https://doi.org/10.48009/2_iis_2020_64-74
Issues in Information Systems
Volume 21, Issue 2, pp. 64-74, 2020

TRUST IN SECURITY AS A SERVICE: A THEORETICAL MODEL

Thomas L. Ngo-Ye, Alabama State University, tngoye@alasu.edu
Derek L. Nazareth, University of Wisconsin-Milwaukee, derek@uwm.edu
Jae J. Choi, Pittsburg State University, jchoi@pittstate.edu

ABSTRACT

In the escalating cyber threat environment, limited in-house cybersecurity expertise and resources are prompting organizations to look to security as a service (SECaaS) providers to tackle and manage their security needs, particularly in the cloud-based environment. Given the sensitive nature of the business relationship between customer organizations and SECaaS providers, trust becomes a critical issue for successful SECaaS adoption. In order to succeed in the marketplace, SECaaS providers need to formulate strategies that establish and maintain trust with customers. In this paper, we provide a theoretical analysis of the antecedents of trust in the SECaaS relationship by integrating formal frameworks of interpersonal trust, organizational trust, trust in business relationships, and trust in e-commerce, supplementing it through anecdotal evidence from the literature. This paper advances a conceptual model of the trust formulation in the context of SECaaS adoption. We argue that the successful adoption of SECaaS is dependent on the level of relevant trusting beliefs and attitude in the trust formation process. This paper has implications for theory and highlights the role of trust in the adopting of SECaaS in the cloud computing era.

Keywords: security as a service (SECaaS), trust, trust beliefs, trust attitude, intention to use, cloud computing

INTRODUCTION

The increasing reliance on cloud computing to host enterprise computing and datacenters has attracted the attention of both industry and academia. Cloud computing provides services that are accessible on demand via the web from cloud computing vendors' computer servers instead of being hosted on a client's in-house servers (Kroenke & Boyle, 2016). Since cloud service providers offer Information Technology (IT) infrastructure including hardware, software, network, and IT staff to setup, maintain, and manage cloud services, clients do not need to devote resources for hardware and software, or IT staff to operate cloud services (Kendall & Kendall, 2014). Cloud services have the advantage of making applications, resources, and services easily accessible and dynamically scalable to satisfy the clients' demand (Beal, 2018). Cloud services can be fully managed by cloud services vendors.

Drivers for outsourcing IT operations to the cloud include Internet technology improvement, reduced operation costs, and scalability (Sullivan & Leon, 2002). The advent of cloud services affords an opportunity for organizations to procure more outsourced services. Between 2011 and 2014, cloud computing technology adoption had crossed the inflection point and demonstrated "S shaped" growth pattern with high growth rates (Adamuthe & Thampi, 2019). According to a 2018 InfoWorld survey, 73 percent of organizations surveyed have at least one cloud application or some part of computing infrastructure already in the cloud (IDG Research, 2018). According to Gartner, public cloud revenue is expected to grow 17.3 percent in 2019 (Gartner, 2018), with an increase of business cloud services in the near future. While the market is currently dominated by a few large cloud providers, it is expected that there will shortly be a host of cloud service providers in the future. Customers of cloud computing will need to perform a thorough analysis when determining which cloud services to choose.

Many factors that affect the success of cloud computing have been identified in the literature. Using an agent-based simulation model, the impact of innovation openness and product complexity on cloud computing diffusion and its performance are examined (Choi, Nazareth, & Ngo-Ye, 2017). In an empirical application of the updated Delone and McLean model of Information Systems Success to cloud computing, it was shown that cloud system quality determines IS success (Donovan, Guzman, Adya, & Wang, 2018). In the context of database use in the cloud environment, public or shared infrastructure of the Internet has been shown to be a contributing factor to poor performance of relational databases (Litchfield, Althwab, & Sharma, 2018). Security, privacy, and provider reputation are considered among the most important factors for cloud service providers' survival. At the individual user level,

prior online experience and fraud exposure were found to be determinants of online privacy concern (Gupta & Chennamaneni, 2018). This study used the theory of reasoned action (TRA) to assess determinants of online privacy protection behavior. In addition, trust violations and reconciliation activity were found to influence the trustworthiness of cloud service providers, through the use of a Dynamic Security-Trust lifecycle model (Ngo-Ye, Nazareth, & Choi, 2017). Clearly, the move from on-site computing to an external provider raises concerns about security, privacy, and trust in the new relationship.

Security as a Service (SECaaS)

Cybersecurity has become an increasingly critical issue for both public and private organizations in the ever-changing landscape of alternative computing provisioning. Securing a company's IS assets includes many interrelated issues: confidentiality, integrity, availability, controls, intrusion detection systems, intrusion prevention systems, wired and wireless network security, host security, malware protection, risk management, business continuity, operational security, and cryptography, among others (Gibson, 2017).

The concept of Security as a service (SECaaS) was first proposed by Hussain & Andulsalam (2011), as a means of securing cloud-based applications. Using an SOA-based architecture, they proposed the use of a Security Manager to integrate applications across multiple secure clouds. The Security Manager provided rudimentary services including selection and configuration of security services as well as single sign-on assistance. Security services could include access control, auditing, risk assessment, intrusion detection, and the like. SECaaS was primarily a conceptual proposal at this stage. It is a sub-category of "software as a service (SaaS)", focusing on security related services (Dobran, 2018). In essence, with the SECaaS model, a customer organization outsources all security activities and services to an outside provider, who handles and manages security for the customer (Brook, 2018). Compared to other types of common cloud computing services, instead of offering access to platform, tool, or application, SECaaS providers offer protection for an organization's data, apps, and operations that run in the cloud (Peterson, 2016). Some common security services include using an anti-virus software over the Internet, anti-malware/spyware, authentication, intrusion detection and management, penetration testing, security analysis, email monitoring, data loss prevention, data encryption, web security, business continuity, disaster recovery, access and identity management, compliance, and security information event management (Dobran, 2018; Brook, 2018).

The rise of SECaaS can be attributed to several factors. First, for most organizations, in-house IT operations can be costly, time-consuming, and error-prone. Installing, maintaining, updating, and patching software, dynamically scaling the platform, and securing data storage are expensive (Dobran, 2018). Like SaaS, when considering the total cost of ownership, using SECaaS involves lower cost than if those security services are provided by the organization (Brook, 2018; Peterson, 2016). Second, the number and forms of external cybersecurity threats is constantly increasing, and it is proving more challenging for IT personnel to effectively fend off attacks from multiple sources (Dobran, 2018; Brook, 2018). The overall damages sustained through cybercrime was estimated to be $3 trillion in 2015 and is expected to double to $6 trillion by 2021 (Dobran, 2018). Third, the shortage of security expertise and resources, especially among small and medium size companies, poses a serious challenge that is only expected to worsen (Brook, 2018; Dobran, 2018).

SECaaS brings many benefits for organizations. First, using SECaaS enables organizations to cut cost and make budgeting more friendly by replacing expensive upfront capital expenditure with lower monthly subscription fees (Wexler, 2017; Brook, 2018). Second, SECaaS providers are more likely to stay current and deploy new technology and latest updates faster than most organizations (Dobran, 2018; Wexler, 2017; Brook, 2018). Therefore, SECaaS customers always have the most updated and latest security tools available (Brook, 2018). Third, SECaaS offers consistent, uniform, and continued protection. For example, SECaaS customers receive constant virus definition updates, which remove reliance on customers' compliance. Fourth, by outsourcing security related tasks to SECaaS providers that have considerable expertise and experience, organizations can concentrate on their core business competencies (Wexler, 2017; Brook, 2018).

The adoption rate of SECaaS is ramping up noticeably. By some estimates, SECaaS accounts for the second biggest slice of cloud computing services spending, behind only Infrastructure as a Service (IaaS) (Wexler, 2017). In 2016, the SECaaS market was already more than $3 billion and it is expected to exceed $8 billion by 2020 (Peterson, 2016; Wexler, 2017). Clearly, SECaaS has become a mainstay in the cloud computing market.

Services provided under SECaaS vary widely. Table 1 lists some of the categories of SECaaS services. Note that the classifications are not comprehensive.

Table 1. SECaaS Categories

Cloud Security Alliance (Cloud Security Alliance, 2016)	**Peterson (Peterson, 2016)**
• Business Continuity and Disaster Recovery • Continuous Monitoring • Data Loss Prevention • Email Security • Encryption • Identity and Access Management (IAM) • Intrusion Management • Network Security • Security Assessments • Security Information and Event Management • Vulnerability Scanning • Web Security	• Cloud Access Security Brokerage • Single Sign-On • Email Security • Website and App Security • Network Security

For SECaaS providers to be favored for outsourcing of security services, one of the primary challenge is to create and maintain a stellar reputation, while also demonstrating their superiority over traditional security services. Given that SECaaS customers have to rely on security applications and services beyond their direct control, trust plays an important role in the adoption of SECaaS. Trust would ultimately determine which SECaaS are used and which are not. Hence, in the race to expand market share of SECaaS providers, whether or not a SECaaS provider can gain trust from customers will likely influence its success or failure. Logically, we raise the following research questions:

What factors affect the customer trust towards SECaaS providers?

Would the trust towards SECaaS providers affect customer intention to use the SECaaS?

To answer these questions, we examine the extant literature and construct a conceptual framework grounded in trust theories while incorporating specific aspects of SECaaS.

We organize the paper in the following manner. In the next section, we introduce the theoretical background of this study. Then we propose a research model and several propositions. Finally, we discuss the implementations of the study, along with potential contributions to theory and practice.

THEORETICAL BACKGROUND

Trust Definition

The focus of this research is to investigate customer trust towards a SECaaS provider. First, we need to address the concept of trust. The definition of trust proposed by Mayer, Davis, and Schoorman's (1995) is a widely accepted definition. According to Mayer et al., trust is "the willingness of a party [trustor] to be vulnerable to the action of another party [trustee] based on the expectation that the other [trustee] will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party [trustee]" (Mayer, Davis, & Schoorman, 1995, p. 712). We adopt their definition of trust in this paper. Trust is recognized as an important construct in the contexts of e-commerce adoption (Ba & Pavlou, 2002; Gefen, Karahanna, & Straub, 2003) as well as innovative technology adoption, such as data mining (Ngo-Ye & Choi, 2013). In these cases, trustors are individuals, while the trustee is often an organization. In the context of trust involving SECaaS, the trustor represents a customer (usually a firm) that needs to judge if a SECaaS provider is trustworthy. Even though the trust appears to be the trust between two organizations, it is frequently an individual in the organization, rather than the organizations themselves, who trusts (Zaheer, McEvily, & Perrone, 1998). Thus, the decision-making individuals of the customer organization (CEO,

CIO, or other managers who make decisions about the use of SECaaS) are identified as trustors in this setting. The trustees in this case will be the SECaaS providers.

Trust Conceptualization

Previous studies have conceptualized trust in many different ways. We are especially interested in the conceptualizations in the e-commerce and business relationship contexts because they are the most relevant to the scenario where a customer trusts a SECaaS provider. The literature on trust spans multiple domains including interpersonal trust, institutional trust, organizational trust, political trust, technological trust, among others. These constructs have roots in psychology, sociology, technology, and economics, among others. For this paper, we restrict trust conceptualizations to those that occur in the e-commerce and business contexts. The genesis of e-commerce trust is rooted in the buyer-seller relationship. We describe the various characterizations of trust and its evolution in the e-commerce context. Schurr and Ozanne (1985) conceptualize trust as belief that promises are reliable and obligations will be fulfilled in the context of buyer-seller relationships. Zucker (1986) theorizes trust as a set of expectations and an implicit contract in the setting of business relationships. Crosby, Evans, and Cowles (1990) conceptualize trust as confidence that the trusted party will behave in the interest of the customer in the context of buyer-seller relationships. Anderson and Narus (1990) theorize trust as expectations about the behavior of the other company in the setting of business relationships. Morgan and Hunt (1994) conceptualize trust as willingness to depend on a party in whom one has confidence in the context of business relationships. Gulati (1995) theorizes trust as expectations that alleviate fear that the other party will be opportunistic in the setting of business relationships. Kumar (1996) conceptualizes trust as belief in dependability and honesty in the context of business relationships. Hart and Saunders (1997) theorize trust as confidence about the behavior and goodwill of others in the setting of business relationships. Zaheer, McEvily, and Perrone (1998) conceptualize trust as the expectation that an actor will fulfill its obligations, be predictable, and be fair and not opportunistic in the context of buyer-supplier relationships. Jarvenpaa, Tractinsky, and Saarinen (1999) theorize trust as willingness to rely when there is vulnerability in the setting of e-commerce. Gefen (2002) conceptualizes trust as willingness to depend based on beliefs in ability, benevolence, and integrity in the context of business relationships.

In sum, researchers regard trust as [1] a set of specific beliefs dealing mainly with integrity, benevolence, and capability of another actor (e.g., (Doney & Cannon, 1997)); [2] a general belief that the other actor can be trusted (e.g., (Zucker, 1986)), sometimes also referred as trusting intentions (McKnight, Cummings, & Chervany, 1998); [3] affect reflected in "feelings" of security and confidence in the caring response of the other actor.

RESEARCH MODEL AND PROPOSITIONS

We regard trust as an attitude that is shaped by decision makers' beliefs that a SECaaS provider will behave in specific ways. We then investigate the process by which the decision makers generate their trusting attitude towards a SECaaS provider. The theory of reasoned action (TRA) (Fishbein & Ajzen, 1975) forms the primary theoretical basis of most of the research on attitude formation. Our current study will take a similar approach. As stated by TRA, an individual's behavior is influenced by one's behavioral intention. Attitude towards a behavior affects one's behavioral intention, and the attitude is in turn the function of beliefs. The underlying logic of TRA is the chain of Beliefs → Attitude → Intention → Behavior. Employing the logic espoused by TRA, we argue that the strength of the trusting attitude depends on one's trust related beliefs about a SECaaS provider, and the trust attitude in turn affects their intention to use the SECaaS products and services from the SECaaS provider. Based on our literature review, three forms of beliefs shape the trust attitude: knowledge-based, institution-based, and calculative-based. In the setting of SECaaS trust, quality of service is also a very important subject. Hence, service-quality-based beliefs are also incorporated in the model.

Trust Consequences – Intention to Use

DeLone and McLean (2003) treat intention to use as one of the dependent variables for measuring IS success. The other measurements for IS success include use, user satisfaction, and net benefits (DeLone & McLean, 2003). Since the use of SECaaS is still in a relatively early stage of adoption, actual use, user satisfaction, and net benefits are difficult to examine. Hence this study only concentrates on intention to use as a consequence of the trust attitude. In addition, this permits investigation of potential customers and entities considering using SECaaS, rather than being

limited to current and mature users. Based on the existing literature, we argue that higher level of trust toward SECaaS providers is associated with higher level of intention to use. Generally speaking, trust is a critical antecedent of participation in commerce, and even more important in online settings due to the greater ease with which a vendor (a SECaaS provider in this case) can behave in an opportunistic way (Reichheld & Schefter, 2000). Trust also helps decrease the ambivalence a customer faces when inconsistent signals are received from the SECaaS provider. In this manner trust encourages the intention to use SECaaS. Hence, we propose:

Proposition 1: Trust in a SECaaS provider will positively influence intention to use SECaaS offered by the SECaaS provider.

Antecedents of Trust

Past research on trust has identified a number of antecedent trust beliefs: knowledge-based trust, institution-based trust (specifically, situational normality beliefs and structural assurance beliefs), calculative-based trust, cognition-based trust (specifically, illusion of control processes and categorization processes), and personality-based trust (specifically, faith in humanity and a trusting stance). The first three are most relevant for SECaaS trust and will be discussed in some detail.

Knowledge-based Beliefs:

Familiarity with a SECaaS Provider

Familiarity is experience with the what, who, when, and how is it happening (Gefen, Karahanna, & Straub, 2003). Familiarity decreases social uncertainty through improved understanding of what is happening in the present (Luhmann, 1979). Familiarity with the manner in which the business partners work and their limitations is also a major antecedent of trust in ongoing business interactions (Kumar, 1996). Familiarity offsets concerns that the other actor may be opportunistic, based on a belief derived from past joint activities when that did not happen (Gulati, 1995). Doney, Cannon, and Mullen (1998) refer to familiarity as a prediction process and argue that trust is created in the process when the trustor's knowledge about the other party enables it to predict the behavior of the other party. Thus, we propose:

Proposition 2: Familiarity with a SECaaS provider will positively influence trust in the SECaaS provider.

Reputation of a SECaaS Provider

Because trust needs to occur before the trustors obtain first-hand knowledge about a specific SECaaS provider, second-hand knowledge, such as reputation, has substantial impacts on the formation of trust. Schoolman, Mayer, and Davis (1996) recommend approaching trust related studies from a social influence aspect. McKnight, Cummings, and Chervany (1998) maintain that reputation may reflect professional competence, benevolence, honesty, and predictability. Prior studies have shown that reputation has substantial influence on trust in online stores (e.g. (Doney & Cannon, 1997; Jarvenpaa, Tractinsky, & Saarinen, 1999)). It is expected that risks associated with SECaaS is greater than risks for purchasing products from online stores because the customer firms have to share sensitive data with the SECaaS providers and rely on them for continued successful operation. It stands to reason that it is hard for customer firms to trust a provider that they have never heard of, or those with a poor reputation. The providers with good reputation will likely garner more trust from customers. Reputation, in this case, is far more involved that a simple rating system, like those used in eBay, or the use of trust seals on a website. Instead, a customer needs to do their due diligence in verifying a SECaaS provider's reputation. Irrespective of how reputations are formed and measured, a good reputation is expected to have substantial influence on the customers' trust towards the SECaaS provider. Based on the analysis put forward, we propose:

Proposition 3: Positive reputation of a SECaaS provider will positively influence trust in the SECaaS provider.

Institution-based Beliefs:

Institution-based trust encompasses one's beliefs about the essential impersonal structures that can allow one to act with expectation of a successful future endeavor (Shapiro, 1987; Zucker, 1986). There are two kinds of institution-based trust: situational normality and structural assurance. Situational normality refers to an appropriately ordered setting that is likely to help a successful interaction (McKnight, Cummings, & Chervany, 1998), which indicates the presence of a normal working structure. In the setting of using SECaaS, situational normality means that the customers expect to see SECaaS products and services that are well designed, provide robust coverage, utilize prevailing standards and protocols, and so on. The maturity of the SECaaS technology also forms part of the situational normality. Before the protocols, and platforms and standards emerge and mature, SECaaS applications development will be chaotic and piecemeal making it harder to achieve high levels of situational normality. Structural assurance refers to the presence of well-established social infrastructure, or the existence of regulations, guarantees, and legal recourse (McKnight, Cummings, & Chervany, 1998). Structural assurance is essential in the setting of using SECaaS, given the high stakes involved in compromised cloud operations. The establishment of regulations and laws is crucial to the formation of the customers' trust in the SECaaS providers. Therefore, we propose that:

Proposition 4: Perceptions of situational normality will positively influence trust in a SECaaS provider.

Proposition 5: Perceptions of structural assurances will positively influence trust in a SECaaS provider.

Calculative-based Risk Beliefs:

The calculative-based aspect of trust concentrates on the risks and benefits of the trusting behavior. Perceived risk is crucial in forming interpersonal, economic, and social relationships (Chiles & McMackin, 1996). In the SECaaS setting, there is a clear economic relationship between the SECaaS providers and the customers. In this relationship, both parties attempt to minimize risks and maximize their utility associated with the relationship. Customers anticipate benefiting from the use of SECaaS through enhanced security, compliance, efficiency, cost reduction, better integration, etc. However, the benefits of using SECaaS may be offset by additional risks, since there are now multiple parties in the context whose independent but interrelated resources are now at risk, including the cloud provider, the SECaaS provider, and the customer. Threats aimed at the SECaaS provider include: hacking the domain name service network server; lying about identity, etc. (Ratnasingam, 2002); spoofing an application; denial of service, particularly flood attacks that could compromise a SECaaS website, resulting in denial of service to legitimate users.

Risks faced by the cloud provider include all of the above, plus availability issues, reliability problems, poor performance, inadvertent exposure, among others. Risks and threats directed at the customer IT resources include hacking, denial of service, malware introduction, SQL injection, data compromise, among others. In the context of SECaaS trust, perceived security risks introduced through the use of a SECaaS provider will erode the customers' trust towards the SECaaS provider. Hence, we propose:

Proposition 6: Calculative-based risk beliefs will negatively influence trust in a SECaaS provider.

Service-quality-based Beliefs:

As stated by DeLone and McLean (2003), service quality is one of the critical factors that affect IS success. The importance of service quality "is most likely greater than previously since the users are now our customers and poor user support will translate into lost customers and lost sales" (DeLone & McLean, 2003). SECaaS provider needs to provide high-quality services to support customers' routine business operations and ensure security of customer's IS, network, and data. Undoubtedly the quality of services is one of the major decision factors of customers' choice of SECaaS providers. The customers' trust in the SECaaS provider cannot be detached from the service quality. Quality of Service (QoS) remains a prominent aspect of cloud computing. There are many dimensions to QoS. Ran (2003) offers a comprehensive assessment of QoS, classifying the aspects into four categories:

- Configuration management and cost related QoS: include cost, regulatory, supported standard, stability/change cycle, and completeness

- Runtime related QoS: include capacity, scalability, reliability, performance, availability, robustness/flexibility, exception handling, and accuracy
- Security related QoS: include confidentiality, authentication, authorization, accountability, and data encryption and non-repudiation
- Transaction support related QoS: integrity

All the categories presented above have an impact on the trust in the SECaaS. Since this study focuses on initial trust formation, when customers work with SECaaS providers on a trial basis, a limited subset of these that are applicable. We argue that there are five aspects of service-quality-related trust issues in a SECaaS:

- Trust in Identity – Confidence that the SECaaS providers are who they say they are
- Service Availability – 24/7 availability of SECaaS and network connection
- Security / Privacy – SECaaS provider does not spy on (or mess with) customers' data
- Response to Failure – When something goes wrong, how customers can reach the SECaaS provider, and how will the situation be handled? What recourse is available?
- Trust in Program Code: Error-free program code, with all the features SECaaS provider promises and also does not change without warning

Given the significance of service quality on customers' decision-making, we propose:

Proposition 7: Service-quality-related beliefs will positively influence trust in a SECaaS provider.

Using the accumulation of the propositions, we assemble a conceptual model of trust in a SECaaS provider, as depicted in Figure 1.

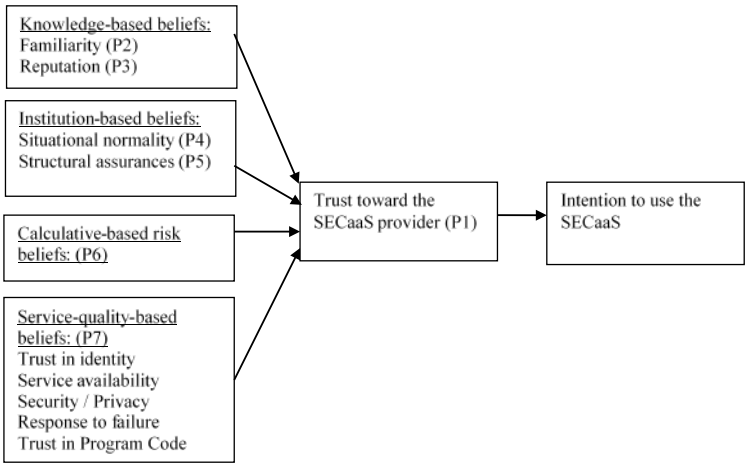

Figure 1. Conceptual Model of Trust in SECaaS

IMPLICATIONS OF THE CONCEPTUAL TRUST MODEL

The cloud services framework makes it possible to implement a standards-based service-oriented computing paradigm, which fundamentally transforms the way companies conduct their business (Curbera, Khalaf, Mukhi, Tai, & Weerawarana, 2003). Fully integrated enterprises are being replaced by business networks in which each participant member provides the others with specialized services. Traditional IT infrastructures and applications managed and owned by one company are giving way to networks of applications/services owned and managed by many business partners. In the cloud computing era, trust is critical because the risks customers encounter are much greater than before given the fact that services and applications will be run at a remote site, sensitive business data will be transmitted back and forth on public networks, and customer is at the mercy of the cloud provider and the SECaaS provider for effective and robust operation.

Drawing from the literature on trust in e-commerce, and adapting it to the cloud computing context, a conceptual model of trust in the emerging area of SECaaS is assembled. Using the theory of reasoned action, relevant antecedents and consequents of SECaaS trust are identified. Testing the model will provide significant implications for SECaaS providers. First, it will identify which antecedents are important in trust formation, particularly in the initial stages of SECaaS adoption. This will allow SECaaS providers to promote their strengths in terms of attracting new customers. Given that multiple antecedents are likely important in trust formation, identification of their relative importance affords SECaaS providers to set themselves apart from other providers. Furthermore, it is likely that SECaaS providers will have a mix of strengths and weaknesses. Results from this research will provide them an opportunity to identify where to put their efforts and resources in order to become a more attractive provider to customers. Building and maintaining trust among customers is likely to be critical for SECaaS providers.

It is important to note that though cost is an important QoS measure, this model does not include cost in the trust formation process. The general sentiment in the security discipline is that improved security entails additional cost, though the correlation is not perfect, i.e. a more expensive solution is not necessarily more secure. As a result, trust will be shaped more by provider characteristics, situational factors, environmental factors, and product characteristics. Cost will eventually be factored into the selection decision, but more likely as a tradeoff between multiple competing objectives.

FUTURE DIRECTIONS

Constructing and validating the instrument, designing and administering the survey, and analyzing and writing up the results represent the next subsequent in this research. Constructs in the model will be measured through Likert-style items. Standard psychometric techniques for instrument validation will be employed. The instrument will be examined by a panel of experts from industry and academia for face validity and completeness. Any wording issues or ambiguity concerns will be addressed at this stage. Next, a pilot study will be conducted to ascertain convergent and discriminant validity of the constructs. This exercise will refine the measures by dropping problematic items from the measures, when warranted. The research model will be tested through a field survey. Potential participants are CIOs and managers tasked with making decisions about information security in the organization. Small to medium sized enterprises will be targeted, as they are the likely customers for SECaaS services. Since the research includes trust formation, target participants include organizations that are seeking to move to a cloud environment as well as those cloud users seeking to acquire SECaaS services. Partial Least Square (PLS) will be used to analyze the data. PLS is an appropriate technique for fitting complex predictive models, and can simultaneously analyze the strengths and directions of the relationships among the constructs in the structural model, and tests the psychometric properties of the scales used to measure the constructs in the measurement model.

A preliminary measure of trust in an SECaaS provider can be assembled from items in prior trust instruments on e-commerce (Gefen et al 2003), organization relations (Hon & Grunig, 1999), and supplemented by novel items specific to SECaaS providers. Candidate items include:

- This SECaaS provider can be relied on to keep its promises.
- I feel very confident about this SECaaS provider's skills.
- This SECaaS provider does not mislead people like me.
- I am willing to let this SECaaS provider manage information security for me.
- This SECaaS provider has a proven track record
- I have faith in dealing with this SECaaS provider.

In conclusion, the emphasis of this research is the trust formation in the early state of adopting Security as a Service. Future research can be conducted to explore the dynamics of trust-building over time as customers continue to use Security as a Service. Customer trust in SECaaS will likely be updated through continuous interaction, affecting their intention to use the SECaaS, and their decision to stay with same SECaaS provider or switch to another provider.

REFERENCES

Adamuthe, A., & Thampi, G. (2019). Short Term and Long Term Forecasting Of Cloud Computing Using Multiple Indicators. *Journal of Information Technology Management, XXX*(1), 14-24. Retrieved May 6, 2019, from http://jitm.ubalt.edu/XXX-1/article2.pdf

Anderson, J. C., & Narus, J. A. (1990). A model of distributor firm and manufacturer firm working partnerships. *Journal of Marketing, 54*(1), 42-58.

Ba, S., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS Quarterly, 26*(3), 243-268.

Beal, V. (2018). *Cloud Service.* Retrieved December 21, 2018, from Webopedia: https://www.webopedia.com/TERM/C/cloud_services.html

Brook, C. (2018, December 5). *What is Security as a Service? A Definition of SECaaS, Benefits, Examples, and More.* Retrieved May 3, 2019, from digitalguardian.com: https://digitalguardian.com/blog/what-security-service-definition-secaas-benefits-examples-and-more

Chiles, T. H., & McMackin, J. F. (1996). Integrating variable risk preferences, trust, and transactions cost economics. *Academy of Management Review, 21*(1), 73-99.

Choi, J., Nazareth, D. L., & Ngo-Ye, T. L. (2017). The Effect of Innovation Characteristics on Cloud Computing Diffusion. *Journal of Computer Information Systems*. doi:10.1080/08874417.2016.1261377

Cloud Security Alliance. (2016). *Defined Categories of Security as a Service (Preview) – Continuous Monitoring as a Service.* Retrieved October 9, 2019, from Cloud Security Alliance: https://downloads.cloudsecurityalliance.org/assets/research/security-as-a-service/csa-categories-securities-prep.pdf

Crosby, L. A., Evans, K. R., & Cowles, D. (1990). Relationship quality in services selling: An interpersonal influence perspective. *Journal of Marketing, 54*(7), 68-81.

Curbera, F., Khalaf, R., Mukhi, N., Tai, S., & Weerawarana, S. (2003). The next step in Web services. *Communications of the ACM, 46*(10), 29-34.

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten year update. *Journal of MIS, 19*(4), 9-30.

Dobran, B. (2018, May 29). *SECaaS: Why Security as a Service is a Trend To Watch.* Retrieved May 3, 2019, from phoenixnap.com: https://phoenixnap.com/blog/secaas-security-as-a-service

Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer-seller relationships. *Journal of marketing, 61*(1), 35-51.

Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the influence of national culture on the development of trust. *Academy of Management Review, 23*(3), 601-620.

Donovan, E., Guzman, I. R., Adya, M., & Wang, W. (2018). A Cloud Update of the DeLone and McLean Model of Information Systems Success. *Journal of Information Technology Management, XXIX*(3), 23-34. Retrieved May 6, 2019, from http://jitm.ubalt.edu/XXIX-3/article3.pdf

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research.* Reading, MA, U.S.A.: Addison-Wesley.

Gartner. (2018, September 12). *Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019.* Retrieved December 21, 2018, from Gartner: https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019

Gefen, D. (2002). Nurturing clients' trust to encourage engagement success during the customization of ERP systems. *Omega, 30*(4), 287-299.

Gefen, D., Karahanna, E., & Straub, D. W. (2003, March). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51-90.

Gibson, D. (2017). *CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide* (4th ed.). YCDA, LLC.

Gulati, R. (1995). Does familiarity breed trust? The implications of repeated ties for contractual choice in alliances. *Academy of Management Journal, 38*(1), 85-112.

Gupta, B., & Chennamaneni, A. (2018). Understanding Online Privacy Protection Behavior of the Older Adults: An Empirical Investigation. *Journal of Information Technology Management, XXIX*(3), 1-13. Retrieved May 6, 2019, from http://jitm.ubalt.edu/XXIX-3/article1.pdf

Hart, P., & Saunders, C. (1997). Power and trust: Critical factors in the adoption and use of electronic data interchange. *Organizational Science, 8*(1), 23-42.

Hon, L. C., & Grunig, J. E. (1999). *Guidelines for Measuring Relationships in Public Relations.* University of Florida. Gainesville, Florida: The Institute for Public Relations. Retrieved June 29, 2020, from https://www.instituteforpr.org/wp-content/uploads/Guidelines_Measuring_Relationships.pdf

Hussain, M., & Abdulsalam, H. (2011). SECaaS: Security as a Service for Cloud-based Applications. *Second Kuwait Conference on e-Services and e-Systems*, (pp. 1-4). Kuwait. doi:10.1145/2107556.2107564

IDG Research. (2018, August 15). *Cloud computing 2018: How enterprise adoption is taking shape.* Retrieved December 21, 2018, from Infoworld: https://www.infoworld.com/article/3297397/cloud-computing/cloud-computing-2018-how-enterprise-adoption-is-taking-shape.html

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication, 5*(2), 1-34.

Kendall, K. E., & Kendall, J. E. (2014). *Systems Analysis and Design* (9th ed.). Upper Saddle River, New Jersey, U.S.A.: Pearson.

Kroenke, D. M., & Boyle, R. J. (2016). *Experiencing MIS* (7th ed.). Upper Saddle River, New Jersey, U.S.A.: Pearson.

Kumar, N. (1996). The power of trust in manufacturer-retailer relationships. *Harvard Business Review, 74*(6), 93-106.

Litchfield, A. T., Althwab, A., & Sharma, C. (2018). Distributed Relational Database Performance In Cloud Computing: An Investigative Study. *Journal of Information Technology Management, XXIX*(1), 16-46. Retrieved May 6, 2019, from http://jitm.ubalt.edu/XXIX-1/article2.pdf

Luhmann, N. (1979). *Trust and Power.* Chichester, England: John Wiley & Sons.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995, July). An integrative model of organizational trust. *The Academy of Management Review, 20*(3), 709-734.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review, 23*(3), 473-490.

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing, 58*(3), 20-38.

Ngo-Ye, T. L., Nazareth, D. L., & Choi, J. J. (2017). Trust in Cloud Computing: Maintaining Long-Term Relationships. *Journal of Information Technology Management, XXVIII*(3), 25-38. Retrieved May 6, 2019, from http://jitm.ubalt.edu/XXVIII-3/article2.pdf

Ngo-Ye, T., & Choi, J. (2013, June). Novice User's Trust on Innovative Technology: A Theoretical Analysis in the context of Data Mining. *International Journal of Intelligent Information Processing, 4*(2), 34-44. doi:10.4156/ijiip.vol4.issue2.4

Peterson, A. (2016, July 18). *Top 5 Security-as-a-Service Providers.* Retrieved May 3, 2019, from technologyadvice.com: https://technologyadvice.com/blog/information-technology/top-5-security-as-a-service-providers/

Ran, S. (2003). A model for web services discovery with QoS. *ACM SIGecom Exchanges, 4*(1), 1-10.

Ratnasingam, P. (2002). The importance of technology trust in web services security. *Information Management and Computer Security, 10*(5), 255-260.

Reichheld, F. F., & Schefter, P. (2000). E-loyalty: Your secret weapon on the Web. *Harvard Business Review, 78*(4), 105-113.

Schoolman, F. D., Mayer, R. C., & Davis, J. H. (1996). Social influence, social interactions, and social psychology in the study of trust. *Academy of Management Review, 21*(2), 337-379.

Schurr, P. H., & Ozanne, J. L. (1985). Influences on exchange processes: Buyers' preconceptions of a seller's trustworthiness and bargaining toughness. *Journal of Consumer Research, 11*(3), 939-953.

Shapiro, S. P. (1987). Policing trust. In C. D. Shearing, & P. C. Stenning, *Private Policing* (pp. 194-220). Newbury Park, CA, U.S.A.: Sage Publications.

Sullivan, T., & Leon, M. (2002). A second chance for outsourcing. *InfoWorld, 24*(2), 32-35.

Wexler, S. (2017, January 17). *Why Security-as-a-Service is Poised to Take Off.* Retrieved May 3, 2019, from cio.com: https://www.cio.com/article/3156291/why-security-as-a-service-is-poised-to-take-off.html

Zaheer, A., McEvily, B., & Perrone, V. (1998). Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science, 9*(2), 141-159.

Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure: 1840-1920. In B. M. Staw, & L. L. Cummings (Eds.), *Research in Organizational Behavior* (pp. 53-111). Greenwich, CT: JAI Press.