Analyzing Persistent Impact of Cybercrime on the Societal Level: Evidence for Individual Security Behavior

Completed Research Paper

Markus Riek
University of Innsbruck
Innsbruck, Austria
markus.riek@uibk.ac.at

Svetlana Abramova
University of Innsbruck
Innsbruck, Austria
svetlana.abramova@uibk.ac.at

Rainer Böhme
University of Innsbruck
Innsbruck, Austria
rainer.boehme@uibk.ac.at

Abstract

Cybercrime has evolved into a serious global problem with considerable social and economic impact. Avoidance, one form of individual security behavior, can lead to long-lasting negative outcomes on the societal level, but is rarely studied. While avoidance effects are difficult to study for recent innovations, theoretical models and data exist for established online services. Building on a parsimonious research model, we study the persistence of aggregate avoidance effects towards the use of online services along with protection behavior using a longitudinal approach. We use structural equation modelling in a secondary analysis of three representative pan-European surveys, conducted in 2012-2014. We find that cybercrime experience increases perceived risk and ultimately leads to avoidance of online banking, online shopping, and unknown websites. It also has a direct impact on two forms of protection behavior, namely: changing security settings and using different passwords. Trend analyses show that these effects are persistent over time.

Keywords: Security behavior, avoidance, protection, economic impacts, cybercrime, structural equation modeling (SEM), survey research, trend analysis

Introduction

Arguably, the world has never been as dynamic, innovative, and uncertain as it is today. A major driver behind these ongoing processes of change is information and communication technology (ICT), which penetrates into virtually all aspects of human life. Becoming ubiquitous, it transforms the ways we work, communicate, learn, shop, and spend our free time. Novel participative online markets (Hawlitschek et al., 2016), like Airbnb and Uber, or decentralized payment networks (Abramova and Böhme, 2016), like Bitcoin and Ethereum, are only selected examples of recent innovations with potentially far-reaching social and economic impacts. Earlier innovations, including online shopping, online banking, and online social networking, are already widely adopted in the developed world (EB82.2, 2015).

Despite many benefits for individual users (Brynjolfsson, 1996; Brynjolfsson et al., 2003), ICT innovations can have unintended or unforeseen adverse consequences (Tarafdar et al., 2015). These include a loss of privacy (Acquisti et al., 2006) and negative cognitions, such as technology stress, addiction, or misuse (Maier et al., 2015; Tarafdar et al., 2007). In response to them, users eventually make efforts to avoid ICT,

partly or even all together (Recker, 2016). Profit-oriented cybercrime is another unintended consequence of ICT innovation, which has turned into a serious global problem. Despite uncertainty about its actual extent (Florencio and Herley, 2013; Jardine, 2015), studies show that affected and concerned individuals tend to avoid ICT as one form of security behavior (Lee and Kozar, 2005; Chen and Zahedi, 2016; Riek et al., 2016). On the societal level, these individual reactions can add up to unfavorable long-lasting economic and social outcomes. Anderson et al. (2013) conjecture that avoidance on the individual level accounts for a large part of the social costs of cybercrime.

In general, individual behavior is regulated by several dimensions of constraint, including markets, social norms, laws, and technology-mediated architectures (Lessig, 1998), which makes reliable examination of its nature, causes and effects an intricate endeavor. Time-dependent changes of perceptions and behavior in dynamic environments add further uncertainty. The issues are often neglected by researchers for justified reasons, including a lack of applicable theory or reliable data. While these reasons are valid for recent innovations, established ICT can be studied empirically at the aggregate level using accepted behavioral theories and longitudinal methods. Finding persistent behavior for established ICT at the societal level can explain present effects (Kehr and Kowatsch, 2015) and, more importantly, also inform future courses of action to reduce negative consequences of ICT innovations. Although inference from older to newer technology is subject to caveats, insights on fundamental long-lasting trends and causalities in individual behavior are generalizable as long as they do not depend on the specifics of a technology.

We make a first step towards finding persistent security behavior on the societal level. We study avoidance and protection behavior of EU Internet users in reaction to cybercrime exposure. We consider avoidance of online shopping, online banking, and online social networking, three established technologies widespread enough to allow for population-wide empirical studies. Furthermore, we believe that avoidance of online services is particularly interesting, as national adoption statistics seem to contradict with the avoidance hypothesis. To illustrate, Figure 1 shows marginal statistics of national adoption levels among Internet users in 27 EU member states for online shopping and online banking. While adoption levels differ across member states, increasing trends can be clearly observed for both services from 2012 to 2014.

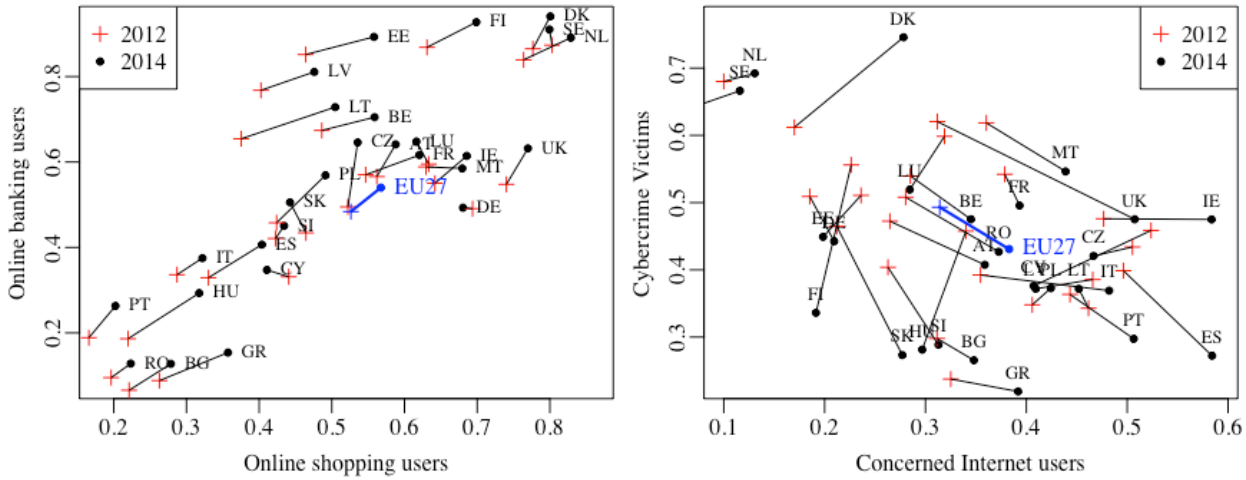

Figure 1. Comparison of EU member states in 2012 and 2014: users of online shopping and online banking (left), fraction of Internet users reporting concerns about and experience of cybercrime (right); Sources: EB77.2 (2012), EB82.2 (2015), authors' analysis

The right part of Figure 1 shows that about half of EU Internet users reported some experience of cybercrime in 2012. While the prevalence of cybercrime varies widely between countries, we see a downward trend on average. Public concern about cybercrime, on the other hand, has grown from 2012 to 2014. Comparing the country-level trends, two contradictions become apparent and challenge earlier hypotheses (Riek et al., 2016) regarding the impact of cybercrime on online service adoption. First, even though reported cybercrime experience decreased on average, cybercrime concern increased in 19 countries (and on average). Second, cybercrime concern and online service use increased simultaneously, despite the

proposed avoidance effect. Obviously, this simple interpretation of aggregated figures in two snapshots does not consider time lag effects and neglects that ongoing adoption may also increase the population of potentially concerned users. Still, the contradictions and the dynamic environment challenge the robustness of existing models and call for a longitudinal perspective in the study of security behavior.

We develop a longitudinal approach to validate the persistence of security behavior on the societal level, in the form of online service avoidance and protective actions. We extend the model of online service avoidance proposed by Riek et al. (2016) to carry out secondary analyses of three subsequent waves of the Special Eurobarometer (EB) report on Cyber Security (EB77.2, 2012; EB79.4, 2013; EB82.2, 2015). This provides us with the rare opportunity to study trends in individual security behavior (and persistence thereof) on the societal level in 27 EU member states. We chose to mainly build on the work by Riek et al. (2016) because it is the only peer-review model amenable to an analysis of the EB data. However, we extend the original model by adding protection behavior and avoidance of unknown websites and using newly available questions in the 2014 survey to improve the original measurement model.

Our approach uses covariance-based structural equation modelling (SEM) to evaluate the robustness of the model over time and a trend analysis to test for the stability of structural links. Our findings confirm that cybercrime experience increases perceived cybercrime risk and that perceived risk leads to the avoidance of online shopping, online banking, and unknown websites on the societal level. Protection behavior is triggered by cybercrime experience, but not by perceived risk. The effects are highly significant for all three EB waves and remain stable over time. Our improved measurement model provides additional confidence for the persistence of the effects. In summary, our results add to the emerging research on negative outcomes of security behavior (Chen and Zahedi, 2016) with four main contributions:

1) We extend the research model with individual protection behavior, measured in three forms: use of different passwords, change of security settings, and installation of anti-virus software.
2) We add avoidance of unknown websites to the model and show that this form of avoidance can partly explain the contradicting trends (illustrated in Figure 1).
3) We verify the robustness of the extended research model with regard to its measurement model and overall goodness of fit. We conduct a trend analysis for the structural links, confirming that security behavior is persistent on the societal level, despite the contradicting trends in the marginal statistics.
4) We improve the measurement model using new questions in the 2014 survey, providing additional support for the first three contributions.

Taking a step back, this study tests the persistence of the models on the societal level over time to develop principled theory of security behavior. This improves our understanding of the current dynamics, including a large-scale adoption of security measures and avoidance of widely used online services. Moreover, it can provide insights on barriers to the adoption of more recent innovative technologies.

The paper is structured as follows. The next section reviews IS literature with regard to "Avoidance as Security Behavior". Then, we introduce our "Research Methodology", which comprises the research model and our longitudinal approach. The "Data" section outlines the Special Eurobarometer reports including descriptive statistics. In the Section "Results", we document the SEM and trend analyses. We discuss the validation of behavioral effects along with our model improvement and limitations, before we conclude.

Avoidance as Security Behavior

In contrast to positive behavioral outcomes, such as adoption and use of technology, negative outcomes, i.e. avoidance or discontinuance, are rarely studied in IS research (Recker, 2016). Accordingly, enabling factors dominate over inhibiting factors in adoption studies. The latter are often simply treated as antipoles of enablers, although they can be fundamentally different (Cenfetelli and Schwarz, 2011). Security research, too, largely neglects avoidance as a viable form of security behavior (Chen and Zahedi, 2016). In this section, we demonstrate that most studies are concerned with 1) adoption of security software, 2) impact of perceived risk on the adoption of other services, or 3) factors influencing engagement in protective actions. We summarize these distinct research streams and identify two key studies on avoidance behavior.

Anderson and Agarwal (2010) review behavioral security literature, showing that the Technology Acceptance Model (TAM; Davis, 1989) and its foundation, the Theory of Planned Behavior (TPB; Ajzen, 1991), are frequently used to explain the adoption of security software. Dinev and Hu (2007), for example,

use TPB to analyze factors influencing the intention to use malware prevention software and find that threat awareness has the biggest impact. Lee and Kozar (2005) conduct a similar analysis for anti-spyware technology. Burns and Roberts (2013) study protective behavior as a result of exposure to cybercrime.

A second stream of research analyses the impact of perceived risk on the adoption of other technologies. Featherman and Pavlou (2003) propose the Perceived Risk (PR) extended TAM. They argue that PR needs to be added to TAM as a third antecedent that inhibits the intention to adopt ICT. Martins et al. (2014) combine PR with the Unified Theory of Acceptance and Use of Technology (UTAUT) in the context of online banking. Through a comprehensive literature review, Riek et al. (2016) demonstrate that PR is an inhibitor of adoption and continuous use of different online services. They find that it is most frequently studied in the context of online banking and least frequently for online social networking.

A third stream of research uses Protection Motivation Theory (PMT; Rogers, 1975) to explain individuals' intention to engage in protective actions based on threat and coping appraisals (Anderson and Agarwal, 2010). The threat appraisal is formed by the perceived severity of and vulnerability to attacks, while the coping appraisal is shaped by response efficacy and self-efficacy (Rogers, 1975). PMT is mostly used in an organizational context. Lee and Larsen (2009) find that it can explain security behavior of business executives, other authors rely on PMT to study employees' intention to comply with IS security policies (Pahnilaa, 2007; Ifinedo, 2012). However, PMT is also used to explain individual behavior of home Internet users (Johnston and Warkentin, 2010; Srisawang et al., 2015; Tsai et al., 2016). Noteworthy, all three research streams investigate active responses to cyber-criminal threats and neglect avoidance behavior.

Liang and Xue (2009) propose the Technology Threat Avoidance Theory (TTAT), which explains threat avoidance as a form of individual coping (Lazarus, 1966) with malicious IT. They suggest that avoidance behavior is fundamentally different from adoption, because "approach behavior always moves the current state toward the desired end state, while the avoidance behavior has no affirmative direction as long as it separates the current state from the undesired end state" (Liang and Xue, 2009, p. 76). They further state that individuals can perform two types of coping to deal with a threat: problem-focused, meaning the implementation of safeguarding measures, and emotion-focused, just accepting the threat. Surprisingly, avoidance of risky situations, e.g., online banking, is not suggested as a coping alternative. Empirical applications of TTAT only test the intention to use safeguards in different contexts (Liang and Xue, 2010; Arachchilage and Love, 2014), making them not significantly different from PMT studies.

We only find two studies (contrasted in Table 8 in Appendix A), which explicitly incorporate avoidance as security behavior. Chen and Zahedi (2016) integrate TTAT into a contextualized PMT model to study individuals' security perception and behavior. They specify three forms of coping: protective action, seeking help, and avoidance. They test their model in a multi-group SEM analysis based on an online survey of 718 individual Internet users in the US and China. Inter alia, avoidance and seeking help are found to be more prevalent reactions to security concerns in China, whereas US citizens rather engage in protective action. Riek et al. (2016) build on the PR-extended TAM model to study the impact of perceived cybercrime risk on the avoidance of online shopping, online banking, and online social networking. Based on a synthesis of IS and criminology literature, they further suggest that *Cybercrime Experience* and *Media Awareness* are antecedents of *Perceived Cybercrime Risk*. They apply a SEM analysis based on a representative sample of EU Internet users with almost 18,000 responses, showing that cybercrime experience and perceived risk lead to the avoidance of all three online services, with the smallest impact on online social networking.

Despite extensive searches in the BusinessPremier database, the AIS and ACM libraries, and IEEEXplore, we were not able to find other peer-reviewed studies which analyze avoidance in the context of security behavior and apply a longitudinal approach.

Research Methodology

Research Model

Our research model integrates core aspects of the major two models on avoidance. We draw upon the parsimonious research model proposed by Riek et al. (2016), which formalizes the impact of *Cybercrime Experience* on *Perceived Cybercrime Risk* and ultimately on the *Avoidance Intention* of online services. Riek et al. (2016) simply define *Avoidance Intention* as the counterpart to adoption and invert the original hypotheses in the PR-extended TAM accordingly. Chen and Zahedi (2016) define avoidance similarly, as:

"[a]voiding the use of the Internet in various degrees, especially avoiding sensitive activities such as online banking, in order to avoid online security threats" (Chen and Zahedi, 2016, p. A2). Our literature review demonstrates that protection behavior is the most commonly studied response to perceived (cybercrime) risk. Therefore, we extend the model of Riek et al. (2016) with reported *Protection Behavior*, which comprises "protective countermeasures to reduce or eliminate the risk of Internet security attacks" (Chen and Zahedi, 2016, p. A2). Our final research model, as depicted in Figure 2, can be tested using the microdata collected in the three EB waves.

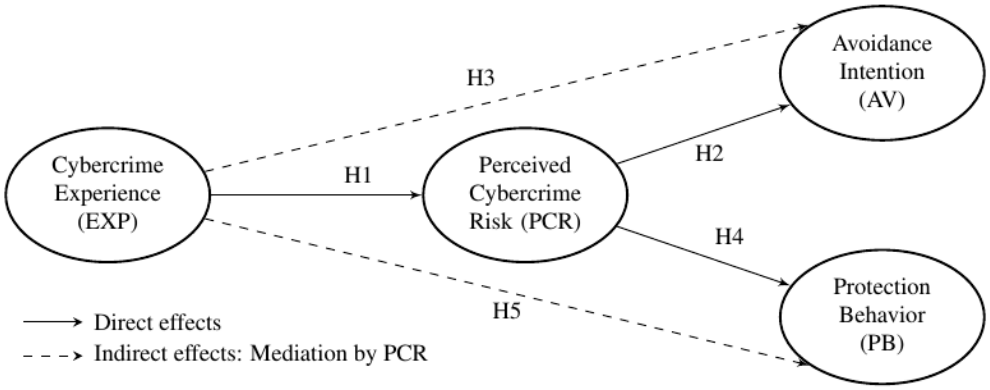

Figure 2. Research model and hypotheses in path model notation

We make further adjustments to the research model of Riek et al. (2016) to enable the longitudinal analysis. We drop the *Media Awareness* and *User Confidence* constructs, because the associated questions have been discontinued in the second and third waves of the EB surveys. Riek et al. (2016) also had to exclude *Media Awareness* from the structural analysis and studied the moderation effects of *User Confidence* in an additional multi-group analysis. To focus on the core aspects, we test the following five hypotheses:

H1: *Cybercrime Experience* increases *Perceived Cybercrime Risk*.

H2: *Perceived Cybercrime Risk* increases *Avoidance Intention* to use online services.

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

H4: *Perceived Cybercrime Risk* increases *Protection Behavior*.

H5: *Cybercrime Experience* increases *Protection Behavior*. The effect is fully mediated by *Perceived Cybercrime Risk*.

Following the original model, we test hypotheses **H1 - H3** for three online services: online shopping, online banking, and online social networking. Furthermore, we add *avoidance of unknown websites* as a fourth form of *Avoidance Intention*. We justify this extension with Liang and Xue's (2009) statement that avoidance behavior has no affirmative direction, as long as it separates the current state from an undesired state (becoming a victim). In our context, individuals may keep using familiar and trusted online services, but avoid unknown websites, which offer the same service. The facilitating role of familiarity and trust has been studied repeatedly in the context of online shopping. Gefen (2000) already demonstrates their importance in online purchase decisions. Lim (2003) classifies sources of perceived risk in B2C e-commerce, finding that uncertainty regarding an unknown vendor is equally important as the general risk of online shopping. In a similar vein, brand image (online and offline) is found to be an essential source, reducing perceived risk and facilitating the adoption (Chen and He, 2003; Kwon and Lennon, 2009).

We test the hypotheses on *Protection Behavior* (**H4** and **H5**) in three additional models, each concerning one protective action: "changing security settings", "using different passwords", and "installing anti-virus software". To allow for a longitudinal perspective, all hypotheses are tested in each EB wave.

Longitudinal Approach

Longitudinal studies are characterized by repeated observations of the same units on the same outcomes at different points in time (Singer and Willett, 2003). In the best case, they are based on panel data, where an initial sample, the panel, is pre-selected and data is collected at several points in time (Steel, 2008). While

panel studies enable in-depth analysis of inter- and intra-individual changes over time, they require substantial resources, which are rarely affordable for sampling large populations.

Trend studies are a viable alternative for research questions which concern aggregated effects on the societal level. Even though they draw on independent samples for each measurement, they can be used to uncover trends, provided that samples represent the same population and are collected using the same methodology (Steel and McLaren, 2008). The EB data is collected independently from different subjects, but with the same representative sampling method, for the same general population, and with the same questions for each wave (see Section "Eurobarometer Data"). While not without limitations, it can be used to examine time-dependent changes in aggregated effects, on the country or EU level. As the data is only available for three points in time, we rule out time-series analysis, which requires numerous observations (often 50 or more) to estimate parameters for associations of measures over time (Box and Pierce, 1970).

Consequently, our approach resembles a trend study, which is structured into two phases. In the first phase, we evaluate the robustness of the measurement models, overall goodness of fit, and the structural links. To do so, we estimate the model for all three EB waves individually and examine the signs and significance of the structural links for all hypotheses. In the second phase, we validate the persistence of aggregated effects by comparing confidence intervals of the structural links for each hypothesis individually.

Data

This section briefly describes the three waves of the Special Eurobarometer series and presents descriptive statistics for all indicators used in the original measurement model. We take results from EB77.2 (2012) as a baseline and analyze trends for marginal statistics by looking at the EB79.4 (2013) and EB82.2 (2015) waves. Finally, we present the improved measurement model along with descriptive statistics for the updated indicators. All references in this section refer to either of the three EB reports.

Eurobarometer Data

The EB surveys on cyber security measure the prevalence of cybercrime, consumer behavior, and attitudes towards security. They were conducted in three subsequent years (March 2012, May-June 2013, and October 2014). An essential consideration for longitudinal research designs is the time metric, i.e., the data collection interval (Steel and McLaren, 2008; Kehr and Kowatsch, 2015). The absence of seasonal effects in cybercrime attacks eliminates the need for equidistant sampling intervals. However, the time metric must fit to the characteristics of the phenomena to be studied (Singer and Willett, 2003). While some dynamics are best studied over weeks, aggregated effects of online service avoidance among the general population can be expected to change more slowly. Kehr and Kowatsch (2015) state that data from a few waves in principle allows the observation of trends. Figure 1 supports this statement by showing a considerable variation in the marginal statistics between 2012 and 2014.

The sampling and data collection method is consistent in all EB waves. Using stratification by country as well as random route and closest birthday rules within countries, all surveys can be considered to be a representative cross-section of European citizens above the age of 15. The first wave yielded a total of 26,593 responses. The subsequent surveys collected more response sets (27,680 in 2013 and 27,868 in 2014), because they include Croatia, which joined the EU in 2013. For the sake of consistency, we do not consider Croatia in our analysis. Respondents were interviewed face-to-face in their respective mother tongues. The question wording for the five different types of cybercrime, used to measure EXP (six types for PCR), did not change in the three EB waves. The English version of all questionnaires is available in the technical appendices of the respective EB reports. The only difference we found is a change in the order of EXP and PCR related question blocks in the 2014 wave.

We drop 9,535 cases from the 2013 wave because respondents reported that they do not use the Internet (8,988 cases in 2014). To replicate the results of Riek et al. (2016), we remove 108 cases for 2013, because they contain "don't know" or "refusal" responses in all questions related to *Perceived Cybercrime Risk* or *Cybercrime Experience* (187 for 2014). 526 further "don't know" responses for *Cybercrime Experience* are recoded to "no experience" (602 in 2014). The remaining missing values (774 in 2013 and 1,472 in 2014) are handled by Mplus using pairwise exclusion. In total, our analysis uses 18,145 cases in 2013, representing 18,875 Internet users using normalized weights (18,880 for 2014 representing 20,081 Internet users).

Descriptive statistics

Table 1 reports descriptive statistics for EU Internet users (15 years and older) in all three EB waves, replicating results from 2012 as a baseline. Small differences to the figures presented in Riek et al. (2016) for 2012 are due to the fact that the original study eliminated a few more cases to account for missing values in the moderation analysis, which we do not replicate in the longitudinal setting.

ID	Latent Variable (Scale) / Indicator	Answers		
	Year	2012	2013	2014
	Number of Internet users (normalized weights)	18605	18875	20081
EXP	**Cybercrime Experience (Ordinal)**			
"How often have you experienced or been victim of …?"		At least occasionally*		
exp1	identity theft	8.2 %	6.4 %	7.0 %
exp2	spam emails	37.9 %	31.6 %	31.3 %
exp3	online shopping fraud	12.4 %	10.0 %	12.6 %
exp5	encountering illegal material	15.2 %	14.4 %	14.6 %
exp6	unavailable online services	12.8 %	11.8 %	7.7 %
PCR	**Perceived Cybercrime Risk (Ordinal)**			
"How concerned are you personally about becoming a victim of …?"		At least fairly*		
pcr1	identity theft	61.3 %	51.7 %	68.0 %
pcr2	spam emails	48.0 %	43.2 %	55.9 %
pcr3	online shopping fraud	49.0 %	42.1 %	55.7 %
pcr4	encountering child pornography	50.6 %	43.6 %	52.2 %
pcr5	encountering illegal material	40.7 %	34.7 %	46.1 %
pcr6	unavailable online services	42.7 %	37.4 %	50.9 %
AV	**Avoidance Intention (Binary)**			
"Due to cybercrime concern, you …"		Yes		
avS	are less likely to buy goods or services online	17.7 %	16.8 %	13.3 %
avB	are less likely to bank online	14.6 %	14.8 %	12.2 %
avN	are less likely to give personal information on websites	36.8 %	34.1 %	12.2 %
avU	only visit websites you know and trust	33.9 %	32.1 %	35.7 %
PB	**Protection Behavior (Binary)**			
"Due to cybercrime concern, you … "		Yes		
pbA	have installed anti-virus software	51.4 %	46.0%	60.6 %
pbP	use different passwords for different websites	25.1 %	24.3 %	31.5 %
pbS	have changed my security settings (e.g., in my browser, …)	16.4 %	16.3 %	17.6 %
Use	**Online service use** (complements Figure 1, not part of the SEM analysis)			
useS	online shopping	52.6 %	50.4 %	56.8 %
useB	online banking	48.4 %	48.4 %	54.0 %
useN	online social networking	51.9 %	53.4 %	60.0 %

* Ordinal scales are aggregated to binary in the table. They enter the SEM analysis with full precision.

Table 1. Descriptive statistics (Base: EU Internet users age 15+)

Cybercrime Experience (EXP) is measured by five indicators on a 3-point frequency scale (never, occasionally, often), where each indicator represents one type of cybercrime. Although the question wording in the EB does not set an explicit time frame for the experience, we can assume that most respondents have an implicit horizon and fading memory (Tourangeau et al., 2000). Otherwise, it is difficult to explain that reported EXP decreased between 2012 and 2014. Broken down by crime types, we find the

largest difference for the reception of spam emails (exp2), which drops from 37.9% of Internet users in 2012 to 31.3% in 2014. Online shopping fraud (exp3), on the other hand, remained on the same level (12.5%). Experience of accidently encountering child pornography (would be: exp4) is not covered in EB surveys.

Perceived Cybercrime Risk (PCR) is measured independently for each type of cybercrime based on the reported concern on a 4-point rating scale (not at all, not very, fairly, very). In 2012, less than half of the respondents reported concern (except for pcr1: identity theft). In 2013, all concern rates drop substantially between -5%-pts. and -10%-pts., but increase even stronger in 2014 (+9%-pts. to +17%-pts.), exceeding the 2012 levels. This "bumpy" nature of measuring cybercrime further challenges the robustness of the model and supports the refinement of the measurement instrument, as described in the next section.

Avoidance Intention (AV) is measured by four binary statements, which are causally linked to PCR in the question wording: "Due to cybercrime concern, you …". Each indicator is included as a single dependent variable, resulting in four models for each year. As in the original model, we measure AV of online social networking (avN) with a proxy: "… less likely to give personal information online". Marginal statistics show that avoidance of online shopping (avS) and online banking (avB) decreased slightly (-2%-pts. to -4%-pts.) from 2012 to 2014 and substantially (-25%-pts.) for avN. Contrary to the other reactions, avoidance of unknown websites (avU), our extension of the model, increased by 2%-pts. over the time analyzed.

Protection Behavior (PB) is measured in the same manner as *AV*, by three binary statements causally linked to PCR. Each indicator represents one self-reported reaction to cybercrime. The most common response is installing anti-virus software (pbA). 51.4% and 60.6% of Internet users reported pbA in 2012 and in 2014, respectively. The use of different passwords (pbP) is less prevalent (25.1%), but also increased (+6%-pts.) over time. Changing security settings (pbS) is least prevalent (16.4%) and increased only slightly (1%-pt.).

Updated Cybercrime Indicators

In addition to the existing indicators, the 2014 wave of the EB offers the opportunity to improve the measurement model by including additional types of cybercrime as indicators for the two latent variables EXP and PCR. Table 2 shows these new indicators (exp7, pcr7, - exp10, pcr10) along with their original wording. The increased pool of indicators with a total of ten different types of cybercrime allows us to remove less suitable crimes from the measurement model (exp2, pcr2, exp4, pcr4, exp5, pcr5, exp6, pcr6). We justify the exclusion of these indicators with the following reasons: 1) they only cause insignificant harm, 2) are not primarily targeted against individual Internet users, or 3) are not observable for them.

Additional cybercrime indicators		**Removed cybercrime indicators**	
exp7, pcr7	"Your social media or email account being hacked"	exp2, pcr2	"Receiving emails or phone calls fraudulently asking for access to your computer, logins or personal details (incl. banking or payment information)"
exp8, pcr8	"Being a victim of bank card or online banking fraud"	exp5, pcr5	"Accidentally encountering child pornography online"
exp9, pcr9	"Being asked for a payment in return for getting back control of your device"	exp4/ pcr4	"Accidentally encountering material which promotes racial hatred or religious extremism"
exp10, pcr10	"Discovered malicious software (viruses, etc.) on your device"	exp6, pcr6	"Not being able to access online services (e.g. banking services or public services) because of cyber-attacks"

Table 2. Improved measurement model: indicators with question wording

In the cases of accidentally encountering extremist (exp4, pcr4) and child sexual abuse material (exp5, pcr5), Internet users are affected only indirectly. Though the possession of the material can be illegal, the recipients who encounter it accidentally are not the primary victims. In the majority of cases, their harm is insignificant compared to the harm caused to the primary victims. Other crimes are barely observable to individual Internet users, partly because they are not targeted at them. This concern is particularly relevant for inaccessible online services caused by cyber-attacks (exp6, pcr6). Spam emails (exp2, pcr2) are directly targeted against consumers and their reception is commonly reported in the EB (31.3% in 2014). We still decide to exclude them from the improved measurement model, as the harm of pure reception is hardly

significant and research shows that the vast majority of spam emails are not successful (Kanich et al., 2008). For the same argument, we exclude malware infections (exp10, pcr10), which were added in 2014.

Consequently, the improved measurement model includes the following five types of cybercrime: identity theft, online shopping fraud, hacked accounts, bank card or online banking fraud, and extortion. All of them are targeted against individual Internet users and can cause significant harm. Descriptive statistics are presented along the improved measurement model in Table 4.

Results

We estimate covariance-based SEM models, as referred to by Henseler et al. (2009), for each year and compare path coefficients between the years, different forms of avoidance, and protection behavior. We estimate model parameters with the specialized statistics software Mplus, using the robust weighted least square (WLSMV) estimation method, which is suitable for non-normal distributed, categorical indicators and large samples (Finney and DiStefano, 2006). Since Mplus supports the inclusion of sampling weights, the consideration of country fixed effects, and the handling of missing values, we can utilize the full power of the three EB data sets and obtain representative results for Internet users across Europe.

The presentation of the results follows the structure of the analysis, which is divided into the two steps proposed by Anderson and Gerbing (1988). Accordingly, we first evaluate the quality of the original and improved measurement models using confirmatory factor analysis (CFA) and then report the structural models. Finally, we take a longitudinal perspective in a trend analysis of the structural links. We evaluate the fit of CFA and SEM models with different approximate fit indices, based on the thresholds for categorical indicators suggested by Yu and Muthen (2002): RMSEA < 0.05, TLI and CFI > 0.95. We report χ^2 values in all tables of model fit (Tables 3, 5, 6, and 7), but do not consider them for evaluation, as the χ^2 test has been reported to be sensitive to a sample size and unreliable for large samples (Finney and DiStefano, 2006).

	2012			**2013**			**2014**		
Item	Loading	Z	R^2	Loading	Z	R^2	Loading	Z	R^2
exp1	0.714 *** (.036)	20.00	.510	0.698 *** (.033)	20.87	.487	0.736 *** (.023)	31.94	.605
exp2	0.623 *** (.026)	23.70	.388	0.664 *** (.036)	18.30	.441	0.704 *** (.031)	22.71	.415
exp3	0.745 *** (.023)	31.97	.555	0.627 *** (.040)	15.83	.393	0.655 *** (.042)	15.72	.480
exp5	0.694 *** (.037)	18.60	.482	0.675 *** (.040)	16.73	.456	0.700 *** (.026)	26.48	.506
exp6	0.703 *** (.043)	16.50	.494	0.682 *** (.050)	13.62	.465	0.721 *** (.035)	20.52	.507
pcr1	0.822 *** (.007)	112.70	.676	0.851 *** (.008)	103.44	.724	0.825 *** (.013)	63.31	.721
pcr2	0.820 *** (.008)	102.33	.672	0.827 *** (.012)	71.51	.684	0.822 *** (.008)	102.49	.684
pcr3	0.807 *** (.010)	77.51	.651	0.816 *** (.008)	99.75	.666	0.786 *** (.015)	51.08	.667
pcr4	0.800 *** (.009)	86.17	.640	0.821 *** (.011)	73.94	.674	0.863 *** (.011)	75.05	.676
pcr5	0.822 *** (.007)	123.78	.676	0.824 *** (.009)	93.22	.679	0.839 *** (.008)	108.22	.682
pcr6	0.795 *** (.007)	121.42	.632	0.819 *** (.010)	79.74	.671	0.752 *** (.010)	76.29	.669
Fit:	$\chi^2(df) = 341(106)$, RMSEA = .011 (.010 − .013), TLI = 0.966, CFI = 0.977			$\chi^2(df) = 326(106)$, RMSEA = .011 (.009 − .012), TLI = 0.957, CFI = 0.970			$\chi^2(df) = 329(106)$, RMSEA = .011 (.009 − .012), TLI = 0.946, CFI = 0.963		

Table 3. Measurement models: standardized factor loadings (SEs in brackets)

Measurement Models

To evaluate the measurement models, we check construct reliability and validity using the three criteria suggested by Fornell and Larcker (1981): 1) standardized factor loadings should be significant and exceed 0.5, 2) composite reliability (CR) should exceed 0.8, and 3) the average variance extracted (AVE) should be greater than 0.5. IS scholars typically suggest a cut-off value of 0.707 for standardized factor loadings, e.g., Straub et al. (2004), because loadings > 0.707 indicate that the construct explains more than half of the variation in the indicator. However, CFA models can be accepted if factors do not explain this much variance for all indicators. In their heavily cited book on multivariate data analysis, Hair et al. present rules of thumb "suggesting that loadings should be at least .5 and ideally .7 or higher." (Hair et al. 2010, p. 818).

Our secondary analysis of a heterogeneous data set unavoidably contains more noise than data collected in a controlled setup. We measure indicators on short scales and use constructs which are created post-hoc from semantically diverse items. This unexplained variance attenuates the factor loadings. Hence, we accept the 0.5 cut-off. AVE represents the amount of indicator variance that is accounted for by the underlying indicators of the construct and should be greater than 0.5. We prefer the use of CR over Cronbach's Alpha, because CR takes into account that indicators can have different loadings (Hair et al., 2010).

	Indicator	Descriptive	Loading	SE	Z	R^2
EXP	**Cybercrime Experience (Ordinal)**	At least occasionally*				
exp1	identity theft	7.0 %	0.855 ***	(.014)	59.76	0.731
exp3	online shopping fraud	12.6 %	0.696 ***	(.053)	13.09	0.484
exp7	hacking of email or OSN account	7.7 %	0.767 ***	(.031)	24.96	0.588
exp8	online banking fraud	7.1 %	0.776 ***	(.044)	17.48	0.602
exp9	blackmail	8.4 %	0.623 ***	(.045)	13.97	0.388
PCR	**Perceived Cybercrime Risk (Ordinal)**	At least fairly*				
pcr1	identity theft	68.0 %	0.834 ***	(.013)	66.74	0.696
pcr3	online shopping fraud	55.7 %	0.776 ***	(.013)	58.13	0.602
pcr7	hacking of email or OSN account	60.3 %	0.832 ***	(.010)	82.53	0.692
pcr8	online banking fraud	63.4 %	0.844 ***	(.011)	78.57	0.712
pcr9	blackmail	47.2 %	0.812 ***	(.010)	79.80	0.659
Model fit: $\chi^2(df) = 159\ (90)$, RMSEA = .006 (.005 − .008), TLI = 0.977, CFI = 0.985;						

Table 4. Improved measurement model (14'): standardized factor loadings

Table 3 reports the CFA results for the original measurement models for all three EB waves, including standardized factor loadings (with significance levels and standard errors in brackets), Z-Scores, and R^2 for each indicator. Approximate fit indices are reported for each model in the lower part of Table 3. The overall fit exceeds the thresholds for good fit in all years. The only deviation is the TLI in the 2014 model, which is slightly below the suggested threshold of 0.95. Since all other indices and the 90% confidence interval for the RMSEA support the good fit for the 2014 model, we deem this to be acceptable. All standardized factor loadings are highly significant ($p < 0.001$) and exceed 0.62, thereby meeting the first criterion. Table 4 reports the CFA results for the improved model (14'), estimated using the third EB wave (2014). The fit indices exceed those in all other models, supporting our updated selection of cybercrimes. The first criterion for construct reliability and validity, standardized factor loadings > 0.5, is met by all indicators.

Criterion	12	EXP	PCR	13	EXP	PCR	14	EXP	PCR	14'	EXP	PCR
CR		0.82	0.92		0.80	0.93		0.83	0.92		0.86	0.91
AVE		0.49	0.66		0.45	0.68		0.50	0.66		0.56	0.67

Table 5. Reliability scores for all measurement models

The second and third criteria are reported for the original models and the improved model (14') together, in Table 5. Overall, PCR performs better than EXP. The second criterion (CR > 0.8) is met by all constructs, except for EXP in 2013, which is exactly at the threshold of 0.8. The third criterion (AVE > 0.5) is met by all PCR constructs and for EXP in the improved measurement model. In 2012 and 2014 the AVE scores of EXP (0.49 and 0.50) are still very close to the threshold. Due to the secondary nature of our analyses, we

consider it close enough to the target value of 0.5 to be deemed acceptable. In 2013, AVE is only 0.45 for EXP. While this only represents poor validity, we still report the models for 2013 and interpret the results with high caution. In summary, CR and AVE indicate best reliability and validity for the improved model.

We finally check for discriminant validity to ensure that different constructs do not measure the same phenomenon. To confirm discriminant validity, the square root of the AVE, noted in bold font on the diagonal in Table 9 (Appendix B), must be greater than the between construct correlations, noted below the diagonal (Henseler et al., 2009). Table 9 confirms discriminant validity for all constructs in all four models. We generally observe that correlations between constructs are low. Again, part of this result can be attributed to the secondary analysis of complex and comparably heterogeneous data sets.

Structural Models

Model		Path coefficients (SEs in brackets)				Fit indices			
	AV	EXP→PCR	PCR→AV	EXP$\xrightarrow{PCR}$AV	EXP→AV	$\chi^2(df)$	RMSEA (90% CI)	CFI	TLI
12	avS	0.258 *** (.020)	0.167 *** (.020)	0.043 *** (.006)	0.020 (.044)	139 (51)	.010 (.008–.012)	.993	.991
	avB	0.258 *** (.020)	0.093 *** (.023)	0.024 *** (.005)	0.142*** (.034)	143 (51)	.010 (.008–.012)	.993	.990
	avN	0.260 *** (.020)	0.061* (.027)	0.021* (.010)	0.121*** (.011)	202 (51)	.013 (.011–.015)	.988	.985
	avU	0.258 *** (.020)	0.145 *** (.025)	0.037 *** (.008)	−0.040 (.027)	140(51)	.010 (.008–.012)	.993	.991
13	avS	0.223 *** (.020)	0.189 *** (.016)	0.042 *** (.007)	−0.051 (.039)	145(51)	.010 (.008–.012)	.989	.986
	avB	0.223 *** (.020)	0.173 *** (.036)	0.039 *** (.008)	0.108 (.067)	159(51)	.011 (.009–.013)	.987	.983
	avN	0.225*** (.020)	0.054 (.033)	0.012 (.008)	0.226 *** (.030)	169(51)	.011 (.009–.013)	.986	.982
	avU	0.223 *** (.020)	0.125 *** (.015)	0.028 *** (.008)	−0.042 (.023)	164(51)	.011 (.009–.013)	.987	.984
14	avS	0.243 *** (.034)	0.133 *** (.026)	0.032 *** (.007)	0.017 (.031)	92(51)	.007 (.004–.009)	.994	.993
	avB	0.243 *** (.034)	0.140 *** (.023)	0.034 *** (.007)	−0.011 (.026)	98(51)	.007 (.005–.009)	.994	.992
	avN	0.244 *** (.035)	−0.022 (.033)	−0.005 (.008)	0.161 *** (.030)	127(51)	.009 (.007–.011)	.990	.987
	avU	0.244 *** (.034)	0.116 *** (.014)	0.028 *** (.006)	−0.001 (.017)	126(51)	.009 (.007–.011)	.990	.987
14'	avS	0.283 *** (.034)	0.148 *** (.024)	0.042 *** (.009)	−0.003 (.044)	97(42)	.008 (.006–.010)	.991	.988
	avB	0.282 *** (.033)	0.135 *** (.020)	0.038 *** (.007)	0.032 (.033)	100(42)	.009 (.006–.011)	.990	.987
	avN	0.282 *** (.033)	0.047 (.027)	0.013 (.008)	0.017 (.028)	116(42)	.010 (.008–.012)	.988	.984
	avU	0.283 *** (.033)	0.157 *** (.017)	0.051 *** (.008)	−0.066** (.022)	92(42)	.008 (.006–.010)	.991	.989

Cybercrime Experience (EXP), Perceived Cybercrime Risk (PCR), Avoidance Intention (AV): Online shopping (avS), Online banking (avB), OSN (avN), Unknown websites (avU); Sign.: $p < 0.001(***); p < 0.01\ (**); p < 0.05(*)$

Table 6. Structural models of avoidance: path coefficients and approximate fit indices

Analyzing the overall model fit first, we find that the 2013 wave performs worst. This result is expected, considering the bad fit of the measurement model. A comparison along the different forms of avoidance shows that online shopping avoidance (avS) models fit the data best and models for online social network avoidance (avN) fit worst. Overall differences between years and forms of avoidance are small and the fit indices indicate at least an acceptable fit for all models in all years.

Concerning structural links, the data supports **H1**. EXP has a significant direct positive effect on *PCR* in all years. The impacts are the highest for the improved measurement model ($\beta = 0.283, p < 0.001$). However, there remains a risk that they are partially caused by questionnaire effects (Tourangeau et al., 2000), as both constructs are measured using the same battery of questions. The swap in the order of both constructs in 2014 does not seem to influence the results.

The data also supports **H2**. PCR has a significant and positive impact on the avoidance of online shopping (avS), online banking (avB), and unknown websites (avU). The effects are highly significant in all EB waves and for the improved measurement model (14'). For avoidance of online social networks (avN), we only find a marginal effect ($p < 0.05$) in 2012. In the remaining models, this effect becomes insignificant.

We find partial support for **H3**. EXP positively effects the AV of online shopping, online banking, and unknown websites. The effects are fully mediated by PCR for online shopping and unknown websites. In the case of online banking, we find a partial mediation for 2012, because the direct effect is significant (β =0.142, $p < 0.001$). The subsequent years also support the full mediation hypothesis for avB. The mediation hypothesis does not hold for avN, because the indirect effects of EXP on avN are not significant.

Model		Path coefficients (SEs in brackets)				Fit indices			
	PB	EXP→PCR	PCR→PB	EXP$\xrightarrow{PCR}$PB	EXP→PB	$\chi^2(df)$	RMSEA (90% CI)	CFI	TLI
12	pbA	0.258 *** (.020)	-0.010 (.027)	-0.003 (.006)	0.063 (.044)	194(51)	.013 (.011–.014)	.988	.985
	pbP	0.259 *** (.020)	0.006 (.016)	0.002 (.004)	0.161 *** (.026)	166(51)	.011 (.009–.013)	.991	.988
	pbS	0.262 *** (.020)	-0.016 (.031)	-0.004 (.008)	0.317 *** (.028)	191(51)	.012 (.011–.014)	.989	.986
13	pbA	0.223 *** (.020)	0.057 * (.027)	-0.013 * (.006)	0.005 (.044)	209(51)	.013 (.011–.015)	.982	.976
	pbP	0.227 *** (.020)	0.034 (.021)	0.008 (.005)	0.228 *** (.034)	188(51)	.012 (.010–.014)	.984	.979
	pbS	0.228 *** (.020)	-0.002 (.019)	0.000 (.004)	0.391 *** (.028)	183(51)	.012 (.010–.014)	.985	.981
14	pbA	0.244 *** (.034)	-0.019 (.031)	-0.005 (.008)	0.069 * (.034)	141(51)	.010 (.008–.012)	.988	.984
	pbP	0.246 *** (.035)	-0.028 (.037)	-0.007 (.009)	0.187 *** (.026)	125(51)	.009 (.007–.011)	.990	.987
	pbS	0.246 *** (.035)	-0.059 (.041)	-0.014 (.011)	0.344 *** (.033)	105(51)	.008 (.006–.01)	.992	.990
14'	pbA	0.282 *** (.034)	0.037 (.027)	0.010 (.007)	-0.052 (.035)	103(42)	.009 (.007–.011)	.989	.985
	pbP	0.281 *** (.034)	0.019 (.035)	0.006 (.011)	0.090 *** (.020)	101(42)	.009 (.006–.011)	.990	.986
	pbS	0.282 *** (.034)	0.021 (.026)	-0.006 (.008)	0.230 *** (.019)	95(42)	.008 (.006–.01)	.990	.987

Cybercrime Experience (EXP), Perceived Cybercrime Risk (PCR), Protection Behavior (PB): Anti-virus (pbA), Different passwords (pbP), Changed security settings (pbS); Sign.: $p < 0.001(***); p < 0.01\ (**); p < 0.05(*)$

Table 7. Structural models of protection: path coefficients and approximate fit indices

Table 7 reports the SEM results for *Protection Behavior* (PB). The overall fit of the protection models is slightly worse when compared to the fit of avoidance models. The worst fit indices are observed in 2013. Among the different types of protection behavior, changing security settings (pbS) fits best in all years, except for 2013. Models of installing anti-virus software (pbA) fit worst in all years.

Concerning structural links, the data also supports **H1** for the PB models, with very similar effect sizes in all years. In contrast to AV, the impact of PCR on PB is not significant. Consequently, **H4** is not supported by the data. We also have to reject the full mediation hypothesis regarding the impact of EXP on PB (**H5**). Indirect effects are not significant in any model. We find marginal effects for **H4** and **H5** in 2013, but we neglect them due to the bad measurement model in this year.

Even though not hypothesized, we find a positive direct effect of EXP on PB, which is highly significant for using different passwords (pbP) and changing security settings (pbS) in all years. It is consistently higher for changing security settings. The installation of anti-virus software (pbA) is neither influenced by EXP nor by PCR. While this may be a surprising result, we conjecture it is due to the high proliferation of anti-virus software, which the majority of Internet users reports to install preventively (see Table 1).

In summary, *Protection Behavior* is rather influenced by *Cybercrime Experience*, whereas *Avoidance Intention* is driven by *Perceived Cybercrime Risk*. The improved measurement model for 2014 underlines the robustness of the results for online shopping (avS) and online banking (avB), as the effects do not change. Interestingly, we find a direct and negative effect of *Cybercrime Experience* on the *Avoidance Intention* of unknown websites ($\beta = -0.066$, $p < 0.01$), which is small, but significant. Reverse causality between both constructs may explain the effect. However, we cannot study this in detail, at least not with the current data set. We encourage future studies to shed more light on this observation.

Trend Analysis

To test for time-dependent changes in the structural links, we compare effect sizes for each hypothesis and each form of avoidance and protection behavior across all models (12, 13, 14, and 14'). We calculate 95% confidence intervals (CIs) for the standardized path coefficients and visually analyze pairwise overlaps in Figure 3. If two CIs do not overlap, we can conjecture that the effects have changed significantly. Since the effects for avoidance of online social networking services are only marginally significant in 2012 and insignificant in the other models, we exclude them from the trend analysis. Each subfigure in Figure 3 reports the results for one hypothesis (in rows) and one form of avoidance or protection (in columns). Each dot represents an individual path coefficient in the respective year and the black line delineates the corresponding CI. The dashed green lines depict the CI of the baseline model in 2012.

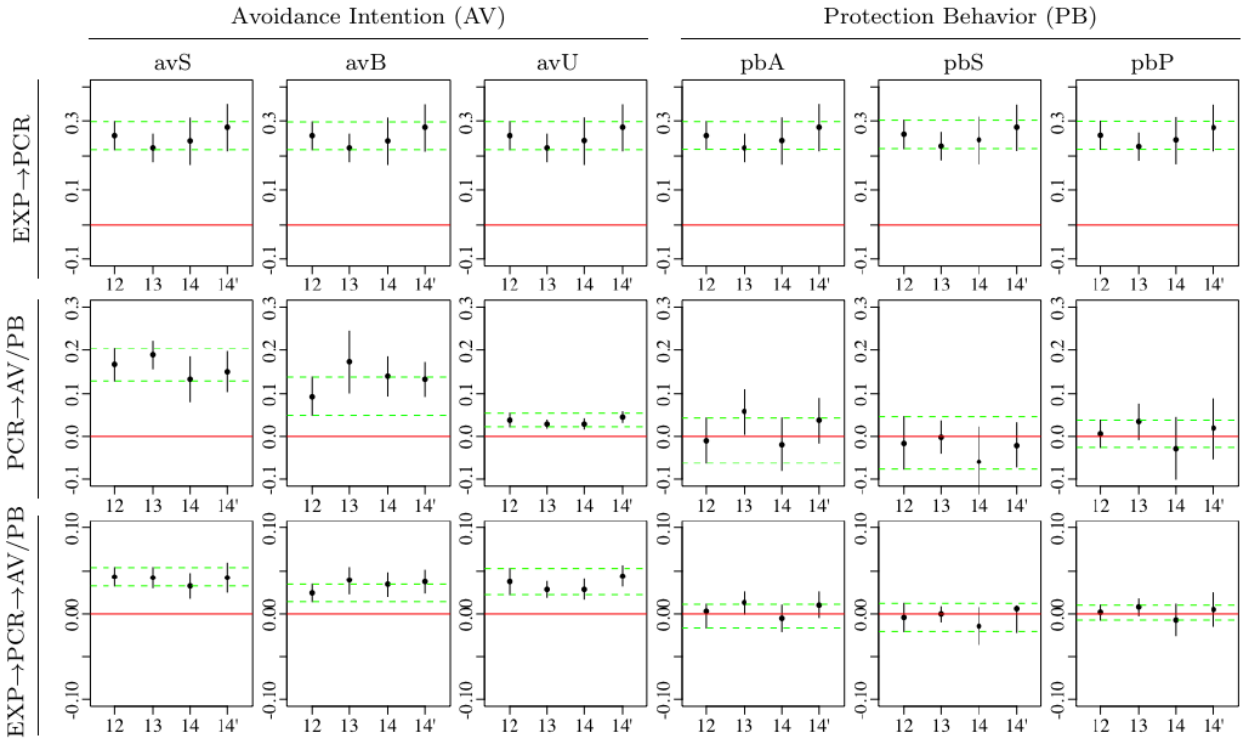

Figure 3. Trends in structural links for the core hypotheses (rows) over the four models (x-axis in each tile); effect size with 95% CI (y-axis in each tile), reference CI of the 2012 model (dashed green line in each tile)

Overall, the largest effect sizes are observed in the top row for the impact of *Cybercrime Experience* on *Perceived Cybercrime Risk* (**H1**). The impact of *Perceived Cybercrime Risk* is significant for *Avoidance*

Intention (**H2**), but insignificant for *Protection Behavior* (**H4**). The bottom row represents the indirect effect of *Cybercrime Experience* on *Avoidance Intention* (**H3**) and *Protection Behavior* (**H5**). Overall, these effects show a pattern similar to the direct effects of *Perceived Cybercrime Risk* on both constructs, but with smaller effect sizes. Note that even though the effects are very small, they are still highly significant for all avoidance models (left part of Figure 3).

Comparing the CIs, we cannot identify significantly different effect sizes. While we only visualize the CI of the baseline model (the dashed green line), all other CIs overlap in a pairwise comparison. Consequently, we conclude that the structural links are stable across the different models and that the impacts of cybercrime on online service avoidance and protection behavior are persistent over time.

Discussion

Limitations

The work has some limitations. First, the rather vague question wording, common for large scale population surveys (e.g., "… you are less likely to do online shopping."), can only provide tendencies of avoidance intention, but does not record precisely defined (actual) behavior. Secondly, our longitudinal approach inherits limitations of the original model and the secondary data analysis, in particular the inability to influence the instrument design. Our results account for between-country variation using fixed-effects in the model, but we do not study the impact of cultural and national characteristics in-depth, e.g., with a multi-level design. While such a study is beyond the scope of this paper, we undertake an additional robustness check for the improved model (14') by comparing EU countries with high Internet adoption (Denmark, the Netherlands, and Sweden) to countries with low Internet adoption (Romania, Portugal, Greece, and Bulgaria). Low adoption countries exhibit better reliability scores for the cybercrime experience construct and have a better model fit. Most hypotheses on the structural links are supported in both groups.

However, some limitations in the measurement model remain. The original model of online service avoidance (Riek et al., 2016) is parsimonious in the sense that it focuses on perceived cybercrime risk as the single factor influencing avoidance. It neglects other factors commonly used in behavioral theories, such as perceived usefulness and perceived ease-of-use. These factors likely have a *positive* effect on *adoption*, hence a *negative* effect on *avoidance* of online services. Unfortunately, we could not include them in our population-wide analyses, because they are not measured in the EB surveys. We also could not include some constructs used by Chen and Zahedi (2016), for example, response efficacy or seeking help (see Table 8).

Consequently, our results are only a step towards building principled theory in the context of avoidance as security behavior. However, we are able to study individual behavior on the societal level, building on the three enormous data sets with responses of more than 57,000 individual Internet users, collected with industry standard sampling and interviewing methods. Moreover, specialized software packages and robust estimation methods prove to be powerful in solving statistical issues in the SEM analyses.

Results and Implications

Using a longitudinal approach, we provide empirical evidence that the main impacts of cybercrime on perceived risk, protection behavior, and avoidance behavior are small, but significant and persistent on the societal level. Our results endorse the robustness of the research model by Riek et al. (2016) to study online service avoidance in reaction to cybercrime. We find the strongest positive impact of cybercrime experience on perceived risk of cybercrime throughout all years. We also confirm the impact of perceived cybercrime risk on the avoidance of online banking, online shopping, and unknown websites. For these forms of avoidance, indirect effects of cybercrime experience are very small, however highly significant. Following Chen and Zahedi (2016), we add three forms of protection behavior to the model and find that using different passwords and changing security settings are directly triggered by cybercrime experience, but not by perceived cybercrime risk. Our improved measurement model for the 2014 wave performs best in terms of overall model fit and supports our choice of cybercrimes to study avoidance behavior. It also adds additional confidence regarding the robustness of the model and underlines its applicability for the validation of the persistence of aggregate cybercrime impacts.

Our results partly explain the contradictions between the marginal distributions of online service adoption and effects observed in the model (discussed in the introduction). However, they are not entirely conclusive.

A potential explanation for the simultaneous decrease in reported cybercrime experience and increase of perceived cybercrime risk is media coverage. It has been shown that the media is a powerful tool to form public opinion and risk perception, in particular with regards to crimes (Wahlberg and Sjoberg, 2000; Jackson, 2011). While media awareness has been part of the original research model, it could not be measured reliably with the questions available in EB surveys. Moreover, the collection of data on media reception has been discontinued in 2013. Thus, we can only speculate about the existence of such an effect. The simultaneous persistence in avoidance and the growing adoption of online services may be explained by different forms of avoidance behavior, which are not entirely observable with our general measurement instrument. Liang and Xue (2009) state that avoidance behavior comprises various actions to evade an undesired end state, in our case victimization. Consumers may adopt different coping mechanisms and avoidance strategies in order to protect themselves against cyber risk.

Unlike the other forms, there is no empirical evidence for the impact of cybercrime on avoidance of online social networking. While Riek et al. (2016) find a marginally significant effect ($p < 0.05$) in 2012, this effect is not persistent over time. We explain this result by the context of the EB instrument, which focuses on security-related issues and types of crime. It largely neglects privacy-related issues, which arguably play a more significant role for social networking (Krasnova et al., 2009). The results highlight the inherently different characteristics of social networking in comparison to online banking and online shopping. While the latter two are fairly standardized routine activities with a direct link to financial transactions, social networking is a hedonic service used for personal pleasure, which requires users to share information and interact with others (Turel, 2015). Consequently, other types of cybercrime, for example cyber-bullying and cyber-stalking, or concerns of data misuse by OSN providers are better indicators for perceived risk in online social networks (Krasnova et al., 2009). The fact that the avoidance models for online social networking fit the data worst in all waves supports this argument.

Taking a step back, the prevalence of cybercrime and the persistence of aggregate effects emphasize the importance of studying individual security behavior on the societal level. This has three theoretical implications for IS research on security behavior. First, IS scholars should shift the focus of avoidance models from customers avoiding a particular vendor to the population of all Internet users avoiding a technology in general. Second, this shift requires dedicated models and a clearer conceptualization of online service avoidance as a behavioral construct, similar to Recker's (2016) work for IS discontinuance. Third, primary data on the societal level is needed to evaluate these models. Our integration of the two existing models of avoidance allows us to study aggregate effects of cybercrime on avoidance and protection behavior over time, but the analysis is limited due to the use of secondary data.

Nevertheless, our results have practical implications. With respect to online shopping, we find that concerned consumers tend to shop at websites they already know and trust. This may foster existing network economics which favor larger providers (Shapiro and Varian, 1998, p. 173), because a certain (perceived) level of cybercrime limits consumer choices and drives them towards well-known, trusted online brands. Put differently, negative consequences of ICT on the societal level may lead to positive outcomes for some market participants. In the most extreme scenario, cybercrime catalyzes a Matthew effect (Merton, 1968) in B2C e-commerce, resulting in very few large providers. This subtle interaction is relevant for business strategies and – more importantly – economic studies of online market structures aiming to inform policy makers, since beneficiaries of cybercrime may have few incentives to fight it alone or in joint efforts.

Conclusion

This paper studies population-wide perceptions and experiences of cybercrime in order to analyze its impact on protection behavior and the avoidance of three established online services on the societal level. Mainly drawing on the research model proposed by Riek et al. (2016), we develop a longitudinal approach to validate the persistence of avoidance and protection behavior for the years 2012 to 2014. Based on three representative pan-European samples, we find that the model is robust in terms of overall fit and structural links, for online banking, online shopping, and unknown websites as a form of avoidance. We reinforce with strong empirical evidence that cybercrime experience increases perceived cybercrime risk, which ultimately leads to avoidance behavior. However, avoidance of online social networking is not significantly influenced by perceived cybercrime risk. In contrast to online service avoidance, protection behavior is not triggered by perceived risk, but directly by cybercrime experience.

The broader objective of this work is to develop principled theory and test the applicability of general behavioral models to study avoidance as a barrier to the adoption of innovative technologies. Here, we chose to study online services as one example of established ICT due to their mature state of adoption and, consequently, availability of population-wide data. In addition to our empirical findings, our study highlights a general problem of collecting reliable data on the societal level with the right instrument and method. To date, we only have population data (and reasonable measurement instruments) for online services that were invented 20 years ago and vastly adopted 10 years ago. Learning from these past innovations can inform IS researchers on a need to study current innovations – as well as their unintended and unforeseen consequence – faster, better, and more systematically. It also calls for a closer collaboration between researchers, domain experts, and statistical institutes in an attempt to measure the relevant aspects of innovative ICT right from the beginning. This is a prerequisite for studying trends and robustness over time. Connecting back to the outset, we are still not aware of population-wide surveys on participative online markets (Airbnb, Uber) and decentralized payment networks (Bitcoin), which include items on security, privacy, and crime.

Appendix A – Comparison of Avoidance Studies

Table 8 compares the studies of Chen and Zahedi (2016) and Riek et al. (2016), who explicitly include avoidance constructs in their research models.

	Chen and Zahedi (2016)	**Riek et al. (2016)**
Theory	TTAT (Liang and Xue 2009); PMT (Rogers 1983)	Perceived Risk-extended TAM (Featherman and Pavlou, 2003); TAM (Davis, 1989)
Subjects	Individual Internet users	Individual Internet users
Context	Security behaviors (US and China)	Impact of cybercrime (EU member states)
Data collection	**Dedicated instrument**; Questionnaire items refer to Internet security attacks in general. **Online survey**: 480 (US) and 238 (Chinese) Internet users recruted in online social networks.	**Secondary analysis**; Questionnaire items refer to specific types of cybercrime. **Face-to-face interviews**; ~18000 Internet users; representative data for 27 EU countries.
Analysis	**SEM**; multi-group analysis to test for the moderation effects of national differences.	**SEM**; multi-group analysis to test for the moderation effects of user confidence.
Similar constructs	***Perceived susceptibility:*** belief about the [...] vulnerability to Internet security attacks.	***Perceived cybercrime risk:*** concern of victimization regarding different types of cybercrime (identity theft, spam e-mails, online fraud, child pornographic content, content of racial hatred, and unavailable services).
	Perceived severity: belief about the [...] potential harm caused by Internet security attacks.	
	Perceived security threat: degree of worry/fear about Internet security threats.	
	Perceived security self-efficacy: belief in own ability to take protective measures [...].	***User confidence:*** belief in own ability to handle online transactions.
	Avoidance: avoiding the use of the Internet in various degrees, especially avoiding sensitive activities such as online banking, in order to avoid online security threats.	***Avoidance intention:*** intention to avoid particular online services (online banking, online shopping or sharing personal information online).
Unique constructs	***Perceived security response efficacy:*** belief about whether or not [...] protective measure can [...] protect against Internet security attacks.	***Media awareness:*** extent to which users are exposed to news reports about cybercrime from different media sources.
	Protective actions: [...] protective countermeasures to reduce or eliminate risk of Internet security attacks.	***Cybercrime experience:*** reported frequency of experiencing different cybercrimes.
	Seeking help: interactions with others in seeking social support and assistance [...].	

Main findings	Positive effect of perceived susceptibility and perceived severity on perceived security threat. Positive effect of perceived security threat and perceived security self-efficacy on protective actions and avoidance. Negative influence of perceived security self-efficacy on avoidance.	Positive impact of cybercrime experience on perceived risk of cybercrime. Positive impact of cybercrime experience and perceived risk of cybercrime on avoidance intention of online banking, online shopping and online social networking. Smallest effects for online social networking.

Table 8. Comparison of avoidance studies

Appendix B – Between-construct Correlations

Model		Constructs (Con.)								
Y.	Con.	EXP	PCR	avS	avB	avN	avU	pbA	pbP	pbS
12	EXP	**.700**	(.021)	(.045)	(.033)	(.012)	(.023)	(.024)	(.024)	(.036)
	PCR	.263***	**.812**	(.019)	(.017)	(.028)	(.020)	(.029)	(.015)	(.029)
	avS	.061	.170***	-	(.035)	(.032)	(.053)	(.025)	(.021)	(.028)
	avB	.170***	.127***	.577***	-	(.050)	(.044)	(.027)	(.017)	(.033)
	avN	.145***	.092***	.305***	.298***	-	(.047)	(.046)	(.046)	(.038)
	avU	.001	.132***	.087	.096*	.327***	-	(.046)	(.041)	(.041)
	pbA	.317***	.066*	.011	.073*	.450***	.203***	-	(.025)	(.043)
	pbP	.174***	.047**	-.027	.010	.414***	.329***	.557***	-	(.033)
	pbS	.075*	.006	-.26	-.038	.452***	.394***	.427***	.532***	-
13	EXP	**.671**	(.020)	(.041)	(.063)	(.023)	(.023)	(.031)	(.030)	(.019)
	PCR	.228***	**.825**	(.016)	(.023)	(.028)	(.015)	(.017)	(.017)	(.026)
	avS	−.013	.177***	-	(.049)	(.049)	(.036)	(.023)	(.030)	(.045)
	avB	.146*	.195***	.578***	-	(.046)	(.022)	(.023)	(.026)	(.050)
	avN	.243***	.103***	.280***	.294***	-	(.017)	(.041)	(.033)	(.033)
	avU	−.008	.114***	.131***	.059**	.324***	-	(.032)	(.019)	(.028)
	pbA	.384***	.087***	.041	.069**	.459***	.201***	-	(.029)	(.018)
	pbP	.245***	.085***	-.019	-.017	.350***	.318***	.549***	-	(.027)
	pbS	.037	.057*	.019	-.046	.459***	.446***	.432***	.534***	-
14	EXP	**.707**	(.035)	(.032)	(.029)	(.029)	(.013)	(.028)	(.020)	(.034)
	PCR	.246***	**.812**	(.025)	(.022)	(.031)	(.011)	(.033)	(.031)	(.030)
	avS	.049	.133***	-	(.023)	(.040)	(.034)	(.052)	(.033)	(.042)
	avB	.019	.133***	.558***	-	(.039)	(.021)	(.026)	(.032)	(.024)
	avN	.160***	.015	.346***	.283***	-	(.021)	(.028)	(.029)	(.042)
	avU	.031*	.110***	.221***	.208***	.307***	-	(.022)	(.018)	(.024)
	pbA	.326***	.024	.098	.055*	.391***	.175***	-	(.029)	(.027)
	pbP	.186***	.016	.100*	.068*	.396***	.220***	.508***	-	(.029)
	pbS	.074*	-.003	.154***	.092***	.455***	.356***	.393***	.456***	-
14'	EXP	**.748**	(.033)	(.039)	(.029)	(.027)	(.018)	(.019)	(.015)	(.034)
	PCR	.281***	**.819**	(.024)	(.024)	(.026)	(.016)	(.023)	(.032)	(.028)
	avS	.038	.149***	-	(.023)	(.040)	(.034)	(.052)	(.033)	(.042)
	avB	.083**	.145***	.557***	-	(.039)	(.021)	(.026)	(.032)	(.024)
	avN	.037	.047	.347***	.284***	-	(.021)	(.028)	(.029)	(.042)
	avU	−.023	.137***	.221***	.209***	.307***	-	(.022)	(.018)	(.024)
	pbA	.222***	.044	.098	.056*	.391***	.175***	-	(.029)	(.027)
	pbP	.096***	.044	.100**	.068*	.396***	.219***	.507***	-	(.029)
	pbS	-.040	.022	.154***	.092***	.454***	.357***	.394***	.455***	-

Lower-left: between construct correlations; Diagonal: $\sqrt{\text{AVE}}$; Upper-right: SEs of the correlations;
Constructs: Cybercrime Experience (EXP), Perceived Cybercrime Risk (PCR), Avoidance Intention (AV): Online shopping (avS), Online banking (avB), OSN (avN), Unknown websites (avU), Protection Behavior (PB): Anti-virus (pbA), Different passwords (pbP), Changed security settings (pbS); Sign.: $p < .001(***); p < 0.01\ (**); p < 0.05(*)$

Table 9. Measurement model: between-construct correlations

References

Abramova, S., and Böhme, R. 2016. "Perceived Benefit and Risk as Multidimensional Determinants of Bitcoin Use: A Quantitative Exploratory Study," in *Proceedings of the Thirty Seventh International Conference on Information Systems (ICIS)*, Dublin, Ireland.

Acquisti, A., Friedman, A., and Telang, R. 2006. "Is There a Cost to Privacy Breaches? An Event Study," in *Proceedings of the 27th International Conference on Information Systems (ICIS)*, Milwaukee, USA.

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179-211.

Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), pp. 613-643.

Anderson, J., and Gerbing, D. 1988. "Structural Equation Modeling in Practice: A Review and Recommended Two-step Approach," *Psychological Bulletin* (103:3), pp. 411-423.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M.J.G., Levi, M., Moore, T., and Savage, S. 2013. "Measuring the Cost of Cybercrime," in *Economics of Information Security and Privacy,* R. Böhme (ed.), Heidelberg: Springer Berlin, pp. 265-300.

Arachchilage, N. A. G., and Love, S. 2014. "Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective," *Computers in Human Behavior* (38), pp. 304-312.

Box, G. E., and Pierce, D. A. 1970. "Distribution of Residual Autocorrelations in Autoregressive-Integrated Moving Average Time Series Models," *Journal of the American Statistical Association* (65:332), pp. 1509-1526.

Brynjolfsson, E. 1996. "The Contribution of Information Technology to Consumer Welfare," *Information Systems Research (*7:3), pp. 281-300.

Brynjolfsson, E., Smith. M. D., and Hu, Y. 2003. "Consumer Surplus in the Digital Economy: Estimating the Value of Increased Product Variety at Online Booksellers," *Management Science* (49:11), pp. 1580-1596.

Burns, S., and Roberts, L. 2013. "Applying the Theory of Planned Behavior to Predicting Online Safety Behavior," *Crime Prevention and Community Safety* (15:1), pp. 48-64.

Carver, C. S. 2006. "Approach, Avoidance, and the Self-Regulation of Affect and Action," *Motivation and Emotion* (30), pp. 105-110.

Centefelli, R. T., and Schwarz, A. 2011. "Identifying and Testing the Inhibitors of Technology Usage Intentions," *Information Systems Research* (22:4), pp. 808-823.

Chen, R., and He, F. 2003. "Examination of Brand Knowledge, Perceived Risk and Consumers' Intention to Adopt an Online Retailer." *Total Quality Management and Business Excellence* (14:6), pp. 677-693.

Chen, Y., and Zahedi, F. 2016. "Individuals' Internet Security Perceptions and Behaviors: Poly-contextual Contrasts between the United States and China," *MIS Quarterly* (40:1), pp. 205-222.

Cheng, E., Lam, D., and Yeung, A. 2006. "Adoption of Internet Banking: An Empirical Study in Hong Kong," *Decision Support Systems* (42:3), pp. 1558-1572.

Chiu, C, Wang, E. T. G., Fang, Y., and Huang, H. 2014. "Understanding Customers' Repeat Purchase Intentions in B2C e-Commerce: The Roles of Utilitarian Value, Hedonic Value and Perceived Risk," *Information Systems Journal* (24:1), pp. 85-114.

Crossler, R. E., Johnston, A. C., Lowry, P. B., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers and Security* (32:1), pp. 90-101.

Davis, F.D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13:3), pp. 319-340.

Dinev, T., and Hu, Q. 2007. "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," *Journal of the Association for Information Systems* (8:7), pp. 386-408.

EB77.2 2012. Special Eurobarometer 390 Cyber Security. Technical Report Wave EB77.2. European Commission, Brussels, Belgium. URL: ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf (visited on 01/04/2017).

EB79.4 2013. Special Eurobarometer 404 Cyber Security. Technical Report Wave EB79.4. European Commission, Brussels, Belgium. URL: ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf (visited on 01/04/2017).

EB82.2 2015. Special Eurobarometer 423 Cyber Security. Technical Report Wave EB82.2. European Commission, Brussels, Belgium. URL: ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf (visited on 01/04/2017).

Featherman, M., and Pavlou, P. 2003. "Predicting e-Services Adoption: A Perceived Risk Facets Perspective," *International Journal Human Computer Studies* (59:4), pp. 451-474.

Featherman, M., Miyazaki, A. D., and Sprott, D. E. 2010. "Reducing Online Privacy Risk to Facilitate e-Service Adoption: The Influence of Perceived Ease of Use and Corporate Credibility," *Journal of Service Marketing* (24:3), pp. 219-229.

Finney, S. J., and DiStefano, C. 2006. "Non-normal and Categorical Data in Structural Equation Modeling," in *Structural Equation Modeling*. *A Second Course,* G. Hancock and R. Mueller (eds.), Greenwich, pp. 269-314.

Florencio, D., and Herley, C. 2013. "Sex, Lies and Cyber-crime Surveys," in *Economics of Information Security and Privacy III*, New York: Springe-Verlag, Chicago, pp. 35-53.

Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp. 39-50.

Freud, S. 1915. *Repression*, Complete Psychological Works of Sigmund Freud, London: Hogarth.

Gefen, D. 2000. "E-commerce: The Role of Familiarity and Trust," *Omega* (28:6), pp. 725-737.

Gefen, D., Karahanna, E., and Straub, D. W. 2003. "Trust and TAM in Online Shopping: An Integrated Model," *MIS Quarterly* (27:1), pp. 51-90.

Hair, J. F., Black, W. C., Babin, B. J., and Anderson, R. E., 2010. *Multivariate Data Analysis,* 7th Edition, Pearson.

Hawlitschek, F., Teubner, T., and Gimpel, H. 2016. "Understanding the Sharing Economy-Drivers and Impediments for Participation in Peer-to-Peer Rental," in *Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS),* pp. 4782-4791, Koloa, Hawaii.

Henseler, J., Ringle, C. M., and Sinkovics, R. R. 2009. "The Use of Partial Least Squares Path Modeling in International Marketing," *Advances in International Marketing* (20:1), pp. 277-319.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers and Security* (31:1), pp. 83-95.

Jardine, E. 2015. "Global Cyberspace is Safer Than You Think: Real Trends in Cybercrime," *Global Commission on Internet Governance Paper Series* (16).

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G. M., Paxson, V., and Savage, S. 2008. "Spamalytics: An Empirical Analysis of Spam Marketing Conversion," in *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS '08), ACM*, New York, USA, pp. 3-14.

Kehr, F., and Kowatsch, T. 2015. "Quantitative Longitudinal Research: A Review of IS Literature, and a Set of Methodological Guidelines," in *Proceedings of the Twenty Third European Conference on Information Systems (ICIS)*, Münster, Germany.

Krasnova, H., Günther O., Spiekermann, S., and Koroleva K. 2009. "Privacy Concerns and Identity in Online Social Networks," *Identity in the Information Society* (2:1), pp. 39-63.

Kwon, W.S., and Lennon, S. J. 2009. "What Induces Online Loyalty? Online versus Offline Brand Images," *Journal of Business Research* (62:5), pp. 557-564.

Lazarus, R. 1966. *Psychological Stress and the Coping Process*, New York: McGraw-Hill.

Lee, M. 2009. "Factors Influencing the Adoption of Internet Banking: An Integration of TAM and TPB with Perceived Risk and Perceived Benefit," *Electronic Commerce Research and Applications* (8:3), pp. 130-141.

Lee, Y., and Kozar, K. A. 2005. "Investigating Factors Affecting the Adoption of Anti-Spyware Systems," *Communications of the ACM* (48:8), pp. 72-77.

Lee, Y., and Larsen, K. R. 2009. "Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software," *European Journal of Information Systems* (18:2), pp. 177-187.

Lessig, L. 1998. "The New Chicago School," *The Journal of Legal Studies* (27:S2), pp. 661-691.

Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* (33:1), pp. 71-90.

Liang, H., and Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems* (11:7), pp. 394-413.

Lim, N. 2003. "Consumers' Perceived Risk: Sources versus Consequences," *Electronic Commerce Research and Applications* (2:3), pp. 216-228.

Lin, K., and Lu, H. 2011. "Why People Use Social Networking Sites: An Empirical Study Integrating Network Externalities and Motivation Theory," *Computers in Human Behavior* (27:3), pp. 1152-1161.

Maier, C., Laumer, S., Weinert, C., and Weitzel, T. 2015. "The Effects of Technostress and Switching Stress on Discontinued Use of Social Networking Services: A Study of Facebook Use," *Information Systems Journal* (25:3), pp. 275-308.

Martins, C., Oliveira, T., and Popovic, A. 2014. "Understanding the Internet Banking Adoption: A Unified Theory of Acceptance and Use of Technology and Perceived Risk Application," *International Journal of Information Management* (34:1), pp. 1-13.

McKnight, D.H., Choudhury, V., and Kacmar, C. 2002. "The Impact of Initial Consumer Trust on Intentions to Transact with a Website: A Trust Building Model," *The Journal of Strategic Information Systems* (11:3), pp. 297-323.

Merton, R.K. 1968. "The Matthew Effect in Science," *Science* (159:3810), pp. 56-63.

Montazemi, A., and Saremi, H. 2013. "Factors Affecting Internet Banking Pre-usage Expectation Formation," in *Proceedings of the 46th Hawaii International Conference on Information System Science (HICSS),* pp. 4666-4675.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior towards IS Security Policy Compliance," in *Proceedings of the 40th Annual Hawaii International Conference on System Science*, Waikoloa, Hawaii, p. 156b.

Pavlou, P.A. 2003. "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International Journal of Electronic Commerce* (7:3), pp. 69-103.

Recker, J. C. 2016. "Reasoning about Discontinuance of Information System Use," *Journal of Information Technology Theory and* Application (17:1), pp. 41-66.

Riek, M., Böhme, R., and Moore, T. 2016. "Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance," *IEEE Transactions on Dependable and Secure Computing* (13:2), pp. 261-273.

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology* (91:1), pp. 93-114.

Shapiro, C., and Varian, H. R. 1998. *Information Rules: A Strategic Guide to the Network Economy*, Harvard Business Press.

Singer, J.D., and Willett, J. B. 2003. *Applied Longitudinal Data Analysis*, New York, USA: Oxford University Press.

Srisawang, S., Thongmak, M., and Ngarmyarn, A. 2015. "Factors Affecting Computer Crime Protection Behavior," in *PACIS Proceedings* (31).

Steel, D., and McLaren, C. 2008. *Design and Analysis of Repeated Surveys*. Working Paper 11–08. Center for Statistical and Survey Methodology, University of Wollongong.

Straub, D., Boudreau, M., and Gefen, D. 2004. "Validation Guidelines for IS Positivist Research," *Communications of the Association for Information Systems* (13:24), pp. 380-427.

Tarafdar, M., D'Arcy, J., Turel, O., and Gupta, A. 2015. "The Dark Side of Information Technology," *MIT Sloan Management Review* (56:2), pp. 61-70.

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., and Ragu-Nathan, T. 2007. "The Impact of Technostress on Role Stress and Productivity," *Journal of Management Information Systems* (24:1), pp. 301-328.

Tourangeau, R., Rips, L. J., and Rasinski, K. 2000. *The Psychology of Survey Responses*, 1st Edition, Cambridge: Cambridge University Press.

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., and Cotten, S. R. 2016. "Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective," *Computers and Security* (59), pp. 138-150.

Turel, O. 2015. "Quitting the Use of a Habituated Hedonic Information System: A Theoretical Model and Empirical Examination of Facebook Users," *European Journal of Information Systems* (24:4), pp. 431-446.

Wahlberg, A. A. F., and Sjoberg, L. 2000. "Risk Perception and the Media," *Journal of Risk Research* (3:1), pp. 31-50.

Walsh, G., Hille, P., and Cleveland, M. 2016, "Fearing Online Identity Theft: A Segmentation Study of Online Customers," in *Proceedings of the Twenty Fourth European Conference on Information Systems (ICIS*), Research-in-Progress Papers, Istanbul, Turkey.

Yu, C., and Muthen, B. 2002. "Evaluation of Model Fit Indices for Latent Variable Models with Categorical and Continuous Outcomes," presented at the *Annual Meeting of the American Educational Research Association*, New Orleans, LA.