Understanding the influence of cybercrime risk on the e-service adoption of European Internet users

Working Paper

Markus Riek*, Rainer Böhme
University of Münster, Department of Information Systems
Leonardo-Campus 3, 48149 Münster, Germany
markus.riek@wwu.de, rainer.boehme@wwu.de

Tyler Moore
Southern Methodist University, Computer Science and Engineering Department
P.O. Box 750122, Dallas, TX 75275-0122, USA
tylerm@smu.edu

Abstract. Cybercrime is a pervasive threat for today's Internet-dependent society. While the real extent and economic impact is hard to quantify, scientists and officials agree that cybercrime is a huge and still growing problem. A substantial fraction of cybercrime's overall costs to society can be traced to indirect opportunity costs, resulting from unused online services. This paper presents a theoretically derived model that utilizes technology acceptance research and insights from Criminology to identify factors that reduce Internet users' intention to use online services. We hypothesize that avoidance of online banking, online shopping and online social networking is increased by prior cybercrime victimization and media reports. The effects are mediated by perceived risk of cybercrime and moderated by the user's confidence online. We test our hypotheses using a structural equation modeling analysis of a representative pan-European sample. Our empirical results confirm the

*Corresponding author.

negative impact of perceived risk of cybercrime on the usage of all three categories of online services and support the role of cybercrime experience as an antecedent of perceived risk of cybercrime. We further show that more confident Internet users perceive less cybercriminal risk and are more likely to use online banking and online shopping which highlights the importance of consumer education.

Keywords. *Information Security, Economics of Cybercrime, Avoidance of E-Services, Consumer Behavior, Perceived Risk, Technology Acceptance Model, Structural Equation Modeling.*

1 Introduction

Online services provide extensive individual, social, and economic benefits for modern society. Online banking has introduced a convenient yet inexpensive and effective way of remotely handling financial transactions (Lee, 2009); e-commerce has increased product availability while decreasing trading costs (Li and Huang, 2009); and online social networks have deepened personal relationships worldwide (Amichai-Hamburger and Hayat, 2011). Reviewing the economic growth literature, Cardona et al. (2013) show that information and communication technology increased labor productivity in the EU by at least 31% (33% in the US) since 1995. Brynjolfsson (1996) emphasizes the importance of the consumer surplus, in particular of online services (Brynjolfsson et al., 2003), which provides additional social welfare, not reflected in the traditional statistics.

Accordingly, 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 (European Commission, 2010). In 2012 Internet use in Europe is already pervasive and still growing, with more than half of the European citizens (53%) accessing the Internet daily (European Commission, 2012). The global Internet use has increased in line, with more than a third of the global population already accessing the Internet and more than 60% of the users living in developing countries (ITU, 2013).

Unfortunately, the growing online space also provides ground for 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 to gain financial profit (Moore et al., 2009). Consumer-oriented cybercrime, which includes identity theft, credit card fraud, and phishing, increases the risk of using online services for all Internet users (Hunton, 2009). To avoid uncertain and risky situations, many Internet users remain reluctant to use online services. Such reluctance leads to many missing out on social and economic benefits provided by an Internet-connected world.

Anderson et al. (2013) show that the majority of cybercrime costs are indirect opportunity costs, created by users avoiding online services. Understanding how these costs are formed is a main prerequisite to dealing with a global cybercrime problem. To find appropriate responses, factors that explain why Internet users' hesitate need to be systematically identified.

Work on the social effects of cybercrime is still rare, as most studies focus on cybercriminal motives and attacks, or provide technical, organizational, and regulatory measures to prevent cybercrime. To fill this research gap, we synthesize work from Information Systems (IS) research on technology acceptance models and Criminology. We come up with a model that explains the impact of cybercrime on the avoidance of online services, by showing how cybercrime generates 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 (European Commission, 2012). We use covariance-based structural equation modeling to test seven hypotheses for three important online services, namely: online banking, online shopping and online social networking.

Our work is structured as follows. Section 2 provides a theoretical background on technology acceptance, Criminology, and cybercrime. Section 3 synthesizes the different findings and proposes our research model. Section 4 explains the methodological approach and data preparation process. Section 5 presents the empirical results. Section 6 discusses theoretical and practical implications and section 7 concludes.

2 Related Work

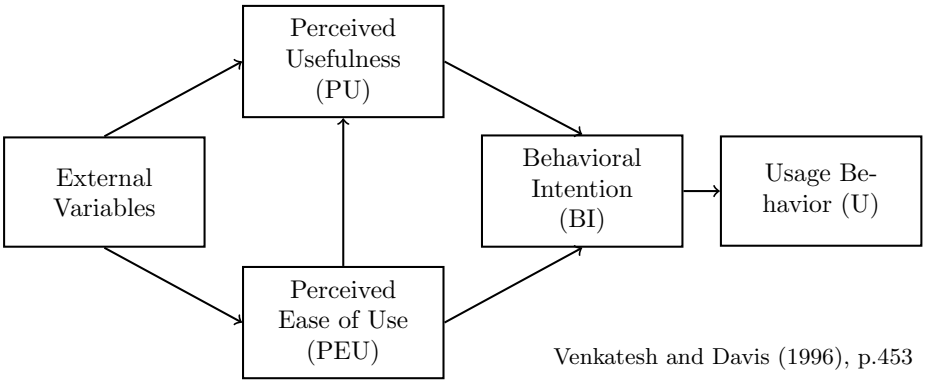
To explain how cybercrime reduces online participation, we synthesize work from different fields. Building on technology acceptance models we explain what factors influence the intention to use online services (2.1). The focus is on the perceived risk of cybercrime as the main factor making users hesitate. Subsequently, we review Criminology literature to investigate antecedents of perceived crime risk and draw analogies to online crime (2.2). Finally, we show existing work on the social effects of cybercrime (2.3).

2.1 Technology Acceptance Models in IS Research

Models explaining and predicting the acceptance of new technologies, combining IS research with behavioral science, business and economics, have been of interest 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 (Venkatesh et al., 2003). We focus on studies applying acceptance models in the context of general online services, online banking, online shopping, and online social networking (OSN).

Technology Acceptance Model. The Technology Acceptance Model (TAM; Davis, 1989), illustrated in its final version in Figure 1, is prominently used in IS research to explain and predict the acceptance of a wide spectrum of new technologies ranging from operating systems to desktop applications to online services (Legris et al., 2003; Yousafzai et al., 2007). TAM is based on the Theory of Reasoned Action (TRA; Fishbein and Ajzen, 1975; Ajzen and Fishbein, 1980), 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, BI determines the actual *Usage Behavior* (U).

Figure 1: Technology Acceptance Model (TAM)



Venkatesh and Davis (1996), p.453

TAM's parsimony, robustness and predictive power (Venkatesh and Davis, 2000) led to wide usage in empirical studies (cf. Table 1). The models are frequently tested using multiple regressions or more sophisticated structural equation modeling (SEM) approaches. The advantage of SEM lies in its ability to include latent variables, while still providing consistent parameter estimates (Urbach and Ahlemann, 2010). The latent variables (PEU, PU, BI, U) are measured based on multiple indicators (i.e., multiple questions in user surveys) using factor analysis and the structural parameters are subsequently estimated using path analysis. Legris et al. (2003) show that the following findings are mostly convergent across TAM studies: PEU and PU increase the BI to use a technology, which ultimately has a positive effect on U.

TAM applications for online services. Even though TAM has been intentionally constructed to explain employee's adoption of company-owned, work-related software (Davis, 1989), many studies show its applicability in other contexts, including online services. In a recent literature review, Hanafizadeh et al. (2013) show that of 165 publications that consider the adoption of online banking between 1999 and 2012, the majority applies acceptance models (mostly TAM) to test relations between the constructs empirically. Chang et al. (2005) found a similar proliferation of acceptance models for online

shopping adoption. Zhou et al. (2007) developed the Online Shopping Acceptance Model (OSAM), extending TAM for application in an online shopping scenario.

Models of OSN adoption mostly focus on other factors, such as network externalities (Lin and Lu, 2011), connectedness and participation (Jiao et al., 2013). Nevertheless, a few studies also applied TAM in the OSN context. Shin et al. (2008) utilize TAM by extending the model with *Perceived Involvement* and *Enjoyment*. Pinho and Soares (2011) also show its applicability by analyzing OSN adoption for a set of 150 students. However, they remark that the use of the parsimonious, unextended TAM model is a limitation of their study.

Other Technology Acceptance Models. Further commonly used acceptance models are the Theory of Planned Behavior (TPB; Ajzen, 1991), which extends TRA with a behavioral control factor and Innovation Diffusion Theory (IDT Moore and Benbasat, 1996), which focuses on properties of the innovation itself to explain its adoption. Arguing that all of them capture important aspects, but none is able to measure technology acceptance sufficiently, Venkatesh et al. (2003) propose the Unified Theory of Acceptance and Use of Technology (UTAUT) model. Integrating eight different technology acceptance models, including TAM, TPB, and IDT, the UTAUT model is increasingly used for analyzing the acceptance of online banking (Hanafizadeh et al., 2013) and is able to explain up to 70% of the variance in the BI variable, exceeding former TAM studies (Venkatesh et al., 2003). However, the base model misses at least one important factor – perceived risk (PR) – vital for all online scenarios (Featherman and Pavlou, 2003).

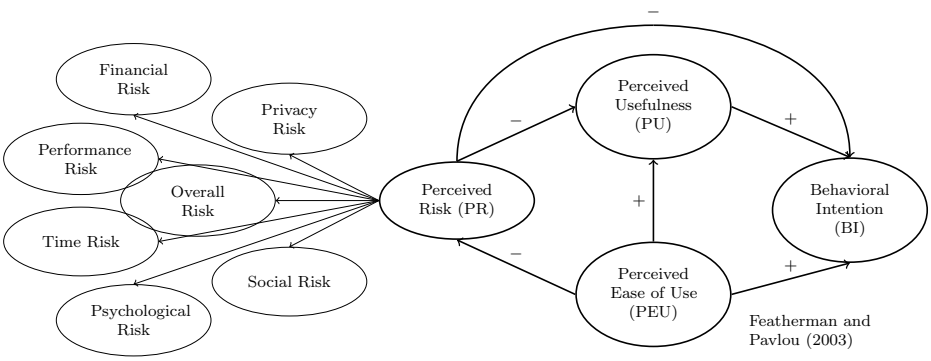
Risk in online transactions. The importance of perceived risk in commercial transactions was already identified by Bauer (1960), who states that shopping always involves risk because the buyer's decision has consequences that can be unpleasant and are not perfectly predictable. The spatial and temporal separation between consumers and retailers and the open architecture of the Internet increase this uncertainty (Pavlou, 2003) and are the reason why PR is more pronounced in online shopping than in traditional brick-and-mortar shopping (Tan, 1999).

Two forms of uncertainty are naturally present: behavioral and environmental uncertainty (Pavlou, 2003). Behavioral uncertainty is concerned with the behavior of dubious, possibly malicious online sellers. Environmental uncertainty reflects more general concern about the security of the Internet as a channel for commercial transactions. Both can increase the level of perceived risk, as the customer is not able to fully monitor the seller's behavior or the security of the online transaction in general (Chiu et al., 2012). 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 (Chiu et al., 2012; Gefen et al., 2003).

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 (Featherman and Fuller, 2003; Pavlou, 2003). By adding PR as a multidimensional construct, originally introduced as a general perceived risk construct by Cunningham (1967), Featherman and Pavlou (2003) systematically integrated perceived risk into TAM. Conducting an empirical study, they found that performance related risks, i.e., time, privacy and financial risks, have the strongest impact on the overall construct of perceived risk, whereas social risks, concerned with losing the current social status, were not found to have a significant influence. Figure 2 shows their model of the PR construct and its interaction within TAM.

Figure 2: Perceived Risk extended TAM



The negative effect of PR on BI exists for initial and repeated online shopping and is larger for users that shop less (Featherman and Fuller, 2003). Martins et al. (2014) confirmed the importance of risks by integrating the UTAUT model with the PR theory, deriving a combined model which is able to explain 81% of the usage behavior variance for 248 online banking customers in Portugal. They also provide further evidence that financial, time and privacy risks are the most salient concerns.

Trust. Trust can be another important factor in the adoption process, as it can mitigate behavioral uncertainty (Pavlou, 2003). Featherman and Pavlou (2003) describe it as the counterpart of perceived risk, as trust in an online seller or the Internet in general reduces the perceived risk of online transactions.

Montazemi and Saremi (2013) 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. Metzger (2006) found similar evidence for OSN users, who express strong concerns about privacy of their personal information, but are less than vigilant about safeguarding it (Awad and Krishnan, 2006). Thus, having trust in the provider is strongly linked to the disclosure of information and thus the participation within the social networks (Metzger, 2006). A number of studies include trust as a construct which influences the adoption of electronic services (e.g., Jarvenpaa et al., 1999; McKnight et al., 2002; Gefen et al., 2003; Pavlou, 2003; Suh and Han, 2003; Lin, 2006).

Technology acceptance of online services. Table 1 shows that technology acceptance models, especially TAM and UTAUT are commonly applied for online services. Most research using risk extended technology acceptance models is conducted within the online banking domain, including comparative studies (e.g., Lee, 2009) and national applications around the globe (e.g., Wang et al., 2003; Riffai et al., 2012; Martins et al., 2014). Trust is more frequently used in the context of online shopping (e.g., Gefen et al., 2003). However, some studies also use PR or both constructs (e.g., Faqih, 2011). The adoption of online social networking is less frequently tested with technology acceptance models, but studies exist that show a their applicability (e.g., Shin, 2010). Technology acceptance models are dominantly tested using means of latent variable path analysis, either SEM or partial least square (PLS) analysis.

Table 1: Influence of Perceived Risk on Online Services Acceptance

Domain	Year	Model	Method	Findings	Reference
eServices	2003	TAM-PR	SEM	PR ↘ PU, BI; PR as 2. order construct	Featherman and Pavlou (2003)
	2003	TAM-PR	ANOVA	PR ↘ PU, BI; PR moderates effects	Featherman and Fuller (2003)
	2003	eTAM	SEM	Credibility, PU, PEU ↗ BI	Wang et al. (2003)
Online Banking	2006	eTAM	SEM	PU, PEU, Tr(Web Security) ↗ BI	Cheng et al. (2006)
	2009	TAM-TPB-PR	SEM	PR ↘ ATU (ultimately BI)	Lee (2009)
	2011	UTAUT-PR	SEM	PR ↘ BI	Im et al. (2011)
	2012	eUTAUT	COR	PR moderates: PU, PEU ↗ BI	Riffai et al. (2012)
	2012	TAM-IDT	PLS	PEU, Tr(Web Security) ↗ BI	Giovanis et al. (2012)
	2013	TAM-Tr	Meta-SEM	Tr ↗ BI	Montazemi and Saremi (2013)
	2014	UTAUT-PR	SEM	PU, PEU, Compatibility ↗ BI; PR ↘ BI	Martins et al. (2014)
	2003	TAM-PR	PLS	Tr ↗ PU, BI	Pavlou (2003)
Online Shopping	2003	TAM-Tr	SEM	Tr, PU ↗ BI	Gefen et al. (2003)
	2010	TAM-PR	SEM	PR(Privacy), Credibility, PEU ↗ BI	Featherman et al. (2010)
	2011	TAM-Tr	PLS	PR ↘ Trust; Trust ↗ BI	Faqih (2011)
	2012	PT-PR	PLS	PR moderates effects	Chiu et al. (2012)
	2010	TRA-TAM	SEM	PR (Security & Privacy) ↘ Tr, BI	Shin (2010)
Online Social Networking	2010	eTAM	SEM	PR not considered	Kwon and Wen (2010)
	2013	TAM-PR-Tr	SEM	No effect for: PR on PU, BI	Alarcón-del Amo et al. (2013)

Model: Extended TAM (eTAM), Trust (Tr), Perceived Risk (PR), Theory of Planned Behavior (TPB), Prospect Theory (PT)
Method: Analysis of variance (ANOVA), Correlation Analysis (COR)
Findings: Positive Effect (↗), Negative Effect (↘)

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 (Chiu et al., 2012) and should be included, either as antecedent (e.g., Featherman and Pavlou, 2003; Im et al., 2011) of PU, PEU, and BI or as a moderating factor (e.g., Featherman and Fuller, 2003; Chiu et al., 2012). PR is a second order construct, as defined by Featherman and Pavlou (2003), and privacy, performance and financial risks are the most salient first order factors. The negative influence of PR on BI or its antecedents, i.e., PEU or PU, is frequently shown. Finally, it is shown that trust reduces PR and increases BI.

2.2 Perceived Risk in Criminology

While the former section shows how perceived risk negatively influences the online society by making users hesitate to use online services, this section sheds light on how people's risk perception of crime is formed. As cybercrime is still a rather new form of criminal activity and its social impact is not studied extensively yet, we show findings from traditional Criminology and translate them to the online context.

Ferraro and LaGrange (1987) show that fear of crime is multidimensional in nature consisting of two distinct components. 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, but the effects between them are still unclear (Rader et al., 2007). 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, because emotional reactions are also an important factor in people's reaction to cybercrime. However, future research should address the risk–fear relationship in the online context.

Victimizaton Effects on Risk Perception. Examining prior victimization as an antecedent of perceived risk of crime reveals mixed results. Most scholars found strong effects (e.g., Tyler, 1984; Skogan, 1987; Liska et al., 1988; Wittebrood and Junger, 2002; Visser et al., 2013). Yet others found just weak or no effects at all (e.g., McGarrell et al., 1997). Gainey et al. (2010) 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 (Ferraro and LaGrange, 1987), we suspect that crime experience leads to an increased concern about it. Visser et al. (2013) provide empirical evidence for the effect based on two representative European surveys conducted in 2006 and 2008.

Media Effects on Risk Perception. The effect media has on risk perception is similarly controversial (Heath and Gilbert, 1996). Reviewing the literature, Wahlberg and Sjoberg (2000) found that media coverage influences risk perception, especially if reports repeat over time. Jackson (2011) 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. As crime reports tend to be rather sensational and alarming, they are likely to increase the public's risk perception (Wahlberg and Sjoberg, 2000).

A majority of research was conducted for TV news. Studies found that watching TV reports increases the feeling of being unsafe (Visser et al., 2013), especially if they resonate personal experiences (Chiricos et al., 2000), cover sensational crimes (Liska and Baccaglini, 1990; Jackson, 2011), and/or are broadcasted frequently (Chiricos et al., 2000). Local crime news tend to have a stronger effect on the perceived risk (Heath and Gilbert, 1996), especially for people living in high crime places (Chiricos et al., 2000). Wahlberg and Sjoberg (2000) suggest that the media needs to be considered as one factor among others, such as prior victimization, experiences in the social environment or demographic factors.

Demographic Factors Influencing Risk Perception. Demographics are important in measuring offline fear of crime, as different social groups are found to have different perceptions of the risks of victimization (Visser et al., 2013). Hale (1996) found that women, elderly, and Caucasians tend to be more fearful compared to their counterparts. However, other studies found different effects, because the influence of demographic factors can change substantially depending on the situation and type of crime (Heath and Gilbert, 1996; Gainey et al., 2010). We conclude that prior victimization and media reports are likely to have an effect on the perceived risk of cybercrime and that context specific demographic variables need to be considered in a model testing these effects.

Risk Perception Effects on Social Participation. Reviewing criminological literature, Hale (1996) found that the fear of becoming a victim and general feeling of being unsafe can have harmful effects on individuals, networks and whole societies. In analogy to the findings of technology acceptance literature, lower levels of general trust, caused by fear of crime, lead to avoidance and defensive behavior (Liska et al., 1988; Rader et al., 2007), which ultimately leads to less participation in social activities (Stafford et al., 2007).

2.3 Perceived Risk of Cybercrime

"Cybercrimes can be defined as any crimes which are committed via the Internet" (European Commission, 2012, p. 34). The information capabilities of

the Internet change the nature of crime, as they provide cyber criminals with simple, cost effective and repeatable means of conducting rapid global-scale attacks, while remaining anonymous and/or unreachable for law enforcement (Clough, 2010). 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.

Cybercrime Effects on Protective Measures. A noteworthy stream of research focuses on the effects of cybercrime on protective behavior of computer users. Anderson and Agarwal (2010) review behavioral security literature, showing that, analogous to technology acceptance, the Theory of Planned Behavior (TPB) is used frequently to explain the adoption of security software. Dinev and Hu (2007) for example applied a TPB model to analyze factors that increase the intention to use applications for malware prevention, finding that threat awareness has the biggest impact. By extending the TPB, Yao and Linz (2008) investigated online privacy protective behavior, highlighting the importance of psychological processes in privacy related research. In a more general approach Burns and Roberts (2013) study online protective behavior as a result of exposure to cybercrime, explaining 81% in the variance of behavioral intention.

Protection Motivation Theory (PMT; Rogers, 1975) is another powerful and frequently used model to explain individual's intention to engage in protective actions based on a threat and a coping appraisal (Anderson and Agarwal, 2010). The threat appraisal is formed by the perceived severity and vulnerability (victimization probability) of the attack and the coping appraisal by the response efficacy and self-efficacy (Rogers, 1975). Lee and Larsen (2009) found that all four factors influence security behavior of business executives, but that coping appraisal factors are less important for IT experts, compared to their counterpart. Focusing on security policies, Ifinedo (2012) uses PMT to show that vulnerability and self-efficacy increase intention to IS security policy compliance. Even though related, this research differs significantly, because it investigates active responses to cybercriminal threats, which is the opposite reaction to the avoidance behavior we study.

Cybercrime Effects on Avoidance of Online Services. So far research on avoidance behavior as a response to perceived risk of cybercrime is rare and isolated. Saban et al. (2002) 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 customers' online purchases and the trust in information found online. Smith (2004) proposes that expectancy theory explains the negative effect cybercrime has on online shopping. However, he does not supply his propositions with any empirical data. Alshalan (2006)

conducted an empirical study on a sample of 987 US households finding that cybercrime experience increases the fear of cybercrime.

More recently, Böhme and Moore (2012) conducted a secondary analysis of the Eurobarometer Cyber Security Report which is also utilized in our analysis. 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) as well as a profound theoretical model. Featherman et al. (2010) provide a theoretical model, which builds on the perceived risk extended TAM (Featherman and Pavlou, 2003), to test the impact of privacy risk on perceived ease-of-use and the intention to use e-commerce. They find that the perceived ease-of-use, the vendor's credibility and capability reduce privacy risk and finally increase adoption. However, the focus on e-commerce and the sole consideration of privacy risk, neglecting for example online fraud, limit their study. To overcome these limitations, we propose our research model in the subsequent section.

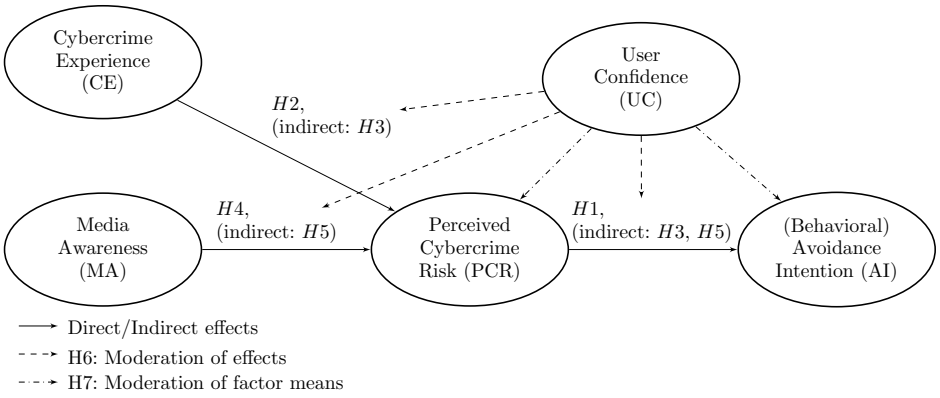
3 Research Model and Hypotheses

Building on the work of Böhme and Moore (2012), we set out to systematically explain the social effects of cybercrime by finding factors that make users avoid online services. The literature review on technology acceptance shows that perceived risk reduces the intention to use online services. Findings from Criminology provide evidence for the increasing effect of prior victimization and media coverage on the individual risk perception. We synthesizes both research streams in the context of cybercrime and come up with our research model, illustrated in Figure 3. This section explains our research model and the hypotheses to be tested in the empirical analysis.

The right part of the model represents the basic elements – Perceived Risk decreasing Behavioral Intention – of the risk-extended TAM (Featherman and Pavlou, 2003) or UTAUT model (Martins et al., 2014). The constructs are incorporated as *Perceived Cybercrime Risk* (PCR) and *(Behavioral) Avoidance Intention* (AI). As we want to explain avoidance (not acceptance) intention of online services, we invert the effect proposed in TAM and UTAUT and hypothesize a positive effect of PCR on AI. The left part of the model represents the criminological extension of the acceptance model. *Cybercrime Experience* (CE) and *Media Awareness* (MA) are included as antecedents, increasing PCR. *User Confidence* (UC) moderates the effects and latent variable means.

We believe that the causal directions of the following hypotheses are justified, as they are based on former studies and further enforced by the questions

Figure 3: Research Model in Path Model Notation



in the Cyber Security Report (e.g.: "Has concern about cybercrime made you change the way you use the Internet?"[1]).

H1: Perceived Cybercrime Risk increases Avoidance Intention to use online services.

Our review of the criminological literature shows that crime has a negative impact on social life, because it makes people avoid situations and places. As studies on technology acceptance find the same negative effects of perceived risk on the adoption of online services in several different scenarios, we believe that the effects can be translated into the online context. Featherman and Pavlou (2003) show that financial, performance and privacy risks are the most influential risk factors. As consumer-oriented cybercriminal attacks are likely to increase these risks, we assume that cybercrime is a major factor increasing perceived online risk and ultimately reducing online service adoption.

H2: Cybercrime Experience increases Perceived Cybercrime Risk.

Prior victimization as an antecedent increasing perceived risk of crime has been controversially discussed in Criminology. However, as perceived risk is assumed to be a function of the probability to get victimized and the severity of the criminal act (Ferraro and LaGrange, 1987), we suspect that cybercrime experience leads to a higher level of perceived cybercrime risk. Furthermore, victimization works as a reminder of vulnerability (Keane, 1995), increasing the perceived risk. We suspect that the effects are stronger in the online context, due to a higher degree of uncertainty in the Internet, caused by spatial and temporal separation of its users.

H3: Cybercrime Experience increases Avoidance Intention to use online services. The effect is fully mediated by Perceived Cybercrime Risk.

Saban et al. (2002) show that cybercrime experience decreases the likelihood of repeated online shopping. Böhme and Moore (2012) confirm the

[1]CSR: Question 7 (European Commission, 2012)

negative effects for online banking and general online participation. We agree with their findings, but hypothesize that the effect is fully mediated by *Perceived Cybercrime Risk*. Accordingly, *Cybercrime Experience* increases *Perceived Cybercrime Risk* (H2), which ultimately increases the *Avoidance Intention* (H1) of e-services.

H4: Media Awareness increases Perceived Cybercrime Risk.

Media reports are found to increase the perceived risk of offline crime, especially if the news cover local crimes. Cybercrimes are likely to be perceived as local crimes, because the Internet is an open, global infrastructure in which all users can be affected by cybercrime. Thus, we suspect that these effects occur online as well. Furthermore, cybercriminal attacks are often reported in a rather spectacular way and victimization statistics are likely to be overestimated (Florêncio and Herley, 2013) which increasing the perceived risk.

H5: Media Awareness increases Avoidance Intention to use online services. The effect is fully mediated by Perceived Cybercrime Risk.

Böhme and Moore (2012) state that Internet users who have heard about cybercrime in news reports or from colleagues are less likely to bank online than those who have not heard such reports. In analogy to *Cybercrime Experience*, we hypothesize that this effect is fully mediated by *Perceived Cybercrime Risk*, i.e., *Media Awareness* increases *Perceived Cybercrime Risk* (H4), which ultimately increases *Avoidance Intention* (H1) of e-services.

H6: User Confidence moderates the effects in the model, in that the effects are smaller for confident users.

Different authors (e.g., Featherman and Fuller, 2003) show that understanding how different consumer segments perceive and evaluate e-services and risks is essential to explain adoption. Accordingly, Protection Motivation Theory highlights the importance of self-efficiacy for the behavioral intention to engage in protective behavior. Therefore, we suspect that the user's confidence in handling online transactions moderates the effects proposed in H1 – H5. We hypothesize that the effects *Cybercrime Experience* and *Media Awareness* have on *Perceived Cybercrime Risk* are smaller for more confident users, as they feel more secure about their online behavior and perceive less uncertainty. Furthermore, we expect that confident users are less likely to reduce their online service usage due to perceived risk of cybercrime.

H7: User Confidence moderates the effects in the model, in that latent variables means for perceived risk of cybercrime and avoidance intention are smaller for confident users.

In addition to different effect sizes we suspect that user confidence influences the means of the latent variables in our model. In particular we hypothesize that more confident Internet users perceive less cybercrime risk and are also less likely to avoid online services.

4 Research Method

To test our hypotheses we use structural equation modeling (SEM) in a secondary analysis of the Special Eurobarometer Cyber Security Report (CSR). This section motivates the use of SEM (4.1) and describes the preparation of the CSR data set (4.2) and the development of the measurement mode (4.3).

4.1 Statistical Method

We use a single-level, cross-sectional structural equation model. SEM can be either covariance-based – here and in the following just referred to as SEM – or variance-based – referred to as partial least squares (PLS) analysis. Both approaches are similar, but SEM is more suited for confirmatory theory testing and PLS rather for theory development or predictive applications (Henseler et al., 2009). We use the covariance-based SEM technique, as we empirically test our theoretically derived model and SEM provides the fit indices to statistically confirm our hypotheses (Henseler et al., 2009; Urbach and Ahlemann, 2010). Moreover, major reasons for using PLS, i.e., a small sample size, formative indicators, and a focus on prediction (Ringle et al., 2012), do not apply in our case. Non-normal data, another common reason for using PLS (Ringle et al., 2012), is accounted for by the robust weighted least square (WLSMV) estimation method developed for non-normal, categorical indicators (Finney and DiStefano, 2006).

We use the statistical software Mplus[2] for the parameter estimation, as it provides all features required by the secondary analysis. First, it supports the WLSMV estimation method (Muthen et al., 1997), which is considered to be the best available approach for categorical, non-normal distributed indicators, given a large sample size (Finney and DiStefano, 2006). Second, it supports the consideration of missing values. Third, it supports the direct incorporation of sampling weights based on the raw data (Asparouhov, 2005) considered to be best available approach for complex samples (Stapleton, 2006).

4.2 Sample 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 (European Commission, 2012). The survey was conducted in March 2012 in all 27 EU member states. A total of 26,593 respondents above the age of 15 have been interviewed face-to-face in their respective mother tongue. Using stratification by country as well as random route and closest birthday rules within countries, the survey

[2]Version 7.11, available at: `http://www.statmodel.com`

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. Further 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 yet. The remaining 1,275 incomplete cases (7.17%) are handled by Mplus using pairwise deletion. Consequently, our analysis is based on 17,773 cases representing 18,605 EU citizens (using normalized weights), considered a representative sample of the European population of Internet users above the age of 15.

Table 2: Questions for Latent Variable Measurement

ID	**Latent Variable (Scale)/ Indicator**	**Answers**		
	Group of users	All*	Confident	Unconfident
	Number of respondents	18.605	4.972	2.196
MA	**Media Awareness (Binary)**			
"In the last year have you heard anything about cybercrime from . . . ?"		Yes		
QE8.1	Television	67.14 %	69.81 %	65.62 %
QE8.2	Radio	23.09 %	30.02 %	16.83 %
QE8.3	Newspaper	33.56 %	41.51 %	21.19 %
QE8.4	Internet	34.54 %	49.10 %	17.34 %
CE	**Cybercrime Experience (Ordinal)**			
"How often have you experienced or been victim of . . . ?"		At least occasionally		
QE10.1	Identity theft	8.22 %	9.18 %	4.81 %
QE10.2	Spam e-mails	38.25 %	52.94 %	20.54 %
QE10.3	Online fraud	12.52 %	16.47 %	6.24 %
QE10.4	Illegal content	15.38 %	18.89 %	9.47 %
QE10.5	Unavailable content	12.87 %	16.42 %	5.98 %
PCR	**Perceived Cybercrime Risk (Ordinal)**			
"How concerned are you personally about becoming a victim of . . . ?"		At least fairly		
QE11.1	Identity theft	61.77 %	54.12 %	67.03 %
QE11.2	Spam e-mails	48.39 %	37.98 %	55.86 %
QE11.3	Online fraud	49.30 %	44.05 %	50.29 %
QE11.4	Child pornography	51.03 %	44.06 %	59.63 %
QE11.5	Content of racial hatred	41.03 %	32.91 %	50.37 %
QE11.6	Unavailable content	43.07 %	39.07 %	42.86 %
AI	**(Behavioral) Avoidance Intention (Binary)**			
"Due to cybercrime concern I'm less likely to . . . ."		Yes		
QE7.2	Online banking	14.67 %	9.05 %	24.38 %
QE7.1	Online shopping	17.85 %	11.42 %	27.25 %
QE7.3	Publishing personal information Online	37.04 %	39.36 %	29.84 %
UC	**User Confidence (Ordinal)**	At least fairly		
QE5	"How confident are you to use the Internet?"	68.99 %		

*EU Internet users above the age of 15.

4.3 Measurement Development

The theoretical constructs identified in our model: *Media Awareness*, *Cybercrime Experience*, *Perceived Cybercrime Risk*, (Behavioral) *Avoidance Intention*, and *User Confidence* are measured based on questions in the CSR.

Answers in the CSR are reported on binary and ordinal scales. The ordinal scales are either 3-point frequency scales reporting the count of cybercrime experience (never, occasionally, often) or 4-point scales that measure the strength of agreement with the given question (not at all, not very, fairly, very). This section introduces the relevant questions for each construct (summarized in Table 2).

Cybercrime Experience is measured by five ordinal indicators. Internet users are asked how frequently they have experienced five different cybercriminal attacks: identity theft, spam e-mails, online fraud, illegal content, and unavailable services. Almost half of the Internet users (49.78%) state that they have encountered one form of cybercrime at least occasionally. Individual types of attacks, except spam e-mails, have not been reported by more than 80% of the respondents and surprisingly also spam e-mails have never been experienced by 61.75%.

Media Awareness represents the extent to which people are exposed to news about cybercrime from different media sources. Respondents were asked on a binary scale whether they have seen or heard about cybercrime from TV, Radio, Newspaper, or the Internet. The majority heard about cybercrime from TV (67.14%), one third from newspapers (33.56%) or the Internet (34.54%), and about one quarter from the radio (23.09%).

Perceived Cybercrime Risk is measured based on six ordinal indicators. Internet users reported their concern of victimization regarding six different types of cybercrime: identity theft, spam e-mails, online fraud, child pornographic content, content of racial hatred, and unavailable services. The types overlap with the crimes measuring cybercrime experience, except for illegal content which is divided into child pornography and content of racial hatred. Most respondents are fairly or not very concerned. Concerns are higher for identity theft (61.77%) and rather low for accidentally encountering illegal content (41.03%). Alshalan (2006) shows that a reason for this difference is the perceived severity of the cybercrime type, as encountering illegal material usually does not cause as much harm as for example identity theft.

(Behavioral) Avoidance Intention is measured by three binary questions. Respondents are asked if they are less likely to use a particular online service due to concerns about cybercrime. Table 2 shows that 17.85% are less likely to do online shopping and 14.67% are less likely to do online banking. The avoidance of sharing personal information online, which is used as a proxy for online social network usage, is higher (37.04%). Each binary indicator is directly included as a dependent variable and three models are tested separately, one for each online service.

User Confidence is measured using one ordinal indicator. Responses in the CSR show that more than two thirds of the Internet users (68.99%) are at least fairly confident and more than one quarter (26.72%) is very confident in conducting online transactions.

Table 3: Standardized Factor Loadings

Latent Variable	Indicator	Mean	SD	Loading	SE	Z-Score	R^2
Media Awareness	QE8.1	0.67	0.47	0.540***	0.041	13.315	0.292
	QE8.2	0.23	0.42	0.729***	0.026	27.788	0.531
	QE8.3	0.34	0.47	0.719***	0.02	35.891	0.517
	QE8.4	0.35	0.48	0.698***	0.026	26.835	0.487
Cybercrime Experience	QE10.1	0.09	0.32	0.681***	0.039	17.293	0.464
	QE10.2	0.49	0.68	0.624***	0.025	25.007	0.389
	QE10.3	0.14	0.38	0.701***	0.025	28.475	0.491
	QE10.4	0.17	0.43	0.707***	0.04	17.622	0.5
	QE10.5	0.14	0.38	0.754***	0.036	21.198	0.569
Perceived Cybercrime Risk	QE11.1	2.74	0.97	0.821***	0.007	114.124	0.674
	QE11.2	2.45	0.98	0.821***	0.008	99.549	0.674
	QE11.3	2.45	0.97	0.805***	0.01	77.395	0.648
	QE11.4	2.54	1.09	0.801***	0.009	86.913	0.642
	QE11.5	2.31	0.98	0.823***	0.007	124.904	0.677
	QE11.6	2.32	0.99	0.795***	0.007	119.106	0.632
AI: Online Banking	QE7.2	0.18	0.38				
AI: Online Shopping	QE7.1	0.15	0.35				
AI: OSN	QE7.3	0.37	0.48				

N = 17,773 $\chi^2(df) = 448.73$ (123) p<.05 = 0 RMSEA = .012 (.011 – .013) TLI = .961 CFI = .968
Significance: *** = $p < 0.001$

5 Results

We use the two-step approach introduced by Anderson and Gerbing (1988). The quality of the measurement model is reported first to prove construct validity and reliability (5.1) and the structural parameters are estimated in a second step (5.2). The moderation effect is tested in a third step, using multiple-group analysis (5.3).

5.1 Measurement Model

We evaluate construct reliability and validity based on the three criteria suggested by Fornell and Larcker (1981). First, the standardized factor loadings should be significant and exceed 0.5. Second, the construct reliability, tested using the composite reliability (CR) indicator, should exceed 0.8. As CR takes into account that indicators can have different loadings, it is more suited in our analysis than the more prominently used indicator Cronbachs Alpha (Hair, 2010). And third, the average variance extracted (AVE), which represents the amount of indicator variance that is accounted for by the underlying items of the construct, should be greater than 0.5, so that the construct explains more than half of the variance of its indicators (Hair, 2010).

All indicators meet the first criterion – significant factor loadings greater than 0.5 (cf. Table 3). Table 4 shows that the second and third criterion are not met by *Media Awareness*, which has unacceptable values for construct reliability and convergent validity (CR = 0.77, AVE = 0.46). Several

Table 4: Discriminant Validity

	CR	AVE	MA	CE	PCR	AI: OS	AI: OB	AI: OSN
Media Awareness (MA)	0.77	0.46	**0.678**	(0.022)	(0.038)	(0.035)	(0.028)	(0.025)
Cybercrime Experience (CE)	0.82	0.48	0.322***	**0.693**	(0.021)	(0.044)	(0.033)	(0.013)
Perc. Cybercrime Risk (PCR)	0.92	0.66	0.008	0.264***	**0.812**	(0.019)	(0.017)	(0.028)
AI: Online Shopping (OS)	-	-	0.028	0.061	0.170***	-	(0.035)	(0.032)
AI: Online Banking (OB)	-	-	0.034	0.172***	0.127***	0.577***	-	(0.05)
AI: OSN	-	-	0.329***	0.152***	0.092***	0.305***	0.296***	-

Lower-left: between construct correlations; Diagonal: $\sqrt{\text{AVE}}$; Upper-right: SE's of the correlations.
Avoidance Intention (AI), Online Social Networking (OSN)

modification indices (MI) underpin the bad influence of *Media Awareness* on the overall model (cf. cross-loadings in Table 9). The statistical problems are likely raised by measuring the latent variable on four binary indicators. Given that the phrasing of the question does not reflect our understanding of cybercrime awareness very well, as hearing about cybercrime from multiple sources may not increase awareness about, it is excluded from the structural analysis. Nevertheless, we suspect that media reports influence the behavior of Internet users and encourage further research on this aspect.

MI further imply that a positive measurement error correlation should be added between QE11.4 and QE11.5[3] (MI: 35, E.P.C.Std.: 0.452). As both questions measure one form of illegal content (QE11.4: Child Pornography, QE11.5: Content of Racial Hatred) and are likely to be interpreted similarly by the respondent, the correlation is legitimate. Table 10 and Table 11 show that all constructs in the reduced model – without *Media Awareness* – fulfill the reliability and validity requirements. Note that AVE value for *Cybercrime Experience* is above the required threshold in the reduced model.

Discriminant validity ensures that different constructs do not measure the same. To confirm discriminant validity, the square root of AVE (noted on the diagonal of Table 4) should be greater than the between construct correlations (Henseler et al., 2009). Table 4 shows that this is given for all constructs. Correlations between constructs are low, but still highly significant ($p<0.001$), except for the correlation between *Avoidance Intention* of online shopping and *Cybercrime Experience*. The low correlations can be traced to the secondary analysis and the heterogeneous data set which includes multiple countries, languages, and cultures. However, the measurement model analysis shows that the reduced model can be reliably and validly measured based on the CSR data.

5.2 Structural Model

Based on the sufficient measurement model the structural parameters are estimated. The overall goodness-of-fit is evaluated using approximate fit

[3] "How concerned are you personally about becoming a victim of [child pornography/content of ratial hatred]?"

Table 5: Structural Models

Path coefficient	Effect	Online Banking	Online Shopping	OSN
CE → PCR		0.258 *** (0.0200)	0.258 *** (0.0200)	0.260 *** (0.0200)
PCR → AI		0.093 *** (0.0230)	0.167 *** (0.0200)	0.061 * (0.0270)
CE → AI	Direct	0.142 *** (0.0340)	0.020 (0.0440)	0.121 *** (0.0110)
	Indirect	0.024 *** (0.0050)	0.043 *** (0.0060)	0.016 * (0.0070)
	Total	0.166 *** (0.0310)	0.063 ′ (0.0430)	0.137 *** (0.0120)
χ^2 (*df*)		143.04 (51)	138.96 (51)	201.56 (51)
RMSEA (90% CI)		.010 (.008 – .012)	.010 (.008 – .012)	.013 (.011 – .015)
TLI / CFI		.990 / .993	.991 / .993	.985 / .988

Perc. Cybercrime Risk (PCR), Cybercrime Experience (CE), Avoidance Intention (AI)
Significance: *** = $p < 0.001$; * = $p < 0.05$; ′ = $p < 0.15$

indices. The values of the chi-square test are reported, but not considered for model fit evaluation, as the test is sensitive to sample size and unreliable for large samples (Finney and DiStefano, 2006). Instead we evaluated different approximate fit indices to test the model fit, based on the thresholds for categorical outcomes (RMSEA < 0.05, TLI and CFI > 0.95; Yu and Muthén (2002)). Table 5 shows that all approximate fit indices indicate good model fit for the three online services, with a slightly better fit for online shopping and online banking. The hypotheses are tested based on the significance of the path coefficients. The path coefficients, their standard error (in brackets), and the level of significance are documented in Table 5.

Perceived Cybercrime Risk increases *Avoidance Intention* among all online services, providing support for H1. The biggest effect is observed for online shopping ($\beta = 0.167$, $p < 0.001$). A smaller, but still highly significant effect is observed for the avoidance of online banking ($\beta = 0.093$, $p < 0.001$). Avoidance of online social networks ($\beta = 0.061$), measured by publishing less personal information online, is only significant at the $p < 0.05$ level.

Cybercrime Experience increases the *Perceived Cybercrime Risk* for all three models ($\beta = 0.258$, $p < 0.001$), providing strong support for H2. Indirect effects of *Cybercrime Experience* on *Avoidance Intention* are found for all domains: online banking ($\beta = 0.024$, $p < 0.001$), online shopping ($\beta = 0.046$, $p < 0.001$), and online social networking ($\beta = 0.016$, $p < 0.05$), supporting H3. Full mediation by *Perceived Cybercrime Risk* is only found for the avoidance of online shopping, as the direct effect is not significant ($\beta = 0.02$). However, the total effect of *Cybercrime Experience* is only significant at a p<0.05 level. Significant direct effects are observed for *Cybercrime Experience* on avoidance of online banking and online social networking, but the total effects are partially mediated by *Perceived Cybercrime Risk*.

Table 6: Invariance Testing

Model	χ^2 (*df*)	CFI	TLI	RMSEA (90% CI)	$\Delta\chi^2$ (*df*)	ΔCFI
Online Banking						
Mod A: Baseline	167.81 (102)	.995	.994	.013 (.009 – .016)		
Mod B: Invariant	213.41 (123)	.993	.993	.014 (.011 – .017)	73.67 (21)	.002
Mod C: Fixed Path Coef.	228.16 (126)	.992	.992	.015 (.012 – .018)	19.46 (3)	.001
Mod D: Fixed Factor Means	265.39 (126)	.990	.989	.017 (.014 – .020)	33.36 (3)	.003
Online Shopping						
Mod A: Baseline	168.25 (102)	.995	.994	.013 (.009 – .017)		
Mod B: Invariant	215.39 (123)	.993	.993	.014 (.011 – .017)	75.03 (21)	.002
Mod C: Fixed Path Coef.	233.62 (126)	.992	.992	.015 (.012 – .018)	20.02 (3)	.001
Mod D: Fixed Factor Means	265.95 (126)	.990	.989	.017 (.014 – .020)	31.57 (3)	.003
Online Social Networking						
Mod A: Baseline	192.78 (102)	.993	.991	.015 (.012 – .019)		
Mod B: Invariant	238.10 (123)	.992	.991	.016 (.013 – .019)	75.05 (21)	.001
Mod C: Fixed Path Coef.	237.59 (126)	.992	.991	.015 (.012 – .018)	9.13 (3)	.000
Mod D: Fixed Factor Means	276.69 (126)	.989	.988	.018 (.015 – .021)	26.86 (3)	.003

5.3 Moderation Analysis

The moderation effects of user confidence are tested by conducting a multiple-group analysis for confident and unconfident Internet users. The descriptive statistics provided in Table 2, show that confident users have reported higher rates of cybercrime experience. The difference is biggest for spam e-mails, which is reported by half (52.94%) of the confident, but only by the fifth part (20.54%) of the unconfident Internet users. Unconfident users on the other hand report higher levels of perceived risk for every form of cybercrime and are more likely to reduce their use of online shopping and online banking. Considering spam e-mails more then half of unconfident Internet (55.86%) users report concern whereas only 37.98% confident users report this concern.

Before testing the moderation effect of user confidence measurement invariance must be ensured. We use the general-to-specific procedure proposed by Millsap and Yun-Tein (2004). Meade et al. (2008) show that for large samples, the chi-square difference test is biased to reject invariance and that a CFI-based difference test should be used instead. A CFI change ($\Delta CFI <= 0.002$) confirms measurement invariance.

Table 6 shows that all fit indices show acceptable fit for all models and all three online services. The baseline model (Mod A) includes both groups with all parameters freely estimated in each group. To test measurement invariance, factor loadings and thresholds are fixed in the invariant model (Mod B). Modification indices suggest a partly invariant model, with the thresholds of QE11.3 being free to vary between groups. Byrne et al. (1989) show that moderation effects can be tested on partly invariant models if at least two intercepts and loadings are fixed.

The invariance of path coefficients is tested by fixing them to be equal between groups (Mod C) and comparing the model fit to Mod B. Table 6 shows that Mod C is invariant to Mod B for all online services, because

Table 7: Moderation Effects: User Confidence

Path coefficient	Effect	Online Banking		Online Shopping		OSN	
		Unconfident	Confident	Unconfident	Confident	Unconfident	Confident
CE → PCR		0.232 *** (0.027)	0.315 *** (0.027)	0.234 *** (0.028)	0.315 *** (0.027)	0.233 *** (0.027)	0.315 *** (0.027)
PCR → AI		0.036 (0.028)	0.138 *** (0.037)	0.100 *** (0.030)	0.197 *** (0.049)	0.010 (0.034)	0.074 (0.045)
CE → AI	Direct	0.190 *** (0.040)	0.208 *** (0.031)	0.032 (0.053)	0.119 * (0.057)	0.277 *** (0.045)	0.093 ** (0.033)
	Indirect	0.008 (0.007)	0.043 *** (0.011)	0.024 ** (0.008)	0.062 (0.016)	0.002 (0.008)	0.023 (0.014)
	Total	0.198 *** (0.037)	0.252 *** (0.036)	0.055 (0.053)	0.181 ** (0.058)	0.279 *** (0.044)	0.117 *** (0.003)
Cybercrime Experience (CE)		0.00 (*fixed*)	0.785 ** (0.267)	0.00 (*fixed*)	0.891 ** (0.297)	0.00 (*fixed*)	1.162 *** (0.271)
Perc. Cybercrime Risk (PCR)		0.00 (*fixed*)	−0.506 *** (0.140)	0.00 (*fixed*)	−0.531 *** (0.142)	0.00 (*fixed*)	−0.621 *** (0.143)
Avoidance Intention (AI)		24.38%	9.05%	27.25%	11.42%	29.84%	39.36%

Significance: *** = $p < 0.001$; ** = $p < 0.01$; * = $p < 0.05$

$\Delta CFI <= 0.002$. The chi-square-based DIFFTEST ($\Delta\chi^2$ (*df*)), provided by Mplus for WLSMV estimation, also shows the lowest values for this model alternation confirming that reactions of confident and unconfident Internet users do not differ significantly. Consequently, H6 needs to be rejected.

The invariance of factor means and intercepts is tested by fixing the factor means for all latent variables and the threshold for the respective question on online service *Avoidance Intention* (Mod D). Table 6 shows that this constrained model exceeds the ΔCFI threshold in all three domains, indicating a significant deviation from the invariant model (Mod B). Conclusively, latent variable means are not invariant and differ between confident and unconfident Internet users.

To compare the differences, factor means are fixed to zero for unconfident users and freely estimated for confident users. Table 7 shows that confident users report more *Cybercrime Experience*, but significantly less *Perceived Cybercrime Risk* and a smaller *Avoidance Intention* of online shopping and online banking. The moderation effect is different for online social network participation, i.e., publishing personal information online, as unconfident users do not reduce their participation in social networks as much as confident users. Consequently, H7 is accepted for online shopping and online banking, but rejected for online social networking.

6 Discussion

Research on the economics of cybercrime has been largely descriptive. 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. Table 8 shows that four out of five tested hypotheses regarding the influence of perceived cybercrime risk and its

Table 8: Tested Hypotheses in Table Notation

Hypothesis	OB	OS	OSN	Description
H1: PCR → AI	✓	✓	(✓)	(✓) Only significant for p<0.05 for OSN
H2: CE → PCR	✓	✓	✓	
H3: CE → AI	(✓)	✓	(✓)	(✓) Partial mediation for OB and OSN
H6: UC moderation	–	–	–	Same effects (H1, H2, H3) in both groups
H7: UC moderation	✓	✓	–	Higher level of PCR and AI for confident users

Perc. Cybercrime Risk (PCR), Avoidance Intention (AI), Cybercrime Experience (CE)
User Confidence (UC), Online banking (OB), Online Shopping (OS), Online social networking (OSN)
H4, H5 are not empirically tested

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 due to unreliable measurement of the media awareness construct. 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 discuss the robustness of our results (6.1) and present theoretical (6.2) and practical implications (6.3).

6.1 Robustness Checks

By testing our research model using secondary data of a complex, multinational 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 multiple-item measures to measure the perceived risk construct, even though it is originally identified as multi-dimensional (Featherman and Pavlou, 2003). 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 to be caused by variation between multiple 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 (see section 4.1) ensure the statistical power and reliability of our empirical results.

6.2 Theoretical Implications

We provide empirical evidence that the risk extended TAM can be applied to measure online service avoidance from a cybercrime perspective. By adding a

perceived cybercrime risk construct to TAM our model supports earlier suggestions (e.g., by Featherman and Pavlou, 2003) to consider negative factors when studying technology acceptance. The SEM results confirm the positive influence of perceived risk of cybercrime on European Internet user's avoidance intention of online banking, online shopping and online social networking.

Perceived risk of cybercrime has the strongest impact on the avoidance of online shopping. According to Pavlou (2003) online shopping includes behavioral uncertainty, caused by dubious merchants, in addition to the environmental uncertainty of the Internet, caused by third party attacks. The high level of uncertainty and the low switching costs reduce customer loyalty in online shopping, making it easier to avoid services.

Opposing to that, switching costs are higher in online banking and customers usually retain with a single vendor. Accordingly, the risk is only based on environmental uncertainty, once trust in the online banking vendor is established. This explains the smaller effect perceived risk of cybercrime has on the avoidance of online banking. Montazemi and Saremi (2013) show the importance of trust in online banking adoption, which even exceeds traditional TAM factors (perceived ease-of-use and perceived usefulness).

We find the smallest effect (only significant at $p<0.05$) of perceived cybercrime risk on the avoidance of online social networking (OSN). As social networking is a rather low-risk e-service, usually not involving financial transactions, we conclude that consumer's avoidance is not significantly driven by perceived cybercriminal risk, but rather by social factors such as network externalities and social ties, which are not included in the current model. The small influence can also be explained by the privacy paradox introduced by Barnes (2006), which states that consumers express privacy concerns, but still publish private data to build up online profiles. Accordingly, users might perceive a general cybercrime risk, but keep using OSNs. These inconclusive findings and the rare application of TAM for OSN adoption suggest further research using different behavioral models (e.g., Lin and Lu, 2011).

Looking at antecedents of cybercrime risk we find a positive effect of prior cybercrime experience on the avoidance of online services, which is at least partially mediated by perceived cybercrime risk for all online services. The full mediation found for online shopping further supports the importance of perceived risk of cybercrime regarding the avoidance of online shopping.

The moderation analysis shows that the strength of the effects in our model is not driven by unobserved variance in user's confidence during online transactions. Differences are found in factor means, as confident Internet users perceive significantly less cybercrime risk and are less likely to change their online behavior even though they report more cybercrime experience. The higher level of existing experience can be explained by different usage patterns. Confident Internet users surf more frequently, which increases the probability of becoming victimized as well as their ability of identify a cy-

bercriminal attacks.

Opposing to that, unconfident users perceive more cybercrime risk and have a higher intention to avoid online banking or shopping. Even though this result was expected, it might be puzzling in combination with the fact that unconfident users reported less cybercrime experience. How can a lower level of cybercrime experience lead to more perceived risk if the effects are the same? We believe that this discrepancy can be explained by missing factors in the model, i.e., media awareness. If, as hypothesized and shown in the literature review, media awareness increases perceived cybercrime risk and the effect is stronger for unconfident Internet users, it can explain the higher factor means. We can not confirm this finding empirically and recommend further research in this direction.

6.3 Practical Implications

Our practical implications are mainly directed towards policy makers, but are also valuable for managers doing business online. The Digital Agenda for Europe highlights the potential of the Internet to be Europe's economic growth engine ensuring social welfare (European Commission, 2010). Increasing e-commerce usage is formulated as one of main goals to reach by 2020. We show that the reduction of perceived risk of cybercrime is essential to facilitate increased online service use and consequently increase business revenues and limit the costs of cybercrime to society. Our findings suggest two sets of actions to reduce the risk of cybercrime perceived by the public.

One way is the reduction of victimization, by continuously improving defense measures and making the online environment safer. However, these improvements must be credibly communicated by companies to assure consumers of the safety of online transactions. Policy makers should create incentives such as trustmarks or security certificates to foster system security and its public communication.

Another set of actions should focus on enhancing Internet user's digital literacy. Our analysis demonstrates that confident Internet users perceive less cybercrime risk and are less likely to avoid online services. To help building user confidence trusted sources of authorative advice about cybercrime and protective behavior should be established. Appropriate means must be developed to raise public awareness about cybercriminal threats, but also educate Internet users to make informed decisions. The target of anti-cybercrime campaigns must rather be on long-term attitude building than on short-term retention. Businesses should implement easy-to-use services to support the confidence building process on the consumer side.

7 Conclusions

Indirect cybercrime costs, incurred by feared Internet users who are reluctant to use online services, are a big problem for todays 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. Adding upon the widely used Technology Acceptance Model our findings suggest the inclusion of a dedicated perceived cybercrime risk construct affecting online service avoidance.

We test the model empirically for three different online services, online banking, online shopping, and online social networking based on a representative European sample. The structural equation modeling analysis provides evidence for the negative impact of perceived risk of cybercrime on the usage 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 imposed by cybercrime on todays Internet-dependent society.

7.1 Limitations and Future Research

Our results have some clear technical limitations. The given scales in the Cyber Security Report lead to the exclusion of the media awareness construct from the empirical analysis. Future research should overcome this problem by testing the research model, including the media awareness construct, based on primary data using the validated instruments suggested in section 6.1.

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., Jarvenpaa et al., 1999; Im et al., 2011) and security behavior (e.g., Dinev et al., 2009). To gain a more comprehensive picture, consumer reactions to cybercrime should be compared between countries within and outside of Europe. Studying changes over time in a longitudinal analysis also promises interesting results, because general Internet usage patterns and cybercrime practices change and develop 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 in order to assess the predictive power of our research model. Featherman et al. (2010) test such a model, unfortunately they just focus on privacy risk and neglect other forms of cybercrime.

The long term goal is the validation of the model in order 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 protective 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 oriented research to the business context, e.g., to study the avoidance of cloud computing services by companies.

Acknowledgments

The authors would like to thank the Eurobarometer team at the European Commission for making the data available and also the German Academic Exchange Service (DAAD) for providing the funding for the research visit during which this study was mainly conducted. The travel to attend WEIS 2014 is supported by the European Commission under grant agreement number 607775 (E-CRIME).

APPENDIX

Additional tables used in the confirmatory factor analysis. Table 9 shows the modification indices of the cross-loadings. Table 10 and Table 11 show the optimized measurement model without the media awareness construct.

Table 9: Modification Indices for Cross-Loadings

Latent Variable	Operator	Indicator	MI	EPC	Std.EPC
Media Awareness	BY	QE10.2	85.387	0.608	0.328
Cybercrime Experience	BY	**QE8.4**	55.661	0.348	0.237
Media Awareness	BY	QE10.1	34.315	-0.409	-0.221
Cybercrime Experience	BY	**QE8.3**	28.46	-0.276	-0.188
Perc. Cybercrime Risk	BY	QE10.2	25.532	-0.152	-0.125
Perc. Cybercrime Risk	BY	**QE8.1**	22.33	0.109	0.09
Media Awareness	BY	QE10.3	22.059	-0.319	-0.172
Perc. Cybercrime Risk	BY	**QE8.3**	11.711	-0.111	-0.091

Table 10: Standardized Factor Loadings: Optimized Model

Latent Variable	Indicator	Mean	SD	Loading	SE	Z-Score	R^2
Cybercrime Experience	QE10.1	0.09	0.32	0.776***	0.041	19.006	0.602
	QE10.2	0.49	0.68	0.556***	0.025	21.9	0.309
	QE10.3	0.14	0.38	0.769***	0.03	26.03	0.591
	QE10.4	0.17	0.43	0.724***	0.042	17.265	0.524
	QE10.5	0.14	0.38	0.740***	0.046	16.021	0.548
Perceived Cybercrime Risk	QE11.1	2.74	0.97	0.821***	0.007	113.882	0.674
	QE11.2	2.45	0.98	0.820***	0.008	99.558	0.672
	QE11.3	2.45	0.97	0.805***	0.01	77.593	0.648
	QE11.4	2.54	1.09	0.801***	0.009	86.91	0.642
	QE11.5	2.31	0.98	0.823***	0.007	124.615	0.677
	QE11.6	2.32	0.99	0.795***	0.007	119.309	0.632
AI: Online Banking	QE7.2	0.18	0.38				
AI: Online Shopping	QE7.1	0.15	0.35				
AI: OSN	QE7.3	0.37	0.48				

N = 17773 χ^2 (df) = 254.07 (70) χ^2/df = 3.63 p<0.05 = 0
RMSEA = .012 (.011 – .014) TLI = 0.98 CFI = 0.984

Table 11: Discriminant Validity: Optimized Model

	CR	AVE	CE	PCR	AI: OS	AI: OB	AI: OSN
Cybercrime Experience (CE)	0.84	0.51	**0.714**	(0.02)	(0.043)	(0.031)	(0.012)
Perc. Cybercrime Risk (PCR)	0.92	0.66	0.258***	**0.812**	(0.019)	(0.017)	(0.028)
AI: Online Shopping (OS)	-	-	0.063	0.170***	-	(0.035)	(0.032)
AI: Online Banking (OB)	-	-	0.167***	0.127***	0.577***	-	(0.05)
AI: OSN	-	-	0.137***	0.092***	0.305***	0.297***	-

Lower-left: between construct correlations; Diagonal: $\sqrt{\text{AVE}}$; Upper-right: SE's of the correlations.
Avoidance Intention (AI), Online Social Networking (OSN)

References

Ajzen, Icek. 1991. The theory of planned behavior. *Organ. Behav. Hum. Decis. Process.* **50**(2) 179–211.

Ajzen, Icek, Martin Fishbein. 1980. *Understanding attitudes and predicting social behaviour*. Prentice-Hall.

Alarcón-del Amo, María-del-Carmen, Carlota Lorenzo-Romero, Giacomo Del Chiappa. 2013. Adoption of social networking sites by Italian. *Inf. Syst. E-bus. Manag.* 1–23.

Alshalan, Abdullah. 2006. Cyber-crime fear and victimization: An analysis of a national survey. Disseration, Mississippi State University.

Amichai-Hamburger, Yair, Zack Hayat. 2011. The impact of the Internet on the social lives of users: A representative sample from 13 countries. *Comput. Human Behav.* **27**(1) 585–589.

Anderson, Catherine L, Ritu Agarwal. 2010. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Q.* **34**(3) 1–15.

Anderson, JC, DW Gerbing. 1988. Structural equation modeling in practice: A review and recommended two-step approach. *Psychol. Bull.* **103**(3) 411–423.

Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michel J.G. Eeten, Michael Levi, Tyler Moore, Stefan Savage. 2013. Measuring the cost of cybercrime. Rainer Böhme, ed., *Econ. Inf. Secur. Priv.*. Springer Berlin, Heidelberg, 265–300.

Asparouhov, Tihomir. 2005. Sampling weights in latent variable modeling. *Struct. Equ. Model.* **12**(3) 411–434.

Awad, Naveen Farag, M S Krishnan. 2006. The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Q.* **30**(1) 13–28.

Barnes, Susan B. 2006. A privacy paradox: Social networking in the United States. *First Monday* **11**(9).

Bauer, Raymond A. 1960. Consumer behavior as risk taking. *Dyn. Mark. a Chang. world* **398**.

Böhme, Rainer, Tyler Moore. 2012. How do consumers react to cybercrime? *7th APWG eCrime Res. Summit*. Las Croabas, 1–12.

Brynjolfsson, Erik. 1996. The contribution of information technology to consumer welfare. *Inf. Syst. Res.* **7**(3) 281–300.

Brynjolfsson, Erik, Michael D. Smith, Yu (Jeffrey) Hu. 2003. Consumer surplus in the digital economy: Estimating the value of increased product variety at online booksellers. *Manage. Sci.* **49**(11) 1580–1596.

Burns, Sarah, Lynne Roberts. 2013. Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prev. Community Saf.* **15**(1) 48–64.

Byrne, Barbara M., Richard J. Shavelson, Bengt Muthén. 1989. Testing for equivalence of factor covariance and mean structures: The issue of partial measurement invariance. *Psychol. Bull.* **105**(3) 456–466.

Cardona, M., T. Kretschmer, T. Strobel. 2013. ICT and productivity: conclusions from the empirical literature. *Inf. Econ. Policy* **25**(3) 109–125.

Chang, Man Kit, Waiman Cheung, Vincent S Lai. 2005. Literature derived reference models for the adoption of online shopping. *Inf. Manag.* **42**(4) 543–559.

Cheng, T C Edwin, David Y C Lam, Andy C L Yeung. 2006. Adoption of internet banking: An empirical study in Hong Kong. *Decis. Support Syst.* **42**(3) 1558–1572.

Chiricos, Ted, Kathy Padgett, Marc Gertz. 2000. Fear, TV news, and the reality of crime. *Criminology* **38**(3) 755–786.

Chiu, Chao-Min, Eric T. G. Wang, Yu-Hui Fang, Hsin-Yi Huang. 2012. Understanding customers' repeat purchase intentions in B2C e-commerce: the roles of utilitarian value, hedonic value and perceived risk. *Inf. Syst. J.* **24**(1) no–no.

Clough, Jonathan. 2010. *Princples of cybercrime*. Cambridge University Press.

Cunningham, Scott M. 1967. The major dimensions of perceived risk.

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

Dinev, Tamara, Jahyun Goo, Qing Hu, Kichan Nam. 2009. User behaviour towards protective information technologies: the role of national cultural differences. *Inf. Syst. J.* **19**(4) 391–412.

Dinev, Tamara, Qing Hu. 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *J. Assoc. Inf. Syst.* **8**(7) 386–408.

European Commission. 2010. A Digital Agenda for Europe. URL `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=com:2010:0245:fin:en:pdf`.

European Commission. 2012. Special Eurobarometer 390 Cyber security. URL `http://ec.europa.eu/public\_opinion/archives/`.

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

Featherman, Mauricio, Mark Fuller. 2003. Applying TAM to e-services adoption: the Moderating Role of Perceived Risk. *Proc. 36th Hawaii Int. Conf. Syst. Sci.* .

Featherman, Mauricio, Paul Pavlou. 2003. Predicting e-services adoption: a perceived risk facets perspective. *Int. J. Hum. Comput. Stud.* **59**(4) 451–474.

Featherman, Mauricio S, Anthony D Miyazaki, David E Sprott. 2010. Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility. *J. Serv. Mark.* **24**(3) 219–229.

Ferraro, Kenneth F, Randy LaGrange. 1987. The measurement of fear of crime. *Sociol. Inq.* 70–101.

Finney, Sara J, Christine DiStefano. 2006. Non-normal and categorical data in structural equation modeling. G Hancock, R Mueller, eds., *Struct. Equ. Model. A Second course*. Greenwich, 269–314.

Fishbein, Martin, Icek Ajzen. 1975. *Belief, attitude, intention and behavior: An introduction to theory and research*. Addison-Wesley Pub. Co.

Florêncio, Dinei, Cormac Herley. 2013. Sex, lies and cyber-crime surveys. Bruce Schneier, ed., *Economics of Information Security and Privacy III*. Springer, New York, 35–53.

Fornell, Claes, David F Larcker. 1981. Evaluating structural equation models with unobservable variables and measurement error. *J. Mark. Res.* **18**(1) 39–50.

Gainey, Randy, Mariel Alper, Allison T Chappell. 2010. Fear of crime revisited: examining the direct and indirect effects of disorder, risk perception, and social capital. *Am. J. Crim. Justice* **36**(2) 120–137.

Gefen, David, Elena Karahanna, Detmar W Straub. 2003. Trust and TAM in online shopping: an integrated model. *MIS Q.* **27**(1) 51–90.

Giovanis, Apostolos N, Spyridon Binioris, George Polychronopoulos. 2012. An extension of TAM model with IDT and security/privacy risk in the adoption of internet banking services in Greece. *EuroMed J. Bus.* **7**(1) 24–53.

Hair, Joseph F. 2010. *Multivariate data analysis*. 7th ed. Prentice Hall.

Hale, Chris. 1996. Fear of crime: A review of the literature. *Int. Rev. Vict.* **4**(2) 79–150.

Hanafizadeh, Payam, Byron W Keating, Hamid Reza Khedmatgozar. 2013. A systematic review of Internet banking adoption. *Telemat. Informatics* **31**(3) 492–510.

Heath, Linda, Kevin Gilbert. 1996. Mass media and fear of crime. *Am. Behav. Sci.* **39**(4) 379–386.

Henseler, Jörg, Christian M Ringle, Rudolf R Sinkovics. 2009. The use of partial least squares path modeling in international marketing. *New Challenges to Int. Mark. (Advances Int. Mark. Vol. 20)* **20**(2009) 277–319.

Hunton, Paul. 2009. The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model. *Comput. Law Secur. Rev.* **25**(6) 528–535.

Ifinedo, Princely. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Comput. Secur.* **31**(1) 83–95.

Im, Il, Seongtae Hong, Myung Soo Kang. 2011. An international comparison of technology adoption. *Inf. Manag.* **48**(1) 1–8.

ITU. 2013. Measuring the Information Society 2013. Tech. rep., International Telecommunication Union, Geneva. URL `http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013\_without\_Annex\_4.pdf`.

Jackson, J. 2011. Revisiting risk sensitivity in the fear of crime. *J. Res. Crime Delinq.* **48**(4) 513–537.

Jarvenpaa, Sirkka L, Noam Tractinsky, Lauri Saarinen. 1999. Consumer Trust in an Internet Store: A Cross-Cultural Validation. *J. Comput. Commun.* **5**(2) 0–0.

Jiao, Yongbing, Jian Yang, Shanling Xu. 2013. A study of the impact of social media characteristics on customer adoption intention of social media. *Proc. 2013 Int. Acad. Work. Soc. Sci.* 1095–1099.

Keane, Carl. 1995. Victimization and fear: Assessing the role of offender and offence **37** 431–455.

Kwon, Ohbyung, Yixing Wen. 2010. An empirical study of the factors affecting social network service use. *Comput. Human Behav.* **26**(2) 254–263.

Lee, Ming-Chi. 2009. Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electron. Commer. Res. Appl.* **8**(3) 130–141.

Lee, Younghwa, Kai R Larsen. 2009. Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *Eur. J. Inf. Syst.* **18**(2) 177–187.

Legris, Paul, John Ingham, Pierre Collerette. 2003. Why do people use information technology? A critical review of the technology acceptance model. *Inf. Manag.* **40**(3) 191–204.

Li, Yong-Hui, Jing-Wen Huang. 2009. Applying theory of perceived risk and technology acceptance model in the online shopping channel. *World Acad. Sci. Eng. Technol.* **53**(4) 816–822.

Lin, Hsiu-Fen. 2006. Understanding behavioral intention to participate in virtual communities. *CyberPsychology Behav.* **9**(5) 540–547.

Lin, Kuan-Yu, Hsi-Peng Lu. 2011. Why people use social networking sites: An empirical study integrating network externalities and motivation theory. *Comput. Human Behav.* **27**(3) 1152–1161.

Liska, Allen E, William Baccaglini. 1990. Feeling safe by comparison: crime in the newspaper. *Soc. Probs.* **37**(3) 360–374.

Liska, Allen E, Andrew Sanchirico, Marc D Reed. 1988. Fear of crime and constrained behavior specifying and estimating a reciprocal effects model. *Soc. Forces* **66**(3) 827–837.

Martins, Carolina, Tiago Oliveira, Aleš Popovič. 2014. Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *Int. J. Inf. Manage.* **34**(1) 1–13.

McGarrell, Edmund F, Andrew L Giacomazzi, Quint C Thurman. 1997. Neighborhood disorder, integration, and the fear of crime. *Justice Q.* **14**(3) 479–500.

McKnight, D. Harrison, Vivek Choudhury, Charles Kacmar. 2002. The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *J. Strateg. Inf. Syst.* **11**(3-4) 297–323.

Meade, Adam W, Emily C Johnson, Phillip W Braddy. 2008. Power and sensitivity of alternative fit indices in tests of measurement invariance. *J. Appl. Psychol.* **93**(3) 568–592.

Metzger, Miriam J. 2006. Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *J. Comput. Commun.* **9**(4) 0–0.

Millsap, Roger E., Jenn Yun-Tein. 2004. Assessing Factorial Invariance in Ordered-Categorical Measures. *Multivariate Behav. Res.* **39**(3) 479–515.

Montazemi, Ali Reza, Hamed Qahri Saremi. 2013. Factors Affecting Internet Banking Pre-usage Expectation Formation. *2013 46th Hawaii Int. Conf. Syst. Sci.* 4666–4675.

Moore, Gary C, Izak Benbasat. 1996. Integrating diffusion of innovations and theory of reasoned action models to predict utilization of information technology by end-users. Karlheinz Kautz, Jan Pries-Heje, eds., *Diffus. Adopt. Inf. Technol.*. Springer, 132–146.

Moore, Tyler, Richard Clayton, Ross Anderson. 2009. The economics of online crime. *J. Econ. Perspect.* **23**(3) 3–20.

Muthen, Bengt, Stephen H C du Toit, Damir Spisic. 1997. Robust inference using weighted least squares and quadratic estimating equations in latent variable modeling with categorical and continuous outcomes. *Psychometrika* **75**.

Pavlou, Paul A. 2003. Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *Int. J. Electron. Commer.* **7**(3) 69–103.

Pinho, José Carlos Martins Rodrigues, Ana Maria Soares. 2011. Examining the technology acceptance model in the adoption of social networks. *J. Res. Interact. Mark.* **5**(2/3) 116–129.

Rader, Nicole E, David C May, Sarah Goodrum. 2007. An empirical assessment of the "Threat of Victimization:" Considering fear of crime, perceived risk, avoidance, and defensive behaviors. *Sociol. Spectr.* **27**(5) 475–505.

Riffai, M M M A, Kevin Grant, David Edgar. 2012. 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.* **32**(3) 239–250.

Ringle, Christian M, Marko Sarstedt, Detmar W Straub. 2012. A critical look at the use of PLS-SEM in MIS Quarterly. *MISQ* **36**(1) iii–xiv.

Rogers, Ronald W. 1975. A protection motivation theory of fear appeals and attitude change. *J. Psychol.* **91**(1) 93–114.

Saban, Kenneth A, Elaine McGivern, Jan N Saykiewicz. 2002. A critical look at the impact of cybercrime on consumer Internet behavior. *J. Mark. Theory Pract.* **10**(2) 29–37.

Shin, Dong-Hee. 2010. The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interact. Comput.* **22**(5) 428–438.

Shin, Dong-Hee, Won-Yong Kim, Won-Young Kim. 2008. Applying the Technology Acceptance Model and flow theory to Cyworld user behavior: implication of the Web2.0 user acceptance. *CyberPsychology Behav.* **11**(3) 378–82.

Skogan, Wesley G. 1987. The impact of victimization on fear. *Crime Delinq.* **33**(1) 135–154.

Smith, Alan D. 2004. Cybercriminal impacts on online business and consumer confidence. *Online Inf. Rev.* **28**(3) 224–234.

Stafford, Mai, Tarani Chandola, Michael Marmot. 2007. Association between fear of crime and mental health and physical functioning. *Am. J. Public Health* **97**(11) 2076–81.

Stapleton, Laura. 2006. An assessment of practical solutions for structural equation modeling with complex sample data. *Struct. Equ. Model.* **13**(1) 28–58.

Suh, Bomil, Ingoo Han. 2003. Effect of trust on customer acceptance of Internet banking. *Electron. Commer. Res. Appl.* **1**(3) 247–263.

Tan, Soo Jiuan. 1999. Strategies for reducing consumers' risk aversion in Internet shopping. *J. Consum. Mark.* **16**(2) 163–180.

Tyler, Tom R. 1984. Assessing the risk of crime victimization: The integration of personal victimization experience and socially transmitted information. *J. Soc. Issues* **40**(1) 27–38.

Urbach, Nils, Frederik Ahlemann. 2010. Structural equation modeling in information systems research using partial least squares. *J. Inf. Technol. Theory* **11**(2) 5–40.

Venkatesh, Viswanath, Fred D Davis. 2000. A theoretical extension of the technology acceptance model: four longitudinal field studies. *Manage. Sci.* **46**(2) 186–204.

Venkatesh, Viswanath, Michael G Morris, Gordon B Davis, Fred D Davis. 2003. User acceptance of information technology: toward a unified view. *MISQ* **27**(3) 425–478.

Visser, Mark, Marijn Scholte, Peer Scheepers. 2013. Fear of crime and feelings of unsafety in european countries: Macro and micro explanations in cross-national perspective. *Sociol. Q.* **54**(2) 278–301.

Wahlberg, Anders A F, Lennart Sjoberg. 2000. Risk perception and the media. *J. Risk Res.* **3**(1) 31–50.

Wang, Yi-Shun, Yu-Min Wang, Hsin-Hui Lin, Tzung-I Tang. 2003. Determinants of user acceptance of Internet banking: an empirical study. *Int. J. Serv. Ind. Manag.* **14**(5) 501–519.

Wittebrood, Karin, Marianne Junger. 2002. Trends in violent crime: A comparison between police statistics and victimization surveys. *Soc. Indic. Res.* **59**(2) 153–173.

Yao, Mike Z, Daniel G Linz. 2008. Predicting self-protections of online privacy. *CyberPsychology Behav.* **11**(5) 615–617.

Yousafzai, Shumaila Y, Gordon R Foxall, John G Pallister. 2007. Technology acceptance: a meta-analysis of the TAM: Part 1. *J. Model. Manag.* **2**(3) 251–280.

Yu, C, Bengt Muthén. 2002. Evaluation of model fit indices for latent variable models with categorical and continuous outcomes. *Paper Presented at the Annual Meeting of the American Educational Research Association*. New Orleans, LA.

Zhou, Lina, Liwei Dai, Dongsong Zhang. 2007. Online shopping acceptance model – a critical survey of consumer factors in online. *J. Electron. Commer. Res.* **8**(1) 41–62.