This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2410795, IEEE Transactions on Dependable and Secure Computing

Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance

Markus Riek, Rainer Böhme, Tyler Moore

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 parsimonious model that builds on 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 cybercrime victimization and media reports. The effects are mediated by the 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 negative impact of perceived risk of cybercrime on the use of all three online service categories 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.

Index Terms—Economics of Cybercrime, Online Service Avoidance, Consumer Behavior, Perceived Risk, Technology Acceptance Model, Structural Equation Modeling.

1 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.

Our work is structured as follows. Section 2 provides a theoretical background on technology acceptance, criminology, and cybercrime. Section 3 inte-

- *Markus Riek and Rainer Böhme, Security and Privacy Lab, Institute of Computer Science, University of Innsbruck, Austria. E-mail: Markus.Riek@uibk.ac.at, Rainer.Boehme@uibk.ac.at.*
- *Tyler Moore, Computer Science and Engineering Department, Bobby Lyle School of Engineering, Southern Methodist University, Dallas, TX. E-mail: Tylerm@smu.edu.*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2410795, IEEE Transactions on Dependable and Secure Computing

grates the literature 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

We synthesize work from different fields, to explain how cybercrime reduces online participation. Building on technology acceptance models we explain what factors influence the intention to use online services (2.1). Then, we review the criminology literature to investigate antecedents of perceived crime risk and draw analogies to cybercrime (2.2). Finally, we review existing work on the social effects of cybercrime (2.3).

2.1 Technology Acceptance in IS Research

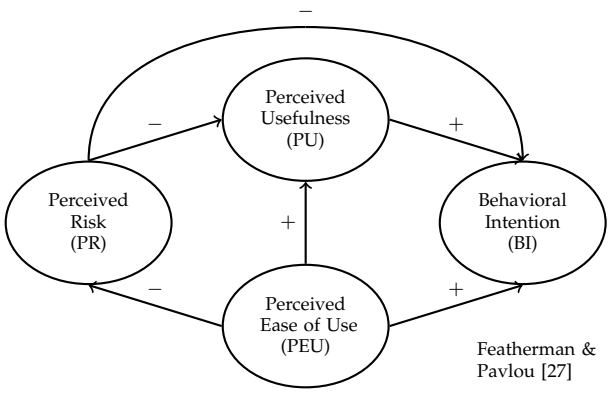
Models, explaining the acceptance of new technologies, have been of interest in IS research since the first commercial use of computers. Several models have been introduced to measure the influence of different factors on the individual intention to use a new technology [12]. We focus on studies applying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

2.1.1 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 BI to use a 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].

Fig. 1. Perceived Risk-extended TAM



2.1.2 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.

2.1.3 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].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2410795, IEEE Transactions on Dependable and Secure Computing

Two forms of uncertainty are naturally present: behavioral and environmental uncertainty [29]. Behavioral uncertainty 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].

2.1.4 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 construct[1]. Fig. 1 illustrates that PR reduces the intention to use an e-service (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.

2.1.5 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].

2.1.6 Technology Acceptance of Online Services.

Table 1 summarizes this section by showing that technology acceptance models, especially TAM and UTAUT, are commonly applied in the online context. 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.

2.2 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 react to cybercrime. However, future research should clarify the risk–fear relationship in the online context.

2.2.1 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

1. originally introduced by Cunningham in 1967 as a general perceived risk construct [34]

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2410795, IEEE Transactions on Dependable and Secure Computing

TABLE 1
Literature on the 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	[27]
	2003	TAM-PR	ANOVA	PR ↘ PU, BI; PR moderates effects	[33]
Online Banking	2003	eTAM	SEM	Credibility, PU, PEU ↗ BI	[42]
	2006	eTAM	SEM	PU, PEU, Tr (Web Security) ↗ BI	[47]
	2009	TAM-TPB-PR	SEM	PR ↘ ATU (ultimately BI)	[1]
	2011	UTAUT-PR	SEM	PR ↘ BI	[46]
	2012	eUTAUT	Correlation	PR moderates: PU, PEU ↗ BI	[43]
	2012	TAM-IDT	PLS	PEU, Tr(Web Security) ↗ BI	[48]
	2013	TAM-Tr	Meta-SEM	Tr ↗ BI	[40]
	2014	UTAUT-PR	SEM	PU, PEU, Compatibility ↗ BI; PR ↘ BI	[35]
Online Shopping	2003	TAM-PR	PLS	Tr ↗ PU, BI	[29]
	2003	TAM-Tr	SEM	Tr, PU ↗ BI	[32]
	2010	TAM-PR	SEM	PR (Privacy), Credibility, PEU ↗ BI	[49]
	2011	TAM-Tr	PLS	PR ↘ Trust; Trust ↗ BI	[44]
	2012	PT-PR	PLS	PR moderates effects	[31]
Online Social Networking	2010	TRA-TAM	SEM	PR (Security & Privacy) ↘ Tr, BI	[45]
	2010	eTAM	SEM	PR not considered	[50]
	2013	TAM-PR-Tr	SEM	No effect for: PR on PU, BI	[51]

Model: Extended TAM (eTAM), Trust (Tr), Perceived Risk (PR), Prospect Theory (PT)
Findings: Positive Effect (↗), Negative Effect (↘)

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].

2.2.2 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].

2.2.3 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].

2.3 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.

2.3.1 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 households finding that cybercrime experience increases the fear of cybercrime [70].

More recently, Böhme & Moore conducted a secondary analysis of the 2012 Eurobarometer Cyber

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2410795, IEEE Transactions on Dependable and Secure Computing

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-commerce and the sole consideration of privacy risk, neglecting crime, limit their study. To overcome these limitations, we next propose our research model.

3 Research Model and Hypotheses

Building on [71], we set out to systematically explain the effects of cybercrime by finding factors that make users avoid online services. We synthesize research on technology acceptance and criminology in the context of cybercrime and propose the research model illustrated in Fig. 2. This section explains our research model and the hypotheses to be tested.

The right part of the model represents the basic elements of the risk-extended TAM [27] or UTAUT model [35] – PR decreasing BI. The constructs are incorporated as *Perceived Cybercrime Risk* (PCR) and *Avoidance Intention* (AI). As we 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.

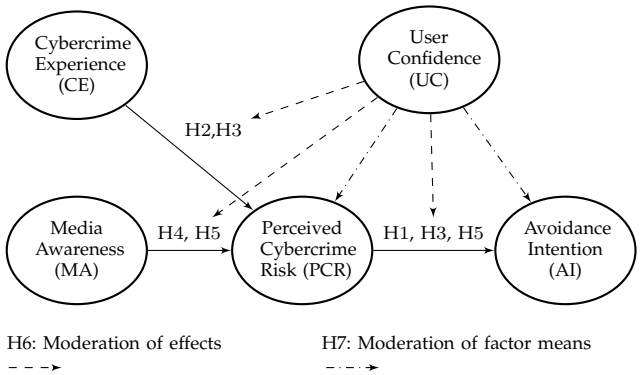
H1: Perceived Cybercrime Risk increases Avoidance Intention from online services.

Technology acceptance studies show the negative effects of perceived risk on the adoption of online services in several different scenarios. Featherman & Pavlou show that financial, performance and privacy risks are the most influential risk factors [27]. As consumer-oriented cybercrime is 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 is controversial among criminologists. However, as perceived risk is assumed to be a function of the probability to fall victim and the severity of the criminal act [52], we suspect that cybercrime experience leads to a higher level of perceived cybercrime 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 users and service providers.

Fig. 2. Research Model in Path Model Notation



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

Saban et al. show that cybercrime experience decreases the likelihood of repeated online shopping [68]. The negative effects are confirmed for online banking and general online participation [71]. 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 online services.

H4: Media Awareness increases Perceived Cybercrime Risk.

Media reports are found to increase the perceived risk of offline crime, especially if they 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. 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 [72], which further contributes to the perception of risk.

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

Böhme & Moore remark that Internet users who have heard about cybercrime in the news or from colleagues are less likely to bank online than those who have not heard such reports [71]. 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 online services.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2410795, IEEE Transactions on Dependable and Secure Computing

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

Various authors (e.g., [33]) show that understanding how different consumer segments perceive and evaluate online services and risks is essential to explain adoption. 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.

H7: User Confidence moderates the effects, in that the means of latent variables 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. 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 in a secondary analysis of the Special Eurobarometer. 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 model (4.3).

4.1 Statistical Method

Structural equation modeling (SEM) is a multivariate analysis technique which performs factor analyses and simultaneously estimates regression coefficients. Linear regression only allows for explaining variables to directly influence the outcome. SEMs by contrast can handle multi-stage effects between (groups of) predictors, while explicitly accounting for measurement error and multi-collinearity [73]. They are frequently used in the social science to explain human decision making based on structured surveys and they have popularity in IS research to measure technology acceptance (see Table 1 in Section2). The technique is limited by high requirements on the data-quality and the causal interpretation depends on additional assumptions. The remainder of this section shows that the Cyber Security Report (CSR) data set meets the requirements. Furthermore, we believe that the causal directions of our hypotheses are justified, as they are based on former studies and further enforced by the question wording in the CSR[2].

To analyze the CSR, we use a single-level, cross-sectional structural equation model. SEMs 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 better suited to confirming theories and PLS to developing theories and making predictions [74]. We use the covariance-based SEM technique to confirm our hypotheses, as we empirically test our theoretically derived model using the fit indices provided by SEM [74]. Non-normal data, another common reason for using PLS [75], is accounted for by the robust weighted least square (WLSMV) estimation method developed for non-normal, categorical indicators [76].

We use the statistical software Mplus[3] for the parameter estimation, as it provides all features required by the analysis. It supports the WLSMV estimation method [77], which is considered to be the best available approach for categorical, non-normal distributed indicators, given a large complex sample [76].

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. Using stratification by country as well as random route and closest birthday rules within countries, 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 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 Internet users (normalized weights).

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

2. CSR: Question 7 "Has concern about cybercrime made you change the way you use the Internet?" [11, p.28]

3. Version 7.11, available at: http://www.statmodel.com

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2410795, IEEE Transactions on Dependable and Secure Computing

TABLE 2
Questions for Latent Variable Measurement

ID	Latent Variable (Scale Level)/ 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 %

*EU Internet users above the age of 15.

question (not at all, not very, fairly, very). Outliers do not need to be considered and the 4-point agreement scales are interpreted as being equidistant. This section introduces the relevant survey items 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. Even spam e-mails have never been experienced by 61.75%. This surprisingly high number is likely to be biased by the question wording "How often have you received emails fraudulently asking for money or personal details?" [11, p.46], which excludes a large amount of spam e-mails.

Media Awareness represents the extent to which people are exposed to news reports about cybercrime from different media sources. Respondents are 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 further 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%). [70] 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 direct harm as for example identity theft.

(Behavioral) Avoidance Intention is measured by three binary questions. Respondents are asked whether 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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2410795, IEEE Transactions on Dependable and Secure Computing

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.

5 Results

We use the two-step approach introduced by [78]. 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 an additional, 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 [79]. 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 Cronbach's Alpha [73]. 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 [73].

All indicators meet the first criterion – significant factor loadings greater than 0.5 (cf. Table 3). Table 6 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 modification indices (MI) underpin the bad influence of *Media Awareness* indicators on the overall model. 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 (since hearing about cybercrime from multiple sources may not increase awareness), we excluded this construct from the structural analysis. Nevertheless, we suspect that media reports raise awareness and influences the behavior of Internet users. We encourage further research on this aspect, using more appropriate instruments.

The MIs further imply that a positive measurement error correlation should be added between QE11.4 and QE11.5[4] (MI: 35, E.P.C.Std.: 0.452). Since both questions measure a 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 7 and Table 8 show that all constructs in the reduced model – without *Media Awareness* – fulfill the reliability and validity requirements. Note that AVE for *Cybercrime Experience* is above the required threshold in the reduced model.

Discriminant validity ensures that different constructs do not measure the same phenomenon. To confirm discriminant validity, the square root of AVE (noted on the diagonal of Table 6) should be greater than the between construct correlations [74]. Table 6 shows that this is satisfied 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

The structural parameters are estimated based on the sufficient measurement model. The overall goodness-of-fit is evaluated using approximate fit 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 [76]. 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; [80]). Table 4 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 errors (in brackets), and the level of significance are documented in Table 4.

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 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. The effect size is likely to be positively biased by context effects, because the *Perceived Cybercrime Risk* battery (QE11) directly succeeds the *Cybercrime Experience* battery (QE10), and same question bias, because both batteries contain almost exclusively the same answer categories. The bias might explain the comparably high

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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2410795, IEEE Transactions on Dependable and Secure Computing

TABLE 3
Measurement Model: 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^{***}	0.020	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^{***}	0.040	17.622	0.500
	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^{***}	0.010	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

N = 17,773 $\chi^2(df) = 448.73$ (123) RMSEA = .012 (.011 – .013) TLI = .961 CFI = .968
Significance level: $^{***} = p < 0.001$; Mean based on respective answer scale

path coefficient between *Cybercrime Experience* and *Perceived Cybercrime Risk*. We believe that the general effect is justified, but its size must be confirmed by future studies.

Indirect effects of *Cybercrime Experience* on *Avoidance Intention* are found for all categories: online banking ($\beta = 0.024$, $p < 0.001$), online shopping ($\beta = 0.046$, $p < 0.001$), and online social networking ($\beta = 0.02$, $p < 0.05$), supporting H3. Full mediation by *Perceived Cybercrime Risk* is only found for the avoidance of online shopping, as the direct effect is not significant ($\beta = 0.02$, $p = 0.653$). The effect size of the total effect is small and marginally significant ($p < 0.15$). 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*.

5.3 Moderation Analysis

The moderation effects of user confidence are tested by conducting a multiple-group analysis. We split the sample into very confident ($N = 4\,972$) and not at all confident (unconfident) Internet users ($N = 2\,196$). To reduce noise and heterogeneity, we exclude "fairly" and "not very" confident users from the analysis. The descriptive statistics in Table 2 show that confident users report 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 one fifth (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.

We use the general-to-specific approach proposed by [81] to test measurement invariance. [82] 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.

All fit indices in Table 9 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. [83] 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 9 shows that Mod C is invariant to Mod B for all online services, because $\Delta CFI <= 0.002$. 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 thresholds for the respective question on online service *Avoidance Intention* (Mod D). Table 9 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 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 5 shows that confident users

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2410795, IEEE Transactions on Dependable and Secure Computing

TABLE 4
Structural Models: Estimated Path Coefficients and Fit Indices

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)	0.046^{***} (0.0060)	0.020^{*} (0.0080)
	Total	0.166^{***} (0.0310)	0.066 (0.0430)	0.141^{***} (0.0130)
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

Significance levels: $^{***} = p < 0.001$; $^{*} = p < 0.05$; $' = p < 0.15$; Standard errors in brackets
Perc. Cybercrime Risk (PCR), Cybercrime Experience (CE), Avoidance Intention (AI)

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. This suggests a distinction between security and privacy risks to be investigated in future work.

6 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).

6.1 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 multi-item measures to measure the perceived risk construct even though it is originally identified as multi-dimensional [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 (Section 4.1) ensure the statistical power and reliability of our results.

6.2 Theoretical Implications

We provide empirical evidence that the perceived risk-extended TAM can be applied to explain online service avoidance from a cybercrime perspective. By adding a perceived cybercrime risk construct to TAM, our model reinforces earlier suggestions (e.g., by [27]) 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. Pavlou proposes that online shopping includes behavioral uncertainty, caused by dubious merchants, in addition to the environmental uncertainty of the Internet [29]. The high level of uncertainty and the low switching

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2410795, IEEE Transactions on Dependable and Secure Computing

TABLE 5
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)
Perceived 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 levels: $^{***} = p < 0.001$; $^{**} = p < 0.01$; $^{*} = p < 0.05$; Standard errors in brackets

costs reduce customer loyalty in online shopping, making it easier to avoid services. By contrast, switching costs in online banking are higher and customers usually interact with a single bank. Accordingly, the perceived risk is largely based on environmental uncertainty, once trust in the online banking provider is established. The importance of trust in online banking adoption (even exceeding traditional TAM factors) is also found by other studies (e.g., [40]). This explains the smaller effect of perceived risk of cybercrime on the avoidance of online banking.

We find the smallest effect (significant at $p < 0.05$) of perceived cybercrime risk on the avoidance of online social networking (OSN). As OSN yields a rather low security risk, rarely involving financial transactions so far, 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 a kind of privacy paradox, which states that consumers express privacy concerns, but still publish private data to build up online profiles [84]. 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., [21]).

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 categories of online services in our study. The full mediation found for online shopping further supports the importance of perceived risk of cybercrime regarding online shopping avoidance.

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 their chance of becoming victimized but also their ability to identify cybercriminal attacks.

Unconfident users, by contrast, perceive more cybercrime risk and demonstrate 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. Our data is too noisy to confirm this finding empirically and we recommend further research in this direction.

6.3 Practical Implications

Our practical implications are mainly directed towards policy makers, but also provide valuable information for online service providers. We show that the reduction of perceived risk of cybercrime facilitates increased online service use. Furthermore, confident Internet users generally perceive less risk and are more likely to use online services. Our findings lead to two sets of actions: reducing perceived risk of cybercrime and increasing Internet user's confidence.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2410795, IEEE Transactions on Dependable and Secure Computing

An obvious action to reduce perceived risk is to reduce victimization by continuously improving defense measures and intensifying criminal prosecution by law enforcement. All actions need to be credibly communicated to assure that the risk of online transactions is correctly perceived by large parts of the population. Policy makers can create incentives such as trustmarks, standards, or security certificates, to foster security investments and encourage clear communication. Service providers can offer financial compensation to victims or consumer satisfaction guarantees to reduce the perceived risk.

To increase Internet users' confidence in dealing with cybercrime risk, their digital literary needs to be improved. Public awareness about cybercriminal threats should be ensured, but more importantly, Internet users need to be educated to make informed decisions to deal with these threats. Therefore, policy makers should establish trusted sources of authorative advice regarding cybercrime and protective behavior, understandable for the public, for example in the form of official websites. Positive examples should be used on these websites to encourage secure behavior, as scary messages may increase perceived risk and lead to avoidance rather than secure use. Service providers should implement clear and easy-to-use services to support the confidence building process.

6.4 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 countermeasures. 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.

7 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.

Acknowledgments

The paper draws on research performed as part of the E-CRIME project funded by the European Union's 7th Framework Programme under grant agreement number 607775. The authors want to thank the Eurobarometer team at the European Commission for making the data available, the German Academic Exchange Service (DAAD) for funding a research visit at SMU, and the reviewers and participants of WEIS 2014 for very useful comments on an earlier version of the paper.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2410795, IEEE Transactions on Dependable and Secure Computing

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. Böhme, 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. Böhme, 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: Toward a 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: An empirical 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. Pinho and A. 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," in *Proc. 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. Popovič, "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.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2410795, IEEE Transactions on Dependable and Secure Computing

[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 influence of perceived ease of use and corporate credibility," *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. Alarcón-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. Wittebrood and M. Junger, "Trends in violent crime: A comparison 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, "Neighborhood 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 newspaper," *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 a national survey," Disseration, Mississippi State University, 2006.
[71] R. Böhme and T. Moore, "How do consumers react to cybercrime?" in *7th APWG eCrime Res. Summit*, Las Croabas, 2012, pp. 1–12.
[72] D. Florêncio 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, *Multivariate data 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. Muthén, "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. Muthén, "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. Consumer Affairs*, 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.

Markus Riek is researcher and PhD candidate in the Security and Privacy Lab of the Institute of Computer Science at the University of Innsbruck. He holds BSc ('11) and MSc ('13) degrees in Information Systems from the University of Münster in Germany.

His research interests focus on economics of information security and in particular economics of cybercrime. He applies behavioral models to explain consumer behavior.

Rainer Böhme is Professor of Security and Privacy at the University of Innsbruck, Institute of Computer Science. Prior to that he was Assistant Professor of Information Systems and IT Security at the University of Münster in Germany. He received his PhD degree ('08) from TU Dresden, Germany, and served as Post-Doctoral Fellow at the International Computer Science Institute in Berkeley, California. His research interest span signal processing and security, digital forensics, privacy-enhancing technologies, as well as economic and behavioral aspects of security and privacy.

Tyler Moore is Assistant Professor of Computer Science and Engineering at Southern Methodist University. He received his PhD from the University of Cambridge. He is an Editor in Chief of the *Journal of Cybersecurity* published by Oxford University Press. At SMU, he serves as Director of the Economics and Social Sciences program at the Darwin Deason Institute for Cyber Security and a Fellow at the John Goodman Tower Center for Political Studies. His research focuses on security economics, cybercrime measurement, and cybersecurity policy.