Citizen Trust Development for E-Government Adoption and Usage: Insights from Young Adults in Singapore

Shirish C. Srivastava  
*HEC School of Management, srivastava@hec.fr*

Thompson S.H. Teo  
*National University of Singapore*

Follow this and additional works at: [http://aisel.aisnet.org/cais](http://aisel.aisnet.org/cais)

**Recommended Citation**  
Available at: [http://aisel.aisnet.org/cais/vol25/iss1/31](http://aisel.aisnet.org/cais/vol25/iss1/31)
Citizen Trust Development for E-Government Adoption and Usage: Insights from Young Adults in Singapore

Shirish C. Srivastava
Department of Operations Management and Information Technology, HEC School of Management, Paris
srivastava@hec.fr

Thompson S.H. Teo
Department of Decision Sciences, School of Business, National University of Singapore

Abstract:

Trust, which has been found to be a significant facilitator for the adoption and usage of new business paradigms like e-commerce, is relatively unexplored in the context of e-government. Using trust literature as the theoretical lens, we propose an e-government trust grid for the adoption and usage of e-government, comprising two dimensions: ‘trust in government’ and ‘trust in Internet technology.’ Based on their levels of trust in the two identified dimensions, nations can fall into one of four quadrants: Adversarial, Competitive, Cooperative, and Collaborative. Using focus groups and interviews with young adults in Singapore, we find that in recent years, Singapore is evolving from the cooperative (low trust in Internet technology and high trust in government) to the collaborative (high trust in Internet technology and high trust in government) quadrant. The study delineates a set of lessons learned from the Singapore experience for engendering citizen trust in e-government. These lessons for governments are: solicit feedback from citizens, demonstrate top leadership commitment and support, build institutional trust, cultivate IT literacy, and enact comprehensive and effective legal systems.

Keywords: e-government, Singapore, trust, citizen, young adults
I. INTRODUCTION

E-government has been explained and conceptualized in different ways in the literature. Some definitions view e-government from a narrow perspective of using information and communication technologies (ICTs) for improving the efficiency of government systems [Hart and Teeter 2000; Koh and Prybutok 2003], while others view it from a broader perspective of system reform and government process reengineering [Grant and Chau 2005; Srivastava and Teo 2008]. In general, e-government can be defined as the use of ICTs and the Internet for enhancing the access to and delivery of all facets of government services for the benefit of all its stakeholder groups, which includes citizens, businesses, and government itself [Srivastava and Teo 2007a; 2007b]. The use of ICTs and the Internet has evolved from mere computerization of government activities to recent trends, such as e-voting facilitating e-democracy [Avgerou et al. 2007]. The latest United Nations (UN) report on e-Government also highlights the changing nature of e-government to connected governance which “revolves around governmental collective action to advance the public good by engaging the creative efforts of all segments of society” [UN Global E-Government Survey 2008: pp. xv].

Studies on e-government have focused on a variety of issues, such as its evolution and development [Grönlund and Horan 2004; Layne and Lee 2001], its adoption and implementation [Moon and Norris 2005; Pan et al. 2006], and its impact on citizens and businesses [Irani et al. 2005; Srivastava and Teo 2006; West 2004]. Despite the important role that trust plays in technology adoption and usage decisions [Gefen 2000; Jarvenpaa and Tractinsky 1999], not many studies have explored the role of trust in the adoption and usage of e-government [Avgerou et al. 2007; Srivastava and Teo 2005]. The importance of the issue, coupled with the relatively sparse research on the topic, are the prime motivations for this study.

Trust has been found to be one of the crucial enablers for the adoption and usage of e-commerce [Pavlou and Fygenson 2006; Teo and Liu 2007]. Despite similarities between e-government and e-commerce, it is surprising that relatively few studies have explored e-government from the trust perspective. In fact, in the case of e-commerce, consumers are exposed to a far lesser degree of dependence compared to e-government. For example, they have the option of changing their e-commerce vendor, but such a possibility does not exist in the case of e-government. Hence, in the absence of adequate trust in e-government Web sites, citizens may either choose to not adopt or revert to the traditional offline means of interaction with the government, e.g., face to face, postal service, or phone. Hence, extrapolating from the case of lesser dependence and control in the business environment, it appears that for the successful adoption and continued usage of e-government, establishment of citizen trust in e-government Web sites is an absolute necessity [Teo et al. 2009; Warkentin et al. 2002].

The adoption and usage of a technology by an intended user is dependent on two vital prerequisites: first, the user should have a perceived need for the solution offered by the technology, and second, the technology should have the ability to fulfill the user’s need satisfactorily. Past literature on technology adoption has shown that, even when these two prerequisites are present, adoption of technology may be inhibited by other factors such as ‘technology fears’ [Hsiao 2003], ‘power and politics’ [Markus and Robey 1983], or ‘lack of trust’ [Jarvenpaa et al. 2000]. Though citizen trust has been recognized as a vital prerequisite for e-government adoption and usage, researchers have not fully explored how trust in e-government develops and manifests among citizens [Srivastava and Teo 2004; Teo et al. 2009]. In this study, we focus specifically on young adults as they are one of the vital segments of populations targeted for adoption and usage of e-government services.

The rest of the paper is organized as follows. First, building from the theoretical origins of trust, we explicate the two dimensions of ‘citizen’s trust development’ for e-government adoption and usage: trust in government and trust in Internet technology. Subsequently, we relate these trust dimensions to the case of Singapore e-government adoption and usage. Next, we understand the evolution of trust in the two explicated dimensions and its impact on e-government usage. Based on the analyses of the Singapore experience, we enumerate a set of lessons learned for governments across the world. Finally, we discuss the implications and contributions of our study.

II. LITERATURE REVIEW AND THEORETICAL DEVELOPMENT

Trust, which has been defined as “a set of expectations shared by all those in an exchange” [Zucker 1986: 54], has a major impact on relationships between transacting groups and is a central defining aspect of many economic and social interactions [Pavlou and Gefen 2004; Warkentin et al. 2002]. It is believed that the trusted party will behave in
a socially responsible manner to meet the expectations of the trusting party [Gefen 2000; Mayer et al. 1995]. Trust is an expectation that alleviates the fear that one’s exchange partner will act opportunistically [Bradach and Eccles 1989]. These definitions of trust take the perspective from which the interacting partners are ‘individuals’ or ‘groups.’ However, the concept of trust has wider implications. It can be used with reference to an object of use, e.g., technology. Sitkin and Roth [1993] define trust as a set of expectations that tasks will be accomplished reliably. So in the context of technology, trust in technology implies believing that the technology can be used to accomplish the desired task satisfactorily. In the scenario of e-government, it emerges that citizens’ trust in government is necessary but not sufficient for its successful adoption and use. Citizens must also have a high level of trust in the enabling technology (Internet) and its capabilities to facilitate its adoption leading to consequent success. Thus, citizens’ trust, leading to adoption and use of e-government systems, has two dimensions: trust in government and trust in Internet technology [Teo et al. 2009].

**Trust in Government**

Trust is based on cognitive processes that discriminate institutions that are trustworthy from those that are distrusted and unknown [Lewis and Weigert 1985]. Further, Rousseau et al. [1998] indicated that trust can be either relational in nature when it is derived by repeated interactions between trustor and trustee over time, or institutional when the institutional factors provide broad support for trust that sustains further risk taking and trust behavior. In the case of government, the level of trust (willingness to expose vulnerabilities) which the citizens have on government may be largely dependent on the level of their confidence (belief in the performance ability) in the government. Papadakis [1999] demonstrated that the level of confidence of citizens in government is largely related to their level of confidence in the performance of different government institutions. In a similar vein, Mishler and Rose [2001] in their seminal paper on the origins of political trust, demonstrated the relatively greater importance of ‘institutional factors’ such as government performance and citizens’ evaluation of government performance over ‘cultural factors’ such as national culture or citizens’ socialization. Moreover, citizens are interacting with the government on an almost regular basis, which makes their trust dependent on their expectations based on past exchanges and is similar to process based trust [Zucker 1986]. This process based trust is instrumental in determining the level of legacy or initial trust which citizens have in the government.

Thus, citizens’ trusting behavior in the government is mostly derived from their experiential social exchange [Lewicki and Bunker 1995; Shapiro et al. 1992] which is akin to knowledge based trust production mechanisms [Blau 1964; Ring and Van de Van 1994]. This relationship based trusting beliefs of citizens in government is the aggregation of the citizens’ belief in the government’s competence, benevolence, and integrity [Mayer et al. 1995; McKnight et al. 2002]. Competence trust is based on the citizens’ assessment of the government’s technical knowledge and ability in general, which is related to successful implementation of e-government systems in particular [Mishra 1996; Sitkin and Roth 1993]. Benevolence trust implies that government is caring and is motivated to act in the citizens’ interests. It includes within its ambit, favorable motives and not acting opportunistically or manipulatively [Cummings and Bromiley 1996; Mishra 1996]. Integrity trust implies government’s honesty and promise keeping [Sheppard and Sherman 1998]. Together, the three reflect the relationship based trust of the citizens in the government.

In addition to the relationship based trusting beliefs, governments also engender institutional trust among citizens [Cullen and Reilly 2007; Papadakis 1999]. Institution based trust is the sociological dimension of trust, and refers to the citizen’s perceptions of the institutional environment – in the case of e-government, the Internet [McKnight et al., 2002]. Governments can influence the structural characteristics of the Internet environment, for example, by enforcing stringent cyber laws to enhance security or implementing various e-government programs, etc. Such institutional interventions by government may also serve to enhance citizen trust in e-government.

**Trust in Internet Technology**

Technology is the prime component of trusting relationships established through the Internet [Sawhney and Zabin 2002]. The use of the Internet for transacting with the government may be inhibited not only because citizens do not trust those collecting data (government) [Hoffman et al. 1999], but also because citizens do not trust the means through which data are collected (Internet technology). When sharing personal information with the government, citizens have greater trust in face-to-face communications than over post, telephone, and the Internet. Thus, for different channels, citizens have different levels of trust that the information shared by them will be secure [Cullen and Reilly 2007].

Citizens’ overall trust in Internet technology can be broadly divided into two parts. First, their trusting belief in the competence and ability of the Internet technology to help improve their interaction with the government as compared to offline channels [McKnight et al. 2002]. This trust is similar to relationship based competence trust. Competence trust develops with continued experience in using the e-government Web sites.
However, for initially trying out and using Internet technology for interaction with the government, a second kind of trust needs to be fostered among the citizens, which is their trust in Internet technology as a safe and secure medium for information transfer. Past research has shown that the perceived risk of having one’s personal identity and financial information being stolen by hackers may deter Web usage [Cullen and Reilly 2007; O’Brien 2000]. This perceived risk can be deterred by building institution based trust, drawn from adherence to technical standards and security procedures [Backhouse et al. 2005]. Institutional trust for Internet technology is similar to impersonal trust or system trust [McKnight et al. 1998; Pennington et al. 2003; Shapiro 1987]. In the case of Internet technology, institutional trust building mechanisms like Internet privacy, security, and encryption standards, and effective cyber laws have gained prominence. Cullen and Reilly [2007] reported that citizens had an enhanced level of trust in sharing information through the Internet if they knew that they “were accessing a secure Web site, had noted a padlock symbol displayed on their browser window, or ‘knew to be secure’” [pp. 7]. Thus, display of institutional confidence building measures on the e-government Web sites (e.g., TRUSTe marks) will increase the level of trust of citizens in government Web sites [Benassi 1999].

Citizen Trust in E-Government

For adopting and using e-government processes, citizens must have intention to “engage in e-government,” which encompasses the intentions to receive and provide information through online channels [Teo et al. 2009; Warkentin et al. 2002]. Although online interaction with the government provides “convenience” and “time savings” for the citizens, as they do not have to travel to the government offices and queue up to wait for services to be delivered,1 past research also indicates that citizen trust plays a vital role in the adoption and usage of e-government initiatives [Carter and Belanger 2005]. In the absence of adequate trust in e-government Web sites, citizens may either choose to not adopt or to revert to the traditional offline means of interaction with the government (e.g., face to face, postal service, or phone) [Teo et al. 2009; Srivastava and Teo 2004]. Carter and Weerakody [2008] showed that despite cultural differences in the adoption of e-government across countries, “trust” is a universal adoption factor. Using Moor’s concept of public value, Grimsley and Meehan [2007] exhibited that objectives for e-government go beyond the commercial goals of efficiency and effectiveness. Public trust in such systems may be dependent on the continuous evaluation of e-government systems. However, the presence of e-government systems may also lead to an increase in citizen trust in government, which is so very important for the success of governmental programs [Tolbert and Mossberger 2006]. In the current study we posit that citizen trust in e-government is dependent on the level of ‘citizen trust in government’ and citizen ‘trust in Internet technology.’

The various levels of citizen trust in e-government can be expressed in the form of a 2X2 matrix [Figure 1]. The different levels of citizen trust in government and in Internet technology indicates different kinds of relationships. Past research has shown that differing relationships between transacting partners, based on the levels of trust between them, leads to different performance outcomes [Dirks and Ferrin 2001]. Thus, differing levels of citizen trust in the two dimensions of trust may lead to different performance outcomes, as shown in Figure 1.

Past literature classifies different kinds of relationships that can exist between transacting partners, ranging from “arms length relationships” to “embedded relationships” [Foster 2002; Greenhalgh and Chapman 1995]. Relationships between the governments and citizens are long term, and fall somewhere between the clearly defined markers of “structural” and “relational,” which have different levels of trust between the two transacting parties. Past studies have also demonstrated that, even in the online scenario, trust plays an important part for relationship building among the transacting partners [Hoffman et al. 1999; Luo, Hsu and Liu 2008]. These relationships can be further finely grained by studying the varying levels of trust between the transacting partners. The four kinds of relationships—collaborative, cooperative, competitive, and adversarial—exhibit different states of trust among the transacting partners having different levels of the four attributes of trust: authenticity, history of fulfillment, the ability to fulfill, and commitment to the relationship [Hattori and Lapidus 2004; Solomon and Flores 2001].

In contrast to other contexts, where trust had been considered only on one dimension of relationship between the two transacting parties, the trustor and the trustee, in the case of e-government we have three transacting parties, citizens who have to have trust in the government as well as Internet technology [Teo et al. 2009]. Hence, for e-government, technology is conceptualized as a ‘transaction partner’ for citizens (in addition to government).

In Figure 1, a low level of citizen’s trust in the government coupled with a low level of citizen’s trust in technology, leads to a condition where the citizens are adversaries to technology as well as government. In this situation, the

---

1 For example, in Singapore the option of filing a tax return at the Inland Revenue Authority of Singapore (IRAS) office exists, yet most citizens choose to file their tax returns online through the Internet because of the convenience and time savings it offers.
lack of trust in both dimensions leads to *unfavorable outcomes* as regards acceptance of e-government initiatives. Such a situation is not conducive to the implementation or success of e-government programs.

A low level of trust in the government coupled with a high level of trust in technology leads to a situation where citizens might use technology as a *competitive* tool with the government. In such a scenario, they may use the increased information transparency brought about by the Internet to circumvent the government rules and/or highlight deficiencies in government. Implementation of e-government programs in such a regimen will lead to *unpredictable* and *sporadic* results. In such a scenario, e-government initiatives by the government, if any, are viewed with suspicion and cynicism by the citizens.

A high level of trust in the government but a low level of trust in the technology indicates a scenario where citizens try to *cooperate* with government efforts but the lack of their trust in the technology inhibits this cooperation. The condition is that of *compromise*, if the government implements its e-government initiatives. Though citizens cooperate with the government, they are not able to proactively contribute to e-government initiatives (due to their lack of trust in technology); hence the full potential is not realized.

A high level of trust in the government’s ability, motivation, and commitment for e-government programs coupled with a high level of trust in enabling technologies leads to *synergy* between the government and citizens. This *collaborative* behavior leads to proactive effort by citizens, as well as the government, toward the success of e-government programs.

Orlikowski and Robey [1991] had conceptualized ‘technology structures’ as separate from ‘organizational structures’ which were very much a part of the structuration process, both influencing and being influenced by the human actors. Technology structures continuously interact with and shape institutional norms, which further influence human actions. Hence, it is appropriate to consider not only citizens’ “trust in government” as a factor for determining citizen action (for adoption and usage of e-government), but also their “trust in Internet technology,” because Internet technology is an integral part of the e-government process.
Further, past research has shown that trust between transacting parties is not static, but evolves over time [e.g., Jones and George 1998; Butler 1991]. Hence, we posit that the level of citizen trust in “government” and “Internet technology” also evolves over time. Though in the previous discussion of the trust framework the four quadrants appear to be static snapshots in time, in actual practice, countries evolve from one quadrant to another. It is possible that at the start of e-government initiatives, a nation may be in a particular quadrant; for example, competitive or cooperative, but through a planned effort they may move towards the collaborative quadrant to enable successful adoption and usage of e-government initiatives. The political and technological legacy of the country determines its initial position in the citizen trust grid at the start of e-government programs, but nations can chart their future trust development process to facilitate successful adoption and acceptance by their citizens.

III. METHODOLOGY

For analyzing the role of citizen trust in e-government adoption and usage, we studied the case of Singapore by using a mix of primary as well as secondary data. We obtained primary data in two stages; first by conducting five focus groups, followed by one-to-one interviews with Singapore e-government users. Supplemental secondary data was obtained from various sources such as government Web sites, speeches of political leaders, e-government implementation reports, newspaper reports, and media releases.

Focus group participants were also asked to mark their perceptions about the state of citizen trust in the years 2003 and 2006 on the two dimensions of the proposed citizen trust grid (trust in government and trust in Internet technology – see Figure 1). So, apart from corroborating the findings emerging from the focus group discussions, the responses on the trust grid were useful in capturing the evolution of citizen trust on the two dimensions of trust in government and trust in Internet technology in the three years. After analyzing the focus group discussions and the perceptual mapping on the trust grid, we validated our findings by conducting one-to-one follow up interviews. Finally, we triangulated findings from focus-groups and interviews with the evidence obtained from various secondary data sources to arrive at a set of lessons learned for successful e-government implementation, from the trust perspective.

The study was conducted in Singapore as it has a fairly advanced e-government and has gone for a planned phase-wise implementation of e-government initiatives, thus providing an excellent research context [Srivastava and Teo 2005; Teo et al. 2009]. Singapore’s emergence as an e-government leader is recognized throughout the world which is reflected in the number of international awards and recognitions it has received. In 2009, Singapore is ranked first in the world for its e-government by Waseda University [Waseda University 2009].

Further, for studying a phenomenon like adoption and usage of e-government, the views of the young adult population are of utmost importance because online users tend to be younger and more educated than offline users of services and may be the target for online services [McKnight et al. 2002]. Hence, for this research we focus on the young adults in Singapore. The participants for the focus groups were solicited from a cross-faculty module in a large university, whereas, the follow up interview participants were young professionals working in Singapore. As in many other research contexts, students in Singapore provide an ideal pool of young adults with real world e-government experience, as interaction with government Web sites is common for the young population in Singapore for various purposes (for example, education, national service, youth activities, and sports) [Gordon et al. 1986; Teo et al. 2009]. In this study, respondents were familiar with the Internet in general and e-government Web sites in particular. The respondents averaged 7.6 years of Web experience and 3.4 years of experience using e-government Web sites. The student respondents in this study, all of whom have sufficient experience with some government Web sites, are being asked about non-hypothetical situations [McKnight et al. 2002]. To ensure that respondents took the survey seriously, the respondents were awarded course credits as an incentive for participation in the study. Hence, the student sample was an extension of the real world scenario and provides a valid sample for our research.

The general principles of confidentiality, anonymity, voluntary participation, and informed consent were adhered to in handling the participants [SRA 2003]. All students from a subject pool were invited to voluntarily participate in the study. The details of the study and the requirements were also mentioned at the outset in the invitation. Participants had the option of choosing our study or any of the other activities in the subject pool module. The results were aggregated so as to maintain the confidentiality and anonymity of the respondents.

For the five focus groups, we invited 50 participants in all (for each focus group, we invited 10 participants). Out of these, a total of 45 participants turned up for the focus groups. Prior to each focus group discussion, the participants were asked to fill in their perceptions of trust on the two dimensions of citizen trust grid for the years 2003 and 2006.

---

2 Prior experience with e-government Web sites was a prerequisite.
After this, each of the focus group discussions was initiated by one of the researchers. To maintain uniformity across the focus group discussions we followed a dialog flow based on the questions presented in Appendix 1. As a follow up, we also conducted 27 interviews with young working professionals in Singapore. Some sample designations of interview respondents were assistant vice president (AVP), senior manager, business analyst, engineer, lawyer, and research scientist. Again, to maintain uniformity, we followed the same script provided in Appendix 1 for the conduct of one-to-one interviews. Focus group and interview transcripts were analyzed for possible common themes on the role of trust for e-government adoption and usage emerging out of the discussion. We classified the findings from the focus group discussions on the two trust dimensions as per our research model: trust in government and trust in Internet technology. The results from the perceptual maps on the trust grid were also analyzed in conjunction with the focus group and interview transcripts to identify trends in the evolution of citizen trust.

IV. RESULTS AND DISCUSSION

Citizen Trust in Government

From the discussions in the focus group, it emerged that trust in government is vital for adoption and usage of any government initiatives. In the case of e-government, citizens do realize that interacting online offers a lot of convenience at a lesser cost, and this is the prime reason for the adoption of e-government Web sites. As one of the respondent remarked,

*It’s convenient and fast, compared to self-help phone service. Therefore this is one of the most efficient ways. The reason I continue using it is because it's immediately available rather than waiting for mailing service. I'm satisfied with its response time, ease of use without the need to follow much instruction.*

Still, trust in government is essential for citizens to consider using it:

*Trust is definitely important for e-government. We have the least corrupted government in the world. You can simply follow what they say and there is no need to worry that your information will be abused … I have confidence in our government, so I’m willing to use the e-service they provide.*

The past actions of the government are responsible for building citizen trust. In the case of Singapore, we mostly found the trust in government and its policies to be quite high:

*They [government] handle things quite well, like we have seen in the case of SARS*[^3] *outbreak and also we have a peaceful environment, means government is doing something right. At least we feel quite safe. In some countries, you cannot feel safe even on the road. Recent initiatives taken by government helps me feel more secure, like the registration of all SIM cards for mobile phones.*

*Singaporeans have an inbuilt trust in the government. We have seen this in the recent elections.*

We also observe from the discussions that the general trust in the government’s ability to perform has also translated to their trusting the government Web sites:

*Since we trust the government, so we trust their Web sites also. Government Web sites are quite safe as they have security features in place. Moreover, they have a reliable team at the backend to make it secure.*

*I believe that government is not only honest, but also capable enough to secure the Web sites and protect the interests of citizens.*

An interesting fact which emerged from the discussion was that, not only the adoption and usage of e-government requires trust in the government, but once adopted, it helps in reinforcing trust by making people more aware of government policies. As one participant mentioned:

*In fact, government Web sites are vehicles of trust development as they make us more aware of government policies.*

From the focus groups, two key points emerged. First, trust in government is essential for the adoption and usage of e-government. Second, the level of trust of citizens in government has been reasonably high over the 2003 to 2006 study time period. The past experiences of citizens in their interactions with the government and also government’s

[^3]: Severe Acute Respiratory Syndrome
past responses to the various national contingencies have been instrumental in creating its trustworthy image, which is similar to process based trust [Zucker 1986].

**Citizen Trust in Internet Technology**

The lack of citizen trust in Internet technology has emerged as a contributing factor in inhibiting adoption and usage of Internet related government or business transactions [Srivastava and Teo 2004; Warkentin et al. 2002]. A few focus group participants expressed their lack of trust in the Internet (especially in the security and privacy aspects). As one of the respondents remarked:

“I do not use the Internet for online banking or any monetary transaction mainly because there are so many viruses and spyware programs. I also feel that cyber criminals are more IT savvy than me.”

Though a few respondents were of the above view, when they were asked to mention any personally known negative Internet security related experiences, none of the participants cited any incident:

Though I have no negative experiences as such, but I still feel that Internet is not safe. I have read about it in the newspapers.

It appeared that most of these negative impressions were based on hearsay and articles in newspapers and magazines. Though some participants were not very certain about the security provisions in the Internet technology, most participants were of the view that they trusted the Internet:

The usual information accessed online is some general information. So I am not aware of the confidentiality. For personal data, the SSL security system is good enough for me to trust the technology. Such trust definitely influences me when I visit these Web sites.

Respondents were also of the opinion that stringent cyber laws in Singapore have been responsible for building trust in technology although they felt a need for universal cyber laws:

Cyber laws in Singapore are quite stringent, though there should be some kind of universal laws for tackling the problem across the world, since the Internet is borderless.

Most participants also felt that the level of trust in the Internet has gone up in the recent years:

Trust in the Internet has gone up. I am now shopping online, banking online, and can give my credit card numbers online. Though trust in the government is all the same, trust in the Internet has definitely gone up over the years.

Knowledge about Internet technology appears to be a major factor in increasing the trust leading to increased adoption and usage:

I think Singapore is proactive in promoting Internet usage. I am now aware of the ways in which I can prevent myself from being a victim on the Internet. There is a lot of convenience in transacting with government online - like you do not have to go to office for filing your tax return.

There were many respondents who mentioned that they trusted the Web sites operated by the government rather than all the other Web sites:

I trust the government Web sites but I am not sure about other Web sites. I believe that the government has taken sufficient safeguards to prevent our personal information from being hacked or stolen.

From the previous discussion, we observe that trust in Internet technology is a major inhibitor/facilitator for the adoption and usage of e-government Web sites by citizens. We also observe that most citizens participating in focus groups find the Internet to be trustworthy, although some of them expressed security concerns. But they have lesser security concerns about using government Web sites. Another fact which emerged from the discussions was that the trust in Internet technology has increased remarkably in recent years. Increased citizen awareness about security standards on the Internet has been a major factor contributing to this increased trust. The citizens’ trust in government has mostly remained the same over recent years, albeit at a high level.
Evolution of Citizen Trust in Singapore
The analysis in the previous section gave us an indication of the trajectory through which citizen trust in government and Internet technology has evolved in the past few years. Descriptive data from focus group participants revealed that on average, they had 7.6 years of Internet experience and all had used Singapore e-government Web sites.

To further examine the evolution of trust, we used the data collected from the responses of the participants about citizen’s trust in the two dimensions of trust grid (trust in government and trust in Internet technology) in the years 2003 and 2006 (Figure 1). The participants marked one position for 2003 and another for 2006 based on their perception of the level of their trust in government and in Internet technology, choosing from quadrants I to IV for each of the years [Figure 2]. The starting point of the arrow represents the year 2003, and the ending point (arrowhead) represents the year 2006. Hence, in Figure 2 each arrow along with the associated percentage figure represents the percentage of respondents following that path from the year 2003 to 2006. For example, if we consider the arrows starting and terminating in grid III, which represents high trust in government and a low trust in Internet (Figure 2), we observe that 22.7 percent of respondents indicated no change in their trust levels in both government and Internet. 40.9 percent of the total respondents moved from grid III to grid IV, indicating an increase in trust in the Internet. 2.3 percent indicated a decrease in trust in the Internet (movement from grid IV to grid III). Also, 2.3 percent of the respondents registered an increase in trust in the government (movement from grid I to III).
Thus, Figure 2 not only represents the levels of trust of the respondents in the years 2003 and 2006 but also shows how their trust has evolved between the years 2003 and 2006.

From this analysis, we observe that over 88 percent (22.7 percent + 40.9 percent + 2.3 percent + 20.4 percent + 2.3 percent) of the respondents marked the starting point (2003) for Singapore in the trust grid as being in quadrant III or IV, which signifies a high level of initial trust in Singapore government in the year 2003 itself. Compared to this result, only about 23 percent (20.4 percent + 2.3 percent) had a high initial trust in Internet technology (quadrants II and IV) in 2003, which substantially increased to over 70 percent (40.9 percent + 20.4 percent + 9.1 percent) in 2006. From the movement charted in Figure 2, we further observe that only about 2.3 percent of the respondents had a decline in trust in government, while the remaining 97.7 percent had either maintained the same level of trust or saw an increase in their trust in government. Similarly, for trust in Internet technology, we observe that only 4.6 percent perceived a decline, while the remaining 95.4 percent either maintained the same level of trust or perceived an increase. From our analysis in this section, we can make some estimation about the present level of trust of Singapore citizens in e-government. We find that, as per our research model, Singapore can be roughly classified to be in either the cooperative (quadrant III) or the collaborative grid (quadrant IV). However, the change is definitely towards the collaborative grid, which is the theoretically driven quadrant for e-government success (Figure 1). This is also ratified by a recent newspaper report, in which Seah Moon Ming, president of Singapore Technologies (ST) Electronics, commenting on e-government in Singapore said,

*The next lap for the government is to foster interaction and collaboration between itself and Singapore’s increasingly ICT and Internet-savvy citizens* [Business Times 2009].

### V. LESSONS LEARNED

From the previous analysis, we see that Singapore is definitely moving toward a path of successful e-government, from the citizen trust perspective. Singapore has been able to sustain a high level of citizen trust in government and has also been able to increase the citizen trust in Internet technology substantially in recent years. It also broadly satisfies the Accenture’s definition of service trust, where governments’ interactions are designed to build an implicit trust and citizens and businesses believe in the value their governments provide [Accenture 2004]. Commenting on the state of e-government in Singapore, Seah Chin Sion, Accenture’s Asia-Pacific managing director for government practice commented,

*In the case of Singapore, our citizen survey showed that Singaporeans overwhelmingly believe the government’s service had improved even relative to three years ago* [Choudhury 2007].

It is opportune to draw a set of lessons learned from the Singapore experience for successful e-government implementation. For this, we triangulate the focus group and interview data with the secondary information from multiple sources about government interventions, which are serving to enhance e-government adoption and usage in Singapore.

The continued efforts by the government for the economic and technological development of the nation made a profound impact on citizens. These initiatives helped in engendering a substantial amount of ‘process based citizen trust’ [Zucker 1986] in the government. Thus, at the start of e-government initiatives, citizen trust in the government was high. In a similar vein, citizens were exposed to a lot of IT systems because of the initiatives of the government. Though they had a general exposure to the background technology, they had no direct experience of interacting with the government online [Singapore i-Government Web site 2008].

Based on this discussion and the analysis in the previous section, it can be considered that at the launch of e-government programs, citizens could roughly be placed in the cooperative quadrant (Figure 1). Hence, at the start of its e-government programs, the Singapore government had two onerous objectives: (1) To maintain the high level of trust which citizens have in the government (as a legacy); and (2) To develop a high level of citizen trust in technologies enabling e-government, so that it gradually moves from the cooperative to the collaborative quadrant. The initiatives taken by Singapore government in its effort to move towards the collaborative quadrant offer a set of lessons which can be adapted and applied by nations across the world for successful e-government adoption and usage. In the following sections, we discuss the lessons learned in the development and maintenance of: (1) trust in government; and (2) trust in Internet technology (summarized in Figure 3).
Singapore has carried out a planned phase-wise implementation of its e-government programs. During the phase-wise implementation, Singapore government proactively incorporated measures for maintaining the high level of citizen trust in government in general, and simultaneously developing citizen trust in government’s ability, motivation, and commitment towards its e-government programs in particular. The development of this dimension of trust is an ongoing process [McKnight et al. 1998]. The two ways by which Singapore government is trying to achieve this objective are: soliciting feedback from citizens and having top leadership commitment and support for e-government.

Lesson #1: Solicit feedback from citizens.

In any IS planning and implementation process, ‘consultation and user participation’ is instrumental in predicting its effectiveness by enhancing the users’ trust [Palanisamy and Sushil 2002; Peffers et al. 2003]. In addition to the creation of trust through user involvement, providing feedback through electronic means connects the user community (citizens) on the Web, which enables transference of trust amongst them [Pavlou and Gefen 2004; Stewart 2003]. Citizens are not the only beneficiaries of online public services, as the ICTs also serve to involve
citizens in providing feedback to government, thereby contributing to policy formulation and review. One of the focus group participants mentioning the importance of feedback said:

Taking feedback and suggestions from citizens is essential. If the suggestion given by me is implemented, I feel that I have contributed to Singapore. I believe that if the suggestion is useful, they (government) will implement it. Giving feedback improves satisfaction of the citizens as they know that there is an outlet for voicing opinions.

With this objective in view, Singapore has effectively utilized ICT channels to take constructive and positive feedback from citizens through its Feedback Unit [Feedback Unit Website 2005]. Through its feedback Web site, the government not only seeks the opinions of citizens on various political issues and legislative bills, but also informs them about the latest legislative developments in the Singapore Parliament. Informing citizens about government policies and actions further reinforces citizens trust in government. The importance of this effort can be gauged by the fact that the feedbacks received are compiled into a monthly report and sent to the Permanent Secretaries of all the Ministries [Singapore i-Government Website 2008]. The feedback unit has certainly been instrumental in engendering trust of the citizens in the government’s initiatives, especially toward e-government.

Lesson #2: Demonstrate top leadership commitment and support.

Top management support elevates the role of IT in an organization leading to greater business use of the Internet [Teo and Too 2000]. Research has shown that top management support is also positively related to innovation adoption and implementation of information systems in organizations [Grover 1993; Meyer and Goes 1998]. In a similar vein at the national level, leadership commitment and support for technological implementations (like e-government programs) are imperative for their successful adoption and usage [Srivastava and Teo 2004]. This also leads to a reduction of the ‘middleman paradox’ and increases the commitment of the implementing agencies towards e-government success [Mahrer and Krimmer 2005].

Commenting on the important role of top leadership support in enhancing e-government in Singapore, one respondent said:

Government is encouraging citizens to use the Internet and its Web sites for transactions. They have reasonably comprehensive cyber laws and for enforcement, Singapore police has an Internet unit to tackle such crimes. They (government) are also encouraging citizens by providing IT related education through various programs. They even offer a discount on certain services if you pay online.

Leadership vision and support were present since the inception of the e-government program in Singapore. In fact, government top leadership was the driving force for most of the e-government initiatives, which helped boost citizen confidence in these programs. The National IT Plans and e-government Action Plans bear testimony to the political support for the ICT systems in the government. A recent initiative by the Singapore government “wireless@sg program” plans to provide Internet access to everyone at most public areas [IDA 2007].

The clear articulation of Singapore’s e-government vision by the top leaders has inspired mindset changes, enhanced citizen’s trust, and enabled government agencies to understand the move toward e-government transformation in Singapore [Ke and Wei 2004]. Thus, in the case of Singapore, top leadership support for various e-government initiatives has been instrumental in enhancing the citizen’s trust in e-government programs, leading to their efficient adoption and usage.

Development and Maintenance of Trust in Internet Technology

Citizen’s trust in government’s competence, ability, and benevolence is a necessary but not sufficient condition for the successful adoption and usage of e-government initiatives. The users of these technological initiatives should also trust the ‘enabling technologies.’ Siegrist et al. [2000] mention that citizens’ perceptions of a technology’s risk and benefits are important components of the entire political process, from the initial decisions, to developing a technology or product, to the acceptance of management approaches, to risk mitigation. For the successful adoption and usage of e-government systems, citizens must be able to see less of the risks and more of the benefits which they can derive from it. Three ways in which it is being engendered in Singapore are by: putting institutional trust building measures in place, proactively providing relevant knowledge and skills, and providing a comprehensive and effective legal system.
Lesson #3: Build institutional trust.

As highlighted by Zucker [1986] "institutional trust" is one of the important trust building mechanisms which can be instrumental in effectively instilling trust among citizens, leading to the success of its e-government initiatives. Based on the feedback from industry and the public, the InfoComm Development Authority [IDA] recognized the need for the widespread usage of trust marks for boosting the level of trust on e-transactions. The National Trust Council [NTC] was formed on February 28, 2001 with the vision of building public confidence in e-transactions. The NTC implemented the first nationwide TrustMark Program, namely, TrustSg seal, which could be awarded by the Authorized Code Owners [ACO] to online merchants who adhere to good e-business practices. TrustSg has now become a government sponsored ‘institutional trust’ building measure for reassuring the public about e-transactions.

The issue of trust also involves privacy and security concerns. Privacy means protecting the possible misuse of the personal information of citizens that the government collects, and security involves protecting e-government Web sites from the attacks of hackers and crackers and their possible misuse. Singapore has both a strong common law tradition and statutory provisions to prevent the misuse of personal information. Personal information is protected under a general law of “duty of confidence” and under sector specific laws such as the Banking Act, Statistics Act, the Official Secrets Act, and the Statutory Bodies and Companies (Protection of Secrecy) Act. The National Internet Advisory Committee (NIAC) released a “Model Data Protection Code for Private Sector” based on internationally recognized standards. This was fine tuned by IDA and NTC, in consultation with members of industry and the public, and promulgated as a “Model Code” for private sector adoption in December 2002. The importance given to privacy by Singapore Government can be gauged by the fact that the NTC has aligned its TrustSg mark with the principles of the ‘Model Code.’

Commenting on the importance of trust and the Singapore Government’s resolve to inculcate trust for e-government services and transactions, the then Deputy Prime Minister (now the Prime Minister) remarked (on the occasion of the launch of eGAPIL on 15 July, 2003):

"We started a nationwide program, called TrustSg to boost customer confidence in online transactions. Our survey shows that 75 percent of Singaporeans who needed to transact with Government did so through electronic means. The United Nations has just conferred a Public Service award on our TrustSg program, which is a vote of confidence in what we are doing."

Lesson #4: Cultivate IT Literacy.

Trust and knowledge are closely related to each other. Bridging the digital divide and increasing knowledge about ICT systems and their capabilities leads to their increased use, which in turn reinforces trust on these systems. Development of trust not only involves adoption of secure systems, but also involves communicating and educating citizens and government officials that such systems are as secure as traditional systems. The importance of IT education for e-government success was stressed by most respondents. Highlighting its importance, one of them explained:

"Media is one of the ways through which government engenders trust. Also, education plays a big role. Trying to reach the elders, who are not so IT literate – by educating them is vital for e-government success. They (government) are holding classes for IT literacy in community centers. I think government has made significant progress in that area."

"Government should advertise the technical safeguards they have in their Web sites so that the public feels safe when they use the Web site."

Li [2003] concluded that e-government is more of an organizational change issue involving citizens, as well as government officials, to trust the technology. Hence, IT literacy is essential not only for citizens, but government officials as well. Singapore government has adopted a two pronged strategy for imparting IT education not only to citizens but also to government officials. The InfoComm Education Program (IEP) ensures that public officers are equipped with the required ICT skills and knowledge. This is an ongoing program, which ensures that public officers have updated ICT knowledge to enable them to exploit the capabilities of ICTs to the maximum for the benefit of citizens and businesses. For citizens, mass e-literacy programs for bridging this digital divide have been adopted by the Singapore government. Trust building initiatives for educating and motivating the public to use e-government systems have also been implemented.

---

4 E-Government Action Plan
**Lesson #5: Enact comprehensive and effective legal system.**

An effective legal system, which assures security, safety, and privacy of citizens and businesses, is vital to the success of any e-government initiative by building the trust of citizens for using the technology. In the current digital economy the legal, regulatory, and business environment required for development are significantly different from those for traditional enterprise. Singapore is one of the first countries in the world to formulate and implement stringent cyber laws to enable the adoption and usage of e-government initiatives by trusting that using the enabling technologies are not risky for them. One of the focus group participants expressing her satisfaction with cyber laws in Singapore mentioned:

*I feel at the moment cyber laws are quite adequate and current in Singapore and trust in the legal system is also quite high.*

However, some felt that more has to be done to make the cyber laws stricter. One of the professionals remarked:

*They already have laws in place but they should be more stringent and there should be severe penalties for offenders.*

The presence of effective cyber laws and enforcement system has served as a major trust booster. Singapore’s Electronic Transactions Act (ETA) of 1998, enacted by the Parliament on June 29, 1998, is one of the earliest enactments of a cyber act in the world. It covers not only digital and electronic signatures, but also electronic records, electronic contracts, and is applicable to all kinds of electronic communications [Basu 2004]. The ETA addresses some of the important issues necessary for providing a conducive cyber-legal environment, such as: commercial code for e-commerce transactions, use of electronic applications for the public sector, liability of network service providers, and provision of Public Key Infrastructure\(^5\) (PKI) [IDA 2007]. The Evidence Act was also amended in 1997 to permit the use of electronic records as evidence in courts. The Singapore government has paid special attention to the issue of Intellectual Property Rights (IPR). Its copyright act was suitably amended in 1999 to improve copyright protection and enforcement measures for copyright owners in the digital environment, thus promoting the use of the Internet for business. The government passed amendments to the Computer Misuse Act in 1998 giving it greater power to take preemptive actions against computer terrorism and cyber crimes [Tan 2003; Jutla et al. 2002].

**VI. LIMITATIONS**

Although the study examines an important issue for the adoption and usage of e-government, it has a few limitations. *First*, the study is specific to the case of Singapore. Different governments may have different structures, especially governments with larger heterogeneous populations which tend to be more complex and may have several layers. This limits the ability to generalize the findings, yet the study provides a starting point for exploring the role of trust for e-government adoption and usage. *Second*, in this research we have conceptualized trust in a general way. The analysis does highlight the important role that trust plays in the e-government adoption and usage. Nonetheless, future research can further explode the black box of ‘trust in e-government’ to examine the relationships of multiple dimensions of trust – e.g., competence, benevolence, and integrity with the adoption and usage intention. *Third*, as illustrated by the findings in this study, the level of trust in e-government is a continuously evolving phenomenon. Hence, through this study we could capture the trend rather than the exact level of trust at a particular point in time. When adapting the findings from this study to other national contexts, governments should assess the levels of trust manifesting in the specific nation to come up with recommendations for that particular nation. *Fourth*, there are multiple risks associated with e-government both for citizens and the government. In this research, we have taken the perspective of the citizens and have restricted our discussion about risk from their perspective. E-government implementation also entails multiple risks for the government. For example, government Web sites may be hacked to display irrelevant (or undesirable) information.\(^6\) Further, a security breach can cause the leakage of classified government information. Such cases may tarnish the image of the government. Future research can examine e-government implementations from the risk perspective of the government.

---

\(^5\) PKI is universally recognized as the most secure platform for e-commerce transactions and addresses all four elements of network security: authentication, non-repudiation, confidentiality, and integrity. It enables ICT network users to exchange digital information securely and confidentially, and refers to the whole system of policies, processes, and technologies including digital certificates, certificate servers, and Certification Authorities (CAs) required for such an exchange.

\(^6\) Cases of government Web sites being hacked or defaced are being increasingly reported in the press in the recent years, e.g., http://news.softpedia.com/news/UK-Government-Website-Hacked-Twice-106435.shtml.
VII. IMPLICATIONS

Implications for Research

The study has several important implications for research. First, we propose and test a model integrating the technological, as well as the social dimensions of trust, in the context of e-government adoption and usage. Though trust has been found to be a significant factor in many other contexts, such as e-commerce [McKnight and Chervany 2001; Lim et al. 2006], current literature on e-government from the trust perspective is relatively sparse. Our study exhibits the importance of considering trust as an important facilitator for the success of e-government initiatives. Second, the theoretically driven model proposed in this study identifies two dimensions of citizen trust in an e-government scenario: trust in government and trust in Internet technology. It is important for future researchers to consider citizen trust on both of these dimensions in the context of e-government. Third, we chart a model tracing the evolution of citizen trust in Singapore, which is moving from the cooperative quadrant (high trust in government and low trust in Internet) to the collaborative quadrant (high trust in government and high trust in Internet technology). The model also describes all of the plausible positions which governments take on these dimensions, viz., adversarial, competitive, cooperative and collaborative. It is important for future research on trust in general, and trust in e-government in particular, to consider citizen trust as a dynamic attribute. Hence, trust building is an evolutionary process dependent not only on the initial conditions, but also on the trust in related dimensions. Literature on the evolution of trust, especially in the context of public sector and governments is relatively sparse. Through this study, we pave the way for such future research. Fourth, we extend the theories on trust by exhibiting that it is important not only to consider the different ‘types’ of trust but that there may also be “multiple dimensions where trust needs to be manifested. Using data from focus groups, interviews, and other multiple secondary sources, we validate our theoretically driven trust grid. Our data analyses which show that Singapore is gradually evolving from the cooperative to collaborative quadrant [Figures 1 and 2] serve as an apt case for distilling learning for nations across the world for e-government implementation.

Implications for Practice

Our study has equally significant implications for governments, policy makers, and public administrators. First, e-government implementation is often being viewed as a “technological initiative” rather than a “citizen trust building initiative.” The trust perspective, used for understanding this case, brings forth the importance of fostering and developing citizen trust for successful e-government adoption and usage. Second, the study exhorts practitioners to focus on trust building measures on multiple dimensions simultaneously for successful adoption and usage of technology. Specifically in the context of e-government, public administrators and policy makers should direct their attention to citizen trust building measures on the two dimensions of: trust in government and trust in Internet technology. The trust grid provides empirical evidence to the governments undertaking e-government initiatives that in addition to investing in latest technologies, they have to invest in citizen trust building initiatives. Third, through the case of Singapore, this research also demonstrates how “citizen trust” may be engendered on the two dimensions of trust, namely, trust in government and trust in Internet technology. We demonstrate that the process of trust building is an evolutionary process and nations around the world should aim for gradually evolving to the collaborative quadrant of the ‘e-government citizen trust grid’ for maximum impact. Fourth, by triangulating the data from focus groups and interviews, with the secondary data from multiple sources about Singapore e-government, we offer a set of trust-centric lessons learned. These “lessons learned” from the Singapore experience can serve as a useful guide for governments, policy makers, and public administrators for enhancing citizen trust, thereby allowing them to implement their e-government programs successfully.

VIII. CONCLUSIONS

Many e-government initiatives around the world have been sporadic and unsystematic [Srivastava and Teo 2004; 2005]. Trust, which is an important concern for e-government implementation has often been overlooked by researchers as well as governments. This has resulted in a lesser than intended impact of e-government initiatives on citizens as well as governments. The present study addresses this important gap in the e-government literature in two ways. First, we propose a theoretically driven citizen trust grid which identifies the two dimensions of trust for the e-government scenario: trust in government and trust in Internet technology. We also conceptualize citizen trust in e-government as an evolving process depending on certain facilitating conditions. Second, based on our research analyzing the case of Singapore e-government, we validate our proposed citizen trust grid and offer a set of ‘lessons learned’ for successful adoption and usage of e-government. The lessons learned from the Singapore experience can help governments around the world plan their e-government implementation programs.

Using the “citizen trust grid,” future research can test its applicability in other scenarios and countries. Most of the factors analyzed in this study are from a country level of analysis. Other factors associated with citizen trust in e-government, e.g., literacy level, digital divide, economic development, the role of non government organizations, etc., can be studied. Future research can also be directed at analyzing the impact that the level of trust in different
dimensions may have on e-government implementation, which consequently impacts the social and economic performance of the nation.

REFERENCES

Editor’s Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web can gain direct access to these linked references. Readers are warned, however, that:
1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the references, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.


APPENDIX 1: GUIDELINES FOR FOCUS GROUP DISCUSSIONS

1. What e-Government Web sites you have visited? Any comments on them. Please share your positive or negative experiences.

2. What is the purpose of your visit to these Web sites? How often do you visit them?

3. In recent years, has the adoption and usage of e-government Web sites by Singapore residents increased? If so, what according to you are the prime reasons for this increased adoption and usage?

4. How important is it for the users to trust the Internet as a useful means of interaction to adopt its usage?

5. How important is citizens’ trust in the government for facilitating e-Government adoption and usage?

6. How is the Singapore government trying to engender trust of its citizens in:
   a. Government
   b. Internet Technology

7. Are the efforts in these directions sufficient?

8. Please give your suggestions for increasing the trust of citizens in government and technology to facilitate e-Government adoption/usage in Singapore.

9. Please give other suggestions for increasing e-Government usage/adoption in Singapore.

ABOUT THE AUTHORS

Shirish C. Srivastava is an assistant professor at HEC School of Management, Paris. He obtained his PhD from the School of Business, National University of Singapore. His research has been published in several international refereed journals such as *MISQ Executive, Journal of Management Information Systems, Journal of Information Technology, Communications of the Association for Information Systems, Journal of Global Information Management, Information Resources Management Journal*, and *Electronic Government: An International Journal*, among others. He has also authored several book chapters and has presented his research in key international refereed conferences such as International Conference on Information Systems (ICIS), Academy of Management (AOM), Academy of International Business (AIB), Institute for Operations Research and the Management Sciences (INFORMS), and Americas Conference on Information Systems (AMCIS). He has been thrice nominated for the prestigious Carolyn Dexter Award at the Academy of Management (AOM) Meetings 2005, 2007 and 2008 and was a finalist for the award at AOM 2007. Recently, he has been nominated for the academy-wide William H. Newman award at the AOM 2009 Chicago, and is the winner of the Gerardine DeSanctis Dissertation Award for the best doctoral dissertation paper in organizational communication and information systems. He has also been a winner at the Society for Information Management (SIM) Paper Award Competition, 2007. His research interests include IT-enabled offshore sourcing, e-government, IS strategy and e-business strategy.

Thompson S. H. Teo is an associate professor in the Department of Decision Sciences at the School of Business, National University of Singapore. His research interests include strategic use of IT, e-commerce, adoption and diffusion of IT, strategic IT management and planning, and offshoring. He has published more than 100 papers in international refereed journals. He is senior associate editor for the *European Journal of Information Systems*, regional editor (Asia and Pacific) for the *International Journal of Information Management*, and is also on several editorial boards such as *Communications of the Association for Information Systems, Internet Research and Omega*. He has co-edited four books on IT and e-commerce, and is also a two-time winner of the SIM Paper Competition Award.

Copyright © 2009 by the Association for Information Systems. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and full citation on the first page. Copyright for components of this work owned by others than the Association for Information Systems must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or fee. Request permission to publish from: AIS Administrative Office, P.O. Box 2712 Atlanta, GA, 30301-2712, Attn: Reprints; or via e-mail from ais@aisnet.org.