doi:10.1111/j.1365-2575.2012.00420.x

Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service

Tejaswini Herath,* Rui Chen,† Jingguo Wang,‡ Ketan Banjara,§ Jeff Wilbur¶ & H. Raghav Rao**

*Department of Finance, Operations and Information Systems, Faculty of Business, Brock University, St. Catharines, ON L2S 3A1, Canada, email: teju.herath@brocku.ca, †Department of Information Systems and Operations Management, Miller College of Business, Ball State University, Indiana 47306, USA, email: rchen3@bsu.edu, ‡Department of Information Systems and Operations Management, College of Business Administration, The University of Texas at Arlington, Arlington, Texas 76019, USA, email: jwang@uta.edu, §Business Development, Iconix, Inc., San Jose, California, email: Ketan.Banjara@iconix.com, ¶Marketing, Iconix, Inc., San Jose, California, email: Jeff.Wilbur@iconix.com, and **Management Science and Systems, School of Management, State University of New York at Buffalo, Buffalo, NY 14260-4000, USA and SSME, Sogang University, Korea, email: mgmtrao@buffalo.edu

Abstract. *Email plays an important role in the digital economy but is threatened by increasingly sophisticated cybercrimes. A number of security services have been developed, including an email authentication service designed to cope with email threats. It remains unknown how users perceive and evaluate these security services and consequently form their adoption intention. Drawing on the Technology Acceptance Model and Technology Threat Avoidance Theory, this paper investigates the factors that affect user intention to adopt an email authentication service. Our results show that user intention to adopt an email security service is contingent upon users' perception of risk and evaluation of both internal and external coping strategies. This study contributes to research in security service adoption, service success and design, and information security behaviour.*

Keywords: information security, security service adoption, email authentication service, internal and external coping strategies, protection motivation theory, technology acceptance

INTRODUCTION

Email has served as a cost-efficient tool that supports and enables information sharing and communication. According to Pew Internet's April 2009 survey, 90% of the adults who use the

internet also use email on a daily basis. However, limitations in technical design, security provisions and legal solutions render email an '*ideal*' attack vector for a variety of cybercrimes. Email is often used to steal personal and financial information through phishing and spamming schemes, which leaves internet users vulnerable to identity theft and online fraud. In their recent Global Threat Report for 2009, Symantec reported 12.7 trillion spam messages, which accounts for approximately 89% of all email messages. Almost 73% of the phishing attacks were in the financial sector (Symantec Corp, 2010). Email is also used to spread viruses, worms, Trojan horses and malware. These threats can result in the alteration of data, corruption of data, theft of personal information and loss of computing capability. A report by SonicWALL Inc. analysed the data of 1.3 million email users from April to July 2007 and found that phishing, viruses and spam emails accounted for 37.4% of all emails, while benign emails accounted for only 6.9% (Harminka, 2007).

Email threats endanger information sharing and communication through email-based systems and, consequently, the commercial activities and business models they support (Wang *et al*., 2009a; 2009b). A number of software systems and services have been developed to protect email security, including email filters and sender authentication mechanisms (e.g. proofPoint, Iconix, IronPort, GlobalSign and Postini) that either block malicious emails from reaching users or help users verify email authenticity. While email filters are now a standard configuration for an enterprise's mail servers as well as the email clients of end users, email authentication services have recently emerged as the next generation email security solution.

Email authentication services verify whether an email is actually sent out from its purported domain. The business model used by email authentication services usually involves financial firms or other business entities that pay service providers to verify emails sent from their domains while individual email users use the services for free. The study focuses on the adoption of an email authentication service, hereafter referred to as eAuth. The eAuth service has a lightweight software plug-in downloadable from the vendor's website and it supports email processing for both webmail such as Yahoo! and Hotmail®, as well as email client programs such as Outlook®. When users open their email, eAuth automatically verifies the authenticity of received emails and displays graphical checkmarks in front of authenticated emails. Currently, eAuth, a leading authentication service, is able to verify over 300 online companies in financial, banking, retailing and service sectors.

While some email security solutions (e.g. spam filters and anti-virus solutions) may be implemented at an enterprise level (or by their mail servers), many authentication services depend on customers' and employees' voluntary adoption and use the services as an add-on for their email clients. As IT security environments tend to be highly decentralised, the information security of an organisation depends on such voluntary protective actions (Warkentin & Johnston, 2006). Given this, we evaluate the drivers of users' voluntary adoption of email authentication services in our study.

Drawing on the Technology Acceptance Model (TAM) and Technology Threat Avoidance Theory (TTAT), we consider users' intention to adopt email authentication services as a form of coping motivation that is influenced by a combination of internal and external coping mechanisms. In this study, internal coping mechanisms refer to mechanisms that are built and

possessed by individuals (e.g. one's own ability to detect and mitigate threats), whereas external coping mechanisms concern those instruments that are purposefully acquired from outside sources (e.g., an email security tool that is purchased). In this vein, we explore the following two research questions: (1) How does threat appraisal and coping mechanism appraisal (both internal and external) affect a user's intention to adopt an email authentication service? (2) What influences external coping mechanism appraisal within the context of email? To date, there exist scant empirical findings that address these questions. The contribution of this paper is twofold. First, guided by TTAT and TAM, our study develops an integrated theoretical model to investigate user intention to adopt an email authentication service. Second, we empirically examine this integrated model in the scenario of eAuth adoption. The empirical validation of the research model yields insightful findings and our research has important implications for security system design and adoption, vendor's privacy practices and education/awareness initiatives.

The paper is organised as follows. We begin the next section with an overview of research and related literature. Next, we develop our research model and hypotheses. The subsequent section elaborates the research methodology and presents the results. Finally, we discuss the theoretical contributions, practical implications and future research avenues of the study.

BACKGROUND AND RELATED LITERATURE

The literature identifies email phishing, pharming, viruses and spam, as key threats and outlines their broad detrimental consequences as email overload, user privacy and information system security. Security and privacy considerations are crucial to research in email security services (Ghosh, 2001). To date, a number of email security services have been proposed, including secured email networks, email registration services and email firewalls (Ducheneaut & Watts, 2005; Gupta *et al*., 2006). However, existing email security systems/services are often criticised by end users for their poor design, unsatisfactory performance and intrusive nature, and consequently their adoption is in question (Bellovin, 2004).

Email threats drive individual users to search for threat-coping strategies that may be understood through the lens of Protection Motivation Theory (PMT). A review of related security literature indicates that, in general, security practices may be understood as a coping mechanism in the face of cyber threats (Woon *et al*., 2005; Workman *et al*., 2008; Herath & Rao, 2009b; Liang & Xue, 2009; 2010; Johnston & Warkentin, 2010), among others). Rooted in coping and fear appeals literature, PMT (Rogers, 1975; 1983) describes coping with a threat as the result of two appraisal processes – a process of threat appraisal that involves the seriousness and likelihood of the threat, and a process of coping appraisal that involves the availability and effectiveness of the recommended preventive behaviour. Later, this theory was amended to include perceived self-efficacy (i.e. the level of confidence in one's ability to undertake the recommended preventive behaviour) as a factor in the coping appraisal process (Rogers, 1983). Liang & Xue (2009) extend this line of thinking to develop TTAT in the context of information systems (IS). TTAT suggests that technology users faced with technology

threats first appraise the existence and degree of the IT threat and then assess what they can do to avoid the threat. Based on these appraisals, they decide which safeguarding measure to use to reduce the threat. Both theories suggest that an individual may be inclined to take protective action as a result of the cognitive appraisal of threat. Threat appraisal subsequently activates the coping appraisal in which the user assesses various coping mechanisms (Liang & Xue, 2009). The coping appraisal process evaluates one's ability to cope with and/or avert the perceived danger. TTAT suggests that in coping with a threat, an individual can thus take a proactive problem solving approach to change the objective reality by carrying out an adaptive behaviour such as the adoption of safeguards.

The adoption of protective technologies can also be evaluated through the prism of acceptance theories such as TAM, which may augment TTAT in explaining external coping appraisal. TAM, a widely used model in IS research, posits that user intention towards the adoption of services is driven by user attitude, which is a joint product of user perception of service usefulness and ease of use (Davis, 1989; Davis *et al*., 1989). Current information security research, however, has argued that traditional technology acceptance theories are primarily associated with positive outcomes such as enhanced productivity and decision-making, and a broader theoretical lens that captures the inherent dynamics in security is needed to understand security tools adoption. Liang & Xue (2009) argue that technology acceptance theories such as TAM do not work well in explaining IT usage contexts that differ from performance improvement such as a threat avoidance context where the user goal is to move away from the state of risk. The adoption of technologies to avoid negative outcomes is a more complex phenomenon and needs the consideration of security context specific factors. The perception of risk or threat is central to the adoption of security technologies, and technology adoption theories, which are mainly concerned with the software that enhances productivity, are insufficient to understand the adoption of protective technologies (Liang & Xue, 2009).

We propose that TAM can be integrated with other relevant theoretical frameworks to give an in-depth understanding of security practices. Specifically, we argue that TTAT in integration with TAM will offer a stronger theoretical underpinning to understanding coping with email risks. In the context of email security, we view the adoption intention of eAuth as a coping motivation. Further, we expect that TTAT constructs (e.g. threat and coping appraisal) will largely explain eAuth adoption intention whereas the formation of appraisal of external coping mechanisms can be accurately assessed through TAM tenets (Figure 1).

Our analysis of eAuth adoption extends the existing literature on TTAT and TAM in two significant ways. First, we argue that security coping mechanisms may consist of both internal and external mechanisms. Unlike prior TTAT research that has focused solely on external mechanisms such as security tools, we consider internal coping mechanisms whereby individuals may rely on their own capability to detect email-borne threats. Prior studies have pointed out that an individual may screen emails through cues such as the 'from line' and 'subject line' to detect malicious and benign emails (Wang *et al*., 2009a). The appraisal of one's email screening capability may be referred to as email screening self-efficacy. Email screening self-efficacy assesses one's own ability to mitigate email threats without the aid of

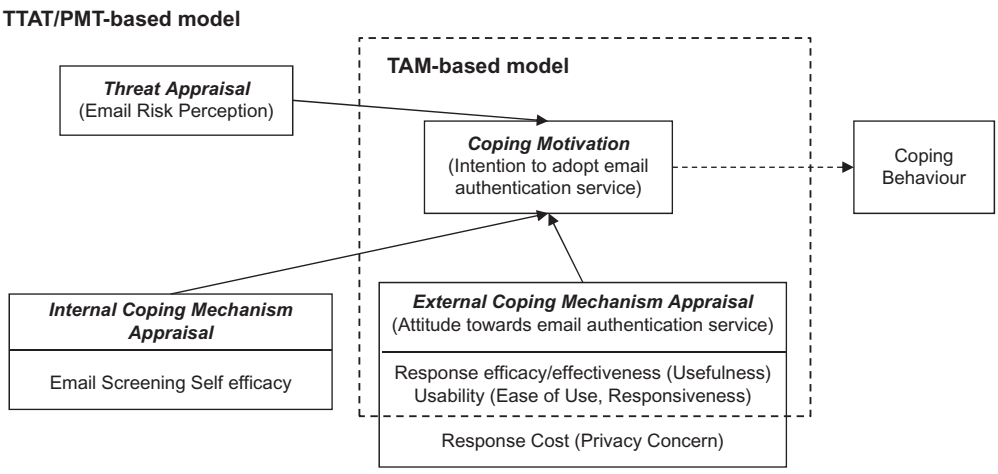

Figure 1. Research framework for security services adoption through PMT, TTAT, and TAM.

technical instruments and, thus, it differs from the self-efficacy construct of TTAT, which evaluates one's own ability to use a given security tool. We envision the internal coping mechanism to have a substitutive effect on external coping mechanisms, i.e. security tools. That is, a user who is well equipped with email screening capability may be less likely to resort to the use of a security tool such as eAuth.

Second, we identify the influences on external coping appraisal within the context of email security. TTAT suggests that perceived effectiveness, cost and self-efficacy in using the security system determine the coping appraisal. In our study, we examine these influences within the tenets of TAM. We view end user attitude towards eAuth as a coping appraisal because its use relates to one's judgment of email threat avoidability. In accordance with our previous discussion, user attitude toward eAuth is considered an external coping mechanism in that it associates with and reflects the outcome of using an external threat-coping instrument (i.e. eAuth system). Perceived effectiveness is a subjective assessment that a safeguarding measure can effectively avoid a potential IT threat (Liang & Xue, 2009). Among the predictors of eAuth effectiveness, we postulate that perceived eAuth usefulness and service responsiveness will have a significant impact. TTAT also suggests that the high cost of security measures may discourage an individual from undertaking protective measures. Regarding email security, email authentication services need to monitor and analyse all incoming email messages. This imposes privacy constraints on users because during the process, the email security services may collect information on email senders, titles and content, as well as analyse user preferences and behaviours. The collection, storage and use of user information, however, may raise privacy concerns and result in the perception of the service as '*privacy invasive*' (Xu & Teo, 2005). We expect that perceived privacy invasion increases the costs of using eAuth and consequently hampers its adoption.

HYPOTHESES DEVELOPMENT

TTAT suggests that coping motivation leads to coping behaviour where motivation is envisioned as the degree to which users are motivated to undertake security measures to avoid IT threats (Liang & Xue, 2009). The objective of this study is to understand coping behaviour in terms of the adoption and use of the email authentication service eAuth. With a somewhat broad definition of protection motivation or avoidance motivation, the PMT literature has most often used intention as a dependent variable (e.g. Stanley & Maddux, 1986; Steffen, 1990; Neuwirth *et al*., 2000). Recently, a TTAT study has also considered an intention-based measure to capture coping motivation (Liang & Xue, 2010). Many technology acceptance theories contend that intention is a strong predictor of technology use behaviour. Thus, in this study we consider *intention to use eAuth* as the final outcome variable. Figure 2 presents the theoretical model developed in this section.

In the current study, threat appraisal is reflected in email risk perception. Email risk perception is defined as an individual's assessment of the risks inherent in email processing activities. The security literature posits awareness of the environment's current state of activity and threats results in behavioural adjustments (Choi *et al*., 2008). Thus, individuals who perceive

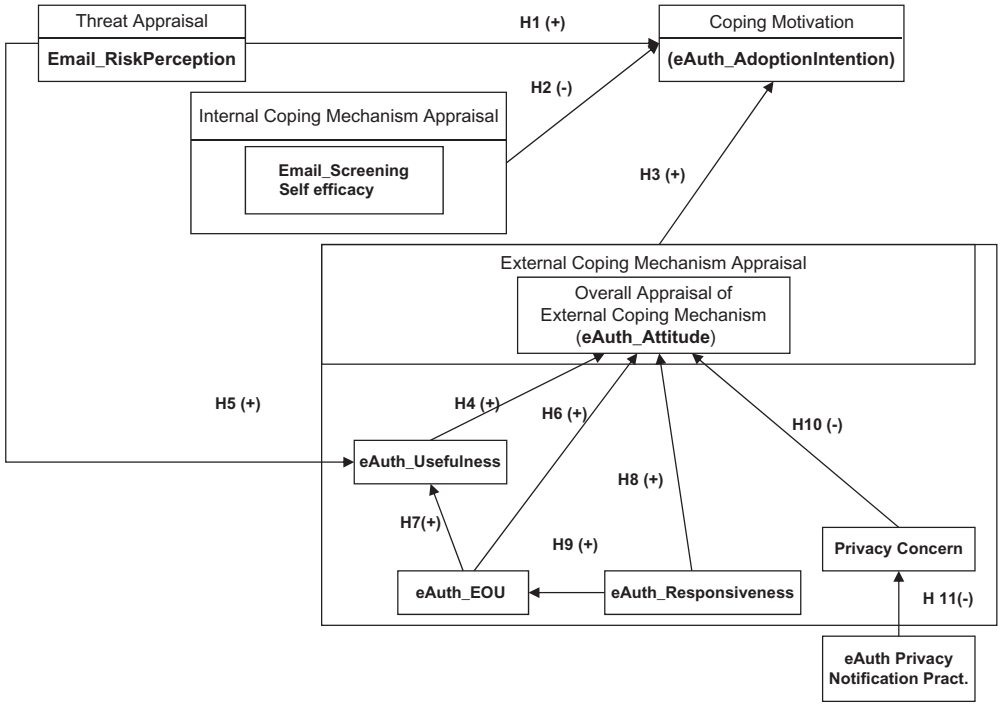

Figure 2. Research model.

a high level of risks tend to be motivated to undertake coping mechanisms. Individuals with low risk perceptions, on the other hand, are less likely to take precautionary measures. Prior studies suggest that when people perceive a threat as severe and likely, they undertake measures that they think are effective in preventing the IS security threat (Woon *et al*., 2005; Workman *et al*., 2008). More particularly, we believe that users who believe that risks posed by emails are likely and may have a considerable impact are likely to use an email authentication service. Thus, we expect:

H1: Email-related risk perceptions will be positively related to the intention to adopt email security services.

When email threats are perceived, internal coping appraisal may be achieved through an evaluation of an individual's ability to screen messages for authenticity using visual or language cues, which is referred to as email screening self-efficacy in this paper. Individuals with high email screening self-efficacy may perceive that they are able to carry out this safeguarding task without the aid of a security tool. In other words, users who feel self sufficient in their ability to screen emails may not feel the need to complement their self-efficacy with external coping mechanisms such as security tools. Consequently, they may view an email security service as less value adding (Lewis *et al*., 2003) and may not consider adopting email authentication services such as eAuth. In general, prior research has shown a strong relationship between self-efficacy and risk-taking behaviour (e.g. Heath & Tversky, 1991; Kruegar & Dickson, 1994; Dulebohn, 2002). Individuals with low email screening self-efficacy, however, may view the email security service as more value adding since it extends their capability in the email authenticity verification process. Thus, we expect that:

H2: Email screening self-efficacy will be negatively related to intention to adopt an external coping mechanism (eAuth service).

The overall appraisal of the external coping mechanism in this study is captured by user attitude towards an email security measure such as eAuth. In this study, attitude refers to an individual's positive evaluative affect about using email security services. Using a security service allows users to develop their attitude towards the service, which, over time, results in a positive or negative outlook regarding adopting it for future use. This is in line with TAM (Davis *et al*., 1989), which suggests that an individual's attitude toward using a technology predicts his or her intention to adopt the technology. Accordingly, we hypothesise:

H3: An individual's attitude toward an email security service will be positively related to his/her behavioural intention to adopt the service.

The appraisal of the external coping mechanism is determined by the evaluation of response effectiveness, usability of response, and response cost. A number of factors may affect the effectiveness of a safeguard. Inappropriate system design, weak infrastructure support and demanding environment, for example, may render a security safeguard less able to detect attacks and take response actions. TTAT contends that response effectiveness has some nexus with perceived usefulness in TAM (Liang & Xue, 2009). Perceived usefulness, defined

as the degree to which a technology is perceived as providing benefits in performing activities, is important to technology acceptance (Davis *et al*., 1989). Positively valued outcomes often increase one's affect towards the means of achieving those outcomes. Perceived effectiveness of a security service in terms of its ability to avoid threats is likely to increase a user's positive attitude towards the service; thus, a positive relationship between perceived usefulness and attitude is envisioned. In the context of our study, if a user perceives the security service to be useful, he or she is likely to have a positive attitude towards the service. Hence, we hypothesise:

H4: Perceived service usefulness will be positively related to the attitude towards accepting the email security service.

This response effectiveness may, however, be affected by threat perception. Individuals who perceive higher levels of risk in email-based information sharing and communications are likely to appreciate the potential utility of email security services more than those who do not. If an individual believes that spam and phishing emails pose a risk, then the individual is likely to see the need for email authentication. On the other hand, if the individual thinks that emails do not pose a high level of risk, he or she is less likely to appreciate the service. This line of thinking is supported by TTAT, which suggests that the perception of threat leads to the sense of urgency that motivates a user to evaluate the coping mechanism. Thus, we expect that:

H5: Email-related risk perceptions will be positively related to the usefulness of email security services.

The second determinant of coping appraisal is the ability to use the service. Perceived ease of use, which refers to the degree to which the prospective user expects the target system to be free of effort, influences attitudes and behaviour by two mechanisms: self-efficacy and instrumentality (Davis, 1989). The easier the system is to use, the greater the user's sense of his/her own ability to carry out the sequences of behaviour needed to operate the system will be. Ease of use removes the cognitive impediments to using the service, which makes the authentication service more accessible to end users. This reduced impediment is likely to result in users having a positive affect towards the service. Echoing the prior literature, we also anticipate that perceived ease of use will positively influence the perceived usefulness of the service.

H6: Perceived service ease of use will be positively related to attitude towards the email security service.

H7: Perceived service ease of use will be positively related to the usefulness of email security services.

Email authentication services such as eAuth operate by checking the authenticity of an email sender. That is, the sender's identity of a given incoming email is checked against the registered information kept in the centralised data repository of the remote eAuth vendor servers. As a consequence, the responsiveness of eAuth may be influenced by the telecommunication infrastructure, speed of data transmission and database queries, among

other things. Email security is usually achieved through options such as strict access controls, constraining usage policies and complicated computing procedures. These designs, however, conflict with norms of service usability that advocate simplicity, flexibility and responsiveness. The usability literature outlines service responsiveness as a key component (Palmer, 2002). Services low in responsiveness may negatively impact the perceived ease of use in that the delays can introduce difficulties in operating and utilising the services that lead to loss of '*control*' (Palmer, 2002). Having to wait too long for information creates negative perceptions and can be frustrating for users. Email serves as a timely and efficient communication channel and, hence, users expect high responsiveness from email-related services. Hong & Tam (2006), in studying information appliances that require online service, found that the extent to which information technology was perceived to provide pervasive and timely connections had a significant positive impact on both usefulness and ease of use. We therefore anticipate:

H8: Perceived responsiveness of the service will positively affect the attitude towards the email security service.

H9: Perceived responsiveness of the service will positively affect the perceived service ease of use.

The last determinant of the coping response is the cost associated with the response. Email security services constantly access user inboxes to examine incoming emails for identification verification purposes. During the process, the email security services may collect information about email users and emails to provide more tailored services. Such information could be used: (1) by the security service; (2) to customise the content and service; (3) to gather information for market research; (4) to share with supporting agents or contractors; and/or (5) to verify compliance with the policies and applicable laws. The collection, storage and use of user information, however, may raise privacy concerns and result in the perception of the service as '*privacy invasive*' (Xu & Teo, 2005). The perceived cost of privacy is evident as many online service vendors exploit user privacy for secondary uses and/or release user information to unauthorised entities without authorisation from the consumers (Thatcher & Clemons, 2000). Online companies and service providers who collect user information sell it to spammers, telemarketers and direct mailers. The loss of individual privacy information can harm the user in a variety of ways, including through spamming, fraudulent credit card charges and identify theft. Prior research in security has argued that users who perceive a high level of privacy risks may abandon the use of such privacy intrusive security services (Dinev & Hart, 2006). Thus, we expect:

H10: Privacy concern will be negatively related to the attitude towards email security service.

To mitigate individual privacy concerns, appropriate organisational privacy practices such as use of privacy policy are advocated. The US Federal Trade Commission (FTC, 2000) proposes fair information practices on four dimensions of privacy management: (1) Notice: providing people notice that personal information is being collected prior to the collection of that information. (2) Access: providing people with access to the data that is collected about them.

(3) Choice: providing people with a choice to allow an organisation to use or share information collected about them. (4) Security: providing reasonable assurance that personal information is kept secure. More and more firms are following the FTC framework to develop their privacy management strategies for user information collection, use, and dissemination (Stewart & Segars, 2002). Additionally, firms have been encouraged to communicate their privacy policies with the customers through awareness and education programmes. Prior studies suggest that appropriate policy design and policy transparency may reduce user concerns regarding privacy losses (Liu *et al*., 2005). We therefore propose:

H11: Transparency of vendor privacy notification practices will be negatively related to user privacy concerns.

METHODOLOGY

Data for hypothesis testing was gathered in a longitudinal study using two surveys. We partnered with a leading email authentication service provider, eAuth Inc., to carry out this project. Two senior personnel from eAuth contributed to an 8-month-long study by (1) developing website portals to publish service-related information and user guidelines; (2) developing customised service programs to enable experiment controls (e.g. verification of whether respondents install and use the service); and (3) allocating a designated server for the email authentication service to study respondents and record their behaviour statistics.

Measurement development

The research hypotheses were empirically tested using data collected in two surveys. The initial set of items was created by analysing the relevant literature. Most measurement items for the principal constructs in this study were adapted from existing measures into the current context to enhance validity and are shown in Appendix A along with the relevant references. All items used a 7-point Likert scale. As there was no existing item for email screening self-efficacy, we developed items to capture one's judgment about one's personal capabilities to perform the task (Bandura, 1997, p. 73). Similarly, we developed items to capture the internet-related risk propensity.

The questionnaire was pre-tested by a group of faculty members and Ph.D. students to check the psychometric properties of the measurement scales. One pilot test was administrated with 30 undergraduate students to provide an additional test of the reliability of the scales and the general mechanics of the study. The measurement instrument was shortened, refined, and validated. The final version of the items used is presented in Appendix B. We incorporated several procedural remedies recommended for survey studies. These included: (1) increasing validity using pre-test and pilot testing of the survey instrument; and (2) protecting respondent anonymity to reduce evaluation apprehension by taking precautionary measures to ensure the confidentiality of data. These procedural remedies are also recommended for controlling common method bias (Podsakoff *et al*., 2003, p. 888).

We used two surveys to capture the data used for this study. Among the constructs used in this study, risk perception and email screening self-efficacy were captured in the first survey, while the remaining constructs related to eAuth (eAuth Usefulness, eAuth_EOU, eAuth-_Responsiveness, Privacy Concern, eAuth_Attitude, Intention to adopt eAuth) were captured in the survey carried out in second stage after the participants had tried the eAuth email authentication service. Details about the process are discussed in further discussion. The precautionary measure of using a two-stage survey was incorporated to minimise the influence that a security tool may have on the risk-related constructs.

Survey administration

The target population of the study is the average email user. Students at a large public university in the north-east USA served as surrogates for the population. Our study required participants to install a client-side security plug-in and required them to finish surveys at several different time periods. A major advantage of using student subjects is that we were better able to avoid substantial attrition between data collection points and thereby avoid a critical threat to validity. The subjects were all junior level undergraduate students in a required first-year course in management IS for all undergraduates majoring in business administration. Hence, the undergrads were not necessarily MIS students but were taking the course to fulfil a general elective. Also, because this was their first course in IS, the students taking this class had not previously been exposed to any formal IS education. Potential respondents were mailed a copy of the research description with a cover letter from the class instructor encouraging their participation. Extra grade points were provided as the incentive for participation. Participation was voluntary and students who chose not to join the study were offered alternatives to get extra grade points.

We collected data before and after the use of eAuth. During the pre-use data collection, the respondents were surveyed about demographic information and email risk perception. Participants were then asked to install and use eAuth service on their personal computers. Training sessions on software installation, working principles of the service, and system basic operations were provided to each user. The post-use data collection was carried out two months later after users had experience with eAuth. The 2-month period was found to be sufficient to cover the initial learning curve of subjects who were new to the service based on the findings from a pilot study with 30 respondents conducted 4 months prior to the main test. The responses for participants who abandoned the use of eAuth service in the interim and/or failed to finish surveys were eliminated. For example, we analysed the statistics data obtained from eAuth servers to identify subjects who did not install the email authentication as scheduled and deleted their responses from our results. We distributed 389 invitations to potential respondents. After deciding whether to participate and the subsequent early dropout period, a total of 186 subjects responded to the first round survey. Two months later, 134 of them completed the second survey. The demographic information is summarised in Table 1.

Table 1. Demographic information of respondents

Gender	66 male (49%), 68 female (51%)	Average age	21 years
		Age Range	19–50 years
Average computer use experience	10 years	Average daily emails received	13 emails
Emails skills (0 none–7 extensive)	5.18 (SD 1.15)	Average daily commercial emails commercial emails received	9 emails
Internet skills (0 none–7 extensive)	5.50 (SD 1.04)	Listserv subscribers	80 (60%)
Participation in online commerce activities for which records of transactions are sent through email		Given email address to shopping or advertising avenue(s) from which information is sent on regular basis	
Very often	15 (11.4%)	Often	14 (10.4%)
Sometimes	89 (66.4%)	Occasionally	108 (80.6%)
Never	28 (20.9%)	Never	11 (8.2%)

RESULTS

The measurement model and structural model were tested using partial least square (PLS) regression. The PLS approach is widely accepted in IS research. PLS provides the ability to model latent constructs even under conditions of non-normality and small- to medium-size samples (Chin, 1998; Ringle *et al*., 2005). The software used was smartPLS 2.0 (Ringle *et al*., 2005). A bootstrap procedure was used to examine the significance of the path coefficients.

Measurement model

Table 2 reports the correlation matrix, the average variance extracted (AVE), and the reliability statistics of the principal constructs. Measurement reliability was assessed using composite reliability and Cronbach's alpha (Cronbach, 1971). A composite reliability of 0.70 or greater (Nunally, 1978) and a Cronbach's alpha of 0.70 (Chin, 1998) is considered acceptable for research. As evident in Table 2, the internal consistencies of all variables are considered acceptable since they exceed 0.70, which signifies tolerable reliability.

The convergent and discriminant validity is inferred when: (1) the square root of each construct is larger than its correlations with other constructs (the AVE shared between the construct and its indicators is larger than the AVE shared between the construct and other items); and (2) the PLS indicators load much higher on their hypothesised construct than on other constructs (own-loadings are higher than cross-loadings) (Chin, 1998). As shown in Table 2, the square roots of the AVE are all greater than all other cross-correlations; this indicates that the variance explained by each construct is much larger than the measurement error variance. All AVEs are well above 0.50, which suggests that the principal constructs capture much higher construct-related variance than error variance. The correlations among all constructs are all well below the 0.90 threshold, which suggests that all constructs are distinct from each other. Confirmatory factor analysis was also conducted. As shown in Table 3, all items load on their own constructs. These were found to be much higher than all cross-

Table 2. Correlations of principal constructs, reliability statistics, and average variance extracted

				Inter-Construct Correlation matrix								
	AVE	CR	CA	1	2	3	4	5	6	7	8	9
EmailRisk Perception (RPerc)	0.76	0.93	0.896	*0.87*								
EmailScreenSelfEfficacy (EScSEff)	0.82	0.97	0.971	–0.06	*0.90*							
eAuth_Attitude (eAAtt)	0.60	0.85	0.778	0.03	0.18	*0.77*						
eAuth_Usefulness (eAUse)	0.89	0.97	0.958	0.21	0.22	0.43	*0.94*					
eAuth_ Ease of Use (eAEOU)	0.76	0.90	0.838	0.13	0.20	0.45	0.50	*0.87*				
eAuth_Responsiveness (eARes)	0.86	0.93	0.842	0.17	0.10	0.40	0.39	0.66	*0.93*			
Privacy Concern (PrvConc)	0.65	0.85	0.732	0.04	–0.21	–0.33	–0.25	–0.24	–0.15	*0.81*		
Privacy Notification (eAPrvNot)	0.82	0.98	0.972	0.03	0.18	0.31	0.55	0.51	0.51	–0.14	*0.90*	
eAuth_AdoptionIntention (eAInt)	0.93	0.98	0.976	0.29	–0.08	0.46	0.53	0.52	0.47	–0.14	0.35	*0.97*

Note: CR: Composite Reliability, CA: Cronbach's Alpha; The diagonal elements (in italics) represent the square root of AVE values.

loadings. Items should load high (>0.7) on their respective constructs and no item should load higher on constructs other than the one it was intended to measure. Cross-loadings of items on latent constructs other than their own were found to be at least one magnitude smaller (Gefen & Straub, 2005). These tests validate the measurement properties of the study's principal constructs.

To investigate common method bias, we first conducted the Harman's single factor test (Podsakoff *et al*., 2003). Common method bias exists when one single factor emerges or when one factor accounts for the majority of the covariance among the variables. Our results showed that none of the emergent factors explain the majority of the covariance. Second, the correlation matrix was examined for highly correlated factors. The common method bias exists when extremely high correlations exist ($r > 0.9$) (Pavlou *et al*., 2007). Table 3 did not reveal such evidence. Third, we conducted a test with an unmeasured latent methods factor. We use a single unmeasured latent method factor to examine common method bias by allowing the items to load on their theoretical constructs as well as on a latent method factor. We found that there were few substantive differences in the statistical results and no paths lost statistical significance. All the path coefficients showed the same direction. Our results indicate that the factor loadings in both models, with and without the method factors, are significant and of similar magnitude. In using the variance test, the indicators explain approximately 79% of the variance in their substantive constructs while explaining less than

Table 3. Confirmatory factor analysis

	RPerc	EIDSEff	eAAtt	eAUse	eAEOU	eARes	PrvConc	eAPrvNot	eAInt
RPerc _1	**0.83**	–0.09	0.01	0.26	0.10	0.10	–0.07	0.01	0.31
RPerc _2	**0.89**	–0.06	0.02	0.13	0.10	0.15	0.12	0.06	0.22
RPerc _3	**0.89**	0.02	0.06	0.13	0.15	0.20	0.04	0.02	0.24
RPerc _4	**0.87**	–0.04	0.01	0.16	0.12	0.16	0.09	0.04	0.21
EScSEff _1	–0.01	**0.81**	0.17	0.24	0.15	0.13	–0.24	0.13	0.00
EScSEff _2	–0.09	**0.90**	0.23	0.23	0.21	0.18	–0.21	0.20	–0.04
EScSEff _3	–0.06	**0.95**	0.14	0.22	0.19	0.11	–0.22	0.16	–0.07
EScSEff _4	–0.07	**0.95**	0.17	0.20	0.18	0.07	–0.19	0.19	–0.10
EScSEff _5	0.00	**0.90**	0.17	0.24	0.20	0.15	–0.18	0.21	0.00
EScSEff _6	–0.03	**0.93**	0.15	0.18	0.17	0.09	–0.21	0.15	–0.07
EScSEff _7	–0.03	**0.87**	0.13	0.23	0.21	0.07	–0.14	0.19	–0.02
EScSEff _8	–0.03	**0.92**	0.17	0.18	0.20	0.06	–0.20	0.15	–0.07
eAAtt _1	0.06	0.15	**0.83**	0.42	0.49	0.42	–0.27	0.34	0.47
eAAtt _2	0.01	0.12	**0.79**	0.25	0.26	0.18	–0.25	0.10	0.30
eAAtt_3	–0.01	0.05	**0.76**	0.27	0.26	0.22	–0.18	0.12	0.33
eAAtt_4	0.00	0.22	**0.70**	0.34	0.32	0.34	–0.31	0.32	0.28
EAUse_1	0.14	0.21	0.38	**0.93**	0.44	0.39	–0.23	0.49	0.43
EAUse_2	0.23	0.17	0.37	**0.94**	0.48	0.33	–0.24	0.49	0.52
EAUse_3	0.23	0.21	0.41	**0.96**	0.47	0.34	–0.24	0.51	0.50
EAUse_4	0.19	0.22	0.45	**0.94**	0.50	0.42	–0.23	0.58	0.55
eAEOU_1	0.19	0.06	0.43	0.52	**0.83**	0.55	–0.20	0.44	0.50
eAEOU_2	0.02	0.31	0.38	0.37	**0.85**	0.55	–0.24	0.40	0.39
eAEOU_3	0.12	0.17	0.38	0.40	**0.93**	0.61	–0.18	0.48	0.47
eARes_1	0.19	0.09	0.34	0.35	0.63	**0.93**	–0.13	0.48	0.44
eARes_2	0.13	0.09	0.40	0.38	0.59	**0.93**	–0.15	0.47	0.44
PrvConc_1	0.00	–0.17	–0.29	–0.20	–0.23	–0.16	**0.80**	–0.09	–0.16
PrvConc_2	0.08	–0.21	–0.23	–0.16	–0.15	–0.16	**0.84**	–0.11	–0.06
PrvConc_3	0.02	–0.13	–0.27	–0.24	–0.19	–0.05	**0.78**	–0.14	–0.11
eAPrvNot_1	0.08	0.20	0.26	0.51	0.44	0.41	–0.13	**0.86**	0.30
eAPrvNot_2	0.04	0.17	0.31	0.51	0.43	0.43	–0.12	**0.91**	0.29
eAPrvNot_3	0.05	0.10	0.29	0.52	0.53	0.46	–0.07	**0.92**	0.34
eAPrvNot_4	0.07	0.12	0.25	0.45	0.45	0.43	–0.09	**0.91**	0.30
eAPrvNot_5	–0.02	0.20	0.34	0.45	0.46	0.46	–0.16	**0.90**	0.27
eAPrvNot_6	–0.02	0.13	0.27	0.46	0.46	0.44	–0.09	**0.92**	0.29
eAPrvNot_7	0.03	0.21	0.26	0.49	0.48	0.50	–0.13	**0.92**	0.29
eAPrvNot_8	0.02	0.16	0.27	0.54	0.46	0.52	–0.17	***0.93***	0.37
eAPrvNot_9	0.05	0.14	0.24	0.55	0.43	0.48	–0.10	***0.88***	0.39
eAInt_1	0.29	–0.04	0.48	0.53	0.54	0.47	–0.19	0.37	***0.97***
eAInt_2	0.29	–0.11	0.39	0.51	0.49	0.44	–0.10	0.31	***0.97***
eAInt_3	0.27	–0.08	0.48	0.51	0.47	0.47	–0.14	0.33	***0.95***
eAInt_4	0.28	–0.08	0.43	0.50	0.53	0.45	–0.11	0.33	***0.98***

1% variance in method factor. Based on these tests (Liang *et al*., 2007), (Herath & Rao, 2009a), we can conclude that common method bias does not present a serious problem for this data.

Structural model

The results of the structural model are shown in Figure 3. The explanatory power of the research model was examined in terms of the portion of variance explained. The results suggest that the model is capable of explaining 30% of the variance in users' behavioural intentions to use the email authentication system. 31% of the variance of the attitude towards the email authentication tool and service is explained by usefulness, ease of use, service responsiveness, and privacy concerns. Furthermore, 43% of the variance in perceived ease of use is accounted for by the responsiveness of the tool, whereas 27% of the observed variance in perceived usefulness appears to be explained jointly by perceived ease of use and risk perceptions. Privacy notification practices appear to explain only two percent of variance in the privacy concerns held by users.

The significance and relative strength of individual links specified by the research model were also evaluated (Figure 3). In support of Hypothesis 1, email risk perceptions have a significant positive impact on behavioural intention to use eAuth security service ($\beta = 0.30$;

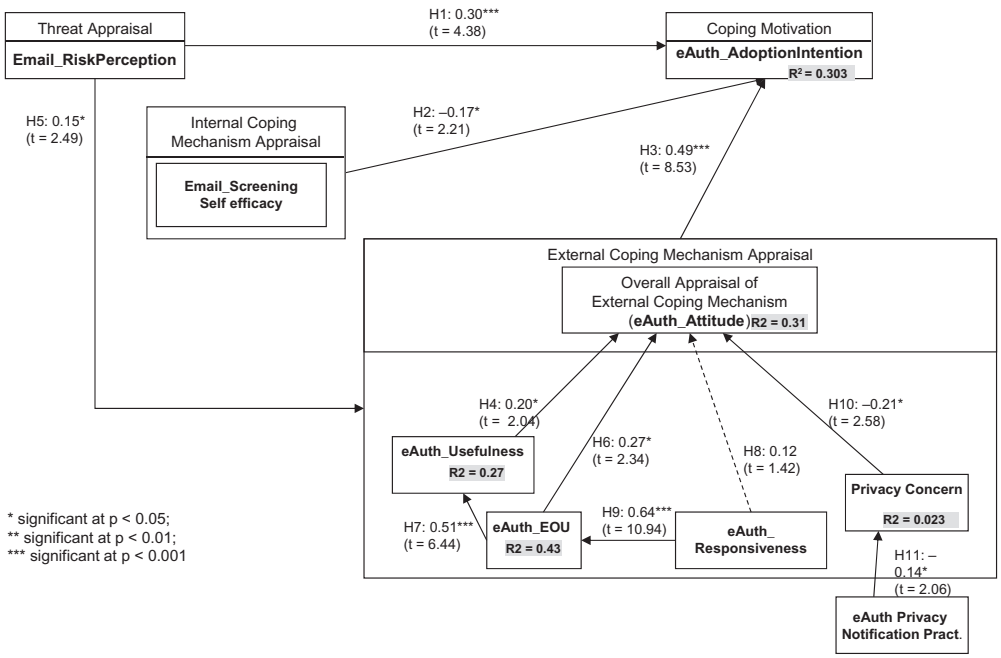

Figure 3. PLS results.

$p < 0.001$). Email risk perception was also found to significantly affect eAuth usefulness ($\beta = 0.15$, $p < 0.05$), which supports Hypothesis 5. In support of Hypothesis 2, email screening self-efficacy was found to have a significant negative impact on intentions to use eAuth ($\beta = -0.17$; $p < 0.05$).

Attitude towards email identification service was found to have a significant positive effect on behavioural intention ($\beta = 0.49$; $p < 0.001$), which supports Hypothesis 3. Attitude was also found to be significantly affected by eAuth usefulness ($\beta = 0.20$; $p < 0.05$), eAuth ease of use ($\beta = 0.27$; $p < 0.05$), and privacy concern ($\beta = -0.21$; $p < 0.05$), thus supporting Hypotheses 4, 6 and 10. Responsiveness of the service ($\beta = 0.12$; $p > 0.05$), however, was found to have an insignificant impact on shaping attitude; thus, Hypothesis 8 was not supported. As postulated in Hypothesis 7, perceived ease of use was found to be positively related to perceived usefulness ($\beta = 0.51$; $p < 0.001$). In support of Hypothesis 9, service responsiveness was found to have a significant impact on ease of use ($\beta = 0.64$; $p < 0.001$). Privacy notification was found to have a significant effect on reduction in privacy concerns ($\beta = -0.14$; $p < 0.05$), which supports Hypothesis 11.

DISCUSSION

Theoretical contributions and practical implications

This study examined the adoption of an email authentication service by potential users as a coping mechanism to deal with email-related threats. The contribution of this paper is twofold. First, guided by TAM and TTAT, the study develops an integrated theoretical model to investigate users' intention to adopt an email authentication service. The new research model, developed under the umbrella of TTAT and TAM theories, integrates internal and external coping mechanisms and provides insight into the risk coping behaviours of email users. Second, the current study empirically validates this integrated model in the scenario of eAuth adoption. Ten of the 11 hypotheses specified in the model were supported. The results attest to the value of this research model.

The current study also informs practice. We briefly discuss the major implications derived from our research hypotheses in the following discussion. We developed the model under the premise that given trends towards increasing cyber risks, individual users will undertake coping strategies to deal with these threats. These coping behaviours, however, will be shaped by individual perceived risks and appraisal of coping mechanisms. Perceived risk was found to be a direct predictor of service adoption intentions. We found that perceived risk in email communication also had an effect on the perceived usefulness of the service. Individuals who have higher perceptions of email risks are more likely to find the authentication service useful and consequently use it. From a vendor perspective, this has implications for advertising products. In general, if users are informed of existing email threats, they are likely to appreciate email security services. Vendors of email security services are, therefore, encouraged to educate potential customers about email threats and should consider education as an integrated component in their marking campaigns.

Email screening self-efficacy, which in this study was considered as an individual's perceptions of his/her ability to identify authentic and relevant emails based on simple cues (such as the '*from*' line and 's*ubject*' line of an email), was found to have an significant negative influence on the intentions of using the eAuth email authentication system. This finding suggests that individuals' confidence in their ability to deal with IT threats is more likely to induce them not to rely on security tools. In line with much of the earlier risk literature, we find that this self confidence is likely to result in risk-taking behaviours such as the avoidance of email security technologies. On the other hand, users who do not find substantial self capabilities are more likely to use security tools.

We anticipated that individual users who wish to use security tools will evaluate the tool based on usefulness, usability, and privacy concerns. The results of the study confirm the importance of perceived usefulness and perceived ease of use in the adoption of security services. In addition to its direct effect on attitude, perceived ease of use exhibited a considerable indirect effect on attitude through perceived usefulness. To be accepted by users, any email authentication service should therefore be designed with an aim to enhancing its usefulness as well as its ease of use. Companies that wish to provide email authentication services may need to consider formulating strategies that lead to the development of positive perceptions of the usefulness of the services.

Service responsiveness was found to be a significant factor in perceived ease of use but, surprisingly, did not have any direct impact on user attitude towards the service. The findings suggest that if a user feels it takes the system too much time to show check marks, he or she may form a negative perception of the ease of use of the services, which could indirectly impact user attitude towards the service. Therefore, this observed strong influence may motivate service providers to design their systems to accommodate faster access and show check marks promptly. The literature considering download delays (e.g. (Rose *et al*., 1999; 2001; Palmer, 2002)) has consistently shown that low responsiveness results in lower perceptions of system quality. Most often, the delay times are attributed to the infrastructure quality. In the case of an email authentication system, in addition to the quality of the telecommunication infrastructure, the response time may depend on the number of email checks performed against the existing database every time the user opens the Inbox. As the number of registered companies and registered users of the service grows, this is a major issue that needs to be considered by service providers. The processing speeds can be enhanced by increasing the processing power or decreasing the number of checks performed. However, in the latter case, responsiveness has to be sacrificed for the sake of enhanced security. This conflict between the intended service functionalities and system responsiveness needs to be addressed by the service provider. The speed of such online services is likely to increase with developments in the internet infrastructure; however, vendors will have very little control over such enhancements. Vendors can explore other technological solutions that can aid in augmenting the processing. For instance, in a solution in line with cached internet visits, a local machine keeping a copy of the most frequently used email senders will reduce the burden of the online checks performed each time the user opens an Inbox. Another possible solution may require a local machine to keep a list

of all sender IDs (or public keys) and, similar to other antivirus products, this machine would only check for new updates periodically.

Since the provisioning of service requires access to a user's personal inbox, the privacy-related perceptions were tested. The results indicated that privacy concerns, despite having a small effect, have a significant negative impact on attitudes. Service providers may need to address this issue to resolve the negative effect it may have on user attitudes and, therefore, on intentions of using the service. One way to reduce user privacy concerns is to improve privacy policies and privacy practices. This study found that privacy notification practices have a significant effect on privacy concern reduction. It is important for service providers to have privacy policies and make them available to the users in noticeable way.

Limitations and future research avenues

The dependent variable considered in this study was the intention to use the service. Though earlier research rooted in Theory of Reasoned Action and Theory of Planned Behaviour has contended and shown that behavioural intention is a strong predictor of the behaviour itself, it still limits the explanatory power of the model by not evaluating the usage itself. The continued use of the security service needs to be studied in future studies.

Future studies that consider a comprehensive taxonomy of the designs of security systems and explore their impact on usefulness, ease of use, and privacy or security perceptions are also warranted. Privacy is a complicated construct and, depending on the context of the service, it may have different effects. Privacy concerns and desired privacy notification practices need to be thoroughly examined in the context of email authentication services. This study did not consider the precursors that may have an effect on email risk perception. Factors such as social influence and individuals' risk propensity may be studied to understand their effect on threat perceptions. In measuring self-efficacy, this study uses 'from line' and 'subject line' for determining authenticity, which may be restrictive. Other screening techniques based on visual or language cues suggested in the phishing literature (Wang *et al*., 2009a) can be considered in future studies to explore internal coping strategies.

Furthermore, this study considers the adoption of an email authentication system by an individual user. Future studies are needed to validate and extend the model in different contexts, particularly in terms of organisational users, workplace culture, different culture groups and different security technologies. The current study uses a student sample. While students are regular email users, the relatively homogenous age group poses some limitations. Research on risky behaviour has shown that younger people are less risk adverse and have lower privacy concerns (Martin & Leary, 2001; Gardner & Steinberg, 2005); thus, studies with more diverse demographic samples are needed to validate these findings.

CONCLUSION

The current study attempts to understand individual intention to adopt an email authentication service, an IT innovation that is used outside conventional work settings. End users use

personal computers for email activities in home settings as well as using personal computers in decentralised systems architectures. Email authentication services are unique IT artefacts that focus on individual users rather than organisational users and are delivered via the internet in real time. We developed a research model under the umbrella of TAM and TTAT that reflects the unique characteristics and usage context of an email security service. We empirically tested the model with the help of two surveys. Our findings suggest that the TAM variables, namely ease of use and usefulness, are significant in the context of voluntary protective technology. However, the security context specific variables such as risk perception, privacy concern, and service delay indicate that technology acceptance theories may not provide a complete understanding of protective technology use. The risk perceptions were found to have a significant impact on usefulness and intentions to use the security tool. Privacy concerns were found to be reduced with notification practice perceptions. These findings suggest that theories considering risk and threat may be needed to give a more complete understanding of protective technology adoption and use.

ACKNOWLEDGEMENTS

The authors would like to thank the SE, AE and referees for their detailed feedback regarding this paper. This research has been supported in part by the Social Sciences and Humanities Research Council (SSHRC) of Canada (Grant no: 410–2010-1848), and the National Science Foundation under grants 1227353 and 0916612. The research of the last (correspondent) author is also supported by the World Class University programme funded by the Ministry of Education, Science, and Technology through the National Research Foundation of Korea (R31-20002) and by the Sogang University Research Grant of 2011.

REFERENCES

Bandura, A. (1997) *Self-Efficacy: The Exercise of Control*. W. H. Freeman, New York, NY, USA.

Bellovin, S.M. (2004) Spamming, phishing, authentication, and privacy. *Communications of the ACM*, **47**, 144–144.

Chin, W.W. (1998) Issues and opinion on structure equation modeling. *MIS Quarterly*, **22**, vii–xvi.

Choi, N., Kim, D., Goo, J. & Whitmore, A. (2008) Knowing is doing: an empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security*, **16**, 484–501.

Cronbach, L.J. (1971) Test validation. In: *Educational Measurement (2nd Edition)*, Thorndike, R.L. (ed.), pp. 443–507. American Council on Education, Washington, DC, USA.

Davis, F.D. (1989) Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Quarterly*, **13**, 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**, 982–1002.

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

Ducheneaut, N. & Watts, L.A. (2005) In search of coherence: a review of e-mail research. *Human-Computer Interaction*, **20**, 11–48.

Dulebohn, J.H. (2002) An investigation of the determinants of investment risk behavior in employer-sponsored

retirement plans. *Journal of Management*, **28**, 3–26.

FTC (2000) FTC report to congress: privacy online: fair information practices in the electronic marketplace: federal trade commission.

Gardner, M. & Steinberg, L. (2005) Peer influence on risk taking, risk preference, and risky decision making in adolescence and adulthood: an experimental study. *Developmental Psychology*, **41**, 625–635.

Gefen, D. & Straub, D. (2005) A practical guide to factorial validity using PLS-graph: tutorial and annotated example. *Communications of the Association for Information systems*, **16**, 91–109.

Ghosh, A.K.A.S.T.M. (2001) Software security and privacy risks in mobile e-commerce. *Communications of the ACM*, **44**, 51–57.

Gupta, A., Sharda, R., Ducheneaut, N., Zhao, J.L. & Weber, R. (2006) Email management: a techno-managerial research perspective. *Communications of the Association for Information Systems*, **17**, 941–961.

Harminka (2007) Latest SonicWALL email security statistics show rising threat from PDF and ZIP spam. HULIQ.

Heath, C. & Tversky, A. (1991) Preference and belief: ambiguity and competence in choice under uncertainty. *Journal of Risk and Uncertainty*, **4**, 5–28.

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

Herath, T. & Rao, H.R. (2009b) Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, **18**, 106–125.

Hong, S.-J. & Tam, K.Y. (2006) Understanding the adoption of multipurpose information appliances: the case of mobile data services. *Information Systems Research*, **17**, 162–179.

Jarvenpaa, S.L., Tractinsky, N. & Vitale, M. (1999) Consumer trust in an Internet store. *Information Technology and Management*, **1**, 45–71.

Johnston, A.C. & Warkentin, M. (2010) Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, **34**, 1–20.

Karahanna, E., Straub, D.W. & Chervany, N.L. (1999) Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly*, **23**, 183–213.

Kruegar, N.J. & Dickson, P.R. (1994) How believing in ourselves increases risk taking: perceived self-efficacy and opportunity recognition. *Decision Sciences*, **25**, 385–400.

Lewis, W., Agarwal, R. & Sambamurthy, V. (2003) Sources of influence on beliefs about information technology use: an empirical study of knowledge workers. *MIS Quarterly*, **27**, 657–678.

Liang, H. & Xue, Y. (2010) Understanding security behaviors in personal computer usage: a threat avoidance perspective. *Journal of the Association for Information System*, **11**, 394–413.

Liang, H., Saraf, N., Hu, Q. & Xue, Y. (2007) Assimilation of enterprise systems: the effect of institutional pressures and mediating role of the top management. *MIS Quarterly*, **31**, 59–87.

Liang, H.G. & Xue, Y.J. (2009) Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly*, **33**, 71–90.

Liu, C., Marchewka, J.T., Lu, J. & Yu, C.-S. (2005) Beyond concern – a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, **42**, 289–304.

Loiacono, E., Watson, R. & Goodhue, D. (2007) WebQual: an instrument for consumer evaluation of web sites. *International Journal of Electronic Commerce*, **11**, 51–87.

Martin, K.A. & Leary, M.R. (2001) Self-presentational determinants of health risk behavior among college freshmen. *Psychology & Health*, **16**, 17–27.

Neuwirth, K., Dunwoody, S. & Griffin, R.J. (2000) Protection motivation and risk communication. *Risk Analysis*, **20**, 721–734.

Nunally, J.C. (1978) *Psychometric Theory*. McGraw-Hill, New York, NY, USA.

Palmer, J.W. (2002) Web site usability, design, and performance metrics. *Information Systems Research*, **13**, 151–167.

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

Pavlou, P.A., Liang, H. & Xue, Y. (2007) Understanding and mitigating uncertainty in online exchange relationships: a principle-agent perspective. *MIS Quarterly*, **31**, 105–136.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y. & Podsakoff, N.P. (2003) Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, **88**, 879–903.

Ringle, C.M., Wende, S. & Will, S. (2005) SmartPLS 2.0 (M3) Beta. Hamburg.

Rogers, R.W. (1975) A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, **91**, 93–114.

Rogers, R.W. (1983) Cognitive and physiological process in fear appeals and attitude change: a revised theory of protection motivation. In: *Social Psychophysiology: A Source Book*, Petty, R. (ed.), pp. 153–176. Guilford Press, New York.

Rose, G., Khoo, H. & Straub, D. (1999) Current technological impediments to business-to-consumer electronic commerce. *Communications of the AIS*, **1**, 1–74.

Rose, G.M., Lee, J. & Meuter, M.L. (2001) A refined view of download time impacts on e-consumer attitudes and patronage intentions toward e-retailers. *The International Journal on Media Management*, **3**, 105–111.

Smith, H.J., Milberg, S.J. & Burke, S.J. (1996) Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, **20**, 167–197.

Stanley, M.A. & Maddux, J.E. (1986) Cognitive processes in health enhancement: investigation of a combined protection motivation and self-efficacy model. *Basic and Applied Social Psychology*, **7**, 101–113.

Steffen, V.J. (1990) Men's motivation to perform the testicle self-exam: effects of prior knowledge and an educational brochure. *Journal of Applied Social Psychology*, **20**, 681–702.

Stewart, K.A. & Segars, A.H. (2002) An empirical examination of the concern for information privacy instrument. [Article]. *Information Systems Research*, **13**, 36–49.

Symantec Corp (2010) Symantec Global Internet Security Threat Report Trends for 2009 (Vol. XV).

Thatcher, M.E. & Clemons, E.K. (2000) Managing the costs of informational privacy: pure bundling as a strategy in the individual health insurance market. *Journal of Management Information Systems*, **17**, 29–58.

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

Wang, J., Chen, R., Herath, T. & Rao, H.R. (2009a) An empirical exploration of the design pattern of phishing attacks. In: *Annals of Emerging Research in Information Assurance, Security and Privacy Services*, Upadhyaya, S.J. & Rao, H.R. (eds), pp. 259–284. Emerald Group Publishing Ltd., Bingley, England.

Wang, J., Chen, R., Herath, T. & Rao, H.R. (2009b) Visual e-mail authentication and identification services: an investigation of the effect on e-mail use. *Decision Support Systems*, **48**, 92–102.

Warkentin, M. & Johnston, A.C. (2006) Chapter II: IT security governance and centralized security controls. In: *Information Assurance and System Security: Managerial and Technical Issues*, Warkentin, M. & Vaughn, R. (eds), pp. 16–24. Idea Group Publishing, Hershey, PA, USA.

Woon, I.M.Y., Tan, G.W. & Low, R.T. (2005) *A Protection Motivation Theory Approach to Home Wireless Security.* Paper presented at the Twenty-Fifth International Conference on Information Systems, Las Vegas, NV, USA.

Workman, M., Bommer, W.H. & Straub, D. (2008) Security lapses and the omission of information security measures: a threat control model and empirical test. *Computers in Human Behavior*, **24**, 2799–2816.

Xu, H. & Teo, H.H. (2005) *Consumers Privacy Concerns toward Using Location-Based Services: An Exploratory Framework and Research Proposal.* Paper presented at the European Conference on Information Systems.

Biographies

Rui Chen is an Assistant Professor of Information Systems and earned his PhD from SUNY Buffalo. His research interests are in the areas of information assurance, emergency management, coordination and collaboration and information technology outsourcing. Some of his publications have appeared in the *Journal of the AIS*, *Communications of the ACM*, *Decision Support Systems* and other journals. He is also a Microsoft Certified System Administrator (MCSE) and Database Administrator (MCDBA).

Jingguo Wang is an Assistant Professor of Information Systems. He graduated from SUNY Buffalo. His work has been published in *Information Systems Research*, *ACM Transactions on Management Information Systems*, *IEEE Transactions on Systems*, *Man, and Cybernetics (Part C)*, *European Journal of Operational Research* and *Decision Support Systems* among others, and has received best paper awards at AMCIS and the International Conference on Internet Monitoring and Protection. His current research interests are in the areas of cybercrime and information security, information search and decision-making.

Ketan Banjara holds an MBA from Santa Clara University, California and a BSc in Computer Science from University of Minnesota – Duluth. Prior to joining Iconix, Ketan was the founder and President of Jivalti Inc., an enterprise IT product feature comparison service, with the core engine based on ontologies and DAML/Semantic web concepts. Jivalti was a NASA industry partner. Ketan's background shows a strong combination of both sales and IT –

specifically networking, security and storage. In his last IT-related job, Ketan was the Deputy Director of the Information Services Department at the County of San Mateo, California.

Jeff Wilbur is Vice President of Marketing at Iconix, Inc. He has worked at Intel, Picazo Communications, NetWorth, Network Resources, Compaq Computer, Mirus Corporation and Sytek. He brings a varied marketing and management background, with a heavy emphasis on bringing innovative products to new markets. Jeff also has a technical background, with a BSc in Electrical Engineering from Kansas State University and an MSc in Electrical Engineering from Stanford University.

H. Raghav Rao, PhD, graduated from Krannert Graduate School of Management at Purdue University. He also has co-edited four books, one of which is on Information Assurance in Financial Services. His work has received best paper and best paper runner-up awards at ISR, AMCIS and ICIS, etc. Dr. Rao has received funding for his research from the National Science Foundation, the Department of Defense and the Canadian Embassy, and he has received the University's prestigious Teaching Fellowship. He has also received the Fulbright Fellowship in 2004. He is a associate editor of *Decision Support Systems*, *Information Systems Research*, *IEEE Transactions in Systems* and *Man and Cybernetics*; co-editor-in-chief of *Information Systems Frontiers*; and Senior Guest Editor of *MIS Quarterly*. He is the recipient of the 2007 SUNY Chancellor's Award for Excellence and is a WCU visiting professor at Sogang University, Korea.

Tejaswini Herath, PhD, is an assistant professor in the Faculty of Business at Brock University, Canada. She graduated from the SUNY Buffalo. She holds MMIS, MSCE from Auburn University, USA and BE from Pune University, India. Previously she worked as a systems analyst and a part-time lecturer at UNBC, Canada. Her primary research interests are in Information Assurance and include topics such as information security and privacy, diffusion of information assurance practices, economics of information security and risk management. Her work has been published in leading journals including the *Journal of Management Information Systems*, *Decision Support Systems*, *European Journal of Information Systems* and *Information Systems Management*, and has been presented at leading conferences. In addition, she has contributed several book chapters.

APPENDIX A: eAuth SYSTEM

The eAuth system reduces the risk of email fraud by authenticating the source of the sender in the following process.

1. Authentication

When an email arrives, the email sender is checked against a list of registered senders with eAuth. eAuth verifies the authenticity of the message using industry standard technologies such as Domain Keys and DomainKeys Identified Mail (DKIM), which are backed by companies such as Cisco, Microsoft, and Yahoo. DomainKeys is an email authentication system that verifies the domain name of an email sender as well as the message integrity. It was later replaced by DKIM. DKIM is a method that involves signing part of an outgoing email with an organisation's private key and assuring the signing organisation to take responsibility for this message. A receiving party can validate the email against the stored public key of an organisation.

2. Identification

Once an email has been verified to be authentic, an icon is displayed in the Inbox to help users instantly recognise messages and know that they are legitimate.

Figure A1. eAuth Client Plug-in side.

APPENDIX B: OPERATIONALISATION OF CONSTRUCTS

	Operationalisation of the constructs (All items measured on 7-point Likert scale)	**References Used**
Security Service Adoption Intention (eAInt)	I am likely to continue using eAuth for email screening I plan to use eAuth for email screening. It is possible that I will continue using eAuth for email screening. I predict that I would use eAuth for email screening.	Venkatesh *et al*. (2003)
Email Screening Self-Efficacy (EIDSEff)	It is easy for me to verify an email as coming from authentic sender based on 'from line' and 'subject line'. I feel comfortable in my abilities to identify emails that may be forged based on 'from line' and 'subject line'. I feel confident in my abilities to identify emails that are authentic based on 'from line' and 'subject line'. I feel confident in my abilities to determine whether the identities of emails are real based on 'from line' and 'subject line'. I feel comfortable in my abilities to identify emails that may be useful to me based on 'from line' and 'subject line'. I feel confident in my abilities to identify emails that are relevant to me based on 'from line' and 'subject line'. I feel confident in my abilities to identify malicious emails, such as phishing emails, based on 'from line' and 'subject line'. I feel confident in my abilities to identify emails that are detrimental based on 'from line' and 'subject line'.	Developed for this study based on Bandura (1997)
Security Service Attitude (eAAtt)	Using eAuth for email screening Good idea Bad Idea Extremely Harmful Extremely Beneficial (R) Extremely Negative Extremely Positive (R) Extremely Good Extremely Bad	Karahanna *et al*. (1999); Venkatesh *et al*. (2003)
Service Usefulness (eAUse)	Using eAuth service enables me to accomplish the task of email authenticity check more quickly. Using eAuth service helped improve identifying authentic emails. Using eAuth service enhances my effectiveness of detecting authentic emails Using eAuth service gives me greater control over email authenticity check.	Karahanna *et al*. (1999; Venkatesh *et al*. (2003)
Service Ease of Use (eAEOU)	My interaction with eAuth tool is clear and understandable. Interacting with eAuth tool does not require a lot of my mental effort. I find eAuth tool easy to use.	Bandura (1997); Karahanna *et al*. (1999)
Risk Perception (RPerc)	My decision to open emails is risky. Opening email will lead to high potential for loss. There is considerable risk involved in potential consequence of opening emails. Opening emails will lead to considerable risks.	Jarvenpaa *et al*. (1999); Pavlou (2003)
Service Responsiveness (eARes)	When I use the eAuth tool there is very little waiting time between opening the Inbox and the response by the tool. The identification icons load quickly.	Loiacono *et al*. (2007)

APPENDIX B: cont.

	Operationalisation of the constructs (All items measured on 7-point Likert scale)	**References Used**
Privacy Notification (eAPrvNot)	I was informed about what information eAuth, Inc. would collect about me. eAuth, Inc. explained why they were collecting the information about me. eAuth, Inc. explained how they would use the information collected about me. eAuth, Inc. gave me a clear choice before disclosing personal information about me to third parties. eAuth, Inc. indicated that it will not release the information about me without my expressed permission. eAuth, Inc. indicated that it is making effort to keep the information about me out of hands of unauthorised individuals. eAuth, Inc. indicated that the information collected about me will be kept secured. eAuth, Inc. indicated that it is making a reasonable effort to ensure that the information collected about me was accurate. eAuth, Inc. has a mechanism to review and change incorrect the information about me.	Liu *et al*. (2005)
Privacy Concern(PrvConc)	I feel that information collected for one purpose will be disclosed to other external party by eAuth, Inc. I feel that procedures in place and steps taken by eAuth to ensure accuracy are not adequate. I think that eAuth, Inc. will not follow the promises outlined in its privacy policy.	Smith *et al*. (1996); Liu *et al*. (2005)