RESEARCH ARTICLE OPEN ACCESS

Cybercrime Risk Avoidance on Online Service.

A.SriCheritha [1], J.VSMRaju [2]
M.Tech (CSE) Student [1], Professor [2]
Department of Computer Science and Engineering
Narayana Engineering College, Nellore
AP – India

ABSTRACT

Online transactions have become a part of everyday life for many users and it has emerged as a big sector of the entire online trade. Most of the online transactions depend upon card transactions that take place through a gateway. This gateway causes threat to inexperienced users about security for their confidential data such as: pin-number and passwords, actual insecurity due to hackers of the gateway, charges by the third-party gateway. The third-party gateway that charges lesser percentage of the amount transacted might provide less security. In-order to avoid such threats, avoiding the gateway by doing the transactions directly through the bank server is more secure, efficient and creates more trust among the users. As proposed system deals w ith reduction of perceived risk of cybercrime, this facilitates increased online service use. Triple DES algorithm is used here for secure payment information transfer.

Keywords:- Cyber Crime, online

I. INTRODUCTION

ONLINE services provide extensive individual and socio- economic benefits to modern society. Online banking has introduced a convenient yet inexpensive and effective way of remotely handling financial transactions [1]; e-commerce has increased product availability while decreasing trading costs[2]; and online social networks have deepened personal relationships worldwide [3]. Reviewing the economic growth literature, Cardona et al. show in [4] that information and communication technology increased labor productivity in the EU by at least 31% (33% in the US) since 1995. Brynjolfsson emphasizes the magnitude of the consumer surplus generated by online services, which provides additional social welfare not reflected in the traditional statistics [5], [6]. Consequently, the European Commission has set further online service diffusion and area-wide broadband roll-out as essential objectives for sustainable economic and social benefits in their Digital Agenda for Europe 2020[7].Unfortunately, the growing online space also creates an exposure to malicious behavior. Utilizing the characteristics of the Internet, such as scalability, anonymity, and global reach, cybercrime emerged as a new form of crime and evolved into a serious industry in which specialized attackers operate globally [8]. Consumer- oriented cybercrime, which includes identity theft, credit card fraud, and phishing, makes the use of online services risky for all Internet users [9]. To avoid precarious situations, many Internet users remain hesitant to use online services. Such reluctance leads many to miss out on the social and economic benefits provided by an Internet-connected world. Anderson et al. agree that the majority of cybercrime costs are indirect opportunity costs, created by users avoiding online services [10]. Understanding how these costs are formed is a main prerequisite to craft appropriate responses for dealing with a global cybercrime problem. Work on the social effects of cybercrime is still rare, as most studies focus on the criminals' motives and attacks, or propose technical, organizational, and regulatory measures to prevent cybercrime. To fill this gap, we synthesize work from information systems (IS) research and criminology. We devise a model that explains the impact of cybercrime on the avoidance of online services by showing how cybercrime creates perceived risk and how this risk makes users hesitant to use online services. We test our model with a secondary analysis of the 2012 Eurobarometer Cyber Security Report (CSR), a representative pan-European survey on the public perception of cybercrime [11]. We use structural equation modeling to test seven hypotheses for three important online services, namely: online banking, online shopping and online social networking.

II. LITERATURE SURVEY

The impact of the Internet on the social lives of users: A representative sample from 13 countries .Y. Amichai- Hamburger and Z. Hayat ,vol. 27, no. 1, pp.585–589, 2011,This study analyses results from the World Internet Project, comprised of representative samples from 13 countries (22,002 participants). The study assess the influence of Internet use over social interactions in separate life domains (e.g. with family members; friends; colleagues; business). The analysis confirms that Internet usage can actually enhance the social lives of its users. Qualifications to the research are discussed while highlighting the different life domains in which we found significant correlations between Internet usage and increased social interactions.

III. TECHNOLOGY ACCEPTANCE IN ITS RESEARCH MODELS

Explaining the acceptance of new technologies, have been of interest in IS research since the first commercial use of computers. Several models have been introduced to measure the influence of different factors on the individual intention to use a new technology [12]. We focus on studies applying acceptance models in the context of general online services, online banking, online shopping, and online social networking (OSN).

IV. TECHNOLOGY ACCEPTANCE MODEL

The Technology Acceptance Model (TAM; [13]) is prominently used in IS research to explain the acceptance of a wide spectrum of new technologies ranging from operating systems to desktop applications to online services [14], [15]. TAM is based on the general Theory of Reasoned Action (TRA; [16], [17]), but tailored to explain and predict the acceptance of information technology. It proposes that Perceived Ease-of-Use (PEU) and Perceived Usefulness (PU) of an application increase the Behavioral Intention (BI) to use it. Ultimately, the BI determines the actual Usage Behavior (U). Legris et al. show that the following findings are typically convergent across TAM studies: PEU and PU increase the BItousea technology, which ultimately has a positive effect on U [14]. Even though TAM has been intentionally constructed to explain employees' adoption of company owned, work- related software [13], many studies show its applicability in other contexts, including online services. A recent literature review shows that of 165 publications that consider the adoption of online banking between 1999 and 2012, the majority applies acceptance models (mostly TAM) [18]. A similar proliferation of acceptance models for online shopping adoption was found by [19]. Zhou et al. developed the Online Shopping Acceptance Model (OSAM), extending TAM for application in an online shopping scenario [20] . Models of online social network adoption, however, mostly focus on other factors, such as network externalities [21], connectedness and participation[22].Nevertheless, a few studies also apply TAM in the OSN context. Pinho & Soares show its applicability by analyzing OSN adoption for a set of 150 students [23]. However, they remark that the use of the parsimonious TAM model is a limitation of their study. Shin et al. utilize TAM by extending the model with Perceived Involvement and Enjoyment [24].

V. OTHER TECHNOLOGY ACCEPTANCE MODELS

Further commonly used acceptance models are the Theory of Planned Behavior (TPB; [25]), which extends TRA with a behavioral control factor, and Innovation Diffusion Theory (IDT; [26]), which explains adoption through properties of the innovation itself. Arguing that all of them capture important aspects, but none is able to measure technology acceptance sufficiently, Venkatesh et al. propose the Unified Theory of Acceptance and Use of Technology (UTAUT) model [12]. Integrating eight different technology acceptance models, the UTAUT model is increasingly used for analyzing the acceptance of online banking [18] and has been shown to explain up to 70% of the variance in the BI variable, exceeding former TAM studies [12]. However, the base model misses at least one important factor – perceived risk (PR) – vital for all online scenarios [27] and especially critical when cybercrime is involved.

VI. RISK IN ONLINE TRANSACTIONS

The importance of PR in commercial transactions was already identified by Bauer in the 1960s, who states that shopping always involves risk because the buyer's decision has consequences that can be unpleasant and are not perfectly predictable [28]. The spatial and temporal separation between consumers and retailers and the open architecture of the Internet increase this uncertainty [29] and are the reason why PR is more pronounced in online shopping than in traditional brick-and-mortar shopping [30]. Two forms of uncertainty are naturally present: behavioral and environmental uncertainty [29]. Behavior and certainty is concerned with the behavior of dubious, possibly malicious online merchants. Environmental uncertainty reflects a more general concern about the security of the Internet as a channel for commercial transactions. Both can increase the level of perceived risk. As individuals feel threatened by uncertain situations and try to avoid them, PR is an important factor potentially limiting the intention to use online services [31], [32].

Perceived Risk in TAM. Consequently, PR is likely to account for variance in the behavioral intention variable of TAM, when applying it to online services [29], [33]. Featherman & Pavlou systematically integrate PR into TAM [27], by adding PR as a multidimensional construct1. Fig. 1 illustrates that PR reduces the intention to use an eservice (BI) directly and indirectly via reducing its PU. The negative impact exists for initial as well as repeated online shopping and is found to be larger for less experienced Internet users [33]. PEU can mitigate the negative effects of PR, because it reduces uncertainty and increases the user's confidence in using an online service [27]. Martins et al. confirm the importance of risks by integrating the UTAUT model with the PR theory [35]. They derive a model which explains 81% of the usage behavior variance for 248 online banking customers in Portugal.

VII. TRUST

Featherman & Pavlou describe trust as the antidote to PR, because trusting the online seller and the Internet in general reduces the PR of online transactions [27]. Therefore, trust can be another important factor in the adoption process of online services, mitigating behavioral uncertainty [29]. A number of studies include trust as a construct that influences the adoption of electronic services (e.g., [32], [36], [37], [38], [39]). [40] show the importance of trust for online banking adoption by conducting a meta analysis, which incorporates 26 SEM models into a single random effects SEM. Their aggregated findings suggest that trust is the most important impact factor on the initial use intention of online banking, outperforming the original TAM factors PEU and PU. Other studies found similar evidence for OSN users. Having trust in the provider is strongly linked to disclosure of information and participation in social networks [41].

VIII. TECHNOLOGY ACCEPTANCE OF ONLINE SERVICES

Most research using risk-extended technology acceptance models is conducted within the online banking domain, including comparative studies (e.g., [1]) and national applications around the globe (e.g., [35], [42], [43]). Trust is more frequently used in the context of online shopping (e.g., [32]). However, some studies also use PR or both constructs (e.g., [44]). The adoption of OSN is less frequently tested with technology acceptance models, however, some studies show their applicability (e.g., [45]). The findings across the different online services and acceptance models are mostly consistent. The general hypotheses of TAM – PU and PEU increase the BI to use an IS service – are confirmed for online services. PR is an important factor in the initial and continuous use of online services [31] and should be included, either as antecedent (e.g., [27], [46]) of PU, PEU, and BI or as a moderating factor (e.g., [31], [33]). PR is a second order construct, as defined by [27], and privacy, performance and financial risks are the most salient first order factors. The negative influence of PR on BI or one of its antecedents, i.e., PEU or PU, is frequently shown. Finally, trust is shown to be reducing PR and increasing BI.

Perceived Risk in Criminology While the former Section explains how perceived risk negatively influences the society by making users hesitate to use online services, this section sheds light on how people's risk perception of crime is formed. Fear of crime is multidimensional in nature consisting of two distinct components [52]. First, the rather rational risk perception, which is often operationalized as a product of the probability of victimization and the severity of the crime. And second, fear as a rather emotional feeling of being unsafe. The two constructs are highly interrelated, and the effects between them are still unclear [53]. As we do not intend to clarify the relation between the two constructs, we focus on perceived risk, but consider fear of crime to be implicitly included, assuming that emotional reactions also influence how people reactto cybercrime. However, future research should clarify the risk–fear relationship in the online context.

Victimizaton Effects on Risk Perception. Examining prior victimization as an antecedent of perceived risk of crime yields mixed results. Most scholars found strong effects (e.g., [54], [55], [56], [57], [58]). Yet others found just weak or no effects at all (e.g., [59]). [60] state that the examination of the link between victimization experiences and perceived risk is not yet conclusive. However, as perceived risk is assumed to be a function of the probability of getting victimized and the severity of the criminal act [52], we suspect that crime experience leads to an increased concern about it. Visser et al. provide empirical evidence for the effect based on two representative European surveys conducted in 2006 and 2008 [58].

IX. MEDIA EFFECTS ON RISK PERCEPTION

The effect media has on risk perception is similarly controversial [61]. Reviewing the literature, Wahlberg & Sjoberg found that media coverage influences risk perception, especially if reports repeat over time [62]. Jackson argues logically that the media plays a role in people's perception of crime risk and severity, as it is the primary source of information about the extent, nature, and seriousness of crime[63]. As crime reports tend to be rather sensational and alarming, they are likely to increase public risk perception [62]. A majority of research was conducted for TV news. Studies found that watching TV reports increases the feeling of being unsafe [61], especially if the reports resonate with personal experiences [64], cover sensational crimes [63], [65], or are broadcasted frequently [64]. Local crime tends to have a stronger effect on the perceived risk [61], especially for people living in high crime areas [64]. It is suggested that the media needs to be considered as one factor among others, such as prior victimization, experiences in the social environment, or demographic factors [62].

X. DEMOGRAPHIC FACTORS AND RISK PERCEPTION

Demographics are important in measuring fear of crime, as different social groups are found to have different perceptions of the risks of victimization [58]. Hale found that women, elderly, and Caucasians tend to be more fearful compared to their counterparts [66]. However, other studies found different effects, because the influence of demographic factors can change substantially depending on the situation and type of crime [61].

XI. PERCEIVED RISK OF CYBERCRIME

The information capabilities of the Internet change the nature of crimes, as they provide cyber criminals with simple, cost effective and repeatable means of conducting rapid global- scale attacks, while remaining anonymous or unreachable for law enforcement [67]. We consider consumer-oriented cybercrime, i.e., cybercriminal attacks that potentially harm internet users, as they have the biggest effect on online service adoption. Therefore, we deliberately exclude some forms of cybercrime such as industrial espionage.

XII. CYBERCRIME AND ONLINE SERVICES AVOIDANCE

Research on online service avoidance as a response to perceived risk of cybercrime is rare and isolated. Saban et al. conducted an exploratory study in three US cities, finding that exposure to spam e-mails, which is considered to be a “weak” form of cybercrime, reduces consumers’ online purchases and the trust in information found online [68]. Smith proposes that expectancy theory explains the negative effect cybercrime has on online shopping. However, his claims are not backed by any empirical data [69]. Alshalan conducted an empirical study on a sample of 987 US house holds finding that cyber crime experience increases the fear of cybercrime [70]. More recently, B¨ohme & Moore conducted a secondary analysis of the 2012 Eurobarometer Cyber Security Report, which is also utilized in our analysis [71]. Using a set of simple logistic regressions, they found that cybercrime experience, media exposure, and cybercrime concern decrease the likelihood of using online services. Their approach provides valuable insights, but lacks a multi-stage consideration of the effects (i.e., cybercrime experience increases cybercrime concern, which ultimately reduces online participation) and an underlying theoretical model. Featherman et al. provide a theoretical model, which builds on the perceived risk-extended TAM [27], to test the impact of privacy risk on perceived ease- of-use and the intention to use e-commerce [49]. They find that the perceived ease-of-use, the vendor’s credibility and capability reduce privacy risk and ultimately increase adoption. However, the focus on e- commerceandthesoleconsiderationofprivacyrisk, neglecting crime, limit their study. To overcome these limitations, we next propose our research model.

4.2 Data We test the research model using the Special Eurobarometer 390, Cyber Security Report (CSR) which was published by the European Commission in July 2012 as part of a series of publications to raise cybercrime awareness and encourage the provision of counter measures [11]. The survey was conducted in March 2012 in all 27 EU member states. A total of 26,593 respondents above the age of 15 were interviewed face-to-face in their respective mother tongues.Usingstratificationbycountryaswellasrandomr outeandc losestbirthdayruleswithincountries, the survey is considered to be a representative sample of European citizens above the age of 15. 8,583 cases are excluded from our analysis, because respondents reported that they do not use the Internet at all.

172 cases (0.96%) are removed, because they contain ”Don’t Know” responses for all perceived risk and/or cybercrime experience related questions. Another 640 ”Don’t Know” responses (3.6%), measuring cybercrime experience, are changed into ”Never”, assuming that respondents who do not know whether they experienced cybercrime have not experienced it. The remaining1, 275 incomplete cases(7.17%) are handled by Mplus using pairwise deletion. Consequently, our analysis is based on 17,773 cases representing 18,605 EU Internet users (normalized weights).

XIII. DISCUSSION

Research on the economics of cybercrime has been largely descriptive. By contrast, we present a theoretically derived model to explain the impact of consumer-oriented cybercrime on online service avoidance and provide empirical support based on a pan-European sample. Four out of five tested hypotheses regarding the influence of perceived cybercrime risk and its antecedents are confirmed for online shopping and online banking (H1, H2, H3, H7). The positive influence of media awareness on perceived risk (H4, H5) is suggested by related research, but not empirically validated. The moderation effect of user confidence is partly confirmed. Effects between constructs are invariant (H6), but latent variable means for perceived risk of cybercrime and avoidance of online banking and shopping are significantly higher for unconfident users (H7). We now discuss the robustness of our results (6.1) and present theoretical (6.2) and practical implications (6.3).

XIV. ROBUSTNESS

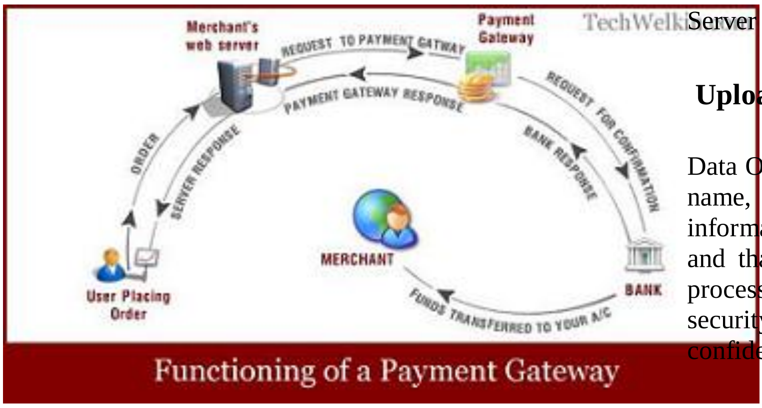
By testing our research model using secondary data of a complex multi-national sample, our study overcomes limitations of similar work, in particular non-representative sampling. However, conducting a secondary analysis requires special consideration of the robustness of the results. We use reflective multiitem measures to measure the perceived risk construct even though it is originally identified as multidimensional [27]. Consequently, the good reliability and validity of the results found for cybercrime experience and perceived cybercrime risk need to be confirmed by future research using validated measurement scales. We find high heterogeneity in the data set, which is likely caused by variation between countries and interviews conducted in different languages. The heterogeneous data set and the short ordinal scales lead to low correlations between indicators and constructs. However, all but one between-construct correlations and the majority of path coefficients are highly significant. The sophisticated surveying process and the large sample size of the Cyber Security Report as well as state-of- the-art analysis methods for complex samples with categorical indicators ensure the statistical power and reliability of our results.

XV. LIMITATIONS AND FUTURE RESEARCH

Our results have some technical limitations. The scales in the Cyber Security Report led to the exclusion of the media awareness construct from the empirical analysis. We suggest to define a dedicated cybercrime awareness construct, derived from the technical awareness construct introduced by [85], and test the research model on primary data. The cross-sectional design and the analysis of a single European sample also limits our results. Several authors demonstrate the importance of cultural aspects when studying technology acceptance (e.g., [36], [46]) and security behavior (e.g., [86]). To gain a more comprehensive picture, consumer reactions to cybercrime should be compared between countries. A longitudinal analysis also promises interesting results, because general Internet usage patterns and cybercrime practices change and evolve constantly. A model-related limitation is the absence of original, positive TAM factors. As consumers consider benefits and risks during the adoption process, a complete model, including perceived ease-of-use and perceived usefulness, should be tested to assess the predictive power of our research model. Featherman et al. test such a model, though unfortunately they just focus on privacy risk and neglect other forms of cybercrime [49]. The long term goal is the validation of the model to predict cybercrime impact on online service avoidance and ultimately indirect cybercrime costs. Such a model would be extremely valuable to understand the cybercrime problem and justify expenses for counter measures. Furthermore, direct and indirect cybercrime costs could be compared to validate existing studies. To complete the picture of social and economic cybercrime impacts, the model could be transfered from consumer research to the business context, e.g., to study the avoidance of cloud computing services.

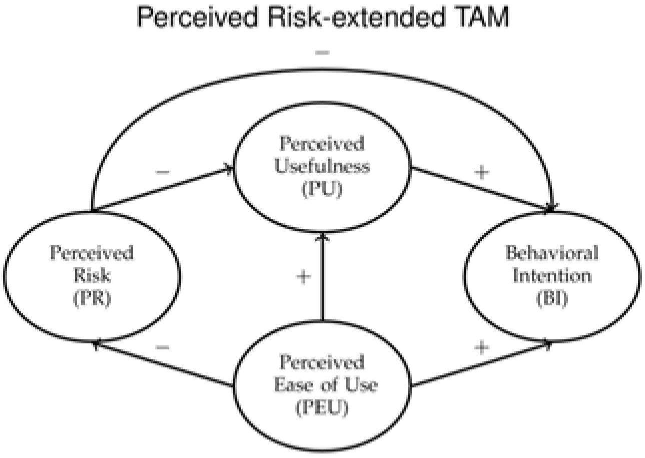
XVI. EXISTING SYSTEM

Three important online services: online banking , online shopping, online social networking .These services use some gateway for transaction that creates an insecure feeling among the users about their data.



XVII. PROPOSED SYSTEM

The reduction of perceived risk of cybercrime .This facilitates increased online service use. Two sets of actions: Reducing perceived risk of cybercrime, Increasing Internet user’s confidence.


Perceived Risk-extended TAM
Perceived Usefulness (PU)
Perceived Risk (PR)
Behavioral Intention (BI)
Perceived Ease of Use (PEU)
−
+
+
−
+
−

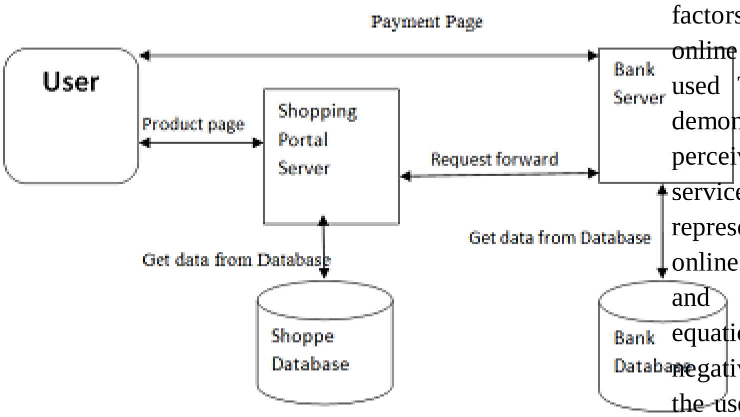


Fig: proposed system architecture

XVIII. CLIENT AND SERVER CONFIGURATION

In this Module we create a two server, one for Data owner and client interface and another for payment detail enter page that page is maintained by bank Server which contains the client bank details.

Upload Product

Data Owner uploads the product information (product name, cost, Acc no..) .All uploaded Product information data are maintained by Server Database and that Server is responsible for all client request process except payment page.This preserves the security as it does not have any chance to misuse the confidential data of the customer.

Bank Server Interface

Banking server is Responsible for direct Client Secure online payment, to avoid the risk of fraud online shopping web portal.It receives the request from the vendor directly without using any third party gateway.So this avoids the need for the third party gateway thereby avoiding the issues such as security and additional cost.

Buyer Portal

This page is provided by bank servers, when client click buy option from shopping portal. This portal is an interface between the client and the shopping port server.It only contains all the private details of the buyer.

XIX. CONCLUSIONS

Indirect cybercrime costs, incurred by fearful Internet users who are reluctant to use online services, are a big problem for today’s Internet-dependent society. We synthesize well-established research on technology acceptance models and criminology in the context of consumer-oriented cybercrime, to analyze factors that drive the counterpart of acceptance – online service avoidance. Building upon the widely used Technology Acceptance Model, our findings demonstrate the value of including a dedicated perceived cybercrime risk construct affecting online service avoidance. We test the model based on a representative European sample for three different online services: online banking, online shopping, and online social networking. The structural equation modeling analysis provides evidence for the negative impact of perceived risk of cybercrime on the use of online services and shows that the biggest impact is on the avoidance of online shopping. The model also explains antecedents of perceived risk of cybercrime, in particular, how prior cybercrime experience increases the perceived risk and ultimately consumer’s avoidance of online services. The effects are invariant between user groups of a different online proficiency (measured by the user’s confidence in doing transactions online). However, the level of perceived risk as well as online shopping and banking avoidance are significantly higher for less proficient Internet users. This highlights the importance of user education and strongly suggests that besides on-going active cybercrime defense (to reduce victimization), increasing Internet user's digital literacy must be a major target to reduce the costs of cybercrime for todays Internet-dependent society.

REFERENCES

[1] M.-C. Lee, "Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit," Electron. Commer. Res. Appl., vol. 8, no. 3, pp. 130–141, 2009.

[2] Y.-H. Li and J.-W. Huang, "Applying theory of perceived risk and technology acceptance model in the online shopping channel," World Acad. Sci. Eng. Technol., vol. 53, no. 4, pp.816– 822, 2009.

[3] Y. Amichai-Hamburger and Z. Hayat, "The impact of the Internet on the social lives of users: A representative sample from 13 countries," Comput. Human Behav., vol. 27, no. 1, pp. 585–589, 2011.

[4] M. Cardona, T. Kretschmer, and T. Strobel, "ICT and productivity: Conclusions from the empirical literature," Inf. Econ. Policy, vol. 25, no. 3, pp. 109–125, 2013.

[5] E. Brynjolfsson, "The contribution of information technology to consumer welfare," Inf. Syst. Res., vol. 7, no. 3, pp. 281–300, 1996.

[6] E. Brynjolfsson, M. D. Smith, and Y. J. Hu, "Consumer surplus in the digital economy: Estimating the value of increased product variety at online booksellers," Manage. Sci., vol. 49, no. 11, pp. 1580–1596, 2003.

[7] European Commission, "A Digital Agenda for Europe," Brussels, 2010. [Online]. Available: http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=com:2010:0245: fin:en:pdf

[8] T. Moore, R. Clayton, and R. Anderson, "The economics of online crime," J. Econ. Perspect., vol. 23, no. 3, pp. 3–20, 2009.

[9] P. Hunton, "The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model, "Comput. Law Secur. Rev., vol. 25, no. 6, pp. 528–535, 2009.

[10] R. Anderson, C. Barton, R. B¨ohme, R. Clayton, M. J. Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in The Economics of Information Security and Privacy, R. B¨ohme, Ed. Heidelberg: Springer Berlin, 2013, pp. 265–300.

[11] European Commission, "Special Eurobarometer 390 Cyber security," Brussels, 2012. [Online]. Available: http://ec. europa.eu/public\ opinion/archives/

[12] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Towarda unified view," MIS Q., vol. 27, no. 3, pp. 425–478, 2003.

[13] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," MIS Q., vol. 13, no. 3, pp. 319–340, 1989.

[14] P. Legris, J. Ingham, and P. Collerette, "Why do people use information technology? A critical review of the technology acceptance model," Inf. Manag., vol. 40, no. 3, pp. 191–204, 2003.

[15] S. Y. Yousafzai, G. R. Foxall, and J. G. Pallister, "Technology acceptance: A meta-analysis of the TAM: Part 1," J. Model. Manag., vol. 2, no. 3, pp. 251–280, 2007.

[16] M. Fishbein and I. Ajzen, Belief, attitude, intention and behavior: An introduction to theory and research. Addison- Wesley Pub. Co., 1975.

[17] I. Ajzen and M. Fishbein, Understanding attitudes and predicting social behaviour. Prentice-Hall, 1980.

[18] P. Hanafizadeh, B. W. Keating, and H. R. Khedmatgozar, "A systematic review of Internet banking adoption," Telemat. Informatics, vol. 31, no. 3, pp. 492–510, 2013.

[19] M. K. Chang, W. Cheung, and V. S. Lai, "Literature derived reference models for the adoption of online shopping," Inf. Manag., vol. 42, no. 4, pp. 543–559, 2005.

[20] L. Zhou, L. Dai, and D. Zhang, "Online shopping acceptance model – A critical survey of

consumer factors in online," J. Electron. Commer. Res., vol. 8, no. 1, pp. 41–62, 2007.

[21] K.-Y. Lin and H.-P. Lu, "Why people use social networking sites: Anempirical study integrating network externalities and motivation theory," Comput. Human Behav., vol. 27, no. 3, pp. 1152–1161, 2011.

[22] Y. Jiao, J. Yang, and S. Xu, "A study of the impact of social media characteristics on customer adoption intention of social media," in Proc. 2013 Int. Acad. Work. Soc. Sci. Atlantis Press, 2013, pp. 1095–1099.

[23] J.C.M.R.PinhoandA.M.Soares, "Examining the technology acceptance model in the adoption of social networks," J. Res. Interact. Mark., vol. 5, no. 2/3, pp. 116–129, 2011.

[24] D.-H. Shin and W.-Y. Kim, "Applying the Technology Acceptance Model and flow theory to Cyworld user behavior: Implication of the Web2.0 user acceptance." CyberPsychology Behav., vol. 11, no. 3, pp. 378–82, 2008.

[25]I.Ajzen,"The theory of planned behavior, "Organ.Behav.Hum. Decis. Process., vol. 50, no. 2, pp. 179–211, 1991.

[26] G. Moore and I. Benbasat, "Integrating diffusion of innovations and theory of reasoned action models to predict utilization of information technology by end-users," in Diffusion and Adoption of Information Technology, K. Kautz and J. Pries-Heje, Eds. Springer US, 1996, pp. 132–146.

[27] M. Featherman and P. Pavlou, "Predicting e-services adoption: A perceived risk facets perspective, "Int.J.Hum.Comput.Stud., vol. 59, no. 4, pp. 451–474, 2003. [28] R. A. Bauer, "Consumer behavior as risk taking," Dyn. Mark. a Chang. World, vol. 398, 1960.

[29] P. A. Pavlou, "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model," Int. J. Electron. Commer., vol. 7, no. 3, pp. 69–103, 2003.

[30] S. J. Tan, "Strategies for reducing consumers' risk aversion in Internet shopping," J. Consum. Mark., vol. 16, no. 2, pp. 163– 180, 1999.

[31] C.-M. Chiu, E. T. G. Wang, Y.-H. Fang, and H.-Y. Huang, "Understanding customers' repeat purchase intentions in B2C e-commerce: The roles of utilitarian value, hedonic value and perceived risk," Inf. Syst. J., vol. 24, no. 1, pp. 85–114, 2014.

[32] D. Gefen, E. Karahanna, and D. W. Straub, "Trust and TAM in online shopping: An integrated model," MIS Q., vol. 27, no. 1, pp. 51–90, 2003.

[33] M. Featherman and M. Fuller, "Applying TAM to e- services adoption:the Moderating Role of Perceived Risk,"inProc.36th Hawaii Int. Conf. Syst. Sci., 2003.

[34] S. M. Cunningham, "The major dimensions of perceived risk," Boston, pp. 82–111, 1967.

[35] C. Martins, T. Oliveira, and A. Popoviˇc, "Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application," Int. J. Inf. Manage., vol. 34, no. 1, pp. 1–13, 2014.

[36] S. L. Jarvenpaa, N. Tractinsky, and L. Saarinen, "Consumer trust in an Internet store: A cross-cultural validation," J. Comput. Mediated Commun., vol. 5, no. 2, 1999.

[37] D. H. McKnight, V. Choudhury, and C. Kacmar, "The impact of initial consumer trust on intentions to transact with a web site: A trust building model," J. Strateg. Inf. Syst., vol. 11, no. 3-4, pp. 297–323, 2002.

[38] B. Suh and I. Han, "Effect of trust on customer acceptance of Internet banking," Electron. Commer. Res. Appl., vol. 1, no. 3, pp. 247–263, 2003.

[39] H.-F. Lin, "Understanding behavioral intention to participate in virtual communities." CyberPsychology Behav., vol. 9, no. 5, pp. 540–547, 2006.

[40] A. R. Montazemi and H. Q. Saremi, "Factors affecting Internet banking pre-usage expectation formation," 2013 46th Hawaii Int. Conf. Syst. Sci., pp. 4666–4675, 2013.

[41] M. J. Metzger, "Privacy, trust, and disclosure: Exploring barriers to electronic commerce," J. Comput. Commun., vol. 9, no. 4, 2006.

[42] Y.-S. Wang, Y.-M. Wang, H.-H. Lin, and T.-I. Tang, "Determinants of user acceptance of

Internet banking: An empirical study," Int. J. Serv. Ind. Manag., vol. 14, no. 5, pp. 501–519, 2003.

[43] M. M. M. A. Riffai, K. Grant, and D. Edgar, "Big TAM in Oman: Exploring the promise of on-line banking, its adoption by customers and the challenges of banking in Oman," Int. J. Inf. Manage., vol. 32, no. 3, pp. 239–250, 2012.

[44] K. M. S. Faqih, "Integrating perceived risk and trust with technology acceptance model: An empirical assessment of customers' acceptance of online shopping in Jordan," in Res. Innov. Inf. Syst., 2011, pp. 1–5.

[45] D.-H. Shin, "The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption," Interact. Comput., vol. 22, no. 5, pp. 428– 438, 2010.

[46] I. Im, S. Hong, and M. S. Kang, "An international comparison of technology adoption," Inf. Manag., vol. 48, no. 1, pp. 1–8, 2011.

[47] T. C. E. Cheng, D. Y. C. Lam, and A. C. L. Yeung, "Adoption of internet banking: An empirical study in Hong Kong," Decis. Support Syst., vol. 42, no. 3, pp. 1558–1572, 2006.

[48] A. N. Giovanis, S. Binioris, and G. Polychronopoulos, "An extension of TAM model with IDT and security/privacy risk in the adoption of internet banking services in Greece," EuroMed J. Bus., vol. 7, no. 1, pp. 24–53, 2012.

[49] M.S. Featherman, A.D. Miyazaki, and D.E.Sprott, "Reducing online privacy risk to facilitate e-service adoption: The influenceofperceivedeaseofuseandcorporatecredibility,"J.Serv. Mark., vol. 24, no. 3, pp. 219–229, 2010.

[50] O. Kwon and Y. Wen, "An empirical study of the factors affecting social network service use," Comput. Human Behav., vol. 26, no. 2, pp. 254–263, 2010.

[51] M.-d.-C. Alarc´on-del Amo, C. Lorenzo-Romero, and G. Del Chiappa, "Adoption of social networking sites by Italian," Inf. Syst. E-bus. Manag., pp. 1–23, 2013.

[52] K. F. Ferraro and R. LaGrange, "The measurement of fear of crime," Sociol. Inq., pp. 70–101, 1987.

[53] N. E. Rader, D. C. May, and S. Goodrum, "An empirical assessment of the "Threat of Victimization:" Considering fear of crime, perceived risk, avoidance, and defensive behaviors," Sociol. Spectr., vol. 27, no. 5, pp. 475–505, 2007.

[54] T. R. Tyler, "Assessing the risk of crime victimization: The integration of personal victimization experience and socially transmitted information," J. Soc. Issues, vol. 40, no. 1, pp. 27– 38, 1984.

[55] W. G. Skogan, "The impact of victimization on fear," Crime Delinq., vol. 33, no. 1, pp. 135–154, 1987.

[56] A. E. Liska, A. Sanchirico, and M. D. Reed, "Fear of crime and constrained behavior specifying and estimating a reciprocal effects model," Soc. Forces, vol. 66, no. 3, pp. 827–837, 1988.

[57]K.WittebroodandM.Junger,"Trendsinviolentcrime :Acomp arison between police statistics and victimization surveys," Soc. Indic. Res., vol. 59, no. 2, pp. 153–173, 2002.

[58] M. Visser, M. Scholte, and P. Scheepers, "Fear of crime and feelings of unsafety in European countries: Macro and micro explanations in cross-national perspective," Sociol. Q., vol. 54, no. 2, pp. 278–301, 2013.

[59] E.F.McGarrell ,A.L.Giacomazzi, and Q.C.Thurman, "Neighb orhood disorder, integration, and the fear of crime," Justice Q., vol. 14, no. 3, pp. 479–500, 1997.

[60] R. Gainey, M. Alper, and A. T. Chappell, "Fear of crime revisited: Examining the direct and indirect effects of disorder, risk perception, and social capital," Am. J. Crim. Justice, vol. 36, no. 2, pp. 120–137, 2010.

[61] L. Heath and K. Gilbert, "Mass media and fear of crime," Am. Behav. Sci., vol. 39, no. 4, pp. 379–386, 1996.

[62] A. A. F. Wahlberg and L. Sjoberg, "Risk perception and the media," J. Risk Res., vol. 3, no. 1, pp. 31–50, 2000.

[63] J. Jackson, "Revisiting risk sensitivity in the fear of crime," J. Res. Crime Delinq., vol. 48, no.

4, pp. 513–537, 2011.

[64] T. Chiricos, K. Padgett, and M. Gertz, “Fear, TV news, and the reality of crime,” Criminology, vol. 38, no. 3, pp. 755– 786, 2000.

[65] A. E. Liska and W. Baccaglini, “Feeling safe by comparison: crime in the news paper,” Soc.Probs., vol.37, no.3, pp.360–374, 1990.

[66] C. Hale, “Fear of crime: A review of the literature,” Int. Rev. Vict., vol. 4, no. 2, pp. 79–150, 1996.

[67]J.Clough,Princples of cybercrime. Cambridge University Press, 2010.

[68] K. A. Saban, E. McGivern, and J. N. Saykiewicz, “A critical look at the impact of cybercrime on consumer Internet behavior,” J. Mark. Theory Pract., vol. 10, no. 2, pp. 29–37, 2002.

[69] A. D. Smith, “Cybercriminal impacts on online business and consumer confidence,” Online Inf. Rev., vol. 28, no. 3, pp. 224– 234, 2004.

[70] A. Alshalan, “Cyber-crime fear and victimization: An analysis of anational survey, ”Disseration, Mississippi State University, 2006.

[71] R. B¨ohme and T. Moore, “How do consumers react to cybercrime?” in 7th APWG eCrime Res. Summit, Las Croabas, 2012, pp. 1–12.

[72] D. Florˆencio and C. Herley, “Sex, lies and cyber-crime surveys,” in Economics of Information Security and Privacy III, B. Schneier, Ed. New York: Springer, 2013, pp. 35–53.

[73] J. F. Hair, Multivariatedata analysis, 7th ed. Prentice Hall, 2010.

[74] J. Henseler, C. M. Ringle, and R. R. Sinkovics, “The use of partial least squares path modeling in international marketing,” Advances Int. Mark., vol. 20, no. 2009, pp. 277–319, 2009.

[75] C. M. Ringle, M. Sarstedt, and D. W. Straub, “A critical look at the use of PLS-SEM in MIS Quarterly,” MIS Q., vol.36, no. 1, pp. iii–xiv, 2012.

[76] S. J. Finney and C. DiStefano, “Non-normal and categorical data in structural equation modeling,” in Struct. Equ. Model. A Second course, G. Hancock and R. Mueller, Eds. Greenwich, 2006, pp. 269–314.

[77] B. Muthen, S. H. C. du Toit, and D. Spisic, “Robust inference using weighted least squares and quadratic estimating equations in latent variable modeling with categorical and continuous outcomes,” Psychometrika, vol. 75, 1997.

[78] J. Anderson and D. Gerbing, “Structural equation modeling in practice: A review and recommended two-step approach,” Psychol. Bull., vol. 103, no. 3, pp. 411–423, 1988.

[79] C. Fornell and D. F. Larcker, “Evaluating structural equation models with unobservable variables and measurement error,” J. Mark. Res., vol. 18, no. 1, pp. 39–50, 1981.

[80] C. Yu and B. Muth´en, “Evaluation of model fit indices for latent variable models with categorical and continuous outcomes,” in Paper Presented at the Annual Meeting of the American Educational Research Association, New Orleans, LA, 2002.

[81] R. E. Millsap and J. Yun-Tein, “Assessing Factorial Invariance in Ordered-Categorical Measures,” Multivariate Behav. Res., vol. 39, no. 3, pp. 479–515, 2004.

[82] A. W. Meade, E. C. Johnson, and P. W. Braddy, “Power and sensitivity of alternative fit indices in tests of measurement invariance.” J. Appl. Psychol., vol. 93, no. 3, pp. 568–592, 2008.

[83] B. M. Byrne, R. J. Shavelson, and B. Muth´en, “Testing for equivalence of factor covariance and mean structures: The issue of partial measurement invariance,” Psychol. Bull., vol. 105, no. 3, pp. 456–466, 1989.

[84] P. A. Norberg, D. R. Horne, and D. A. Horne, “The privacy paradox: Personal information disclosure intentions versus behaviors,”J.ConsumerAffairs,vol.41,no.1,pp.100–126,2007.

[85] T. Dinev and Q. Hu, “The centrality of awareness in the formation of user behavioral intention toward protective information technologies,” J. Assoc. Inf. Syst., vol. 8, no. 7, pp. 386–408, 2007.

[86] T. Dinev, J. Goo, Q. Hu, and K. Nam, “User behaviour towards protective information

technologies: the role of national cultural differences," Inf. Syst. J., vol. 19, no. 4, pp.391–412, 2009.