Communications of the Association for Information Systems

Volume 38 Article 8

1-2016

A Broader View of Perceived Risk during Internet Transactions

James Lee Jr.
Mississippi State University, jim.lee@esalota.com

Merrill Warkentin
Mississippi State University

Allen C. Johnston
University of Alabama at Birmingham

Recommended Citation
Lee, James Jr.; Warkentin, Merrill; and Johnston, Allen C. (2016) "A Broader View of Perceived Risk during Internet Transactions," *Communications of the Association for Information Systems*: Vol. 38 , Article 8.
DOI: 10.17705/1CAIS.03808
Available at: http://aisel.aisnet.org/cais/vol38/iss1/8

Communications of the Association for Information Systems

Research Paper ISSN: 1529-3181

A Broader View of Perceived Risk during Internet Transactions

James Lee, Jr.
Mississippi State University
jim.lee@esalota.com

Merrill Warkentin
Mississippi State University

Allen C. Johnston
University of Alabama at Birmingham

Abstract:

Ubiquitous networking facilitates Internet access across multiple network environments, whose value is tied directly to user perceptions of its ability to securely execute transactions. Prior research has cited awareness, trust, and risk as critical determinants of adoption but has failed to examine these factors as they relate to infrastructure and its provider. Because information in transit is at risk from a network environment's vulnerabilities, we focus on the implications of such risk on Internet activities. We examine the multiple parties that must be trusted to complete and facilitate an online transaction. We propose that the user must trust not only the information recipient to act benevolently but also the technologies and organizations that facilitate the online exchange.

Keywords: Information Security, Ubiquitous Networking, Perceived Risk, Network Trust, Network Environment.

This manuscript underwent peer review. It was received 06/18/2013 and was with the authors for 10 months for 2 revisions. The Associate Editor chose to remain anonymous.

1 Introduction

Stephen is sipping his latte in front of his computer at his favorite coffee shop. He frequents this coffee shop because they provide great lattes and free Wi-Fi. Tomorrow is Valentine's Day, and he decides to order his wife flowers from a popular Web retailer. He has used this retailer before and he trusts that they will deliver his flowers on time and protect his personal information. With little effort, he navigates to the retailer's website, selects a beautiful arrangement, enters in shipping and payment information, completes the purchase, and thinks he has secured a nominee for husband of the year. Unfortunately for Stephen, Erica knew that online flower sales traditionally elevate the day before Valentine's Day, so she spoofed the coffee shop's wireless network and waited for someone to browse to that particular flower vendor. Despite Stephen's best efforts to use a trusted Web retailer that used secure protocols, Erica was able to capture Stephen's sensitive information. Once Stephen gets back to work, things will get much worse. Erica also surreptitiously installed a virus that spreads throughout networked machines on the same domain.

This story illustrates how one network environment's vulnerabilities can compromise the security of another network environment. A network environment encompasses the organizations providing Internet connectivity, the physical location and surroundings, network architecture, and hardware infrastructure, and each contribute to the environment's security profile. Network environments include workplaces, schools, homes, public locations (coffee shops, restaurants, public libraries, etc.), and anywhere with cellular access, and each has unique security characteristics that vary the amount of risk to transmitted information (Hansman & Hunt 2005; Straub & Welke 1998). Information in transit over any of these networks is vulnerable to compromise at the point of origination through the network infrastructure to the intended or unintended recipient.

Lee et al. (2013) have developed a simplified diagram of the parties involved with online communications (see Figure 1). It portrays the data-handling nodes that are potential targets of hacker attacks. The "active parties" are human agents that can use the information: the sender, receiver, hackers, or a secondary recipient. Information is transmitted through "passive parties" (the sender's local area network (LAN), internet service provider, telecom service provider, recipient's LAN). Passive parties manage the infrastructure required to transmit data. Both "active" and "passive" parties use information technology (IT) artifacts to achieve their individual goals. IT artifacts are "bundles of material and cultural properties packaged in some socially recognizable form such as hardware and/or software" (Orlikowski & Iacono, 2001, p. 121). Information "senders," "recipients," and "secondary recipients" use end devices (e.g., laptops, mobile phones, tablets, etc.) and LANs. "LAN providers" manage the hardware and software (e.g., Wi-Fi access points, switches, routers, etc.) required to provide LAN services. The "internet service providers" and "telecom service providers" operate the infrastructure, backbone, and routing systems that interconnect the LANs. (Tarasewich & Warkentin, 2000; Tarasewich, Nickerson, & Warkentin, 2002) "Hackers" exploit IT artifact vulnerabilities with IT artifacts that provide attack vectors (e.g., promiscuous network interface controllers, malware, penetration testing software, etc.) to intercept the information at any of these points (Hansman & Hunt 2005). While each of these parties play an important role in enabling an online transaction, general users may not be cognizant of the internet service providers or the telecom service providers. Therefore, this research focuses on how users view the LAN environment to form intentions and execute online transactions.

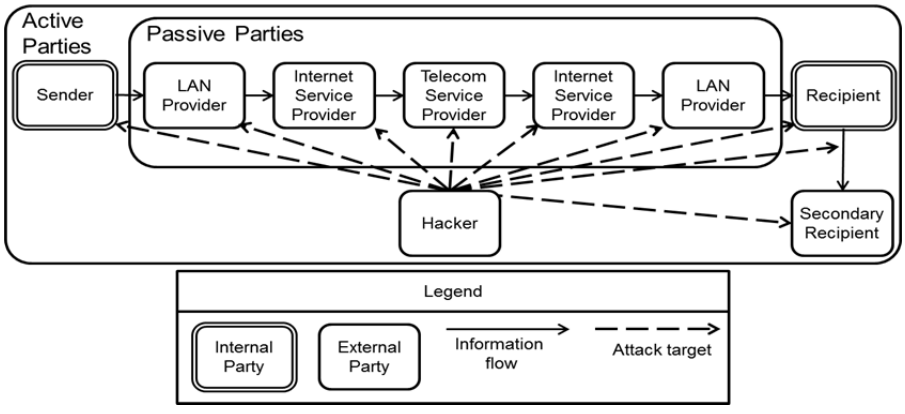

Figure 1. Information Flow and Attack Targets

1.1 LAN Attack Vectors

Lee et al.'s (2013) model describes where information is susceptible to an attack, but it does not describe how the information is susceptible. The goal of computer security is to maintain confidentiality, integrity, and availability of information (Loch, Carr, & Warkentin, 1992) by mitigating vulnerabilities through security controls (National Institute of Standards and Technology, 2009). The LAN is the user's portal to the Internet. The LAN is where the user controls what information is sent. Keeping information secure can be as simple as not sending sensitive information over untrusted networks. Untrusted networks contain vulnerabilities that provide hackers with targets to compromise victims' information. The purpose of attack vectors range from gathering information to denying services (Hansman & Hunt 2005). A typical attack starts with sniffing, or scanning, to capture information. One then uses the captured data to launch higher-order attacks such as impersonation attacks, replay attacks, modification attacks, channel accessible by non-endpoint (also known as man-in-the-middle attacks), malware injection, and denial-of-service attacks (Hansman & Hunt 2005; Higgins 2007; The Open Web Application Security Project, 2009). We address these attack vectors in the following paragraphs.

One of the key vulnerability points in an online transaction is the local infrastructure (Byrd, 2011). A sniffing or snooping attack compromises the sender's information's *confidentiality* by capturing information transmitted over the network infrastructure. One performs it by either capturing packets over the airwaves on a legitimate Wi-Fi network or by establishing a rogue network that spoofs the legitimate network. This attack typically targets initial connection information (i.e., usernames, passwords, secret keys, etc.), which provides the attacker with credentials that to the attacker can use launch second-tier attacks (Stewart, Tittel, & Chapple, 2008). Sidejacking is a common scanning attack that gathers a victim's cookies and uniform resource locator (URL) trail, which allows the attacker to hijack the victim's session and gain access to online accounts (Garcia 2010; Higgins 2007). The initial connection authentication information enables the attacker to target the victim, target the victim's intended destination, or establish a channel accessible by non-endpoint attack to further exploit the victim.

Targeting the victim based on authentication credentials enables the attacker to gain access to the victim's computer. Once access is established, the attacker can perform several higher-order attacks ranging from denial of service to malware injection. Typically, denial-of-service attacks only result in a compromise of *availability*, but an attacker can use them to distract the victim from the attacker's executing a *confidentiality* or *integrity* attack. Because denial-of-service attacks indirectly target a user's information, we focus on confidentiality and integrity attacks. Malware injection is dangerous because the user may have decided to engage in a low-sensitivity transaction based on low perceived risk to the information, yet could suffer a compromised system from which an attacker can surreptitiously exfiltrate *sensitive* information at a later date.

Focusing at the other end of the transmission, the attacker could leverage the victim's intended information recipient by using impersonation or masquerading attacks, replay attacks, and modification attacks. Impersonation attacks use the captured information to mimic the victim. Similarly, a replay attack mimics the victim by replaying the captured packets against the victim's intended destination system. If the system uses improved authentication mechanisms and session sequencing, the attacker would execute a modification attack by modifying the information in the packets prior to replay (Stewart et al., 2008). Alternately, if the user and the endpoint use additional advanced authentication encryption techniques, the attacker could use a man-in-the-middle attack the way the hacker did in the introductory scenario. This attack permits malicious individuals (Willison & Warkentin, 2013) to intercept a communication between two parties by splitting the original connection, spoofing the encryption certificates, and acting as a proxy to the victim. Victims believe they are securely communicating with the intended endpoint but they are communicating through the attacker (The Open Web Application Security Project, 2009). Figure 2 illustrates the attack, which compromises the victim's confidentiality and integrity and allows the attacker to view and modify the victim's transmission (MITRE, 2011). A successful man-in-the-middle attack enables the attacker to perform additional attacks such as address resolution protocol spoofing, directory name service spoofing, and hyperlink spoofing to redirect the victim to the attacker's desired destinations (The Open Web Application Security Project, 2009).

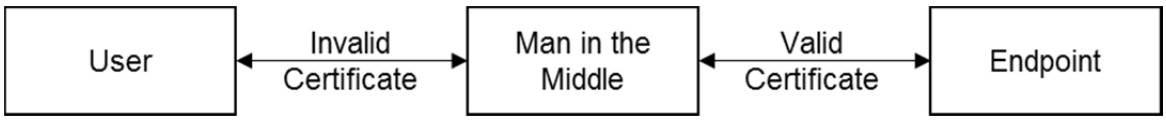

Figure 2. Man-in-the-middle Attack

The typical mitigation strategy for man-in-the-middle attacks is endpoint authentication using digital certificates and secure socket layer connections. One can thwart this countermeasure by mimicking the intended endpoint using falsified credentials and establishing two secure socket layer connections: one with the victim using an invalid certificate and one with the victim's intended endpoint using a valid certificate (see Figure 2). Victims may only receive a certificate error that they will likely dismiss and, consequently, engage in transacting with the man-in-the middle attacker (Garcia, 2010; The Open Web Application Security Project, 2009). This type of man-in-the-middle attack enables the attacker to capture all of the victim's traffic that one thought endpoint encryption secured.

Service providers have deployed countermeasures to combat specific vulnerabilities; however, the purpose and concepts of the attacks presented remain the same. For example, regardless of any encryption mechanism, sniffing still seeks to capture information about the information transmitted, which is then decrypted using various techniques. One can even break the Advanced Encryption Standard 256 with the right algorithm and computational power (Bogdanov, Khovratovich, & Rechberger, 2011). Hackers have access to incredible computational power at inexpensive prices through cloud computing. Individuals have used the cloud was used to crack Wi-Fi's protected access pre-shared key for less than USD$2.10 (Rashid, 2011) and the Sony PlayStation network for less than USD$1.68 (Goodin, 2011).

New stories of successful attacks and personal experiences shape users' perceptions of network environments. There is a history of organizations failing to deploy the appropriate countermeasures. A prime example of an organization that has implemented inadequate security measures is the TJX Companies' breach in 2006 in which "(a)n intruder exploited these failures and obtained tens of millions of credit and debit payment cards that consumers used at TJX's stores, as well as the personal information of approximately 455,000 consumers who returned merchandise to the stores" (Federal Trade Commission, 2008, p. 1). TJX's failure to use appropriate wireless security countermeasures highlights an example of an attack on a network environment that could have been prevented if the appropriate countermeasures were deployed. While organizations have recognized this deficiency, unsecured Wi-Fi is prevalent in many public locations and hackers are savvy to these vulnerabilities. The Federal Bureau of Investigation and other government agencies have reported malware injection incidents through pop-ups displayed when individuals establish a Wi-Fi session at hotels (Internet Crime Complaint Center, 2012). The weak security postures of public Wi-Fi hotspots make these attacks possible. The network environment includes the infrastructure architecture, which contributes to the network's security. Hackers exfiltrated target customer data in 2013 in an attack that Target could have prevented with a properly segmented network (Krebs, 2014). While the public may not understand the intricacies of the attack or the proper mitigation techniques, the event influenced users' perceptions of network security and the safety of their sensitive information.

1.2 Research Purpose

Not all network environments are susceptible to the same attack vectors, which makes some environments more trustworthy than others. Users can reduce the probability of a compromise by only engaging in sensitive online activities in trusted network environments. How that trust if formed and how risk is evaluated are important facets of information systems research because they drive online behavior. To understand these concepts, we seek to address the following research questions (RQ):

RQ1: How does trust in the parties involved in an online transaction influence users' intent to provide sensitive information online?

RQ2: What role does general information security awareness have in determining perceived risk?

To investigate these research questions, we use a decision process model and theories from extant literature to describe each decision phase. We address pre-activity attributes, describe the users' decision process to form perception of an activity, describe how these perceptions form intentions that are followed

by actions, and describe the outcomes of those actions. Specifically, we propose that users establish their general information security awareness (Bulgurcu, Cavusoglu, & Benbasat, 2010) in the pre-activity phase and use it to determine perceived risk and network trust when placed in a situation that requires the transmission of sensitive information. We also propose that network trust forms perceptions of risk to the information with a downstream influence on intent (Ajzen, 1991), action (Davis, Bagozzi, & Warshaw, 1989), and, finally, outcomes that ultimately influence pre-activity attributes.

Previous research has investigated users' behavioral intention to transact in e-commerce by including the network infrastructure as a transparent actor in the transaction and have focused on the perceived risk stemming from the information recipient—the Web service provider, Web retailer, or e-government agency (Dinev & Hart 2006; Featherman & Pavlou 2003; Jarvenpaa, Tractinsky, & Vitale, 2000; Pavlou, 2003; Warkentin, Gefen, Pavlou, & Rose, 2002).

This focus on the ultimate information recipient nominalizes the intermediary network IT artifact because the enabling technology is absent. We approach the IT artifact from an ensemble view as an embedded system that is enmeshed with the conditions of use (Orlikowski & Iacono 2001), which provides intrinsic risks to an Internet activity. Shifting the focus from the Web service provider to the network environment helps widen the understanding of Internet behaviors by examining users' perceived risk and network trust to protect information from malicious outsiders. Figure 3 illustrates this differentiated focus. The sender of information (e.g., consumer) must trust the LAN provider (e.g., coffee shop), the infrastructure (e.g., Wi-Fi network), and the information receiver (e.g., a Web retailer) to protect their information from hackers and secondary recipients (e.g., third-party marketers). The dashed line indicates prior research's focus on the intended information recipient (Web service provider or retailer), while the solid line depicts our focus on the network environment.

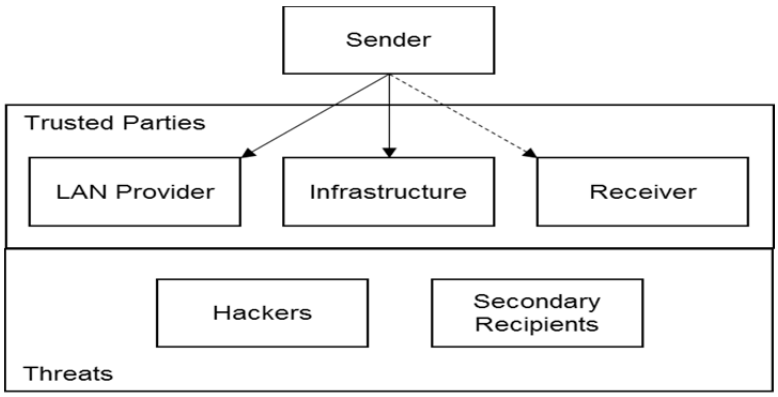

Figure 3. Trusted Parties and Threats in an Internet Transaction

This paper proceeds as follows: in Section 2 we highlight foundational research in the extant literature. In Section 3, we logically thread existing theories through the decision process model while building a theoretical framework to base our propositions. In Section 4, we present potential findings, implications, limitations, and future research opportunities. Finally, in Section 5, we conclude the paper.

2 Literature Review

The dominant research paradigm for researching the nomological net of Internet behavior explores users' intention to transact with the endpoint of a communication channel—specifically a Web retailer or e-service provider. These studies focus on the endpoint's characteristics and exclude the characteristics of the network provider or the network infrastructure (e.g., Antón & Earp 2004; Culnan & Armstrong, 1999; Dinev & Hu, 2007; Featherman & Pavlou 2003; Hoffman, Novak, & Peralta, 1999; Malhotra, Kim, & Agarwal, 2004; Pavlou, 2003). Cho (2004) evaluates variables that determine aborting transactions with Internet retailers and specifically looks at the cognitive evaluation of the endpoint's attributes with consumers' attitudes and past behaviors. Dinev and Hart's (2006) extended privacy calculus model compares consumers' personal internet interest, internet privacy concerns, and perceived internet privacy risk with Internet trust to determine individuals' willingness to provide personal information to transact on the Internet. The instrument items the authors use to measure trust directly address the competence, reliability, and safety of Internet websites and omit the network environment. Jarvenpaa et al. (2000)

examine trust in store, attitude, and risk perception as antecedents for the willingness to buy from an Internet store. The scales they use to measure the Internet store's perceived characteristics include reputation, perceived size, store trustworthiness, and attitudes towards the store, and the scales capture general Web-shopping risk attitudes by generically querying on Internet risk.

The potential offenders in the prior research mentioned included the intended endpoint (e.g., Web retailer) and nominalized the physical environment where the transaction occurred. The result is that trust and risk evaluations are solely dependent on the intended recipient without regarding the network environment. We argue that incorporating the network environment it into evaluations is appropriate because the infrastructure is collection of technologies that enable online activities to occur. Without the network infrastructure in the trust evaluation, a user's intent to transact with a Web retailer is implicitly derived from the user's beliefs in the technological infrastructure characteristics (Pavlou, 2003). We agree that the onus for trust lies with the intended recipient and that Web retailers can affect environmental trust by implementing certain countermeasures (Benassi, 1999; Bhimani, 1996). However, these countermeasures can be ineffective in combating the infrastructure's vulnerabilities that we identify in Section 1. Network environment vulnerabilities make the LAN an important IT artifact during the transaction decision process because it provides hackers with attack opportunities.

The crime-specific opportunity structure adapted from Clarke (1995) by Willison and Backhouse (2006) identifies the physical environment as a required element for exploiting victims because it provides criminals with targets. The model also suggests that individual's lifestyle and routine activities provide parties external to the transmission with opportunities to compromise data. Willison and Backhouse (2006) state that a vacant house without guardianship is a viable and attractive target to those that would wish to steal from or damage it. A public Wi-Fi access point without encryption cannot protect data in transit and are in many ways like a vacant house without guardianship. That is, they are a soft target for hackers. Behavioral patterns also can contribute to supplying victims (Willison & Backhouse, 2006), such as men waiting the day before Valentine's Day to buy flowers. Social engineering provides hackers with intelligence on targets to identify user behaviors that they can exploit, such as frequently using a coffee shop's Wi-Fi or a particular Web retailer.

The network environment provides individuals with targets that they attack using techniques that exploit vulnerabilities (Hansman & Hunt, 2005). One must address infrastructure vulnerabilities by altering the characteristics of the network environment. Exploitable network characteristics create an environment with the potential for one to opportunistically steal users' information, and, thus, result in loss. The possibility of such a loss is risk, and information risk is when information is the asset that can be lost (Loch et al., 1992). Previous research has viewed the opportunistic behavior stemming from the risks associated with engaging with a Web retailer; however, the research nominalizes the risk introduced by the network environment by aggregating it into the transaction.

Prior research has identified trust as one's willingness to be vulnerable and accept risk (Gefen, Benbasat, & Pavlou, 2008; Mayer, Davis, & Schoorman, 1995). The management literature has addressed the trust-risk relationship (Bauer, 1967; Cunningham, 1967; Gefen et al., 2008; Jacoby & Kaplan, 1972; Mayer et al., 1995) and the information systems research adopted it to e-commerce transactions with little regard to the network environment (Culnan & Armstrong, 1999; Dinev & Hart, 2006; Hoffman et al., 1999; Pavlou, 2003). We extend the prior research by focusing on the potential offender external to the transaction that exploits the vulnerabilities of the technological infrastructure instead of the internal transaction characteristics of the Web retailer. The literature has provided a solid foundation for exploring user behavior in multiple network environments for a transaction requiring sensitive information that is applicable to trust of the network environment. We start by creating a decision-process model to map relevant theories to each decision phase and discuss how each construct may influence users' decision to transmit sensitive information while operating in multiple network environments.

3 Theoretical Framework

Previous studies have focused on decisions based on the intended information recipient's characteristics. Our research focuses on decisions based on the network environment's characteristics, and one can view our research as a parallel process to other online behavior models. Lee et al. (2013) have created a dichotomous framework depicted in Figure 4 that combines Jarvenpaa et al.'s (2000) consumer/retailer trust model with a consumer/network trust model. This study adds detail on the trust and risk evaluation

from a service provider and infrastructure perspective to the consumer/network trust portion model and provides broader view of perceived risk during Internet transactions.

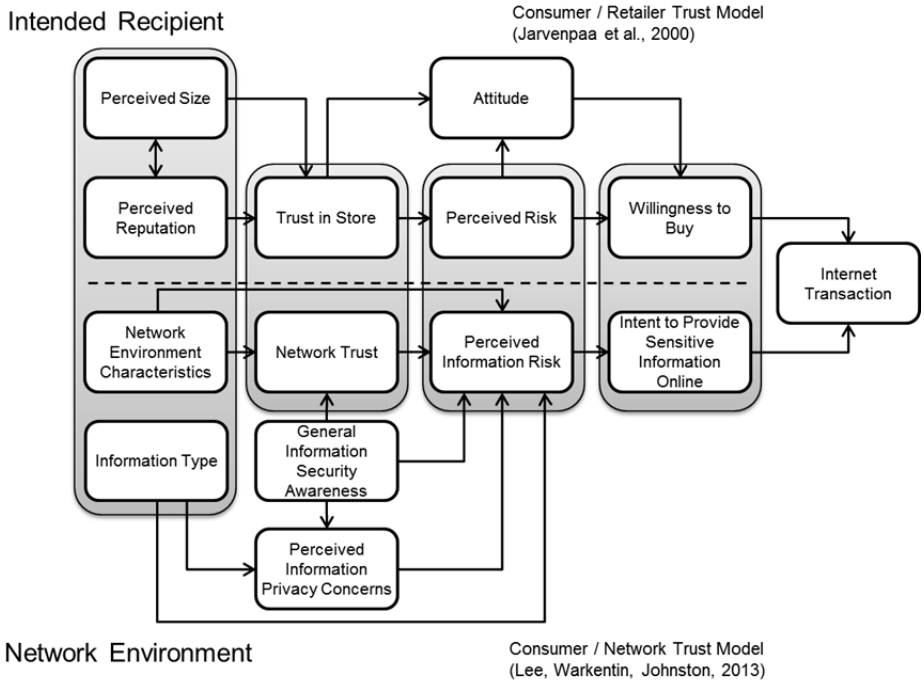

Figure 4. Lee et al.'s (2013) Dichotomous Consumer Transaction Model

The threat to the consumer exists from opportunistic behavior executed by the intended recipient and individuals exploiting network environment vulnerabilities. Jarvenpaa et al. (2000) suggest that perceived size and perceived reputation of an Internet retailer can evoke trust. Perception of size is a consumer's subjective evaluation of the retailer's actual size and not measured by the store's sales volume or products for sale. Perceived reputation is the degree to which a consumer believes the retailer is honest and benevolence toward its customers. Both perceived size and perceived reputations are judgments of a store's attributes that individuals use to determine trust in store. Similarly, one must evaluate the network environment characteristics prior to engaging in online activities to determine if the network is capable of protecting information from harm. This evaluation determines network trust.

Determining network trust requires cognizance of how the network environment characteristics affect the environment's ability to protect information. This knowledge also provides an understanding of the impact of an information breach. General information security awareness is fundamental for effective information security (Furnell, 2008; Goodhue & Straub, 1991) and provides users with the understanding proper information-handling practices (Siponen, 2000; Straub & Welke, 1998). The integrated model includes general information security awareness as a construct that informs users of the environmental dangers and influences their information privacy concerns.

Trust is a governance mechanism that enables an exchange. Jarvenpaa et al. (2000) focuses on trust in store, which is parallel to network trust in Figure 4. Trust in store is the trustworthiness of the Internet store, whereas network trust is the trustworthiness of the network environment the buyer is using to connect to the Internet. Jarvenpaa et al. (2000) focused on the impact the trust in store has on perceived risk, which is appropriate from an e-commerce perspective. Lee et al.'s (2013) model includes information types to generalize the model to all personal Internet activities beyond e-commerce.

The dichotomous model also has two types of risk. The network environment and intended endpoint are sources of risk during an online transaction (Pavlou, 2003), and both sources are present in the integrated model in Figure 4. Jarvenpaa et al.'s (2000) perceived risk is directed towards the buyer's being mistreated by stores. This risk focuses on losses a buyer may experience from the seller's action. However, in an online transaction, the seller is not the only source of risk. The network environment can lead to information compromise, which puts the information at risk. Figure 4 parallels the risk from the

Internet store with perceived information risk. This risk is the potential of loss of data (e.g., credit card information) during the transaction that is attributed to the network vulnerabilities.

The different facets of risk inhibit one's ability to engage in e-commerce (Featherman & Pavlou, 2003). Risks associated with the retailer impact purchasers' willingness to buy (Jarvenpaa et al., 2000). Risks associated with the network environment will impact purchasers' intent to provide sensitive information online. The key difference in these constructs is that one accepts the potential loss from the retailer and the other accepts the potential loss from the network environment. Consumers must accept both types of risk prior to engaging in online transactions.

3.1 Decision Process Model

Separating out the network environment factors from the integrated model presented in Figure 4 focuses the discussion on decisions about the network environment. We identify five phases in a decision-process model and map each construct to each phase in Figure 5. We use the consumer purchase decision process (Turban, King, Lee, Warkentin, & Chung, 2002, p. 88) as the basis for our generalized decision process model. Prior to any activity, individuals will have attributes that they will use to make a decision. For example, in the consumer purchase decision process, purchasers have a need or want. Once an individual is placed in a situation, they assess the benefits of action versus costs and the result of that assessment then informs a decision, which the individual then transfers into an action. That action then creates outcomes that change the individual's pre-activity state for future decisions. In the context of our research, we are interested an individual's general information security awareness during the pre-activity phase and the individual's evaluation of network trust and perceived risk, which results in the individual's intent to provide sensitive information online. This intent then leads to an internet transaction, which ultimately influences the individual's general information security Awareness for any future decisions.

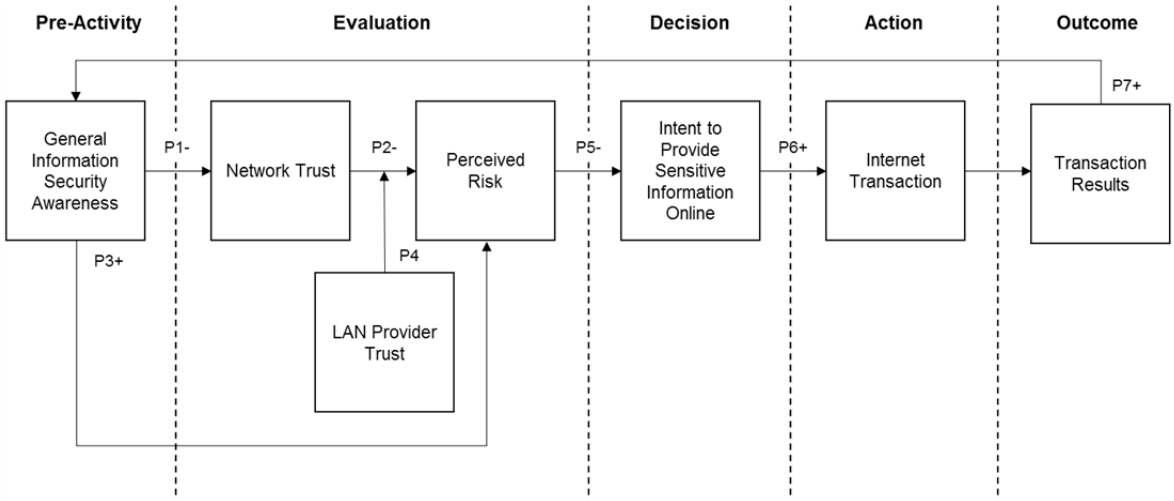

Figure 5. Research Model Mapped to a Decision Process

3.2 Pre-activity

Many different personal attributes such as traits, attitudes, and beliefs form the basis for decision making that exist prior one's being in a decision making situation (Sherman & Fazio, 1983). The theory of planned behavior (Ajzen, 1991) addresses attitudes, feelings towards subjective norms, and behavioral control for specific behaviors of interest, but one can generalize the theory to apply more broadly to describe a person's pre-activity cognitive state. Among these broader concepts that relate to the present study are propensity to trust (Mayer et al., 1995), disposition to trust (McKnight, Choudhury, & Kacmar, 2002), cognitive dissonance (Festinger 1957), risk propensity (Sitkin & Pablo, 1992), and risk tolerance (Barsky, Juster, Kimball, & Shapiro, 1997). While these are important constructs in evaluating the trust/risk relationship, they do not provide insights on information security-related attributes. We proffer that general information security awareness is a key information security construct that drives the evaluation of network trust and perceived risk

3.2.1 General Information Security Awareness

Cognitive appraisals of threat sources require an understanding of potential threats. Protection motivation theory presupposes that the threatened individual is aware of the threat and is able to comprehend the noxious event (Rogers, 1975). Lack of awareness of the threat may lead to ignoring the threat and increase one's vulnerability (Goodhue & Straub, 1991). The innovation diffusion theory identifies awareness as the first step by identifying three types of knowledge: awareness knowledge, how-to knowledge, and principles knowledge. Awareness knowledge is simply the understanding that the technology exists. Once a technology is recognized, one establishes how-to knowledge by understanding how to properly apply the technology (Rogers, 1995). Awareness knowledge in the context of protective technology adoption refers to an understanding of the threats and consequences of not using protective technologies, and how-to knowledge refers to the availability and effectiveness of using protective technologies to safeguard the user against unwanted consequences (Dinev & Hu, 2007). Conceptually, we adopt this view of awareness for protective technologies as an awareness of the information security's characteristics. If one is aware of the protective technologies (i.e., countermeasures, safeguards, controls, etc.), then one is aware of the threats, vulnerabilities, and impacts of consequences of using the environment. Simply put, knowing the cure presupposes knowing the disease.

Bulgurcu et al. (2010) posit that information-security awareness is an antecedent to attitude, which drives one's intention to comply with information-security policies. Understanding general information security provides users with knowledge of the dangers of operating in different network environments. Without this awareness, users are blind to the environmental vulnerabilities that we discuss in Section 1, which can lead to their falsely assessing environmental threats and networks' trustworthiness. Misplaced trust may cause the user to place sensitive data at risk by transmitting in an unsecure environment and, thus, causing a loss of sensitive information. General information security awareness is a baseline understanding of the ways information can be stolen and misused and provides insights into the sensitivity level of information transmitted on the Internet.

We use Bulgurcu et al. (2010) construct as an antecedent to perceived risk and one's information sensitivity level in an Internet transaction. Substituting intention to comply with intention to transact nets a generalized version of the awareness construct that we can use for our purposes. Bulgurcu et al. posit that information security awareness comprises general information security awareness and information security policy awareness. While both of these constructs are important requirements for organizational compliance, generalizing awareness to personal Internet activities removes organizational policies from the Internet activity. Consistent with Bulgurcu et al. (2010), we define general information security awareness as one's fundamental understanding of potential security issues and impacts developed through experiences and education.

3.3 Evaluation

Decisions are made once an individual is in a situation that requires action. Our situation of interest is when a user has the ability to engage in personal Internet activities from different network environments that require sensitive information. Engaging personal Internet activities ultimately depends on the situational factors that are, themselves, variant depending on characteristics of the network environment and the information necessary to complete a particular transaction. While other factors, such as communication urgency, convenience, cost, or facilitating conditions (Venkatesh, Morris, Hall, Davis, & Davis, 2003), could influence personal Internet behaviors, these factors indirectly relate to our focus of perceived risk and network trust. We suggest that the evaluation phase of the decision process model includes determining network trust and perceived risk.

3.3.1 Network Trust

The network environment includes the LAN provider, physical location and surroundings, network architecture, hardware infrastructure, and software configuration. The physical location may be a coffee shop, workplace, school, anywhere with a cellular data connection, or home. The physical surroundings can affect the security posture of the network from the number of people present to the seating configuration, both of which contribute to the possibility of shoulder surfing. Closely related to the physical location is the organization responsible for LAN access. The organization may be a retailer, restaurant, employer, university, mobile phone service provider, or an individual operating a home network. The LAN provider will determine the wired or wireless network architecture, the hardware infrastructure, and

software that deliver connectivity. Network environments vary in the architecture, technology, and processes employed. These variations result in unique security capabilities and vulnerabilities.

Mayer et al. (1995) and Schoorman and Mayer's (2007) follow-up editorial identify trust as one's willingness to be vulnerable and one's willingness to take risks based on perceived trustworthiness. Trustworthiness is a trusting belief that evaluates a trustee's characteristics (Gefen, Karahanna, & Straub, 2003) by assessing the trustee's ability, benevolence, and integrity (Mayer et al. 1995). The ability evaluation determines if the trustee's aptitude in the activity's domain is sufficient to protect the trustor from negative outcomes. Benevolence is a judgment of goodwill from the trustee towards the trustor. Integrity measures if the trustor's principles align with the trustee and are followed during the activity (Mayer et al., 1995). IS researchers have used these definitions of trust to examine mobile commerce (Siau & Shen, 2003), e-service adoption (Featherman & Pavlou, 2003; Lee & Turban, 2001), Internet and mobile payment services (Lu, Yang, Chau, & Cao, 2011; Lee, Warkentin, & Choi, 2004), online shopping (Gefen et al., 2003; McKnight et al., 2002), e-government (Grimsley & Meehan, 2007; Warkentin, Gefen, Pavlou, & Rose, 2002), and virtual teams (Paul & McDaniel, 2004). Jarvenpaa et al. (2000) suggest that perceived size and reputation can garner trust. Others have shown that trust can be obtained from recommendation agents (Wang & Benbasat, 2005), trust-assuring claims (Kim & Benbasat, 2006), or directly from characteristics of an IT artifact (Vance, Elie-Dit-Cosaque, & Straub, 2008).

While trust has been an important research construct in examining Internet activities, the primary focus has been on the information sender's trust in the information recipient, such as an online retailer, government agency, or other e-service provider (McKnight et al., 2002) rather than trust in the IT artifact (Vance et al., 2008). Though some scholars have directly referenced the existence of the IT artifact in an evaluation of trust, its impact has been predominantly marginalized. Pavlou (2003) identifies perceived risk and trust as key drivers to intention to transact with Web retailers and encapsulates one's willingness to be vulnerable to a Web retailer to include both the Web retailer's and the technological infrastructure's characteristics. Similarly, Jarvenpaa et al. (2000) look at the trust in store and nominalize the IT artifact while researching Internet shopper behaviors. Part of the issue may stem from the factors of trustworthiness (ability, benevolence, and integrity). Of the three factors, only ability is germane to an IT artifact because the IT artifact lacks moral agency and cannot exhibit benevolence or integrity. IT's ability to perform depends on the protocols and implementation practices used to establish the network environment characteristics. Users judge the ability of the characteristics to protect information against compromise and determine if the IT artifact is trustworthy.

Removing the IT artifact from the trustworthiness evaluation limits the understanding of the artifact's impact on user behavior because it aggregates all of the trust relationships required to conduct Internet activities into a single evaluation. One evaluates many trust relationships during an Internet transaction. The integrated theoretical model presented in Figure 4 divorces the Web service provider/retailer trust evaluation from the infrastructure trust evaluation and differentiates these two trust sources by trust in store and network trust. Users evaluate the characteristics perceived size and perceived reputation of the online store to determine trust in store (Jarvenpaa et al., 2000). Simultaneously, users evaluate the network environment characteristics to determine the network environment's ability to protect sensitive information. Determining if a network environment has the ability requires an understanding of information security. Therefore, we propose:

P1: General information security awareness is negatively associated with network trust.

3.3.2 Perceived Risk

Risk is present when a threat that causes negative consequences may possibly exist that can compromise a user's information (Loch et al., 1992). Perceived risk is one's evaluation of the outcomes that have the potential for loss during an event (Dowling & Staelin, 1994; Sitkin & Pablo, 1992) regardless of the actual threat and subsequently actual risk. Perceived risk is an inhibitor to one's engaging in e-commerce activities because of product-specific risk (Dowling & Staelin, 1994; Featherman & Pavlou, 2003), seller-specific risk (Featherman & Pavlou, 2003; Jarvenpaa et al., 2000), and network environment-specific risk. Perceived risk in an online transaction manifests through the loss of sensitive information because of environmental vulnerabilities. It is the residual uncertainty that the information could be compromised after one evaluates the trustworthiness of the parties in the transaction. Evaluating risk requires the decision maker to label the situation as positive or negative based on the individual's determination of the probability of loss (Sitkin & Pablo, 1992). To make this evaluation, information at risk and an awareness of how the environment's characteristics can lead to a loss must exist. The type of

information and the risk to that information based on environmental threats is the residual risk, which are from threats outside the relationship with the trustee (Mayer et al., 1995). Therefore, we propose:

P2: Network trust is negatively associated with perceived risk.

P3: General information security awareness is positively associated with perceived risk.

3.3.3 LAN Provider Trust

IT artifacts cannot exist without someone maintaining and operating them. LAN providers are the entities that maintain and operate the users' gateway to the Internet. Often, providing Internet connectivity is not a core competency of an organization but is either a necessary business enabler or a value-added service. We use a coffee shop in the introductory scenario: its primary business is supplying coffee to its customers, and free Wi-Fi is a value-added service that attracts customers. Organizations' reputations will impact how users perceive the services the organizations provide, and their reputations can extend to non-core competency areas. TJX's core competency is retail services, and consumers trusted TJX to protect their information. However, TJX's breach in 2006 highlights that the network infrastructure that TJX used did not have sufficient security controls, which resulted in damage to the company's reputation (Culnan & Williams, 2009). Therefore, we propose:

P4: LAN provider trust moderates the relationship between network trust and perceived risk.

3.4 Decision

A decision of whether or not to engage in an online transaction depends on one's assessing network trust and the perceived risk associated with the transaction. The decision to act is behavioral intention, which itself indicates the level in which one is willing to perform a specified behavior (Ajzen, 1991). Risk reduces intentions because of the possibility of undesirable consequences (Featherman & Pavlou, 2003). The intention to provide sensitive information, through actions such as e-commerce, often depends on one's evaluating the intended recipient and the network environment (Pavlou, 2003). We propose decoupling this evaluation by controlling the variables for the intended recipient and manipulating the network environments. By doing so, we proffer that the outcome of the trust/risk evaluation of the network environment drives behavioral intention. Therefore, we propose:

P5: Perceived risk is negatively associated with intent to provide sensitive information online.

3.5 Action

Intentions must be formed prior to cognitively engaging in actions (Petter, DeLone, & McLean, 2008). These intentions must be accompanied by the appropriate control conditions for the behavior (Ajzen, 1991). This does not mean that behavioral intention and perceived behavioral control are the only factors that contribute to behavior. In a meta-analysis of prior research, Sutton (1998) indicates that the theory of reasoned action and the theory of planned behavior explain 19 to 38 percent of the variance in behavior. However, without the intention or ability to engage in an activity, one cannot perform the behavior.

Researchers have used behavioral intentions as an antecedent to behavior in technology adoption (Davis, 1989; Venkatesh et al., 2003) and online transaction behavior (Pavlou & Gefen, 2004). As the integrated theoretical model illustrates, for an e-commerce transaction, the behavior is dependent on the formation of both willingness to buy (Jarvenpaa et al., 2000) and intent to provide sensitive information online. If the intended recipient variable path has been satisfied to form the wiliness to buy, then we can focus on the network environment. Therefore, we propose:

P6: Intent to provide sensitive information online is positively associated with the internet transaction.

3.6 Outcome

The outcomes of prior transactions inform future evaluations through enactive mastery (Bandura, 1982). Researchers have shown outcomes of prior risky decisions to affect the factors of perceived trustworthiness: ability, benevolence, and integrity (Mayer et al., 1995). Experiences with sending sensitive information from different network environments would shape a user's understanding of the network environment characteristics' ability to protect information. These positive and negative experiences of operating in network environments build general information security awareness. If

negative consequences occurred because of a prior transaction(s), then it is logical to assume that one would become more cognizant of security vulnerabilities associated with that network environment. Therefore, we propose:

P7: Transaction results are positively associated with general information security awareness.

Note that experiences only contribute to a general cognizance of security and do not impact the deeper understanding of information security. We can illustrate the differences in understanding by comparing awareness knowledge and how-to knowledge. Awareness knowledge is the general cognizance of technology, while how-to knowledge is understanding how to execute computing activities (Rogers, 1995). When a negative experience occurs, users gain awareness knowledge of the situational dangers. If they perform a root cause analysis, then users will understand how the data breach occurred and will advance their how-to knowledge. Additionally, non-negative experiences may result in an over-confidence in a technology's ability to protect information. For example, users may continuously send sensitive information using unsecure networks, and, because they did not experience a data breach, they may perceive environments as more secure than the actual security posture.

4 Contributions, Implications, and Future Research

4.1 Theoretical Application

People's traveling on business and staying at a hotel is a common phenomenon, and one can apply our theoretical model to investigate their online behavior. While Internet access is the most important amenity in mid-priced business hotels (Moskowitz & Krieger, 2003), it is not the hotel's core competency. Once the basic Internet requirement is met, other factors such as cleanliness, restaurants, staff, beds, pools, price, and proximity to airports, downtown, and shopping are important when travelers select hotels (Stringam & Gerdes, 2012). An example of applying the theory to this phenomenon is a business traveler, John, who selects his favorite hotel with Wi-Fi because it was close to the airport and fits the company's budget. While at the hotel, he needs to email a sensitive file. He has a moderate general information security awareness, and he knows that hackers could steal information. He logs onto the hotel's Wi-Fi network with his room number, so he assumes that he can trust the network. After all, he always stays at this hotel chain that is providing the LAN, and he trusts the chain so he trusts the network. His general information security awareness makes him understand that there are risks, but his network trust, strengthened by his LAN provider trust, reduces his perceived risk. He forms an intent to provide sensitive information online and engages in an Internet transaction. The most likely transaction result is that the file sends successfully and is not intercepted. However, the majority of hotel guest networks lack adequate security protections (Ogle, Wagner, & Talbert, 2008), and he could have been victim of a man-in-the-middle attack. The data breach would have a negative impact on his opinion of the hotel (Berezina, Cobanoglu, Miller, & Kwansa, 2012) and would inform his general information security awareness for future online activities.

4.2 Theoretical Contributions

IS research has often nominalized the IT artifact into the background of the literature. We propose that our model highlights antecedents for online behaviors that occur in parallel to prior research's focus on characteristics of the intended information recipient. Our research has the potential to provide insight on users' trust of multiple network environments, their evaluation of information privacy based on varying types of information, and their perception and acceptance of risk to information while engaging in Internet activities. Researchers can apply this parallel track to numerous online activities including e-commerce, e-government, electronic medical records, virtual teams, or any other activity that requires sending sensitive information. Examining network trust in these contexts could provide knowledge on the impact of the IT artifact on a wide range of phenomenon. Furthermore, by framing our theoretical model in a decision process, one can extend the model by further decomposing behavioral drivers in each phase of the decision process.

4.3 Practical Implications

The boundaries of network environments are blurring. Users now operate in multiple environments with varying degrees of protective technologies. While network technology continues to proliferate, IS research has often been criticized as having nominalized the IT artifact into the background of the literature (Orlikowski & Iacono, 2001), which may hurt the practical relevance of IS research because practitioners

are not provided with actionable information. We suggest that the network environment is an explicit actor during online transactions.

We provide a long-overdue acknowledgement that infrastructure matters and transaction behavior involves more than just assessing risk/trust in the human points of contact, which potentially redefines how we perceive the consumer transaction process. Furthermore, by framing our theoretical model in the context of a transactional decision process, others can extend the model by further decomposing behavioral drivers in each phase of the decision process. These decisions are required for the conscious and active use of individual controlled protective technologies to protect information assets (Dinev & Hu, 2007). If a user's device becomes compromised on one network, then the infected device poses a threat to all accessible networks and, therefore, is a threat to the assets which security policies are designed to protect. Understanding the drivers behind users' behavior while on networks outside of an organization's control can provide a foundation for improving public information security education training and awareness (SETA) programs.

In addition, organizations controlling the network environments could offer additional protections for consumers to reduce the environment's perceived risk. Using Wi-Fi security protocols at public locations could provide the user with additional safeguards from the vulnerabilities we describe earlier. Combining these countermeasures with additional controls between the endpoints, such as virtual private networking, secure socket layer, or transmission layer security, would further reduce the risk to the loss of sensitive information in transit. If patrons of retail stores that provide public Wi-Fi are aware that the store uses additional security measures, then patrons could exhibit more network trust. This trust may extend to the retailer by showing patrons the ability, benevolence, and integrity to protect them from harm.

4.4 Potential Limitations and Future Research

The antecedents to behavior can be far reaching beyond the constructs we present. We understand there are many dimensions of complex constructs, but we chose to focus on measuring the core concepts of trust and risk to ensure our research's maximum theoretical effectiveness. Throughout this manuscript, we identify potential variables that one could add to the model such as individual facilitating conditions (Venkatesh et al., 2003) and discuss expansion to include the ability, benevolence, and integrity (Mayer et al., 1995) towards the IT artifact provider. Additional situational factors may influence the trust and risk decision and should be controlled for when empirically testing the proposed relationships. One could also examine other trust phenomenon, such as trust's transferability from a primary trustor/trustee relationship to a secondary trustor/trustee relationship. For example, one may trust a retailer to refrain from engaging in opportunistic behavior when a trustor is purchasing an item; however, does this trust transfer to the retailer's public Wi-Fi network?

Demographic factors could also provide additional insight to user behavior in multiple network environments. Jones and Fox (2009), in a study for the PEW Institute, found that older generations are significantly more likely to seek health information online than younger generations. Older users' desire to seek out online health information could relate to the linkage between health status and the use of online health information (Lueg, Moore, & Warkentin, 2003) because health problems tend to increase with age. Generational differences also exist for online banking activities. Generation X users are significantly more likely to conduct online banking than any other generation (Jones & Fox, 2009). Future research could attempt to determine if demographic characteristics are a determinant of the constructs we identify in this manuscript.

Outside of our focus on individual security behavior, organizational facilitating conditions exist that could influence behavior (Venkatesh et al., 2003). Some organizations block certain types of Internet traffic that prevents personal Internet transmissions from occurring. Future research could investigate the influence of information security policies on behavior while connected to the organization's network versus an alternative network environment. Another avenue could examine if job performance expectations (Venkatesh et al., 2003) overshadow perceived risk due to the intrinsic or extrinsic rewards of the work (Davis et al., 1989). Furthermore, the effectiveness of information security policies and information security policy awareness (Bulgurcu et al., 2010) could provide valuable insights into educating users on the appropriate environments to transmit sensitive information.

Advancing this research poses challenges that researchers must recognize. Researchers must take care when operationalizing and measuring proposed constructs because contextual factors may significantly impact the findings. General information security awareness is cognizance of the threats and

countermeasures used to protect information. This knowledge is processed and used during memory-based judgments where the individual uses experiences to inform current actions (Campbell, 2001). Using knowledge in a memory-based judgment requires cognitive engagement and may not have as a great of an impact on decisions compared to what is on the top of the individual's mind (Unnava, Burnkrant, & Erevelles, 1994). If the individual is thinking about the urgency of the online transaction, then the situation may impact individual's risk tolerance and they may act in an unsafe manner despite knowing the dangers.

Performing a case study would provide qualitative evidence of the propositions. For example, a case study of an organization in a partner network in which each partner organization formed dependencies on the data and information exchange between them would reveal insight toward the propositions. How the level of trust in the parent and partner organization impacts perceive risk could provide insights on how these relationships form and strengthen. An assessment through deep inspection of the entire partner network and its users and administrators could reveal that organizations may not trust the technology but trust outsourced service providers to implement secure solutions. Recent incidents involving Target and Sony provide interesting scenarios in which there are sensitive data transfers across retailer, financial agencies, and supplier networks.

5 Conclusion

Previous Internet behavioral research has nominalized the IT artifact and concentrated on understanding the relationship between the user and the intended information recipient. We posit that ubiquitous networking has increased the attack vectors for information in transit, and, therefore, that the network environment must be accounted for when researching Internet behaviors. Leveraging extant literature, we propose a theoretical model that suggests a user with high general information security awareness will demonstrate a lower level of network trust and a higher perceived risk while operating in network environments known to be vulnerable to the exploits previously described. Network trust is determined by the degree to which users feel the network environment can protect their information from harm and forms perceived risk. LAN provider trust moderates this risk even though providing Internet services may not be the provider's core competency. When the residual risk to information is low, then one forms a positive intent to provide sensitive information online. This intention drives the internet transaction behavior, which results in outcomes that influence general information security awareness for future decisions.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

Antón, A. I., & Earp, J. B. (2004). A requirements taxonomy for reducing web site privacy vulnerabilities. *Requirements Engineering,* 9(3), 169-185.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist, 37*(2), 122-147.

Barsky, R. B., Juster, F. T., Kimball, M. S., & Shapiro, M. D. (1997). Preference parameters and behavioral heterogeneity: An experimental approach in the health and retirement study. *Quarterly Journal of Economics*, *112*(2), 537-579.

Bauer, R. A. (1967). Consumer behavior as risk taking. In D. Cox (Ed.), *Risk taking and information handling in consumer behavior* (pp. 23–33). Cambridge, MA: Harvard University Press.

Benassi, P. (1999). Truste: An online privacy seal program. *Communications of the ACM, 42*(2), 56-59.

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

Bhimani, A. (1996). Securing the commercial Internet. *Communications of the ACM, 39*(6), 29-35.

Bogdanov, A., Khovratovich, D., & Rechberger, C. (2011). Biclique cryptanalysis of the full AES. In *ASIACRYPT* (pp. 344-371). Seoul, South Korea: International Association for Cryptologic Research.

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

Byrd, C. (2011). Unsafe at any SSID. *ISSA Journal, 9*(3), 12-17.

Campbell, J. (2001). Memory demonstratives. In C. Hoerl & T. McCormack (Eds.), *Time and memory: Issues in philosophy and psychology* (pp. 177-194). Oxford: Clarendon Press.

Cho, J. (2004). Likelihood to abort an online transaction: Influences from cognitive evaluations, attitudes, and behavioral variables. *Information & Management, 41*(7), 827-838.

Clarke, R. V. (1995). Situational crime prevention. In M. Tonry & D. Farrington (Eds.), *Building a Safer Society. Strategic Approaches to Crime Prevention* (pp. 91-150). Chicago, IL: University of Chicago Press.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104-115.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the ChoicePoint and TJX data breaches. *MIS Quarterly, 33*(4), 673-687.

Cunningham, S. (1967). The major dimensions of perceived risk. In D. Cox (Ed.), *Risk taking and information handling in consumer behavior*. Cambridge, MA: Harvard University Press.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982-1003.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective informaiton technologies. *Journal of the Association for Information Systems, 8*(7), 386-408.

Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research, 21*(1), 119-134.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*(4), 451-474.

Federal Trade Commission. (2008). *Agency announces settlement of separate actions against retailer TJX, and data brokers Reed Elsevier and Seisint for failing to provide adequate security for consumers' data.* Retrieved from http://www.ftc.gov/opa/2008/03/datasec.shtm

Festinger, L. (1957). *A theory of cognitive dissonance*. Stanford, CA: Stanford University Press.

Furnell, S. (2008). User behaviour: End-user security culture: A lesson that will never be learnt? *Computer Fraud & Security, 2008*(4), 6-9.

Garcia, A. (2010). Fighting sidejacking. *eWeek, 27*(20), 38.

Gefen, D., Benbasat, I., & Pavlou, P. A. (2008). A research agenda for trust in online environments. *Journal of Management Information Systems*, *24*(4), 275–286.

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

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. *Information & Management, 20*(1), 13-27.

Goodin, D. (2011). PlayStation Network hack launched from Amazon EC2: Cloud economics strikes again. *The Register*. Retrieved from http://www.theregister.co.uk/2011/05/14/playstation_network_attack_from_amazon/

Grimsley, M., & Meehan, A. (2007). E-government information systems: Evaluation-led design for public value and client trust. *European Journal of Information Systems, 16*(2), 134-148.

Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers & Security*, *24*(1), 31-43.

Higgins, K. J. (2007). Sidejacking' tool unleased. *Dark Reading*. Retrieved from http://www.darkreading.com/security/perimeter-security/208804667/index.htmlLas

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM, 42*(4), 80-85.

Internet Crime Complaint Center. (2012). Malware installed on travelers' laptops through software updates on hotel internet connections. Retrieved from http://www.ic3.gov/media/2012/120508.aspx

Jacoby, J., & Kaplan, L. B. (1972). The components of perceived risk. *Advances in Consumer Research, 3*(3), 382-383.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information and Technology Management, 1*(1), 45-71.

Jones, S., & Fox, S. (2009). Generations online in 2009. *PEW Internet & American Life Project.* Retrieved from http://www.pewinternet.org/2009/01/28/generations-online-in-2009/

Kim, D., & Benbasat, I. (2006). The effects of trust-assuring arguments on consumer trust in Internet stores: Application of Toulmin's model of argumentation. *Information Systems Research, 17*(3), 286-300.

Krebs, B. (2014). Email attack on vendor set up breach at Target. *Krebs on Security*. Retrieved from http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/#more-24313

Lee, C- P, Warkentin, M, & Choi, H. (2004). The role of technological and social factors on the adoption of mobile payment technologies. In *Proceedings of the Tenth Americas Conference on Information Systems*.

Lee Jr., J., Warkentin, M., & Johnston, A. C. (2013). *Complex multi-factor trust in the online environment*. In Gefen, D. (ed.), *Psychology of trust: New research* (pp. 157-170). New York, NY: Nova Science Publishers.

Lee, M., & Turban, E. (2001). A trust model for consumer Internet shopping. *International Journal of Electronic Commerce, 6*(1), 75-91.

Loch, K. D., Carr, H. H., & Warkentin, M. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173-186.

Lu, Y., Yang, S., Chau, P. Y. K., & Cao, Y. (2011). Dynamics between the trust transfer process and intention to use mobile payment services: A cross-environment perspective. *Information & Management, 48*(8), 393-403.

Lueg, J. E., Moore, R. S., & Warkentin, M. (2003). Patient health information search: An exploratory model of Web-based search behavior. *Journal of End User Computing, 15*(4), 49-61.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

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

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334-359.

MITRE. (2011). *CWE-300: Channel accessible by non-endpoint ("man-in-the-middle").* Retrieved from http://cwe.mitre.org/data/definitions/300.html

Moskowitz, H., & Krieger, B. (2003). Consumer requirements for a mid-priced business hotel: Insights from analysis of current messaging by hotels. *Tourism and Hospitality Research, 4*(3), 268-288.

National Institute of Standards and Technology. (2009). *Recommended security controls for federal information systems and organizations* (No. 3, SP 800-53). Gaithersburg, MD.

Ogle, J., Wagner, E. L., & Talbert, M. P. (2008). Cornell hotel network study highlights weaknesses in Internet security. *US Fed News Service*.

Orlikowski, W. J., & Iacono, S. (2001). Research commentary: Desperately seeking the "IT" in IT research—a call to theorizing the IT artifact. *Information Systems Research, 12*(2), 121-134.

Paul, D. L., & McDaniel, R. R., Jr. (2004). A field study of the effect of interpersonal trust on virtual collaborative relationship performance. *MIS Quarterly, 28*(2), 183-227.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101-134.

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research, 15*(1), 37-59.

Petter, S., DeLone, W. H., & McLean, E. R. (2008). Measuring information systems success: Models, dimensions, measures, and interrelationships. *European Journal of Information Systems*, *17*(3), 236-263.

Rashid, F. Y. (2011). Amazon EC2 used to crack password encryption on wireless networks. *eWeek*. Retrieved from http://www.eweek.com/c/a/Security/Amazon-EC2-Used-to-Crack-Password-Encryption-on-Wireless-Networks-490541/

Rogers, E. M. (1995) *Diffusion of innovations*. New York, NY: The Free Press.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology: Interdisciplinary and Applied, 91*(1), 93-114.

Schoorman, F. D., & Mayer, R. C. (2007). An integrative model of organizational trust: Past, present, and future. *Academy of Management Review, 32*(2), 344-354.

Sherman, S. J., & Fazio, R. H. (1983). Parallels between attitudes and traits as predictors of behavior. *Journal of Personality, 51*(3), 308-345.

Siau, K., & Shen, Z. (2003). Building customer trust in mobile commerce. *Communications of the ACM, 46*(4), 91-94.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Sitkin, S. B., & Pablo, A. L. (1992). Reconceptualizing the determinants of risk behavior. *Academy of Management Review, 17*(1), 9-38.

Stewart, J. M., Tittel, E., & Chapple, M. (2008). *Certified information systems security professional*, *information security* (4th ed.). Indianapolis, IN: Wiley Publishing.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Stringam, B. B., & Gerdes, J. (2012). An investigation of the traveler rating lexicon across hotel segments. *Journal of Quality Assurance in Hospitality & Tourism, 13*(3), 187-211.

Sutton, S. (1998). Predicting and explaining intentions and behavior: How well are we doing? *Journal of Applied Social Psychology, 28*(15), 1317-1338.

The Open Web Application Security Project. (2009). *Man-in-the-middle attack*. Retrieved from www.owasp.org/index.php/Man-in-the-middle_attack

Tarasewich, P., & Warkentin, M. (2000). Issues in wireless e-commerce. *ACM SIGEcom Exchanges*, *1*(1), 19-25.

Tarasewich, P., Nickerson, R.C., & Warkentin, M. (2002) Issues in mobile e-commerce. *Communications of the AIS* 8(3), 41-64.

Turban, D., King, D., Lee, J., Warkentin, M., & Chung, M. H. (2002). *Electronic commerce: A managerial perspective* (2nd ed.). Englewood Cliffs, NJ: Prentice Hall.

Unnava, H. R., Burnkrant, R. E., & Erevelles, S. (1994). Effects of presentation order and communication modality on recall and attitude. *Journal of Consumer Research*, *21*, 481-490.

Vance, A., Elie-Dit-Cosaque, C., & Straub, D. W. (2008). Examining trust in information technology artifacts: The effects of system quality and culture. *Journal of Management Information Systems, 24*(4), 73-100.

Venkatesh, V., Morris, M. G., Hall, M., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

Wang, W., & Benbasat, I. (2005). Trust in and adoption of online recommendation agents. *Journal of the Association for Information Systems, 6*(3), 72-101.

Warkentin, M., Gefen, D., Pavlou, P. A., & Rose, G. M. (2002). Encouraging citizen adoption of e-government by building trust. *Electronic Markets, 12*(3), 157-162.

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: Considering systems risk from a criminological perspective. *European Journal of Information Systems, 15*(4), 403-414.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37(1), 1-20.

About the Authors

James Lee, Jr., CISSP, is the Cybersecurity Division Director for Marine Forces Reserve. He earned his PhD in MIS at Mississippi State University under the Department of Defense Information Assurance Scholarship Program (IASP). His research focus is on behavioral information security, specifically examining policy development and enforcement. He has presented his research at several conferences, and is forthcoming in the *Journal of Computer Information Systems*. Prior to entering the IASP, he performed system engineering for highly complex systems that supports all communication capabilities aboard Marine Corps Installations. He holds an MBA from The George Washington University, and a BS in Management/Information Systems from Park University.

Merrill Warkentin is a Professor of MIS and the Drew Allen Endowed Fellow in the College of Business at Mississippi State University. His research, which focuses on behavioral issues in IS security and privacy, has appeared in *MIS Quarterly*, *Journal of the AIS*, *Decision Sciences*, *European Journal of Information Systems*, *Decision Support Systems*, *Information Systems Journal*, *Information & Management*, *Communications of the AIS*, *DATABASE for Advances in Information Systems*, and others. He has chaired several international conferences and will serve as the Program Chair for AMCIS2016 in San Diego. Dr. Warkentin is also currently an AE and Acting SE for *MIS Quarterly*, Guest Editor (twice) for *European Journal of Information Systems*, and an AE for *Information & Management,* and others. He is an SE for the *AIS Transactions on Replication Research* and the Eminent Area Editor (for MIS) at *Decision Sciences*, and was formerly the Chair of the IFIP Working Group on Information Systems Security Research (WG8.11/11.13). He is the author or editor of seven books.

Allen C. Johnston is an Associate Professor of IS and the Director of the MS MIS program in the School of Business at the University of Alabama at Birmingham (UAB). The primary focus of his research is in the area of behavioral information security. His research can be found in such outlets as *MIS Quarterly*, *Journal of the AIS*, *European Journal of Information Systems*, *Communications of the ACM*, *Journal of Global Information Management*, *Journal of Organizational and End User Computing*, *Journal of Information Privacy and Security*, and The *DATABASE for Advances in Information Systems*. He currently serves as AE for *European Journal of Information Systems* and the *Journal of Information Privacy and Security*, serves on the Editorial Review Board for *The DATABASE for Advances in Information Systems*, and is a founding member and current Vice Chair of the IFIP Working Group on Information Systems Security Research (WG8.11/11.13).