable understanding of any of your trading partners' B2B e-commerce capabilities and your firm's relationship with this partner?

If any of the questions were answered with a ''no'' response, respondents were not granted access to our survey. The prescreening questions eliminated 149 individuals, leaving 872 potential respondents. Out of 872 qualified respondents[8], 266 (31 percent) completed the survey. Of the 266 completed surveys, 11 surveys were eliminated due to inconsistencies between responses, 45 were eliminated due to excessive missing responses, and 5 were eliminated due to excessive selection of the ''no basis for

[6]EMPanel (EMPanelonline.com) was used to reach potential respondents. EMPanel solicits potential respondent groups at industry conferences and through online connections to develop panels for a broad range of industries and positions within those industries. They have a designated coordinator for academic panels to work on the specific needs of research projects and ensure integrity of the panels. Respondents can be excluded for any reason by the researchers and EMPanel maintains a ''three strikes you're out rule,'' which specifies exclusions in three studies will have an individual removed from all panels. EMPanel was paid $24 per ''good'' respondent and they in turn compensated the respondents.

[7]The research study, survey, and participant solicitation processes were all approved through the appropriate Institutional Review Board process for research related to human subjects.

[8]The survey company is contracted for a certain number of responses and once that number is reached, the researcher closes the survey. So only individuals that have started the survey when the target number of respondents is reached are allowed to continue to completion. Others receiving the solicitation are informed that the survey is closed if they attempt to access the survey after the number of respondents have been received.

judgment'' response. The final sample consisted of 205 useable survey responses.

For the final sample, the total missing data rate was 1.33 percent, comprised of 0.66 percent for missing responses and 0.67 percent for ''no basis for judgment'' responses. Structural equation modeling requires complete data to estimate the measurement and structural models. We used expectation maximization to estimate missing data values.9

Table 1 presents respondent and organizational demographic information. The majority (94.1 percent) of respondents were male. The most frequently occurring age group was between 37 and 47 years old (34.6 percent). Respondent age was also skewed toward higher levels with 94.5 percent of respondents over the age of 32. All respondents had at least some college education with Bachelor's followed by Master's degrees being the most frequent education level completed. The most frequently occurring job function was CIO/CTO (41 percent), followed by IT security staff (12.2 percent), and auditors—including traditional, IT, external, and internal audit (10.8 percent). Over 49 percent of respondents had been in their current job between 5 and 13 years.

Most respondents (92.2 percent) worked for publicly traded organizations. Over 90 percent of respondents evaluated cyber supply chain relationships with an external cyber supply chain partner (not tabulated). Manufacturing was the most frequently occurring industry segment (25.4 percent), followed by aerospace and defense, and wholesale/retail. The majority of organizations (65.8 percent) had been using cyber supply chains for a period of 1 to 9 years. Trading partners were at different stages in their development and use of cyber supply chain capabilities. According to respondents, the majority (74.1 percent) of their trading partners were in the integration or infusion stage of cyber supply chain capabilities.[10] The most frequently occurring cyber supply

[9]Full Information Maximum Likelihood (FIML) can also be used to estimate structural models with missing data. The results are qualitatively identical when using FIML for structural model estimation.

[10]Respondents were asked to select the choice that best characterizes the state of their trading partners' cyber supply chain capabilities. Adoption: Incoming business documents are electronically received and printed. A staff member is required to key-in outgoing messages. B2B applications run on a standalone PC/workstation or terminal. Integration: Incoming business documents are received electronically, stored in files, and can be printed on demand. Outgoing business documents are also created as files by internal applications and are electronically sent. B2B applications are either run on a PC/workstation or are based in a mainframe/mini-computer where internal business applications are run. This setup replaces the keying-in and printing-out of messages with files, speeding up the process and makes incoming messages particularly useful, since they do not require re-keying prior to use by another system (e.g., production scheduling or accounting). Infusion: B2B transaction processing is seamlessly integrated with internal business applications such as purchasing, order entry, production scheduling, inventory management, accounts receivable/payable, shipping, and so on. Business documents are exchanged internally and externally (with trading partners) in a nearly ''paperless'' environment with little human intervention. Strategic: B2B applications are viewed as strategic information technology (IT) and are instrumental in reengineering (changing) internal business processes and functions with trading partner(s) and redefining organizational structure. B2B is seen as an integral part of the organizational context and is a major factor in strategic and information systems planning. Sharing databases, participating in just in time/quick response (JIT/QR) programs are examples of this top-down, organization-wide, strategic view of B2B and other related information technologies.

chain partners were customers (61.0 percent), followed by wholesalers, manufacturers, and financial institutions. The most frequently used cyber supply chain functions were purchasing/order management (72.2 percent), billing payment, and shipping/receiving. The distribution of trading partner cyber supply chain purchases and sales was bimodal. For many organizations, purchases and sales were below $2.25 million (66.3 and 60.0 percent, respectively). However, 21.5 and 24.4 percent of organizations had cyber supply chain purchases and sales in excess of $4.75 million, respectively. The respondent and organizational demographics indicated data collection processes were successful in targeting individuals with the knowledge, experience, and expertise to evaluate the potential cyber supply chain risks as well as the ability to influence cyber risk interactions.

TABLE 1

Respondent and Organizational Demographics

Category	Frequency (n = 205)	Percent
Gender		
Male	193	94.1
Female	12	5.9
Not answered	0	0
Age (in years)		
< 22	1	0.5
22 to 27	1	0.5
27 to 32	9	4.4
32 to 37	34	16.6
37 to 42	37	18.0
42 to 47	37	18.0
47 to 52	32	15.6
52 to 57	29	14.1
> 57	23	11.2
Not answered	2	1.0
Highest level of education		
High school	0	0
Some college	21	10.2
Associates degree	6	2.9
Bachelor's degree	92	44.9
Master's degree	73	35.6
PhD	11	5.4
Not answered	2	1.0
Primary job function		
IT auditor (internal)	10	4.9
IT auditor (external)	3	1.5
Non-IT auditor (external)	2	1.0
Non-IT auditor (internal)	7	3.4
IT security staff	25	12.2
B2B e-commerce manager	11	5.4
CIO/CTO	84	41.0
Other	63	30.7
Not answered	0	0

Continued on next page

TABLE 1 (continued)

Category	Frequency (n = 205)	Percent
Experience in current job function (in years)		
< 1	1	0.5
1 to 5	25	12.2
5 to 9	53	25.9
9 to 13	48	23.4
13 to 17	25	12.2
17 to 21	20	9.8
21 to 25	19	9.3
25 to 29	13	6.3
> 29	0	0
Not answered	1	0.5
Organizational Structure		
Publicly traded	189	92.2
Not publicly traded	12	5.9
Not answered	4	2.0
Industry		
Manufacturing	52	25.4
Insurance	17	8.3
Financial/real estate	16	7.8
Wholesale/retail	22	10.7
Technology	3	1.5
Utilities	8	3.9
Health	18	8.8
Communication	1	0.5
Aerospace & defense	27	13.2
Transportation	9	4.4
Other	29	14.1
Not answered	3	1.5
Cyber supply chain stage[a]		
Adoption	25	12.2
Integration	80	39.0
Infusion	72	35.1
Strategic	27	13.2
Not answered	1	0.5
Organizational use of cyber supply chain in years		
< 1	5	2.4
1 to 5	70	34.1
5 to 9	65	31.7
9 to 13	28	13.7
13 to 17	17	8.3
17 to 21	10	4.9
21 to 25	3	1.5
25 to 29	2	1.0
> 29	3	1.5
Not answered	2	1.0
All organizational cyber supply chain partners		
Customers	125	61.0
Wholesalers/Distributors	113	55.1
Manufacturing	99	48.3
Financial institutions	86	42.0
Shipping companies	65	31.7
Government	45	22.0
Other	16	7.8
Not answered	1	0.5

Continued on next page

TABLE 1 (continued)

Category	Frequency (n = 205)	Percent
Cyber supply chain purchases with this trading partner for current fiscal year in dollars		
< 250,000	65	31.7
250,000 to 750,000	29	14.1
750,000 to 2.25 million	42	20.5
2.25 million to 2.75 million	4	2.0
2.75 million to 3.25 million	5	2.4
3.25 million to 3.75 million	4	2.0
3.75 million to 4.25 million	2	1.0
4.25 million to 4.75 million	3	1.5
> 4.75 million	44	21.5
Not answered	7	3.4
Cyber supply chain sales with this trading partner for current fiscal year in dollars		
< 250,000	68	33.2
250,000 to 750,000	22	10.7
750,000 to 2.25 million	33	16.1
2.25 million to 2.75 million	9	4.4
2.75 million to 3.25 million	2	1.0
3.25 million to 3.75 million	4	2.0
3.75 million to 4.25 million	4	2.0
4.25 million to 4.75 million	4	2.0
> 4.75 million	50	24.4
Not answered	9	4.4

[a]Cyber supply chain stages defined as follows: Adoption: Incoming business documents are electronically received and printed. A staff member is required to key-in outgoing messages. B2B applications run on a standalone PC/workstation or terminal; Integration: Incoming business documents are received electronically, stored in files, and can be printed on demand. Outgoing business documents are also created as files by internal applications and are electronically sent. B2B applications are either run on a PC/workstation or are based in a mainframe/minicomputer where internal business applications are run. This setup replaces the keying-in and printing-out of messages with files, speeding up the process and makes incoming messages particularly useful, since they do not require re-keying prior to use by another system (e.g., production scheduling or accounting);

Infusion: B2B transaction processing is seamlessly integrated with internal business applications such as purchasing, order entry, production scheduling, inventory management, accounts receivable/payable, shipping, and so on. Business documents are exchanged internally and externally (with trading partners) in a nearly ‘‘paperless’’ environment with little human intervention; and

Strategic: B2B applications are viewed as strategic information technology (IT) and are instrumental in reengineering (changing) internal business processes and functions with trading partner(s) and redefining organizational structure. B2B is seen as an integral part of the organizational context and is a major factor in strategic and information systems planning. Sharing databases, participating in just in time/quick response (JIT/QR) programs are examples of this top-down, organization-wide, strategic view of B2B and other related information technologies.

Development of Measures

All questions used a seven-point Likert type scale anchored on 1 (strongly disagree) and 7 (strongly agree). In addition, respondents had the option to select ‘‘No basis for judgment.’’ Items for the reflective constructs (trading partner’s dependence on

organizational relationship [Ganesan 1994; Kumar et al. 1998], trading partner's core technical competency [Hart and Saunders 1998; Armstrong and Sambamurthy 1999], an organization's power over a trading partner ([Kumar et al. 1998; Hart and Saunders 1998], an organization's commitment to a trading partner [Ganesan 1994; Hart and Saunders 1998], and an organization's trust of a trading partner [Zaheer, McEvily, and Perrone 1998; Hart and Saunders 1998]), were adapted from prior studies. The validity of these scales was assessed during measurement model testing using confirmatory factor analysis (CFA). The results indicate all scale items load on their respective constructs at a minimum level of 0.70 except for one item, pwr1, in the power scale which loaded at 0.634. All scale item loadings are significant (p , 0.05). Based on these results, all scale items were retained. Table 2 provides scale items with their corresponding range, median, mean, standard deviation, and construct loading from measurement model validation.

Since the demand for assurance over a supply chain partner has not been previously examined, a C-SCRM demand for assurance scale to measure this construct was developed. Initial validation of the scale was conducted with data from a hold-out sample using principal axis factoring with oblique (D ¼ 0) rotation. All scale items loaded on a single factor at a minimum of 0.70. Scale average variance extracted (AVE) and Cronbach's alpha scores are 0.71 and 0.88 respectively (not tabulated).

The cyber supply chain risk construct was derived using both reflective and formative measurement techniques (Jarvis, MacKenzie, and Podsakoff 2003). The decision to model a given construct as formative or reflective is driven by the nature of the construct and the item measures developed. Reflective constructs are based on the premise that an unobservable latent construct causes change in a group of observable measures. The observable measures, or items, are expected to move in the same direction in response to changes in the associated latent construct, are somewhat internally consistent, and are substitutable. Thus, removal of an item from the latent construct measurement model will not alter the meaning of the latent construct (Jarvis et al. 2003). In contrast, formative constructs are based on the premise that observable measures come together to create the latent construct. Therefore, changes in a single formative item measure can cause changes in the associated latent construct. Formative items are not expected to move in the same direction, nor are they expected to be internally consistent or substitutable. Inappropriate removal of a formative item may alter the meaning of the latent construct (Jarvis et al. 2003).

A two-step process was utilized to produce the reflective construct, organizational cyber supply chain risk, from three formative constructs: business level risk, application-user level risk, and technical level risk. In step 1, formative constructs were estimated with measurement items developed by Sutton et al. (2008). In step 2, the formative measures validated in step 1 were used to produce principal component analysis (PCA) respondent factor scores for business level, application-user level, and technical level risk constructs. These PCA respondent factor scores serve as reflective items of the

TABLE 2

Descriptive Statistics

Variable Measures	Item	Range	Median	Mean	Std. Dev.	Item Load
Dependence						
Your organization's relationship is crucial to this trading partner's future performance. 1) Strongly Disagree to 7) Strongly Agree (Ganesan 1994)	dep1	7	5	4.53	1.82	0.887
This trading partner is dependent on your organization. 1) Strongly Disagree to 7) Strongly Agree (Ganesan 1994)	dep2	7	4	3.98	1.85	0.824
It would be difficult for this trading partner to replace the business generated from their relationship with our organization. 1) Strongly Disagree to 7) Strongly Agree (Kumar et al. 1998)	dep3	7	4	4.07	1.76	0.799
Core Technical Competency						
This trading partner is competent in accurately and efficiently processing electronic transactions. 1) Strongly Disagree to 7) Strongly Agree (Hart and Saunders 1998)	ctc1	7	6	5.42	1.45	0.926
The trading partner's computer systems are reliable. 1) Strongly Disagree to 7) Strongly Agree (Hart and Saunders 1998)	ctc2	7	6	5.44	1.34	0.928
This trading partner is extremely knowledgeable about the potential of current B2B e-commerce IT? 1) Strongly Disagree to 7) Strongly Agree (Armstrong and Sambamurthy 1999)	ctc3	7	6	5.33	1.41	0.800
Power						
Some of your organization's actions have a negative effect on this trading partner, but they cannot do anything to prevent it. 1) Strongly Disagree to 7) Strongly Agree (Kumar et al. 1998)	pwr1	7	4	3.61	1.65	0.634
Your organization, if it wanted to, has the capability to make things difficult for this trading partner. 1) Strongly Disagree to 7) Strongly Agree (Kumar et al. 1998)	pwr2	7	4	4.12	1.87	0.844
Your organization, if it wanted to, has the capability to tie this trading partner up in an expensive legal battle. 1) Strongly Disagree to 7) Strongly Agree (Kumar et al. 1998)	pwr3	7	4	3.87	1.91	0.816
Commitment						
Your organization assumes that renewal of agreements with this trading partner generally will occur. 1) Strongly Disagree to 7) Strongly Agree (Hart and Saunders 1998)	com1	7	6	5.27	1.52	0.833
Your organization believes that, over the long run, the relationship with this trading partner will be profitable. 1) Strongly Disagree to 7) Strongly Agree (Ganesan 1994)	com2	7	6	5.48	1.57	0.921
Your organization focuses on long-term goals with this trading partner. 1) Strongly Disagree to 7) Strongly Agree (Ganesan 1994)	com3	7	5	5.11	1.66	0.825
Trust						
Deadlines set by this trading partner are honest and accurate. 1) Strongly Disagree to 7) Strongly Agree (Hart and Saunders 1998)	trt1	7	5	5.10	1.44	0.803
This trading partner is honest in business dealings. 1) Strongly Disagree to 7) Strongly Agree (Hart and Saunders 1998)	trt2	7	6	5.52	1.42	0.955
This trading partner has always been evenhanded in their negotiations with our organization. 1) Strongly Disagree to 7) Strongly Agree (Zaheer et al. 1998)	trt3	7	6	5.26	1.40	0.791
Demand for C-SCRM Assurance						
Your organization would desire a formal review by your internal audit department of this trading partner's B2B e-commerce risks. 1) Strongly Disagree to 7) Strongly Agree	ad1	7	4	4.12	1.64	0.796
Your organization would find third-party certification of this trading partner's B2B e-commerce risks advantageous. 1) Strongly Disagree to 7) Strongly Agree	ad2	7	4	4.37	1.60	0.846
Your internal auditors would consider recommending to management that this trading partner be required to attain assurance over their B2B e-commerce related systems. 1) Strongly Disagree to 7) Strongly Agree	ad3	7	4	4.17	1.62	0.890
Cyber Supply Chain Risk Reflective Scale						
Business Level Risk Factors	blr	6.11[a]	0.01	0	1	0.879
Application-User Level Risk Factors	aulr	5.90[a]	0.04	0	1	0.989
Technical Level Risk Factors	tlr	5.81[a]	0.11	0	1	0.882

[a] Absolute values.

global construct cyber supply chain risk. This two-step process recognizes that an organization's cyber supply chain risk is simultaneously influenced by individual trading partner relationships as well as the organization's own global C-SCRM policies and procedures. Organizations evaluate and institute risk policies, procedures, and controls

to simultaneously manage business level, application-user level, and technical level risks across all supply chain partners. Thus, these risk policies, procedures, and controls will be consistent and complementary with respect to business level, application-user level, and technical level risks, and, to varying degrees, affect individual partner risk inherited by the organization. As such, these three levels of risk will move in tandem to reflect an acceptable or desirable level of organizational cyber supply chain risk.

Consistent with step 1 discussed above, the business level risk, application-user level risk, and technical level risk formative constructs were evaluated for scale validity. Because formative items were not expected to be internally consistent, classical measurement theory tests for assessing construct validity were not applicable. Instead formative items were evaluated on multicollinearity (Diamantopoulos, Riefler, and Roth 2008) and outer-item weights (Chin 1998). Table 3 lists variance inflation factors (VIF) and outer-item weights for the formative items used in this study. A review of prior literature indicates a lack of consensus concerning an unacceptable level of formative item multicollinearity. Recommended VIF levels range from a low of 3.3 (Petter, Straub, and Rai 2007) to a high of 10 (Diamantopoulos et al. 2008). Consistent with Petter et al. (2007), we adopted a conservative VIF of 3.3 as a cutoff for formative item elimination. One application-user level risk item and two technical level risk items were eliminated as VIF scores exceeded 3.3. All other formative items (45) were retained.

Outer-item weights were assessed using components based structural equation modeling (Ringle, Wende, and Will 2005). Again, prior literature is unclear concerning the best treatment of insignificant item weights. Diamantopoulos and Winklhofer (2001) recommend removing non-significant items for parsimony. However, Bollen and Lennox (1991) and Diamantopoulos et al. (2008) recommend retaining all items as removal of a non-significant item may alter the meaning of the formative construct. We used the approach advocated by Bollen and Lennox (1991) and Diamantopoulos et al. (2008) and retained all formative items.[11] While this approach may include formative items that do not significantly contribute to the estimation of the formative construct, the prior elimination of formative items with VIF equal to or greater than 3.3 assured that the retained formative items were not inappropriately influencing formative construct estimation. Table 3 presents scale items, VIF scores, and outeritem weights and associated t-values.

Step 2 estimated individual respondent factor scores for business level, application-user level, and technical level risk constructs based on their respective factor scores using the validated formative items from step 1. PCA with oblique (D ¼ 0) rotation was used to generate item eigenvalues. The eigenvalues for business level risk indicated the

[11] The decision to retain formative items, whether significant or not, is a matter of debate in the statistical literature. We chose to retain all formative items for completeness and richness. If we remove all items with t-values below 1.282 (p , 0.10, two-tailed) and re-estimate the structural model, the results are qualitatively identical. If we include all items regardless of VIF scores and re-estimate the structural model, the results are qualitatively identical.

TABLE 3

Cyber Supply Chain Risk

Formative Measures	Item	VIF	Weights	t-value
Business Level Risk Factors				
Understanding by trading partner (TP) of their business processes, where e-commerce fits into those processes, value of business process integration with TPs, and where benefits are derived.	blr1	2.13	−0.014	0.038
Trading partner's ability to assess the use/success of technology and the benefits of B2B implementation/technology investment (including return on investment).	blr2	2.83	0.158	0.658
Trading partner's costs of meeting regulatory requirements and their organization's understanding of associated risks of non-compliance (including inter- and intra-state compliance issues).	blr3	1.96	0.221	1.121
Trading partner's technical understanding at a level that facilitates creation of a transformational vision for change and the ability to implement successful change management strategies to achieve objectives, gain acceptance, and support sustainability of the change.	blr4	2.40	−0.119	0.465
Trading partner's understanding of the intended functionality of a system at the analysis/requirements stage and tying of the system to business processes that are evolved or engineered accordingly to meet the business objective.	blr5	3.03	−0.013	0.170
Trading partner's level of adherence to contractual requirements including such things as product volume, sales prices, time/service commitments, and settlement (including legal agreements such as non-repudiation and the level of legal binding).	blr6	2.15	0.106	0.432
Trading partner's due diligence in implementing B2B relationships at the business, technology, and security levels to assure users understand data classification/ownership/security when handling partner data and the partner maintains appropriate segregation of data to appropriate users.	blr7	2.58	−0.224	0.929
Trading partner's understanding of risks associated with their projects and accordingly executing effective project management.	blr8	2.47	0.271	1.340
Trading partner's understanding of the technical complexities and associated costs of B2B development, implementation, and maintenance; and the legal ramifications, costs of implementing versus not implementing non-repudiation agreements, costs of new business rules, and loss of personal marketing contacts.	blr9	2.79	−0.068	0.402
Trading partner's team expertise for guiding all aspects of B2B e-commerce projects along with training for project teams and users.	blr10	2.79	−0.262	1.250
Trading partner's broad management involvement in IT/business planning while maintaining independence in the selection of technology preferences.	blr11	2.37	0.584	3.140
Trading partner's integration of applications into organizational procedures and guidelines—including comprehensive documentation.	blr12	2.18	−0.300	1.488
Auditability of trading partner's system based on effective monitoring controls and audit trail (history of electronic data, updates, changes).	blr13	1.95	0.349	2.006
Trading partner's ability to protect a distinguished brand in an e-commerce environment.	blr14	1.76	0.147	0.686
Trading partner's resilience to a business interruption.	blr15	1.72	0.069	0.512
Application-User Level Risk Factors				
Appropriate level of training for trading partner's users and related cost constraints	aulr1	2.19	−0.005	0.007
Will the target trading partner (TP) use a proposed B2B system (considering such issues of whether there is a champion for the project, sufficient IT sophistication to integrate within TP's systems environment, and ease of use of application)?	aulr2	2.20	0.089	0.371
When upgrading systems based on new technologies or business partner request, the trading partner has sufficient coordination and change control procedures in place to maintain reliability and protect transaction validation procedures	aulr3	2.38	−0.061	0.230
Trading partner's understanding of and agreement on data structure/scope/business rules for exchange of information	aurl4	2.51	−0.400	2.122
Is there benefit of B2B ventures to the trading partner and is the e-business marketplace sustainable?	aulr5	2.30	0.019	0.258
Clear and sufficient contract documentation on policies, procedures, connectivity guidelines, limitations, review plan, etc. (Service Level Agreements)	aulr6	2.17	0.135	0.671

TABLE 3 (continued)

Formative Measures	Item	VIF	Weights	t-value
Application controls in place for completeness, accuracy, and processing integrity (i.e. trading partner's applications function as intended).	aulr7[a]	3.65	NA	NA
Trading partner's implementation of new B2B applications include testing for assurances on hardware/software capability to support applications, availability of supporting applications 24/7, and performance and capacity of data exchange	aulr8	2.83	0.379	1.940
Third party assurance of transaction validity	aulr9	1.58	0.075	0.493
Marketing cost to sell the trading partner on a given B2B application	aulr10	1.73	0.234	1.130
Privacy of data agreements	aulr11	2.04	−0.155	0.758
Alignment of trading partner's business processes with implemented B2B e-business technologies	aulr12	2.31	−0.025	0.083
Adequacy of the security over access to trading partner's business application systems	aulr13	2.19	0.177	0.797
Inaccurate, inadequate, or outdated documentation on systems software/hardware provided by trading partner	aurl14	1.89	0.167	0.726
Trading partner's inability to have an enterprise view of the full range of trading partner relationships	aulr15	2.08	0.371	1.867
Technical Level Risk Factors				
Change management processes in place to assure maintenance of security and integrity of systems as technology evolves rapidly.	tlr1	2.18	0.079	0.686
Trading partner's security over all networks and network interactions ensure transmission integrity and provide guaranteed delivery transaction to the correct trading partner.	tlr2	2.79	0.030	0.0261
Technology sophistication/expertise differential between trading partners and related selection of appropriate standards and hardware/software by the right people in this trading partner's organization.	tlr3	2.41	−0.047	0.122
Trading partner's maintenance of data accuracy during systems conversion and application usage.	tlr4	2.80	−0.114	0.366
Completeness and accuracy of trading partner's data processing activities.	tlr5	3.09	0.077	0.306
Metrics related to capacity, resiliency, and monitoring in order to better predict/control performance by trading partner.	tlr6	2.09	−0.274	1.322
Security of communication technology (infrastructure)—including vulnerability of ISP and/or public internet, vulnerability to malicious code (e.g. viruses), security vendors expected survival, and the trading partner's general security model.	tlr7	3.00	0.100	0.353
Trading partner's vulnerability to loss of availability of data, systems, applications, etc., whether loss is accidental, intentional, or by poor design.	tlr8	2.71	0.187	0.674
Trading partner's setting of appropriate user profiles to assure information is appropriately compartmentalized by information types and classified by access levels.	tlr9	3.17	0.082	0.357
Controls to enforce compliance with regulatory requirements and to enforce regulations	tlr10	2.67	0.026	0.035
Comprehensive access management to applications/operating systems protected via controls (e.g. firewalls) in place to assure confidentiality, availability, and integrity (e.g. unauthorized access).	tlr11[a]	3.76	NA	NA
Channel security through appropriate controls (e.g. encryption implemented according to regulations) including validation and authentication of transaction partner.	tlr12	2.74	0.186	0.775
Ease of transition of information to new B2B systems, ease of integration with trading partner's systems, consistency in methods of partner, and ability to efficiently route B2B transactions to the right internal applications.	tlr13	2.58	0.462	1.76
Flexibility and scalability of the trading partner's system (hardware/software independence).	tlr14	2.78	0.157	0.719
Redundancy and failover of trading partner's systems (in relation to downtime tolerance).	tlr15[a]	4.10	NA	NA
Adequacy of trading partner's disaster recovery plan.	tlr16	2.12	−0.184	0.990
Adequate staff expertise available on an as-needed basis.	tlr17	2.26	−0.241	1.142
Comprehensive systems documentation of trading partner's systems.	tlr18	2.26	0.190	0.834

[a] Items dropped.

existence of a single construct, while the eigenvalues for application-user level risk (eigenvalues ¼ 6.98 and 1.11) and technical level risk (eigenvalues ¼ 8.89 and 1.14) formed two constructs. However, examination of the scree plots suggested the existence of one dominant construct for application-user level risk and one dominant construct for technical level risk. Parallel analysis confirmed this supposition. The results indicated that eigenvalues less than 1.34 for application-user level risk and 1.39 for technical level risk were spurious. Based on the analysis of the scree plots and eigenvalues, we generated respondent factor scores for the business level risk,

application-user level risk, and technical level risk constructs using PCA constrained to a single factor. Principal axis factoring with oblique (D ¼ 0) rotation was used to assess scale validity for the reflective cyber supply chain risk scale. All scale items load on the cyber supply chain risk construct at a minimum of 0.70. Scale average variance extracted (AVE) and Cronbach's alpha scores are 0.84 and 0.94, respectively. Table 2 also presents scale items for these constructs along with corresponding ranges, medians, means, standard deviations, and construct loadings from measurement model validation using CFA.

V. MEASUREMENT AND STRUCTURAL MODEL RESULTS

Validation of the measurement model is conducted using covariance based structural equation modeling (SEM). The validity of the measurement model constructs as well as the overall measurement model fit are assessed prior to testing the structural model (Hair, Black, Babin, Anderson, and Tatham 2010). Table 4 reports the correlations, composite reliability scores, AVE, and square root of AVE for all constructs. The composite reliability scores of all reflective constructs exceed 0.70 (Nunnaly and Bernstein 1994). All AVE are higher than 0.50, and the square root of all AVE are larger than the correlations between the reflective constructs (Chin 1998). All inter-construct correlations are below the standard threshold of 0.85 (Kline 2005). These results support the convergent and discriminant validity of the reflective constructs (Chin 1998; Fornell and Larcker 1981).

Indices used to assess the overall measurement model fit include the Chi-square statistic (v2¼275.569, df¼168, p¼0.00), the root mean squared error of approximation (RMSEA ¼ 0.056, LO ¼ 0.044, HI ¼ 0.068), the Tucker Lewis Index (TLI ¼ 0.957), the comparative fit index (CFI¼0.966), and the standardized root mean square residual (SRMR¼0.052). These results suggest satisfactory fit for the measurement model (Hair et al. 2010). Because the item measures used in this study are perceptual and obtained using a single survey completed by single respondents, common method bias is a concern (BurtonJones 2009). We assessed the existences of common method variance within the measurement model using the unmeasured latent factor approach, as recommended by P. Podsakoff, MacKenzie, Lee, and N. Podsakoff (2003). The results indicate that all measurement items load significantly on their intended construct. Measurement item loadings on the unmeasured latent construct are not significant (p . 0.10) and range from 0.073 to 0.148. These results indicate common method bias is not a concern within this study.

Figure 2 presents the structural model with path loadings and significance levels for the hypothesized relationships. One of the central questions in this study relates to the roles of cyber supply chain risk, power, and trust on the demand for assurance over a supply chain partner's C-SCRM processes. These factors are particularly relevant in cyber supply chain relationships as these relationships require a level of openness and

coordination of critical organizational information resources and systems in order to provide comparative advantage. With this openness comes third party cyber risk (Bissell et al. 2019; Bitsight 2019) and, potentially, trust. Organizations do not develop cyber supply chain risk and trust perceptions in isolation. Instead, cyber risk and trust serve as nexuses for the influence of the interorganizational relationship antecedents, dependence, power, technical competence, and commitment. The influence of the interorganizational relationship antecedents on perceptions of trading partner cyber risk and trust—and ultimately, the effect of trading partner cyber risk and trust on C-SCRM assurance desirability—are tested by estimating the structural model shown in Figure 2.

Prior to evaluating hypothesized relationships, the overall fit of the structural model should be evaluated. Fit indices used to assess the overall fit of the structural model include the Chi-square statistic (v2 ¼ 294.721, df ¼ 179, p ¼ 0.00), RMSEA ¼ 0.056 (LO ¼ 0.044, HI ¼ 0.067), TLI ¼ 0.957, CFI ¼ 0.963, and SRMR ¼ 0.069. These results indicate satisfactory fit for the research model (Hair et al. 2010). In addition, all hypothesized relationships are significant in the predicted direction at a minimum of p , 0.05. The model provides strong support for the overall R-A theory of competition that provides a basis for understanding supply chain relationships and the role of dependence, technical competence, power, commitment, trust, and cyber supply chain risk on an organization's desire to enhance information quality and scope in assessing a supply chain partner's behavior.

H1 predicts that increasing levels of a supply chain partner's dependence increase the dominant partner's power over the trading partner. The results indicate a positive (0.644) and significant (p , 0.001) association between partner dependence and power over the partner. In addition, supply chain partner dependence explains 41.5 percent of the variation in power.

The effects of increasing power over a supply chain partner on cyber supply chain risk are addressed in H2. As predicted, increases in power over the partner are positively (0.181) and significantly (p , 0.05) related to increases in cyber supply chain risk inherited from the partner. However, power explains little (3.3 percent) of the variation in cyber supply chain risk. Thus, the ability of a dominant partner to dictate C-SCRM policy and procedures to a given supply chain partner does not appear to substantially impact cyber supply chain risk. This suggests that cyber supply chain risk may be better managed as an egalitarian relationship, consistent with that posited in the R-A theory of competition (Morgan and Hunt 1999; Hunt and Davis 2008).

H3 predicts that increasing levels of cyber supply chain risk are positively associated with an organization's increasing demand for assurance over a supply chain partner's C-SCRM processes. The results indicate a positive (0.216) and significant (p , 0.05) relationship between cyber supply chain risk and the demand for assurance over a partner.

TABLE 4

Construct Correlations, Average Variance Extracted, Square Root of Average Variance Extracted, and Composite Reliability

Panel A: Construct Correlations[a], Average Variance Extracted (AVE)[b], Square Root of AVE[c]

	Demand for C-SCRM Assurance	Cyber Supply Chain Risk	Core Technical Competency	Commitment	Dependence	Power	Trust
Demand for C-SCRM Assurance	0.714 0.845						
Cyber Supply Chain Risk	0.300	0.843 0.918					
Core Technical Competency	0.158	0.139	0.786 0.887				
Commitment	0.206	0.113	0.559	0.741 0.861			
Dependence	0.273	0.161	0.165	0.534	0.701 0.838		
Power	0.398	0.182	−0.074	0.162	0.655	0.593 0.770	
Trust	0.248	0.137	0.758	0.668	0.343	0.046	0.728 0.853

Panel B: Composite Reliability

Demand for C-SCRM Assurance	Cyber Supply Chain Risk	Core Technical Competency	Commitment	Dependence	Power	Trust
0.881	0.941	0.917	0.895	0.876	0.812	0.888

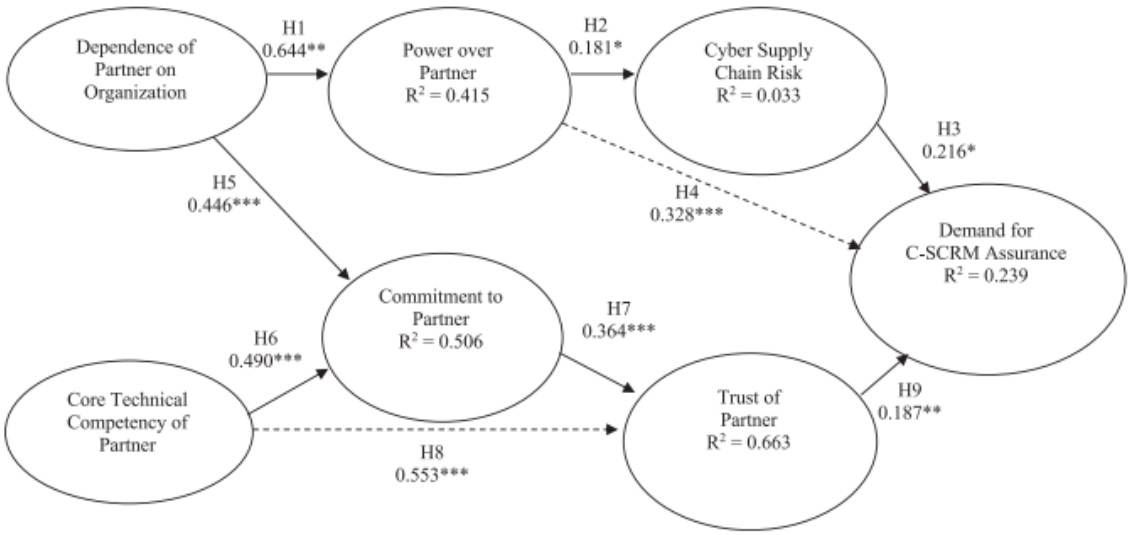
[a] Construct correlations are shown below the diagonal.
[b] AVE is the upper number on the diagonal.
[c] The square root of AVE is the lower number on the diagonal.

The mediating effect of cyber supply chain risk on the positive association between power over a supply chain partner and the demand for assurance is addressed by H4 and evaluated using bootstrapping (bias corrected, 10,000 sampling iterations) to obtain the total, direct, and indirect effects for the mediation relationship predicted in H4. The result indicates an indirect effect of 0.039 (CI ¼ 0.95), a direct effect of 0.328 (CI ¼ 0.99), and a total effect of 0.367 (CI ¼ 0.99). These results provide support for H4 and indicate cyber supply chain risk partially mediates the relationship between power over a supply chain partner and the demand for assurance.

H5 posits that as supply chain partner dependency on an organization increases, the organization's commitment to the partner relationship increases. The results, shown in Figure 2, indicate a positive (0.466) and significant (p , 0.001) relationship between supply chain partner dependence and commitment to the partner suggesting that dependence strengthens the commitment to a partner and the trading relationship.

H6 addresses the relationship between supply chain partner core technical competency and commitment to the partner. The results indicate that partner core technical competency is positively (0.490) and significantly (p , 0.001) associated with increasing commitment. The results also indicate that partner dependence and core technical competency together account for 50.6 percent of the variation in commitment to the supply chain partner.

FIGURE 2
Model Results



*, **, *** Indicate significance at the levels of < 0.05, 0.01, 0.001, respectively.

The positive effects of increasing commitment to the supply chain partner on trust of the partner are addressed by H7. The results show that an increase in commitment is positively (0.364) and significantly (p , 0.001) associated with an increase in trust of a supply chain partner.

The mediating effect of commitment to a supply chain partner on the positive association between perceived core technical competency of the partner and trust of the partner is addressed by H8 and evaluated using bootstrapping (bias corrected, 10,000 sampling iterations) to obtain the total, direct, and indirect effects for the mediation relationship predicted in H8. The results indicate an indirect effect of 0.178 (CI¼0.99), a direct effect of 0.553 (CI¼0.99), and a total effect of 0.732 (CI¼0.99). These results provide support for H8 and indicate commitment to the partner partially mediates the relationship between core technical competence of the partner and trust of the partner. In addition, as reflected in Figure 2, the components of the mediation relationship jointly explain 66.3 percent of the variation in trust.

H9 predicts that an increase in trust of a supply chain partner will be positively associated with an increase in demand for assurance over a partner's C-SCRM processes. The results indicate significant support (p , 0.01) for the hypothesized (0.187) relationship. Finally, cyber supply chain risk and trust of partner jointly explain 23.9 percent of the variation in the demand for C-SCRM assurance over its partner.

VI. DISCUSSION

Cybersecurity breaches continue to permeate the press with over 4,500 data breaches publicly disclosed in the U.S. since 2005 (Lord 2018; Eaton et al. 2019). Organizations have been under pressure to increase the effectiveness of their enterprise risk

management programs with a focus on (1) identifying and prioritizing risks, (2) implementing control systems to mitigate risk exposure, and (3) monitoring the effectiveness of control systems in actually mitigating risks. In addition, companies, their boards, investors, and supply chain partners are demanding more with an eye toward better C-SCRM processes and verification of those processes (Olyaei et al. 2018; Eaton et al. 2019; Bissell et al. 2019; Frank, Grenier, and Pyzoha 2019). Yet, companies continue to struggle with getting beyond an enterprise centric view that focuses on firewalling a single organization from cyber threats to a broader extended enterprise realization that cyber risks from third parties, particularly tightly coupled supply chain partners, have substantial potential for allowing cyber-attackers through those security fortresses (Sutton 2006; Johnson 2016; Colicchia et al. 2019).

The focus of this study is on the AICPA's new assurance services over an organization's C-SCRM in the form of an SOC for Supply Chain report (AICPA 2020b). This SOC recognizes that C-SCRM processes are not just limited to technical risks, but expand into relational factors affecting the coordination with supply chain partners. Cyber supply chain risks are affected by management level decisions and strategies as well as operational implementation and execution of cyber supported internal operations (AICPA 2020b; Sutton et al. 2008). This broader nexus of relational, managerial, operational, and technical risks is the central focus of the emerging C-SCRM research (Sutton et al. 2008; No and Vasarhelyi 2017; Duncan 2019; Colicchia et al. 2019) and practice agendas (Olyaei et al. 2018; Bitsight 2019; Bissell et al. 2019). Thus, in line with the calls for AIS research that advances our theoretical and practical understanding of how cybersecurity issues can be addressed, managed, and controlled (Janvrin and Wang 2019), our research provides an initial understanding of the role of C-SCRM assurance in interorganizational relationships.

A large integrative model has been presented in this study to capture relational components of the supply chain relationship as well as the broad based C-SCRM processes to understand the joint drivers of the demand for assurance from both the relational and risk perspectives. The results provide strong support for the R-A theory of competitiveness. Key among the tenants of R-A theory is that trading partners may still be motivated to enter into relationships where they are at a power disadvantage and recognize that constrained self-interest seeking behavior is more likely to lead to optimal comparative advantage. R-A theory also suggests that information an organization needs to assess the trading partner's behavior is both imperfect and costly to attain. Our research shows that the desire to improve information about the trading partner's behavior and verify the reasonableness of commitment and trust placed in that trading partner have a combined impact on the demand for assurance. All three conditions are key to the development of sustainable, long-term trading relationships that are based on joint value creation. The results provide evidence of a market that demands the type of assurance put forth by the AICPA (2020a) SOC for Supply Chains, and provide a strong theoretical foundation for understanding the relational complexities that must be addressed within C-SCRM processes.

Beyond the theory and practice contributions, our study provides a significant methodological contribution. While prior research theorizes that second order factors may include both formative and reflective measures at different levels (Jarvis et al. 2003), the nature of our construct for cyber supply chain risk where first order constructs are formative and second order factors are reflective, has not been previously used, validated, and analyzed. We demonstrate the multi-level validation of such a construct to support use in a covariance based SEM. The same method would be appropriate using components based SEM, such as partial least squares. Such a technique can be invaluable in leveraging research results where there is a dual objective of identifying a comprehensive set of measures that can be useful for practice and providing a solid basis for measurement within a research context (e.g., Sutton et al. 2008).

As in all studies, there are limitations to be considered in evaluating the results and framing future research. First, we used a research firm to solicit our respondents due to the difficulty of identifying and soliciting participation from individuals having the broad based expertise required to complete the survey. This approach does not allow traditional tests for response bias such as comparing early and late responses or reporting response rates. Rather, all data were obtained over a 72-hour period with a single e-mail request. Once the number of responses for which the research firm had been contracted was obtained, the survey was closed and potential respondents accessing the site were not allowed access. However, the benefits of using the research firm outweighed any risks as it allowed us to obtain responses from a large set of experts in a study area requiring access to managers with complex expertise.

Second, our research did not explore in-depth the type of competitive advantage that was provided by individual supply chain participants and the nature of specific types of advantage that might influence model components. Further exploration in future research on these antecedents will enhance our understanding. Little is understood at this point as to the role comparative advantage plays in supply chain relationships.

Third, our measure of the demand for C-SCRM assurance is an open measure of independent external assurance that may or may not be provided by professional accountants. We chose to focus on the service itself as opposed to the specifics of the provider. However, an item measure does focus on external auditors and loads well with the other item measures for assurance demand. Further, our measure does not specifically address the supply aspect nor the cost, although our respondents would be aware of the costs associated with various independent providers that may provide such services. Our results simply establish the demand for assurance.

REFERENCES

American Institute of Certified Public Accountants (AICPA). 2020a. *SOC for Supply Chains Backgrounder*. New York, NY: AICPA.

American Institute of Certified Public Accountants (AICPA). 2020b. *Appendix A: Information for Management*. New York, NY: AICPA.

American Institute of Certified Public Accountants (AICPA). 2020c. *Appendix B: Comparison of SOC for Supply Chain, SOC 2, and SOC for Cybersecurity Examinations and Related Reports*. New York, NY: AICPA.

Anderson, S., and W. Lanen. 2002. Using electronic data interchange (EDI) to improve the efficiency of accounting transactions. *The Accounting Review 77* (4): 703–729. https://doi.org/10.2308/accr.2002.77.4.703

Armstrong, C., and V. Sambamurthy. 1999. Information technology assimilation in firms: The influence of senior leadership and IT infrastructures. *Information Systems Research 10* (4): 304–327. https://doi.org/10.1287/isre.10.4.304

Arnett, D. B. 2011. *Resource-Advantage Theory: The Research Tradition Period*. Legends in Marketing: Shelby D. Hunt. Washington, DC: Sage Publishing.

Arnold, V., T. Benford, J. Canada, and S. Sutton. 2015. Leveraging integrated information systems to enhance strategic flexibility and performance: The enabling role of enterprise risk management. *International Journal of Accounting Information Systems 19*: 1–16. https://doi.org/10.1016/j.accinf.2015.10.001

Arnold, V., T. Benford, C. Hampton, and S. Sutton. 2010. Competing pressures of risk and absorptive capacity potential on commitment and information sharing in global supply chains. *European Journal of Information Systems 19* (2): 134–152. https://doi.org/10. 1057/ejis.2009.49

Arnold, V., T. Benford, C. Hampton, and S. Sutton. 2012. Enterprise risk management as a strategic governance mechanism in B2B enabled transnational supply chains. *Journal of Information Systems 26* (1): 51–76. https://doi.org/10.2308/isys-10253

Arnold, V., T. Benford, C. Hampton, and S. Sutton. 2014. Enterprise risk management: Re-conceptualizing the role of risk and trust on information sharing in transnational alliances. *Journal of Information Systems 28* (2): 257–285. https://doi.org/10.2308/isys-50812

Arnold, V., C. Hampton, D. Khazanchi, and S. Sutton. 2004. *Enterprise Risk Management: Identifying Risks in B2B E-Commerce Relationships*. Altamonte Springs, FL: Institute of Internal Auditors Research Foundation.

Bedard, J., C. Jackson, and L. Graham. 2005. Issues and risks in performing SysTrust engagements: Implications for research and practice. *International Journal of Accounting Information Systems 6* (1): 55–79. https://doi.org/10.1016/j.accinf.2004.10.001

Bergh, D. D., B. L. Connelly, D. J. Ketchen, Jr., and L. M. Shannon. 2014. Signalling theory and equilibrium in strategic management research: An assessment and a research agenda. *Journal of Management Studies 51* (8): 1334–1360. https://doi.org/10.1111/joms. 12097

Beugre´, C., and W. Acar. 2008. Offshoring and cross-border interorganizational relationships: A justice model. *Decision Sciences 39* (3): 445–468. https://doi.org/10.1111/j.1540-5915.2008.00199.x

Bharadwaj, S., P. Varadarajan, and J. Fahy. 1993. Sustainable competitive advantage in service industries: A conceptual model and research propositions. *Journal of Marketing 57* (4): 83–99. https://doi.org/10.1177/002224299305700407

Bissell, K., R. Lasalle, and P. Cin. 2019. *Ninth annual cost of cybercrime study: Unlocking the value of improved cybersecurity protection*. Available at: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

Bitsight. 2019. *Third party cyber risk for financial services: Blind spots, emerging issues and best practices*. Boston, MA: Bitsight/Center for Financial Professionals.

Bollen, K., and R. Lennox. 1991. Conventional wisdom on measurement: A structural equation perspective. *Psychological Bulletin 110* (2): 305–314. https://doi.org/10.1037/0033-2909.110.2.305

Boulianne, E., and C. Cho. 2009. The rise and fall of WebTrust. *International Journal of Accounting Information Systems 10* (4): 229– 244. https://doi.org/10.1016/j.accinf.2009.10.002

Boyle, B., R. Dwyer, R. Robicheaux, and J. Simpson. 1992. Influence strategies in marketing channels: Measures and use in different relationship structures. *Journal of Marketing Research 29* (4): 462–473. https://doi.org/10.1177/002224379202900407

Burton-Jones, A. 2009. Minimizing method bias through programmatic research. *Management Information Systems Quarterly 33* (3): 445–471. https://doi.org/10.2307/20650304

Cäker, M. 2008. Intertwined coordination mechanisms in interorganizational relationships with dominated suppliers. *Management Accounting Research 19* (3): 231–251. https://doi.org/10.1016/j.mar.2008.06.003

Chen, I., A. Paulraj, and A. Lado. 2004. Strategic purchasing, supply management, and firm performance. *Journal of Operations Management 22* (5): 505–523. https://doi.org/10.1016/j.jom.2004.06.002

Chin, W. 1998. *The partial least squares approach to structural equation modeling. In Modern Methods for Business Research*, edited by G. Marcoulides, 295–336. Hilldale, NJ: Lawrence Erlbaum Associates.

Chua, W., and H. Mahama. 2007. The effect of network ties on accounting controls in a supply alliance: Field study evidence. *Contemporary Accounting Research 24* (1): 47–92. https://doi.org/10.1506/7156-201W-1290-83H4

Coletti, A., K. Sedatole, and K. Towry. 2005. The effect of control systems on trust and cooperation in collaborative environments. *The Accounting Review 80* (2): 477–500. https://doi.org/10.2308/accr.2005.80.2.477

Colicchia, C., A. Creazza, and D. Menachof. 2019. Managing cyber and information risks in supply chains: Insights from an exploratory analysis. *Supply Chain Management 24* (2): 215–240. https://doi.org/10.1108/SCM-09-2017-0289

Dekker, H. 2003. Value chain analysis in interfirm relationships: A field study. *Management Accounting Research 14* (1): 1–23. https://doi.org/10.1016/S1044-5005(02)00067-7

Diamantopoulos, A., and H. Winklhofer. 2001. Index construction with formative indicators: An alternative to scale development. *Journal of Marketing Research 38* (2): 269–277. https://doi.org/10.1509/jmkr.38.2.269.18845

Diamantopoulos, A., P. Riefler, and K. Roth. 2008. Advancing formative measurement models. *Journal of Business Research 61* (12): 1203–1218. https://doi.org/10.1016/j.jbusres.2008.01.009

Duncan, R. 2019. How to secure your supply chain. *Network Security 2019* (3): 18–19. https://doi.org/10.1016/S1353-4858(19)30038-8

Eaton, T., J. Grenier, and D. Layman. 2019. Accounting and cybersecurity risk management. *Current Issues in Auditing 13* (2): C1–C9. https://doi.org/10.2308/ciia-52419

Emerson, R. M. 1962. Power-dependence relations. *American Sociological Review 27* (1): 31–41. https://doi.org/10.2307/2089716

Emsley, D., and F. Kidon. 2007. The relationship between trust and control in international joint ventures: Evidence from the airline industry. *Contemporary Accounting Research 24* (3): 829–858. https://doi.org/10.1506/car.24.3.7

Fan, Y., and M. Stevenson. 2018. Reading on and between the lines: Risk identification in collaborative and adversarial buyer-supplier relationships. *Supply Chain Management 23* (4): 351–376. https://doi.org/10.1108/SCM-04-2017-0144

Ferrell, O. C. 2011*. Resource-Advantage Theory: The Development Period. Legends in Marketing*: Shelby D. Hunt. Washington, DC: Sage Publishing.

Fornell, C., and D. Larcker. 1981. Evaluating structural equation models with unobservable variables and measurement error*. Journal of Marketing Research 18* (1): 39–50. https://doi.org/10.1177/002224378101800104

Frank, M., J. Grenier, and J. Pyzoha. 2019. How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. *Journal of Information Systems 33* (3): 183–200. https://doi.org/10.2308/isys-52374

Free, C. 2008. Walking the talk? Supply chain accounting and trust among UK supermarkets and suppliers. *Accounting, Organizations and Society 33* (6): 629–662. https://doi.org/10.1016/j.aos.2007.09.001

Ganesan, S. 1994. Determinants of long-term orientations in buyer-seller relationships. *Journal of Marketing 58* (2): 1–19. https://doi.org/10.1177/002224299405800201

Gendron, Y., and M. Barrett. 2004. Professionalization in action: Accountants' attempt at building a network of support for the WebTrust seal of assurance. *Contemporary Accounting Research 21* (3): 563–602. https://doi.org/10.1506/H1C0-EU27-UU2K-8EC8

Gordon, L., M. Loeb, W. Lucyshyn, and L. Zhou. 2015. The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy 34* (5): 509–519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

Hair, J., W. Black, B. Babin, R. Anderson, and R. Tatham. 2010. *Multivariate Data Analysis*. Upper Saddle River, NJ: Pearson Prentice Hall.

Hart, P., and C. Saunders. 1997. Power and trust: Critical factors in the adoption and use of electronic data interchange. *Organization Science 8* (1): 23–42. https://doi.org/10.1287/orsc.8.1.23

Hart, P., and C. Saunders. 1998. Emerging electronic partnerships: Antecedents and dimensions of EDI use from the supplier's perspective. *Journal of Management Information Systems 14* (4): 87–111. https://doi.org/10.1080/07421222.1998.11518187

Hunt, S. 1995. Resource-advantage theory of competition: Toward explaining productivity and economic growth. *Journal of Management Inquiry 4* (4): 317–332. https://doi.org/10.1177/105649269500400403

Hunt, S. 1997a. Competing through relationships: Grounding relationship marketing in resource-advantage theory. *Journal of Marketing Management 13* (5): 431–445. https://doi.org/10.1080/0267257X.1997.9964484

Hunt, S. 1997b. Resource-advantage theory: An evolutionary theory of competitive behavior? *Journal of Economic Issues 31* (1): 59–78. https://doi.org/10.1080/00213624.1997.11505891

Hunt, S. 1997c. Resource-advantage theory and the wealth of nations: Developing the socio-economic research tradition. *Journal of Socio-Economics 26* (4): 335–357. https://doi.org/10.1016/S1053-5357(97)90001-9

Hunt, S. 1999. The strategic imperative and sustainable competitive advantage: Public policy implications of resource-advantage theory. *Academy of Marketing Science Journal 27* (2): 144–159. https://doi.org/10.1177/0092070399272003

Hunt, S. 2000. *A General Theory of Competition: Resources, Competences, Productivity*, Economic Growth. Thousand Oaks, CA: Sage Publications.

Hunt, S., and D. Davis. 2008. Grounding supply chain management in resource-advantage theory. *The Journal of Supply Chain Management 44* (1): 10–21. https://doi.org/10.1111/j.1745-493X.2008.00042.x

Hunt, S., and R. Morgan. 1994. Relationship marketing in the era of network competition. *Marketing Management 3* (1): 19–28.

Hunt, S., and R. Morgan. 1995. The comparative advantage theory of competition. *Journal of Marketing 59* (2): 1–15. https://doi.org/10. 1177/002224299505900201

Jamal, K., M. Maier, and S. Sunder. 2003. Privacy in e-commerce development of reporting standards, disclosure, and assurance services in unregulated markets. *Journal of Accounting Research 41* (2): 285–309. https://doi.org/10.1111/1475-679X.00104

Janvrin, D., and T. Wang. 2019. Editorial: Implications of cybersecurity on accounting information. *Journal of Information Systems 33* (3): A1–A2. https://doi.org/10.2308/isys-10715

Jarvis, C., S. MacKenzie, and P. Podsakoff. 2003. A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *The Journal of Consumer Research 30* (2): 199–218. https://doi.org/10.1086/376806

Johnson, C. 2016. You Outsource the Service but not the Risk: Supply Chain Risk Management for the Cyber Security of Safety Critical Systems. *Proceedings of the 34th International System Safety Conference*, Orlando, FL, August 8–12.

Khazanchi, D., and S. Sutton. 2001. Assurance services for business-to-business electronic commerce: A framework and implications. *Journal of the Association for Information Systems 1* (11): 1–54. https://doi.org/10.17705/1jais.00011

Kline, R. 2005. *Principles and Practice of Structural Equation Modeling*. New York, NY: The Guilford Press.

Kumar, N., L. Scheer, and J. B. E. M. Steenkamp. 1998. Interdependence, punitive capability, and the reciprocation of punitive actions in channel relationships. *Journal of Marketing Research 35* (2): 225–235. https://doi.org/10.1177/002224379803500208

Lavastre, O., A. Gunasekaran, and A. Spalanzani. 2012. Supply chain risk management in French companies. *Decision Support Systems 52* (4): 828–838. https://doi.org/10.1016/j.dss.2011.11.017

Lord, N. 2018. *The history of data breaches*. Available at: https://digitalguardian.com/blog/history-data-breaches

Luo, Y. 2007. The independent and interactive roles of procedural, distributive, and interactional justice in strategic alliances. *Academy of Management Journal 50* (3): 644–664. https://doi.org/10.5465/amj.2007.25526452

Moorman, C., G. Zaltman, and R. Despande. 1992. Relationships between providers and users of marketing research: The dynamics of trust within and between organizations. *Journal of Marketing Research 29* (3): 314–328. https://doi.org/10.1177/002224379202900303

Morgan, R., and S. Hunt. 1994. The commitment-trust theory of relationship marketing. *Journal of Marketing 58* (3): 20–38. https://doi.org/10.1177/002224299405800302

Morgan, R., and S. Hunt. 1999. Relationship-based competitive advantage: The role of relationship marketing in marketing strategy. *Journal of Business Research 46*(3): 281–290. https://doi.org/10.1016/S0148-2963(98)00035-6

Nicolaou, A. 2008. Research issues on the use of ERPS in interorganizational relationships. International *Journal of Accounting Information Systems 9* (4): 216–226. https://doi.org/10.1016/j.accinf.2008.09.003

Nicolaou, A., and D. McKnight. 2006. Perceived information quality in data exchanges: Effects on risk, trust, and intentions to use. *Information Systems Research 17* (4): 332–351. https://doi.org/10.1287/isre.1060.0103

No, W., and M. Vasarhelyi. 2017. Cybersecurity and continuous assurance. *Journal of Emerging Technologies in Accounting 14* (1): 1– 12. https://doi.org/10.2308/jeta-10539

Nunnaly, J., and I. Bernstein. 1994. *Psychometric Theory*. New York, NY: McGraw-Hill.

Olyaei, S., C. Ambrose, and J. Wheatman. 2018. Innovation Insight for Security Rating Services. Stamford, CT: Gartner.

Petter, S., D. Straub, and A. Rai. 2007. Specifying formative constructs in information systems research. *Management Information Systems Quarterly 31* (4): 623–656. https://doi.org/10.2307/25148814

Podsakoff, P., S. MacKenzie, J. Lee, and N. Podsakoff. 2003. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *The Journal of Applied Psychology 88* (5): 879–903. https://doi.org/10.1037/0021-9010.88. 5.879

Ringle, C., S. Wende, and A. Will. 2005. *SmartPLS 2.0 (beta)*. Available at: www.smartpls.de

Seal, W., A. Berry, and J. Cullen. 2004. Disembedding the supply chain: Institutional reflexivity and inter-firm accounting. *Accounting, Organizations and Society 29* (1): 73–92. https://doi.org/10.1016/S0361-3682(02)00055-7

Son, J., S. Narasimhan, and F. Riggins. 2005. Effects of relational factors and channel climate on EDI usage in the customer-supplier relationship. *Journal of Management Information Systems 22* (1): 321–353. https://doi.org/10.1080/07421222.2003.11045839

Soosay, C. A., and P. Hyland. 2015. A decade of supply chain collaboration and directions for future research. *Supply Chain Management 20* (6): 613–630. https://doi.org/10.1108/SCM-06-2015-0217

Spence, M. 1973. Job market signaling. *The Quarterly Journal of Economics 87* (3): 355–374. https://doi.org/10.2307/1882010

Sutton, S. G. 2006. Extended enterprise systems' impact on enterprise risk management. *Journal of Enterprise Information Management 19* (1): 97–114. https://doi.org/10.1108/17410390610636904

Sutton, S., and C. Hampton. 2003. Risk assessment in an extended enterprise environment: Redefining the audit model. *International Journal of Accounting Information Systems 4* (1): 57–73. https://doi.org/10.1016/S1467-0895(03)00010-1

Sutton, S., C. Hampton, D. Khazanchi, and V. Arnold. 2008. Risk analysis in extended enterprise environments: Identification of critical risk factors in B2B e-commerce relationships. *Journal of the Association for Information Systems 9* (4): 151–176. https://doi.org/10.17705/1jais.00155

Sutton, S., V. Arnold, T. Benford, and J. Canada. 2009. *Why Enterprise Risk Management is Vital: Learning from Company Experiences with Sarbanes-Oxley Section 404 Compliance.* Altamonte Springs, FL: Institute of Internal Auditors Research Foundation.

Vosselman, E., and J. van der Meer-Kooistra. 2009. Accounting for control and trust building in interfirm transactional relationships. *Accounting, Organizations and Society 34* (2): 267–283. https://doi.org/10.1016/j.aos.2008.04.002

Yilmaz, C., B. Sezen, and E. Kabaday. 2004. Supplier fairness as mediating factor in the supplier performance-reseller satisfaction relationship. *Journal of Business Research 57* (8): 854–863. https://doi.org/10.1016/S0148-2963(02)00485-X

Zaheer, A., B. McEvily, and V. Perrone. 1998. Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science 9* (2): 141–159. https://doi.org/10.1287/orsc.9.2.141