THE UNIVERSITY of EDINBURGH

Edinburgh Research Explorer

“Why would money protect me from cyber bullying ?”

A mixed-methods study of personal cyber insurance

Citation for published version:
Jain, R, Hrle, T, Marinetti, M, Jenkins, A, Böhme, R & Woods, DW 2024, “Why would money protect me from cyber bullying ?”: A mixed-methods study of personal cyber insurance. in *2025 IEEE Symposium on Security and Privacy.* IEEE Symposium on Security and Privacy, Institute of Electrical and Electronics Engineers, 46th IEEE Symposium on Security and Privacy, San Francisco, California, United States, 12/05/25.

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
2025 IEEE Symposium on Security and Privacy

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

OPEN ACCESS

Download date: 25. Jan. 2025

"Why would money protect me from cyber bullying ?": A Mixed-Methods Study of Personal Cyber Insurance

Rachiyta Jain*, Temima Hrle*, Margherita Marinetti†, Adam Jenkins‡, Rainer Böhme†, and Daniel W. Woods*§
*University of Edinburgh, United Kingdom
{rachiyta.jain, temima.hrle, daniel.woods}@ed.ac.uk
†University of Innsbruck, Austria
{margherita.marinetti, rainer.boehme}@uibk.ac.at
‡King's College London, United Kingdom
{adam.jenkins@kcl}.ac.uk
§British University in Dubai, United Arab Emirates

***Abstract*—Individuals can become victims of security incidents, privacy violations, online scams, and social media abuse. In addition to prevention, users should create response strategies in case misfortune strikes. To better understand response to digital harm, we conducted the first study of personal cyber insurance in the US and the UK.**

We explored the supply-side via a content analysis of 24 cyber insurance policies. The results show personal cyber insurance compensates security, privacy and fraud incidents, with a slim majority also covering cyberbullying. Comparing these results to prior work, we find that coverage in the US and UK has significant differences to coverage in Germany.

We study the demand-side via a survey distributed to 584 participants with an even US/UK split. Just 1.6% of respondents have cyber coverage and 8.5% are aware of the product. We introduce the concepts of risk uncertainty and coverage uncertainty, finding both are prevalent for personal cyber insurance. Studying coverage uncertainty, we discover a gap between insurers and participants, which is broadest for online fraud and narrowest for identity theft and cyberbullying. Turning to risk uncertainty, we discovered that in the aggregate users are relatively well calibrated regarding the frequency of different incidents. Individuals estimate that fraud incidents have the greatest impact, followed by security and privacy incidents. Cyberbullying has very low estimated impact. Regarding purchasing a policy, participants raised uncertainties about contractual details, reporting requirements, victimization statistics, and access to security solutions.

1. Introduction

Widespread adoption of computer systems and digital services has brought many benefits, but also created new types of harmful incidents. These include ransomware [1], data breaches [2–5], scams [6, 7], and online abuse [8]. These incidents cannot be eliminated with current technical mitigations [8, 9].

This reality motivates an understanding of response strategies. Strategies can involve playbooks [10], digital forensics [11], crisis communications to preserve reputation [12], restoring systems and data from back-ups [13], and—the focus of our paper—insurance to smooth the financial consequences [14].

Corporate cyber insurance has existed since the late 1990s [15]. The product covers incidents including data breaches, system outages, ransomware, and even liability arising out of content published on the Internet [14]. Cyber insurance influences incident response (IR) by pushing policyholders to use in-network IR firms, often coordinated by a lawyer [16]. Insurance has been less consistent in improving pre-breach cybersecurity [17–19], although the ransomware epidemic forced insurers to revise their business model [20]. For these reasons, cyber insurance is becoming an important part of how cyber risk is managed.

Research into cyber insurance has almost exclusively focuses on corporate insurance. A systematic review diagnosed a "paucity" of research on personal cyber insurance [21]. This matters because individuals and corporations likely require different products. This can be illustrated by considering specifics risks—corporations are not susceptible to romance scams, for example [22]—but structural differences are more relevant to theories of digital harm.

In the modern economy, firms have a dual security mandate in protecting their own intellectual property and computer systems (first-party risk), while also upholding responsibilities to customers and shareholders (third-party risk). The importance of managing third-party risk can be seen in nine figure liability awards following high-profile corporate data breaches [23]. It is unclear whether individuals are exposed to third-party cyber risk in the same way.

Another difference is that corporations can afford to hire specialists to manage security, and also to negotiate insurance contracts [24]. In contrast, users face challenges in implementing digital security advice related to time constraints, technical complexity, and a sense of futility [25]. It

is natural to ask whether users face uncertainty about cyber insurance. This seems likely given the challenges individuals face in evaluating even well-established products such as health insurance [26].

We conduct a mixed-methods exploratory analysis of this novel product to address the following questions:

RQ1 Which incidents does personal cyber cover ?
RQ2 How do users estimate the associated risks ?
RQ3 What coverage uncertainties do users have ?

We conduct a two-stage content analysis of 24 cyber insurance policies. The first stage inductively identified incidents from the policies, and the second stage analyzed which policies offer coverage (**RQ1**). We then designed a survey instrument that asked 584 individuals to estimate the frequency and impact of the incidents from the content analysis (**RQ2**). We also probe users' understanding of each incident, and uncertainties about the wider product (**RQ3**).

Contributions We conduct the first study of personal cyber insurance in the US and the UK. Policies cover a diverse set of incidents that span security (cyber attack and cyber extortion), privacy (data breach), fraud (online fraud and identity theft) and even cyberbullying. US/UK coverage differs significantly from German policies [27], which motivates future studies of how coverage differs across international markets and over time. The product is still in the early adopter phase—1.6% of respondents have cyber coverage and 8.5% are aware of the product.

Our conceptual distinction between risk uncertainty and coverage uncertainty helps to explain two challenges insurers and users must jointly overcome. To manage digital harm, users need resources to reduce quantitative risk uncertainty, as evidenced by respondents under-estimating the impact of cyberbullying (median of $0) and over-estimating the frequency of cyber extortion. This is partly solved by reducing coverage uncertainty, for example insurers can explain why they compensate the non-trivial cost of moving homes as part of bullying coverage. Addressing both uncertainties can help users understand why money is useful in responding to cyberbullying, and also create digital risk strategies that address security, privacy, and fraud incidents.

Roadmap The next section provides the necessary background on insurance and justifies the research questions. Section 3 describes our empirical strategy and methods. Sections 4–6 present the results, organized by research question. Section 7 places our work in the context of previous studies. Section 8 discusses implications, limitations, and directions for future work. Section 9 offers conclusions.

2. Background

Before discussing how insurance fundamentally differs from other cybersecurity solutions, it is worth first identifying similarities. Cyber insurance is a service purchased from an external provider in exchange for a yearly premium, much like how security SaaS solutions can be bought by subscription. Insurers also collect security information about policyholders through questionnaires [28] and external network scans [29], much like how both can be used for supply chain management [30] and compliance audits [31]. The key difference is that in the technology industry, security services are the product, whereas insurance offers a financial product, namely the promise of financial compensation, and security services are a means of more sustainably delivering the core value proposition.

Insurers' promise of financial compensation creates novel theoretical considerations because of two forms of uncertainty. First, *risk uncertainty* results from not knowing whether the policyholder will suffer a loss and what size it will be. This means insurers have uncertain profits, whereas a cybersecurity provider receives a guaranteed subscription fee regardless of whether the customer suffers a loss. Second, *coverage uncertainty* results from not knowing whether and what proportion of the loss will be compensated by the insurer. Coverage uncertainty is reduced—but not eliminated—by the insurance policy contract, which tries to describe the claims that will be paid and those that will not. However, policies often contain ambiguities that only become clear when the claim is made [32].

These uncertainties play out differently for insurers and policyholders. Insurers are professional risk managers, unlike most policyholders. When it comes to risk uncertainty, policyholders lack global information about the frequency and impact of losses. This can lead to sub-optimal decisions like choosing limits that are too high (wasting money) or too low (potential catastrophe). However, policyholders have secret information about their risk profile, which can create adverse selection, in which policyholders use secret information to decide whether to buy insurance [33].

In contrast, insurers access global information by building actuarial models that calculate the probability of losses, adjusted for the policyholder's characteristics [34]. Insurers benefit from the law of large numbers, which makes total claims across a portfolio of policies more predictable. Insurers' main risk uncertainty concerns catastrophic risk, the potential for one event to cause losses across multiple policyholders [15, 35]. Such events can bankrupt insurers if they do not hold enough funds in reserve.

Coverage uncertainty is more problematic for policyholders because policies are legalistic documents drafted by the insurer, and the insurer makes the initial decision on whether to pay. These issues are compounded by the reality that most individuals do not read contracts [36, 37]. To reduce this asymmetry, insurance law defaults to providing coverage when the policy is ambiguous [32].

Summary The promise of compensation for uncertain future losses is the defining feature of insurance. In evaluating a specific insurance product, policyholders face *risk uncertainty* about the size and frequency of losses, and *coverage uncertainty* about whether the policy will pay-out on a specific loss. These issues are likely to be compounded by personal cyber insurance given the novelty of both the underlying risk and the insurance product. These considerations motivate our study into individuals' risk uncertainty (**RQ2**) and coverage uncertainty (**RQ3**).

3. Methods

We conducted a mixed-methods multi-stage study to understand risk and coverage uncertainty in the context of personal cyber insurance. Even though we are primarily interested in the demand-side (**RQ2–3**), the lack of prior work meant we had to first study the supply-side in order to probe users about risks that are covered by actual policies (**RQ1**). Stage 1 identified what is commonly covered by conducting an inductive content analysis of 24 real-world insurance policies, which is described in Section 3.1. This stage was conducted by two trained lawyers who both analyzed all policies. The themes from this iterative analysis directly informed the design of a survey instrument, which is described in Section 3.2. Stage 2 collected survey responses from 584 participants recruited from a crowdsourcing platform. Table 5 in the Appendix contains demographic information. Figure 1 visualizes this empirical strategy.

3.1. Content Analysis

3.1.1. Collecting Insurance Policies. We collected US and UK personal cyber insurance using the following data sources: (i) regulatory databases; (ii) a web search engine; and (iii) insurer websites. Data was collected from October 2021 to September 2022. It took so long because of the high volume of search results, which are dense legal contracts. In particular, the regulatory database required manually processing hundreds of regulatory filings, each containing 1-tens of PDFs. We opted against scraping files to respect the platform's terms of service.

We included policies sold to individuals, and excluded policies for organizations. For the US, we only collected policies that had been approved by the regulator, which resulted in 21 policies. Insurance is regulated differently in the UK, which meant there was no information on regulatory approval, so we relied on policies collected from the web. We only identified 3 UK policies, which likely reflects both a less developed market and that UK regulators do not force transparency like in the US.

We extracted US policies from the System for Electronic Rates & Forms Filing (SERFF), which contains insurance policies approved by US states. We searched manually in the four largest US states in line with prior work.[1] Our search terms included "cyber", "personal cyber", "individual cyber", and "consumer cyber." We directly extracted 15 relevant policies from SERFF. We found a further 6 policies by searching for specific insurers' policies via web searches (see Appendix A for the list), and then finding the cyber policy as an optional endorsement under that insurer's home insurance filing in SERFF. It was infeasible to search all home insurance policies due to the size of the market.

There is no equivalent regulatory database to SERFF in the UK. Instead we relied on web searches, acknowledging these policies may not have been approved by a regulator. We identified 52 unique insurers operating in the UK (see Appendix A). We then queried a web search engine with *'insurer website' 'keywords'*, which yielded two policies. We inputted the same keywords into the insurer's websites if a search function existed, which yielded one more policy.

3.1.2. Policy Analysis. We adopted the two-stage approach used in a study of corporate cyber insurance [14]. To create a codebook, the first stage inductively identified digital harm incidents from the policies. Since each policy uses different terms and definitions because the products are not yet standardized, we grouped similar units under progressively higher-level themes. For example, "Transfer of Funds" was directly extracted from a policy. It was first grouped under "Fraud and Cyber Crime", which was updated to "Deceptive Funds Transfer", which belongs to the final theme "Online Fraud". This process terminated with six high-level themes that could not be merged without losing fidelity to the underlying data.[2]

The second stage involved building a codebook (see Appendix B), and then classifying whether each policy covered each theme and sub-theme. An insurance policy is an indivisible unit of analysis because internal references can change coverage, such as when an exclusion or defined term modifies a coverage statement. The sub-themes consisted of specific costs covered under each theme, such as ransom payment under Cyber Extortion. The two coders agreed on 98.4% (US) and 100% (UK) of the 144 classifications (covered vs not) on high-level themes. If a theme was covered, sub-theme agreement ranged from 87% to 96% (US) and 83% to 100% (UK) depending on the theme.

3.2. User Survey

The findings from the content analysis informed the key questions in our survey instrument, which was distributed to individuals between June and September 2023.

3.2.1. Survey Design. Our survey instrument had three main sections: (M1) qualitative understanding of covered incidents; (M2) quantitative risk estimates of covered incidents; and (M3) insurance purchasing and attitudes. We asked for demographic information first in order to elicit risk estimates in the participant's local currency. We also collected a lightweight scale, SA-6 [40], of security attitudes (see Table 3 in the Appendix). We included two attention checks, one instructed response item and one red herring.

The first two main sections asked participants about each of the high-level themes/incidents identified in the content analysis, such as cyberbullying and identity theft (see Section 3.1). To study coverage uncertainty (M1), we asked participants to define each incident and rate their perceived difficulty in doing so. We then presented a definition from

1. Research into corporate cyber insurance also searched the 3 or 4 largest states [14, 38, 39]. Policies are highly similar across states [14], and so there are diminishing returns to searching additional states.

2. For example, a non-insurance reader correctly observes that Identity Theft is a subset of Online Fraud. However, we did not merge these themes because most policies have a standalone section for Identity Theft.

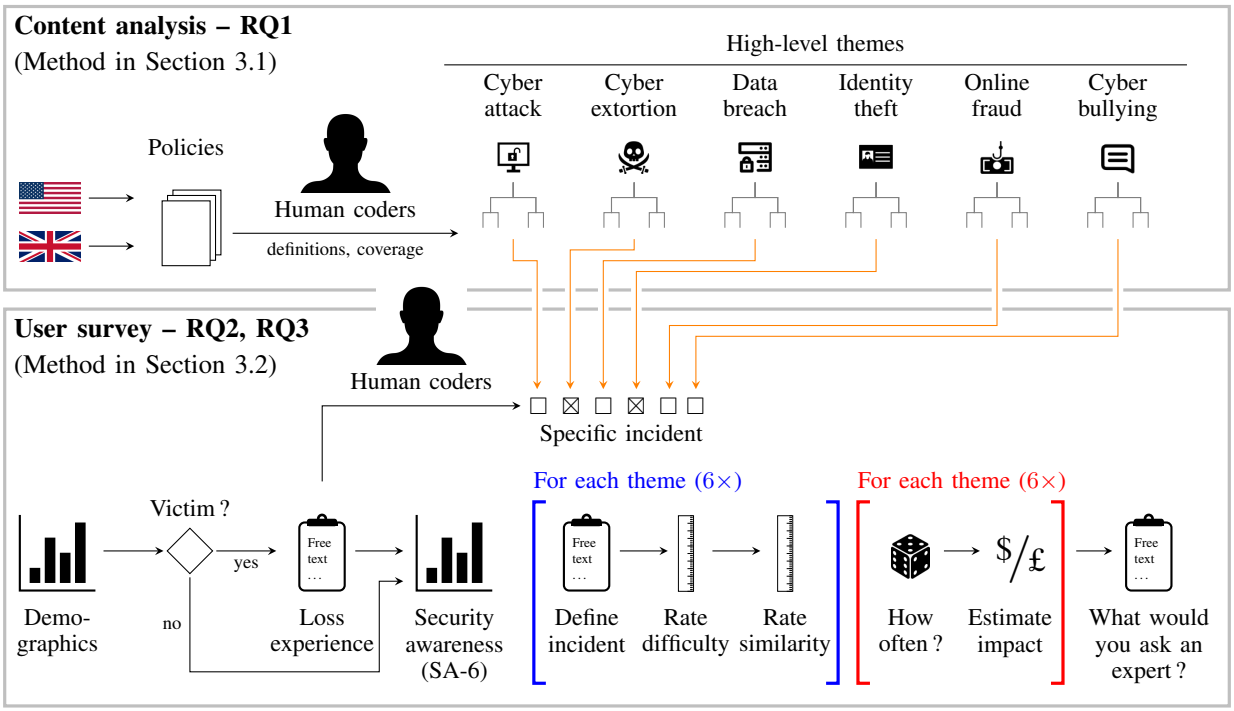

Figure 1. Overview of our research design. The content analysis of the supply-side informed the questionnaire design for the demand-side survey.

a real policy, asking them to rate the similarity to their definition. We collected self-reports because a participant can more accurately assess their own understanding compared to a researcher assessing this based on a definition provided under time-pressure. We randomized the order of questions about covered incidents in both M1 and M2.

To study risk uncertainty (M2), we asked about the likelihood and impact of each covered incident. For likelihood, we presented 5 options with a qualitative and numerical option, such as "Rarely (once in 50 years)". For impact estimates, the participant used a sliding scale from 0 to 100k with a granularity of around 200 units in the local currency. We chose a maximum at the upper-end of realistic losses, accepting the estimates would be right-censored. This ensures participants can submit a reasonable granularity and avoids anchoring on an extreme upper bound.

The third main section (M3) asked whether the respondent has coverage for cyber incidents, offering 'Do Not Know' as an option. Finally, we asked an open question: "Before purchasing [personal cyber insurance], if you had an opportunity to speak to an expert, what would you ask?"

3.2.2. Recruitment. We recruited US and UK participants using Prolific. Prior work reveals crowdsourcing is commonly used in security and privacy research [41], and there is "tempered support" for the generalizability of findings [42]. Data from Prolific is deemed superior to MTurk and "generally representative for questions about user perceptions and experiences" [43]. This is appropriate for our exploratory study of perceptions.

We recruited 584 participants with an even split of US and UK. We discarded 19 responses for failing an attention check or completing in an unusually short time, although the participants were still paid. We only offered the survey in English, and allowed participants to complete on any device. A researcher error meant we did not screen for gender in the UK sample, which resulted in a bias (63%) towards participants who identify as female.

3.2.3. Survey Analysis. We conducted both qualitative and quantitative analysis. First, we coded the descriptions of the incidents that victims had personally suffered into 8 non-exclusive categories of cybercrime (see Section B for the codebook). To test reliability, a second coder analyzed a subset and achieved a high Cohen's Kappa score ($\kappa = 0.84$). We also inductively coded the free-text on uncertainties about personal cyber insurance.

Second, we ran regressions to understand associations between risk estimates and cyber risk experience, awareness, and comprehension. We estimate four specifications for each incident from the content analysis, two each for *expected frequency* and *estimated impact* as dependent variables, with and without controls. For expected frequency, we use the response to the question ("How often would you expect to experience each of the following? – *[incident]*") and fit an ordered probit model with maximum likelihood to account for the ordinal nature of the data. To calculate the pseudo R^2 goodness of fit metric, we assume equidistance and refit with ordinary least squares (OLS). We proxy estimated impact with the logarithm of the dollar amount entered with the

	Security & Privacy			Scams		Social media
Incident (Theme)	Cyber attack	Cyber extortion	Data breach	Identity theft	Online fraud	Cyber-bullying
Policies with coverage	100%	100%	63%	92%	100%	54%

Figure 2. Incidents that are covered by the policies in our sample.

sliding scale in response to the question "How much money would you need to cover your losses [...]" for the specific incident, and estimate with OLS. UK participants' responses were converted from pounds to dollars. We considered a specification with untransformed dollar amounts, but the log transformation produced less skew in the residuals.

All specifications include three independent variables. *Loss experience* is a binary indicator taken from the coded descriptions. It takes the value one for participants whose free-text description of their cyber threat experience matches the specific incident, and zero otherwise.[3] *Security awareness* is the unweighted mean calculated from the SA-6 scale. *Perceived difficulty* is the participant's self-assessment of how difficult it was to define the incident, interpreted as an equidistant cardinal scale. As controls, we include country, gender identification, age group, and two binary indicators that split the education and income categories approximately at their median values. We kept the specifications unchanged for all incidents to prevent model selection bias. Detailed regression results are reported in the Appendix.

3.3. Ethics

We obtained ethical approval for the second stage from our Institutional Review Board. The first stage was deemed low risk because it was not personal data, and we respected the websites' terms of service. For the second stage, our main concerns were data management, trigger warnings, and fair compensation. We collected informed consent, and our information sheet included a warning that we would ask questions about cyberbullying and online fraud, which may cause distress to victims. We compensated participants by multiplying the UK national living wage (above both the UK and US federal minimum wage) with our estimated time of completion, namely 20 minutes. The participants' mean completion time was much lower, so we believe compensation was fair. We followed a secure data management plan.

4. Personal Cyber Insurance Coverage (RQ1)

This section identifies which incidents are covered by personal cyber insurance. Our findings are the cyber equivalent of fire, flood, or mold under a property insurance policy.

3. As no participant reports an experience of cyberbullying, we replace this variable with the general experience of victimization ("Have you personally been the victim of a breach of security (e.g., hacking, theft of personal data)?").

Figure 2 shows all personal cyber insurance policies cover losses arising out of security, privacy, and fraud incidents. A slim majority of policies (54%) also covered social media harm from *Cyberbullying* incidents. The rest of this section explores how these different types of incidents are covered, as well as the costs that can be compensated.

Security & Privacy Incidents. The policies covered three types of security and privacy incidents, namely *Cyber Attack*, *Cyber Extortion*, and *Data Breach*. All policies covered cyber attack incidents, which is defined broadly using the language of computer security. For example, the majority (71%) of US policies include the same definition that mentions "Unauthorized Access" and "viruses, worms, Trojans, spyware and keyloggers". Other policies included variations on this terminology including "Hacking Attack", "Virus", and "Cyber Disruption Occurrence". In terms of the cyber attack costs that are covered, most policies provided coverage for *Data Recovery* and *System Restoration*. US#5 defines system restoration costs as "replacing and restoring computer programs, removing malicious code, and configuration of the device". Two policies cover relocation expenses for the family, likely because these policies name smart homes as a covered system.

All policies cover *Cyber Extortion*, which is defined in terms of the attacker making a threat. One policy defines it as demands for money based on a "credible" threat to commit a cyber attack. Another policy also covers the threat to leak "[the policyholder] or a family member's personal information", which shows *Cyber Extortion* is also relevant to data privacy. The vast majority of policies (83%) cover ransom payments as well as recovery costs, which suggests insurance can incentivize both paying the ransom and recovering from back-up.

Finally, *Data Breach* incidents were covered by the majority (63%) of policies. One fundamental question was whether the policy assumed the policyholder was a custodian of other people's data, or whether the policy assumed the victim's data was breached. Most policies used the custodian approach, which has links to the theory of interdependent privacy [44, 45]. Six policies used the following definition: "Data breach means the loss, theft, accidental release or accidental publication of 'personally identifying information' or 'personally sensitive information" as respects to one or more affected individuals". These policies pay for a forensics investigation into the breach, as well as legal advice on how to respond, much like with corporate insurance [14, 16]. In contrast, a policy (US#6) covers the scenario in which the policyholder's data was lost by someone else. This policy covers the policyholder's mental health counseling, lost wages, relocation expenses, and PR consultancy fees.

Fraud Incidents. All personal cyber insurance policies cover *Online Fraud*, which captures incidents where a cyber criminal socially engineers the victim for the criminal's financial gain. The most common definition covered events including: (i) unauthorized use of a card or bank account registered to the insured; (ii) the forgery of a check; (iii) acceptance of counterfeit currency; and (iv) "An intentional and criminal deception of an 'insured' to

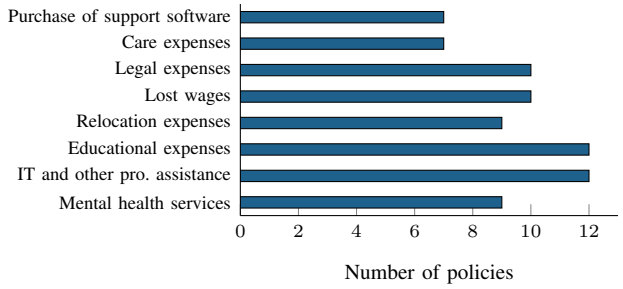

Figure 3. Specific costs covered related to Cyberbullying.

TABLE 1. SUMMARY STATISTICS OF CODED ATTACK EXPERIENCES.

Type of experience	Cases	% of victims* Total	UK	US	Median # chars
Cyber attack	24	7.4	8.7	6.5	75
Cyber extortion	6	1.9	2.2	1.6	188
Identitify theft	14	4.3	3.6	4.9	100
Financial fraud	113	35.0	34.8	35.1	96
Data breach	113	35.0	26.8	41.1	102
Phishing	17	5.3	8.7	2.7	111
Online account compromise	91	28.2	33.3	24.3	93

*Columns do not sum to 100 because experiences are non-exclusive.

induce the 'insured' to part voluntarily with something of value". The policies use diverse terms including: "financial fraud"; "fraud event"; "forgery"; "cyber crime event"; "cyber crime"; "cyber financial fraud occurrence"; "funds transfer event"; and "deceptive transfer fraud".

Most insurers require that the fraud is "wholly or partially perpetrated through a 'computing device"'. All insurers offering *Online Fraud* coverage will reimburse the direct financial loss, namely the "amount fraudulently taken from the insured" (US#8). Another policy (US#4) covers costs related to legal issues flowing from the fraud: "salary lost; attorney fees; lawsuits protection; removal of criminal or civil judgments or any challenge to the information in a consumer credit report".

Most policies also cover *Identity Theft* incidents, in which "someone illegally uses your identity without your consent" (US#6). The typical definition focused on the criminal's actions, not how the personal information (e.g. social security number) was obtained. *Identity Theft* coverage often contains a list of specific costs that are covered, unlike the vague costs that are covered under *Cyber Attack* or *Online Fraud*. For example, 45% of the policies that covered identity theft would pay for re-filing applications, attorney fees, and notarizing affidavits. Such costs are incurred when communicating with bureaucratic institutions in order to recover identity. Some insurers also compensate the disruption to individuals' lives by covering lost wages (41%), and child or elderly care costs (36%). Unsurprisingly, personal cyber insurance covers similar costs to those covered under standalone personal identity insurance [39].

Social Media Incidents. We were surprised to discover that a slim majority (54%) of products covered *Cyberbullying*. All policies require at least two cyberbullying incidents to have occurred, although what constitutes an incident is not clear. Communications are required to be electronic, such as "texting, instant messaging, chat rooms, photos and other content posted on social media" (US#15). Some insurers used definitions that required serious negative consequences, beyond simply receiving messages. For example, US#3 required either "debilitating shock, mental anguish, or mental injury that has been diagnosed by a licensed physician" or "inability of you or a family member to attend school or work full-time for more than one week".

Policies do not directly compensate mental anguish, but instead cover the cost of responding to the bullying (see Figure 3). Covered costs include paying for professional services and compensating victims for lost wages and alternative care arrangements. In the extreme, some policies cover private education fees and relocation costs if the family has to move school or home.

Summary (RQ1) Personal cyber insurance is designed to cover not only security and privacy incidents, but also frauds and social media abuse. The diversity of definitions raises the potential for coverage uncertainty, which we explore in Section 6. Some incident definitions are broad, such as cyber attack or online fraud, to cover a range of exploitation techniques and social engineering pre-texts. Other definitions focus on specific incidents like cyber extortion, identity theft, and cyberbullying. Specific incidents are associated with clearer descriptions of coverage.

Personal cyber insurance has some similarities to other digital insurance coverage. The identity theft coverage is highly similar to the standalone identity insurance products that insurers have sold since the 2000s [39]. Similarly, the security and privacy coverage—cyber attack, cyber extortion, online fraud, and data breach—has clear parallels to corporate cyber insurance [14]. However, there are subtle differences due to how incidents impact firms and individuals differently. The closest coverage to cyberbullying is corporate media liability coverage [14]. The key difference is that media liability covers legal costs when a firm's internet publishing harms third-parties, whereas personal cyber insurance covers first-party costs when the policyholder is harmed by third-parties' internet content.

5. Understanding Risk Uncertainty (RQ2)

We asked respondents to estimate the frequency and impact of each incident, and estimated past victimization by coding free-text descriptions of incidents (see Section 3.2.3).

Historic Experience We found that a majority (57.2%) of the participants had been victims of a cyber incident. 45% of victims suffered an incident in the last year. This suggests an annual victimization rate of 25%, which is high relative to prior work [46, 47]. One explanation is that we asked about generic cyber incidents, whereas, for example, Breen et al. [46] asked about specific crimes like non-delivery fraud and extortion.

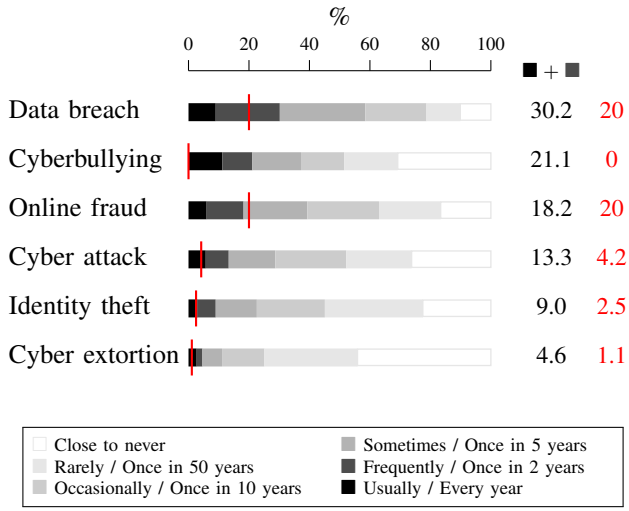

Figure 4. Expected and actual frequency of incidents. Bars show responses to the question *"How often would you expect to experience each of the following?"*. Red text/markers show the percentage of the population who experienced an incident that was coded as belonging to the event type.

After labeling the victim's descriptions of incidents[4], Table 1 shows participants were most likely to experience financial fraud and data breaches. Identity theft and cyber extortion are comparably rare. Comparing victimization rates to those found in prior work, our US participants experienced cyber extortion (1.1% vs 0.1%) and online fraud (20% vs 12% for banking vs credit-card fraud) more often than respondents in a representative survey of individuals in the US [46]. In contrast, 41% of our US participants reported being a victim of a data breach, whereas this was 73% in another study [3]. These discrepancies are typical when comparing cybercrime surveys. Differences often result from the wording of survey questions [47, 48].

Estimated Frequency Turning to risk uncertainty, Figure 4 shows how participants estimate the frequency of different incidents. Participants believe that cyber extortion is the least likely to occur, which is correct based on our survey (see Table 1) and prior work [46]. The participants also correctly estimate that identity theft is a comparatively rare cyber crime [47]. Data breach is believed to be the most likely to occur, even though online fraud was equally as frequent in the participants' loss experience (see Table 1).

In order to understand how individual characteristics impact estimated frequency, we ran various regressions (see Section 3.2.3 for the specifications), which can be found in the Appendix. Table 2 summarizes how each independent variable impacts the estimated frequency/impact of each of the six incidents. Prior loss experience is associated with increased estimated frequency across four of the six incidents. A plausible explanation is that these victims correctly estimate they face higher risk, either because they take less precautions or have higher exposure to digital risk. This

4. These labels are non-exclusive because one experience can have multiple components, such as a data breach leading to identity theft.

TABLE 2. SUMMARY OF FACTORS INFLUENCING EXPECTED FREQUENCY AND ESTIMATED IMPACT.

	Loss experience		Security awareness		Perceived difficulty	
Incident type	freq.	impact	freq.	impact	freq.	impact
Cyber attack	+			+		
Cyberbullying	+			+		+
Cyber extortion			+			
Identity theft			+			
Online fraud	+					
Data breach	+			+		

All effects are statistically significant at the $p \leq 0.05$ level (or higher) after controlling for socio-demographics variables. We did not find any significant negative effects. See the Appendix for full regression models.

creates the potential for adverse selection, because prior experience is currently a secret data point given insurers cannot ask about prior cyber claims due to low adoption. An alternative explanation is that victims over-estimate frequency due to the ease of remembering the incident that they suffered (availability bias).

Respondents with higher security awareness had higher estimated frequency of identity theft and cyber extortion, but not the other four incidents. This means the estimated frequency of all incidents had a statistically significant relationship with either loss experience or security awareness, but not both. Given that cyber extortion and identity theft are the rarest incidents, there may not have been enough observations to establish a relationship. This would be consistent with an interpretation in which both loss experience and security awareness are related to an unobserved confounding variable, for which loss experience is a more reliable proxy.

Still, we do not believe these regressions provide enough explanatory power—the pseudo R^2 only exceed 0.05 for online fraud and data breach—to confidently say much more than 'expected frequencies are heterogeneous and difficult to predict'. For example, the regressions show the difficulty of defining an incident has no statistically significant relationship to the expected frequency of that incident.

Estimated Impact We also asked respondents to estimate the cost of each cyber loss event on a sliding scale. Very few participants chose the maximum possible value ($100k/£100k), which suggests the design choice of a sliding scale with an upper bound did not unduly right censor the results. However, the absolute value of estimates is likely to be anchored on this value [49]. For this reason, we focus on the relative ranking of different types of harm.

The severity estimates follow the groupings we introduced in Section 4—namely social media (cyberbullying), security and privacy harms (data breach, cyber attack, and cyber extortion), and fraud (online fraud and identity theft)—with each group displaying a similar distribution of estimates. One interesting finding is that, for all incidents, there is no statistically significant difference between the median impact estimate of victims and non-victims. This means prior experience is linked to increased perceived like-

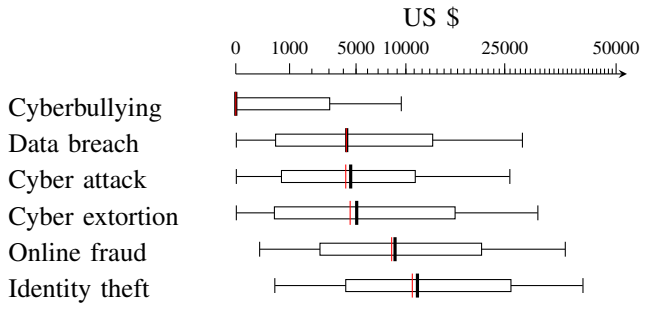

Figure 5. Self-reported compensation needed to cover each incident. Black bars show the sample median ($N = 565$). Red markers are medians of the 323 self-reported cybercrime victims. The differences are not statistically significant at the 5 % level (Mann–Whitney test). Boxes show quantiles and ranges are 10 % and 90 % percentiles. Note the non-linear scale ($\propto \sqrt{\text{US \$}}$).

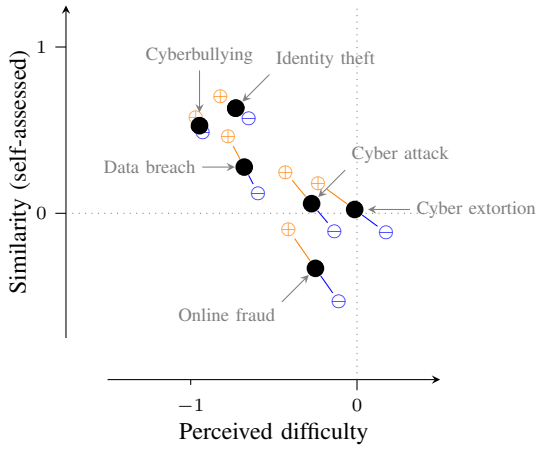

Figure 6. Perceived difficulty of defining an incident versus self-reported similarity with a definition from a real policy. Scatterplot of means per threat. Orange markers ⊕ show means of participants who score above median on the SA-6 security awareness scale. Blue markers ⊖ are the means of the opposite subsets. Dotted lines indicate the midpoints of scales.

lihood of cyber losses, but not increased perceived impact. However, security awareness was associated with higher severity for half of the incidents (see Table 2).

Participants believed cyberbullying was significantly less damaging than all other incidents. The median estimate was zero and the lowest non-zero estimate ($20) was at the 52nd percentile. Notably, participants who found cyberbullying harder to define also expected it to have a greater impact ($p \leq 0.001$, see Table 7). This is likely because the direct harm is emotional, which is difficult to compensate. Notably, most of the insurer costs are related to the response, such as moving home or school. It could be that participants are estimating the impact of less severe cyberbullying incidents.

The security and privacy incidents all display a similar distribution of impact estimates. This grouping is by no means natural given cyber attack and cyber extortion involve the compromise of the individual's computer systems, whereas data breach involves compromising the security of a third-party who holds the individual's personal data. Cyber extortion displays the largest tail of these incidents, with the 75% and 90% quantiles exceeding $10k.

Finally, users believe financial frauds are most impactful. Again they can be distinguished based on whether the respondent is defrauded in online fraud, or a third-party who think they are interacting with the victim, such as a bank, is defrauded in identity theft. Participants believe identity theft is more harmful, with higher median and quantiles.

Summary (RQ2) There is considerable uncertainty about the frequency and impact of covered incidents. The aggregated expected frequency is relatively well-calibrated with both loss experience in our sample and also in prior work [46, 47]. However, a minority (4.6%) of respondents believe cyber extortion happens with over 50% probability, even though it occurs with frequency 0.1% in a representative survey [46]. Turning to severity, participants estimate that online frauds are more impactful than security and privacy incidents. Cyberbullying was an outlier in that most participants believed incidents had next to no financial impact, overlooking how severe incidents can become.

6. Understanding Coverage Uncertainty (RQ3)

Section 6.1 explores how participants understand the six types of incidents covered by personal cyber insurance. Section 6.2 identifies uncertainties about the product.

6.1. Incident Definitions

Participants were asked to define each incident, and rate the difficulty of doing so. Participants were then asked to self-report the similarity to an actual definition. Figure 6 reveals participants with higher security awareness found it easier to define terms and also had higher self-assessed accuracy in doing so. The gap between high and low-awareness participants was smallest for cyberbullying and largest for cyber extortion and online fraud.

Figure 7 disaggregates the data, and shows participants who have been a victim of any type of incident find it easier to define terms. There is a general correlation between the ease of definition and the similarity to the actual definition, however, Figure 7 reveals interesting exceptions at the level of individual responses. Extreme surprises exist in which a participant believes an incident is *very easy* to define but then discovers their definition is *not at all similar* to the policy definition. Extreme surprises are most common for online fraud, whereas there were no extreme surprises in defining data breach or identity theft. The rest of this section zooms into each type of incident.

Security & Privacy Incidents. Participants experienced most difficulty defining cyber extortion (see Figure 6). Many participants said they did not know, although some follow this with a guess, with one participant correctly guessing "extortion (blackmailing) via online means" and another falsely guessing "maybe where they try and gain your data". Users who correctly define cyber extortion outline threats based on both availability and confidentiality. Availability

based threats invoke ideas like "blocking access" or the promise to "unlock a computer system". The term "encryption" was mentioned in just 1.2% of the definitions of cyber extortion. Other participants focused on confidentiality threats to "post compromising photos" or "release stolen information". These differences matter because lost personal data and reputation damage is much harder to compensate than the cost of recovering or replacing a computer system.

Turning to cyber attacks, definitions were broad, with one participant noting the term was "vague", and another noting that cyber attack "could be any number of things". Indeed, one participant noted they had "got Data Breach and Cyber Attack mixed up!!". This vagueness lead to a broad range of impacts including "DDOS, ransomware or data breach.", "taking down websites", "wip[ing] information", and so on. Many participants used definitions where the victim was not an individual, which explains why one participant observed: "I think of a cyber attack as being more aimed at a government or business".

Most participants identified that data breaches related to sensitive data being leaked, with some explicitly mentioning accidental disclosure. A handful of participants used specific examples of high-profile breaches in their definitions, such as Target, Asda (a UK supermarket chain), and the "Northern Ireland police". A common theme was the failure of companies to act as data custodians, as exemplified by one participant's concise definition of a data breach: "when companies fail to protect personal details". Section 4 showed most policies cover incidents where the individual policyholder suffers a breach, which does not match the participant's mental model of a company being breached.

There was an interesting divide between security definitions based on the role of authorization from the entity who manages the data, and privacy definitions that emphasize the role of permission/consent from the data subject. For example, one participant defined data breach as "sensitive information being shared with parties without your consent", which is common in AdTech [50–52].

Fraud Incidents. Participants reported that their definitions for online fraud were least similar to the policy definitions, despite perceptions that it was only moderately difficult to define (see Figure 6). Some participants suffered extreme surprises after defining it as: (i) "someone pretending to be you"; and (ii) "when someone misrepresents oneself online". The participants judged these were *not at all similar* to the insurance policy definition of "a direct loss of money, securities or cryptocurrency which is fraudulently taken from the insured". A major difference is that both definitions (i and ii) focus on acts not outcomes, whereas the insurance definition focuses on the financial loss.

Participants believe their definitions of identity theft were most similar to the insurance definition (see Figure 6). Despite the perceived similarity, we identified various approaches to defining identity theft. One approach followed the insurance definition by using a scenario where the victim's stolen identity is used to defraud a third-party, typically to "take out loans" or "[to get] a credit card", without compromising the security of existing accounts. In contrast, some participants used account takeover scenarios where the stolen identity was used to steal from the victim, such as by "withdrawing money from your account or making purchases or investments". The second kind of incident would fall under insurers' definitions of online fraud.

Some definitions of identity theft do not even fit into the 'fraud incident' category. Some participants defined identity theft like a data breach, such as "illegally obtaining personal information". Other definitions included "p[retend]ending to be someone else to use services", which would cover both account takeover and also consensual sharing of a Netflix account. The definition "pretending to be someone else online" covers benign use of fictional personas.

Social Media Incidents. In defining cyberbullying, a common approach emphasized the online aspect without clarifying how the bullying was carried out or what the effect was, such as "bullying someone using the internet". When definitions mentioned the consequences of the bullying, the severity ranged from "a nuisance" to "causing distress" to "tormenting someone". In terms of victims, a 50–59 year old female associated it "primarily with school age/ teenage/ college and maybe 30 20s people", while another said typical victims were "teens or specifically those in the LGBT community".

Another interesting dimension was the role of social media. One participant suggested the definition of cyberbullying "might as well just be twitter", while another specifically mentioned "hate speech through twitter". Another interesting focus was how bullies exploited anonymity, such as the definition "hiding behind a keyboard to be intentionally cruel to someone". Generally speaking, participants were serious about cyberbullying, although the exception proves the rule with the definition: "when some snowflake is upset because people used mean words to them online".

6.2. Uncertainty about Cyber Insurance

The final part of our survey contained direct questions about personal cyber insurance. Table 5 shows that the majority (82% US vs 77% UK) of our sample are not covered for cybercrime under an existing policy. "Do not know" was a common response, especially in the UK (23% UK vs 15% US), which shows there is cyber coverage uncertainty under traditional products. Just 2.8% of US and 0.4% of UK respondents believed they had insurance coverage for cybercrime. None of these respondents reported buying specialist personal cyber insurance. They explained they had coverage under home insurance or "via credit cards".

A minority (8.5%) of respondents were aware that specialist cyber insurance policies existed. Some of these respondents may have become aware due to earlier survey questions, which we now recognize is an error in research design. In spite of this, the low figure points to the novelty of the product. We now explore what respondents would ask an expert before purchasing personal cyber insurance.

Coverage Uncertainty. The most common questions concerned the insurance contract, which is encapsulated in the following response: "How much does it cost, what does

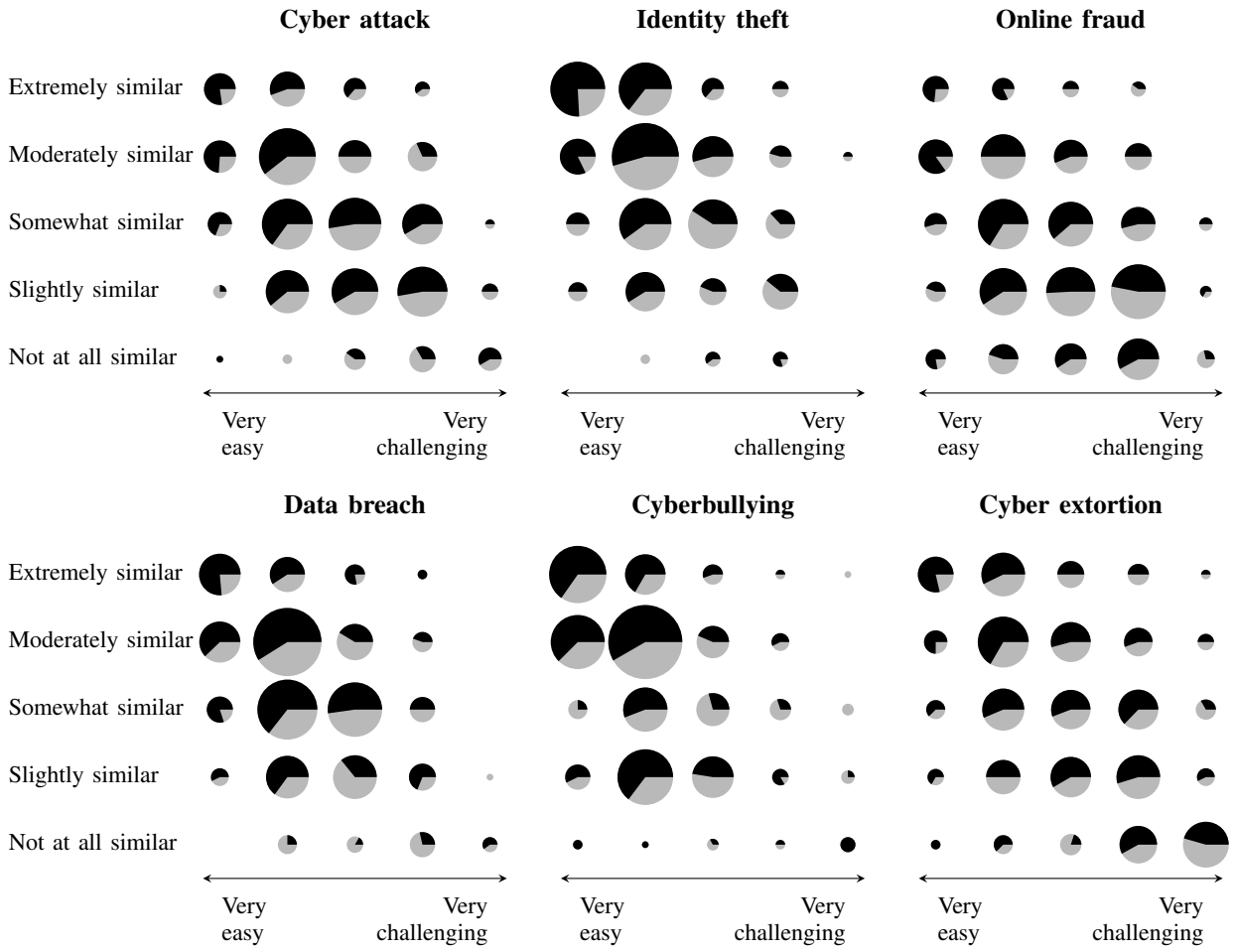

Figure 7. Mapping the understanding of cyber concepts: perceived difficulty of defining an incident versus self-reported similarity with a contractual definition provided by us. The area of the pie charts corresponds to the frequency in each cell and the fraction of black represents the share of respondents in each cell who are self-reported cybercrime victims (of any type).

it cover, and what are the payout limits?" One common question related to who and what was covered by the policy, such as whether it covered "everyone in the house". One participant explained that "for the family I'd consider [buying] it." Another participant asked "what devices would be covered", revealing a mental model where specific systems are insured rather than an individual and their assets.

Questions about coverage often implied a need for details, such as a request for advice with an "emphasis on fine print" or another who wanted to know about "any hidden terms and conditions". Interestingly, one participant linked back to prior questions by noting "my definitions of the previous crimes were broader than yours". Participants rarely asked about specific losses, although exceptions include questions like "does this cover my time in dealing with the aftermath" and "will they help fight cases for me if I need to go to court".

Another common question was how claims could be made or evaluated, focusing on the required evidence. One participant captured a common sentiment with the observation that "insurance companies notoriously don't like to pay out". Participants anticipated specific hurdles including providing proof that: "i have not acted negligently" or "passwords etc were not written down or given to someone else however trusted". A handful of participants questioned whether intangible losses can be compensated, such as "why would money protect me from cyber bullying?"

Risk Uncertainty Another theme was the need to understand the underlying risk. These included both questions about likelihood, such as "how often do these crimes happen" and "what are the chances of a personal attack, for example 1 to 100", as well as questions about impact like "How much money would I stand to lose if my information were compromised?". These participants were possibly primed by earlier survey questions that asked them to estimate this. Nevertheless, it points to the problem of risk uncertainty and the need for reliable cybercrime statistics.

Loss Prevention Services Beyond quantifying the risk, some participants expected insurers to help reduce risk. This expectation is reflected in questions like: "do you

have tools to prevent [cybercrime]"; "do you work with law enforcement to help recover losses?"; and, "do I get regular information about cyber attacks to keep me up to date about the latest methods criminals are using". These questions suggest potential demand for a product that combines risk reduction and risk transfer, as is commonly imagined in theoretical models of cyber insurance [53]. The loss prevention approach was taken to its extreme by respondents who wondered whether cyber risk (and the need for insurance) could be eliminated, such as questions like "can't I avoid it rather than get insurance?" or "wouldn't investing in a good security suite for all devices suffice?".

Questioning the Value of Insurance This points to a wider theme of questioning or even rejecting the value of insurance. Many participants also emphasized the role of alternative sources of compensation. One participant optimistically notes "even if I did lose some [money] the bank would refund as it's genuine fraud", and another notes that "usually the bank will help". Other participants suggested they had little to lose, such as the response "why would I need this insurance when I have no savings".

Some participants believed risk was eliminated by technical solutions. For example, one participant asked "If everything that's important to me is in the cloud, and all I fear is a breach of my data, do I really need Cyber Insurance?". In making similar arguments, other participants used technical terms like "AWS S3 immutable bucket" or "running a secure Linux distro". These participants did not explain how these solutions protected against fraud or cyberbullying.

Some participants provided a sobering reminder that private insurance is a luxury that many individuals cannot afford. For example, one participated pointed to their precarious financial situation by saying "even if I had a job, it'd be minimum wage, so I could hardly even afford to eat, let alone pay for this bs". This was not the only example of hostility towards insurers. One participant suggested that personal cyber insurance is "just another way for insurers to make additional revenue", while another implied insurers were fraudulent by asking "are you not engaging in a fraud, taking my money?"

Summary (RQ3) Just 8.5% of respondents were aware of specialist personal cyber insurance. Given an opportunity to speak with an expert about purchasing, respondents would ask questions about coverage, the claims process, risk exposure, and security services. Some participants suggested that security solutions could eliminate the risk, and others assumed a bank would compensate fraud losses.

Coverage uncertainty varies more between incidents than between high and low security awareness users. In particular, participants' definitions of cyberbullying and identity theft are most similar to insurance definitions, with the smallest gap between users with high/low security awareness. Broadly defined incidents, such as online fraud and cyber attack, are difficult for individuals to define, as are unfamiliar terms such as 'extortion'.

7. Related Work

Section 7.1 explains how our work relates to usable security, emphasizing our research design choices. Section 7.2 outlines our contribution to research into digital insurance.

7.1. Usable Security Research

We adopted many research design choices from usable security research [41], although we introduced deviations to address the peculiarities of insurance. First, usable security typically studies technical solutions that are well-known and understood by academics. In contrast, this study needed to first characterize cyber insurance via a content analysis (**RQ1**), which then informed the design of a realistic user study. The novelty of personal cyber insurance also meant we could not ask participants about their naturally occurring experience with it, which was the most common type of risk representation used in usable security study [41].

Rather than collect naturally-occurring experiences of cyber insurance, we asked one question about naturally occurring historic victimization and twelve questions about expectations of future victimization and impact. The forward-looking questions (**RQ2**) break from prior work, which has focused on establishing historic victimization rates. Such academic studies recruited participants from the US [46], EU [54], Germany [55], and beyond [8]. Statistical bureaus and private firms often conduct similar studies [47, 48]. Our results suggest that users tend to rank the prevalence of cyber incidents in line with historic victimization rates [46, 47, 54, 56]. However, we caution against comparing the magnitude of rates given these are highly influenced by subtle differences in survey questions [48].

Our survey also used a simulated scenario, the second most common type of risk representation in usable security research [41]. For example, password strength was studied by asking users to imagine they are setting a password to protect a valuable account [57]. Unlike these studies, we did not simulate a specific security scenario because cyber insurance mitigates a diverse bundle of security, privacy, fraud, and social media incidents. Instead we simulated a conversation with an expert to explore their uncertainties.

Finally, we also used the rarest representation in usable security research [41], namely mentioned risk, by asking users to define different cyber incidents without outlining a scenario. We did so to avoid priming users because insurance is designed to respond to a wide range of scenarios. The results confirmed that users readily understand data breaches [56], but we contribute novel results allowing comparison with other incident types (see Figure 6).

Our legal definition question was reminiscent of a task in a user study on privacy policies in that both studies presented users with legalistic definitions [58]. The difference is that Sen et al. [58] do so to prepare participants for a task, whereas we provided insurance policy language to allow users to evaluate the output of their task. Our choice to use self-evaluation follows prior studies that asked participants

for further explanation about tasks like creating drawings of the Internet [59] or smart speaker privacy [60].

7.2. Digital Insurance Research

Researchers have been investigating corporate cyber insurance since at least 2000, which has been summarized in various literature surveys [53, 61–64]. The focus on corporate insurance is not surprising given the market reached $14 billion in size in 2023 [65], meanwhile the personal cyber insurance market was "not yet developed" as of 2019 [66]. Our results suggest this remains the case, possibly due to risk and coverage uncertainty.

Prior empirical studies primarily describe insurers' business models with the goal of understanding whether insurance helps to improve cybersecurity. Research questions include; what does cyber insurance cover [14] and do traditional products cover cyber [67]; what information is collected [29]; how is insurance priced [68]; and how do insurers organize crisis response [16, 69]. The broad consensus is that insurers are underwhelming in improving security before the incident, but that insurers have a positive impact over how policyholders respond to incidents [17, 20]. The empirical studies of corporate insurance used data sources including: legal documents like policy contracts [14, 67], application forms [14, 28], and pricing schemes [14, 68]; expert interviews [20, 29, 69, 70]; insurance claims [71]; and the websites of insurers [16]. We relied on insurance policies for **RQ1**. The other data sources providing an interesting direction for future work.

Our main contribution is addressing the "paucity" of research on personal cyber insurance [21]. Two studies of personal digital insurance were published in 2023. The first shows US personal identity insurance covers costs like credit monitoring, travel and care costs while replacing documents, and psychological counseling [39]. The second explores German personal cyber products [27]. Some coverage is overlapping with the US/UK, such as fraud (e.g. fraudulent online sales and identity theft), data recovery and restoration, and legal costs. However, no German products cover cyber extortion, whereas all US and UK policies do. Further, German products cover legal costs related to the policyholder bullying others [27], whereas US products cover costs resulting from the insured's family being victims. These stark differences could be cultural or equally due to regulatory differences, such as the legality of paying ransoms, an interesting topic for future work.

Summary Our **RQ1** findings show that cyber insurance in the US and UK is a lot broader than personal identity insurance [39] and has significant differences to personal cyber insurance in Germany [27]. Our findings for **RQ2–3** reveal a novel demand-side perspective by directly surveying potential buyers, the first such study of personal cyber insurance, and also provides forward-looking cyber risk estimates, unlike prior work that looks at historic victimization.

8. Discussion

8.1. Implications

Evolution of Insurance (RQ1). It is concerning that many policyholders do not know if they have cyber coverage (see Table 5) or believe their home insurance policy covers cyber incidents (see Section 6.2). For a historical parallel, many businesses believed traditional policies covered cyber losses in the early 2000s. This belief led to disputes when insurers refused to pay claims by arguing, for example, that electronic data does not constitute tangible property [19]. Personal insurers must decide and then communicate whether home policies cover cyber losses.

Even for specialist products, insurers must continue to tailor coverage to the changing digital landscape. Cyberbullying coverage is an important innovation to cover malicious incidents, but there is mounting (and contested) evidence that teen mental health is negatively impacted by digital systems operating as intended [72]. While this specific harm may be better covered by health insurance, cyber insurers should reconsider coverage as new digital harms arise.

Another question is whether products should vary across geographies, which seems unwise given the Internet is global. However, comparisons with prior work [27] reveals that German and US/UK products vary significantly on ransom coverage. One explanation could be laws or societal norms given ransom payments are controversial [69].

Turning to evidentiary standards, many participants worried about what evidence was needed to make a claim (see Section 6.2). Insurers must first define what is required of insureds, such as whether writing passwords down invalidates the policy[5], *and* work out how to collect evidence.

Rather than focus on contractual language and evidence, insurers could work with policyholders to reduce risk as envisioned in the context of corporate insurance [53, 73]. This would involve insurers offering discounts or subsidies for policyholders to adopt security controls. Many participants even mentioned this idea without being prompted. Some harms can be mitigated by traditional computer security. However, individuals adopting these solutions cannot mitigate cyberbullying or identity theft; these harms are respectively caused by social media platforms failing in content moderation, and large businesses failing to protect customer data. Ultimately, this reality—that a lot of digital harm is outside the individual user's control—is precisely what motivates digital insurance, which allows individuals to at least transfer some of the financial consequences.

Reducing Risk Uncertainty (RQ2). Individuals expectations of incident frequency are relatively well-calibrated in the aggregate (see Figure 4). However, insurance is bought by individuals. 5% of participants estimate cyber extortion to happen every one or two years, which is over 500 times higher than the population baseline [46]. This could lead to over-investment. In contrast, under-investment in prevention

5. This would make little sense given cybercriminals are unlikely to have local access to the insured's home.

could result from most users believing cyberbullying has close to no financial impact (see Figure 5).

There is a natural question about who should educate users about the likelihood and impact of incidents, especially given many users said they wanted cybercrime statistics before purchasing cyber insurance (see Section 6.2). On the one hand, insurers hold accurate information from observing claims outcomes. On the other hand, they have a conflict of interest in providing such advice. Instead, a neutral institution could collect and share cybercrime statistics tailored to cyber insurance purchasing. Historically this was provided by the insurance broker, but they have declined in popularity as consumers buy insurance online. This problem is comparable to advice about digital security, where users face a myriad of information sources [25, 74].

Reducing Coverage Uncertainty (RQ3). To reduce coverage uncertainty, users can either be educated on insurance terminology, or insurers can adopt clearer terminology. It appears the latter is more promising given that coverage uncertainty varies more across incidents than across high/low security awareness users (see Figure 6). Examples of incidents with clear terminology include cyberbullying and identity theft, which are understood even by non-specialists. However, non-specialists have trouble defining cyber extortion, likely because it is new. Cyber attack and online fraud are different in that participants believe they can define them, but these definitions do not match insurers' definitions (see Figure 6). In general, specific incidents appear to be easier for individuals to understand.

8.2. Limitations

In exploring a new cyber risk solution (insurance), we used mixed-methods to understand the product from both a supply (**RQ1**) and demand (**RQ2–3**) perspective. We are confident the content analysis (**RQ1**) has high internal validity as it was conducted by qualified lawyers who achieved a high inter-coder reliability score. However, external validity could be an issue because we did not collect a product for many of the largest insurers in the US or UK. Most have not released a personal cyber product. External validity will be eroded over time as these insurers introduce products, and existing products evolve to address new digital harms.

The survey findings (**RQ2–3**) have limitations related to sampling, and response biases. First, our sample comprised Prolific workers and was not representative of the US/UK populations. These pragmatic choices were guided by prior work showing Prolific responses are "generally representative for questions about user perceptions" [43]. Second, our risk estimates (**RQ3**) are limited by various response biases. First, not all users are confident estimating probabilities, such as meaningfully distinguishing between say 0.01 and 0.001. To improve consistency, we sacrificed granularity and offered participants 5 options with both a qualitative and quantitative label, such as "Rarely (1 in 50 years)". We recommend readers focus on the relative ranking of the quantitative risk estimates, as the absolute values are likely impacted by response biases.

8.3. Future Work

We hope our exploratory study will provide a basis for many more studies on personal cyber insurance. For supply-side studies, coverage will vary across international markets and also over-time. This motivates replicating our **RQ1** analysis with a sample of US/UK policies created after 2022 or with policies from other countries. Beyond policy analysis, research should explore how personal cyber insurers collect risk information, process claims, influence security and so on. Templates for each study can be found in the literature on corporate cyber insurance (see Section 7.2).

To improve insurance decisions and wider digital risk management, future work should explore how to reduce risk uncertainty (**RQ2**). An open research problem is establishing ground-truth on victimization rates, especially as these human-made incidents are influenced by the interplay between defenders, threat actors, and law enforcement. Researchers must revise research instruments to estimate the prevalence of new crimes. A second problem concerns how to best communicate risk information to users, which is well suited to the human-computer interaction community.

Studying what is not covered is a promising direction for coverage uncertainty (**RQ3**). Our user study was constrained to incidents covered by cyber insurance, but a more open-ended design could identify incidents that are not covered, an important topic for digital risk management. Another direction is to test novel coverage terminology, which may be easier for users to comprehend.

9. Conclusion

We conducted an exploratory study of the supply and demand sides of the personal cyber insurance market. Analysis of 24 personal cyber insurance policies reveals that it covers a diverse set of incidents spanning security, privacy, fraud, and social media abuse. This includes covering stolen funds, hiring incident responders (both technical and legal), lost wages, and even psychological counseling. We discovered personal cyber insurance coverage in the US and UK has significant differences to coverage in Germany [27].

Potential buyers face uncertainty about both the underlying risk and also coverage. Most respondents estimated the ordering of incident frequency in line with historic victimization rates. Respondents also estimated that fraud incidents were the most costly, followed by security and privacy incidents, with cyberbullying incidents having next to no costs that could be compensated by insurance. When considering buying a policy, participants raised uncertainties about contractual details, reporting requirements, victimization statistics, and access to security solutions.

These results point to the need for insurers to develop comprehensible coverage, and for a trusted authority to advise on the risk of different incidents. A particularly interesting question is whether insurers can integrate risk reduction into their business model, which many participants expressed interest in.

References

[1] Camelia Simoiu, Joseph Bonneau, Christopher Gates, and Sharad Goel. "I was told to buy a software or lose my computer. I ignored it": A study of ransomware. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 155–174, 2019.

[2] Kurt Thomas, Frank Li, Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelika Moscicki, et al. Data breaches, phishing, or malware? understanding the risks of stolen credentials. In *Proc. of the ACM Con. on Comp. and Comm. Sec.*, pages 1421–1434, 2017.

[3] Peter Mayer, Yixin Zou, Florian Schaub, and Adam J Aviv. "now i'm a bit angry" Individuals' awareness, perception, and responses to data breaches that affected them. In *Proc. of the 30th USENIX Sec. Symp.*, pages 393–410, 2021.

[4] Peter Mayer, Yixin Zou, Byron M Lowens, Hunter A Dyer, Khue Le, Florian Schaub, and Adam J Aviv. Awareness, intention,(in) action: Individuals' reactions to data breaches. *ACM Trans. on Computer-Human Int.*, 30(5):1–53, 2023.

[5] Svetlana Abramova and Rainer Böhme. Anatomy of a high-profile data breach: Dissecting the aftermath of a crypto-wallet case. In *Proc. of the 32nd USENIX Sec. Symp.*, pages 715–732, 2023.

[6] Massimo Bartoletti, Stefano Lande, Andrea Loddo, Livio Pompianu, and Sergio Serusi. Cryptocurrency scams: Analysis and perspectives. *IEEE Access*, 9:148353–148373, 2021.

[7] Steve Mansfield-Devine. The imitation game: How business email compromise scams are robbing organisations. *Comp. Fraud & Sec.*, 2016(11):5–10, 2016.

[8] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, et al. SoK: Hate, harassment, and the changing landscape of online abuse. In *IEEE Symposium on Security and Privacy*, pages 247–267, Oakland, CA, May 2021.

[9] Ross Anderson. *Security engineering*. John Wiley & Sons, 2008.

[10] Rock Stevens, Daniel Votipka, Josiah Dykstra, Fernando Tomlinson, Erin Quartararo, Colin Ahern, and Michelle L Mazurek. How ready is your ready? assessing the usability of incident response playbook frameworks. In *Proc. of the 2022 CHI Conf. on Human Factors in Comp. Sys.*, pages 1–18, 2022.

[11] Chris Prosise, Kevin Mandia, and Matt Pepe. *Incident response & computer forensics*. McGraw-Hill, 2003.

[12] Richard Knight and Jason RC Nurse. A framework for effective corporate communication after cyber security incidents. *Computers & Security*, 99:102036, 2020.

[13] Leah Zhang-Kennedy, Hala Assal, Jessica Rocheleau, Reham Mohamed, Khadija Baig, and Sonia Chiasson. The aftermath of a crypto-ransomware attack at a large academic institution. In *27th USENIX Sec. Symp. (USENIX Security 18)*, pages 1061–1078, 2018.

[14] Sasha Romanosky, Andreas Kuehn, Lillian Ablon, and Therese Jones. Content analysis of cyber insurance policies: How do carriers price cyber risk? *J. of Cybersecurity*, 5(1), 2019.

[15] Rainer Böhme, Stefan Laube, and Markus Riek. A fundamental approach to cyber risk analysis. *Variance*, 12(2):161–185, 2018.

[16] Daniel W Woods, Rainer Böhme, Josephine Wolff, and Daniel Schwarcz. Lessons lost: Incident response in the age of cyber insurance and breach attorneys. In *Proc. of the 32nd USENIX Sec. Symp.*, 2023.

[17] Daniel W Woods and Tyler Moore. Does insurance have a future in governing cybersecurity? *IEEE Security & Privacy*, 18(1):21–27, 2020.

[18] Jamie MacColl, Jason RC Nurse, and James Sullivan. Cyber insurance and the cyber security challenge. *Royal United Services Institute Occasional Paper Series*, 2021. [Online; accessed 19-Sep-2022].

[19] Josephine Wolff. *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks*. MIT Press, 2022.

[20] Gareth Mott, Sarah Turner, Jason RC Nurse, Jamie MacColl, James Sullivan, Anna Cartwright, and Edward Cartwright. Between a rock and a hard (ening) place: Cyber insurance in the ransomware era. *Computers & Security*, 128:103162, 2023.

[21] Richard McGregor, Carmen Reaiche, Stephen Boyle, and Graciela Corral de Zubielqui. Cyberspace and personal cyber insurance: A systematic review. *Journal of Computer Information Systems*, 64(1):157–171, 2024.

[22] Tom Buchanan and Monica T Whitty. The online dating romance scam: causes and consequences of victimhood. *Psych., Crime & L.*, 20(3):261–283, 2014.

[23] Josephine Wolff. *You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches*. MIT Press, 2018.

[24] Daniel Arce, Daniel W. Woods, and Rainer Böhme. Economics of incident response panels in cyber insurance. *Computers & Security*, 140, May 2024.

[25] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 272–288. IEEE, 2016.

[26] George Loewenstein, Joelle Y Friedman, Barbara McGill, et al. Consumers' misunderstanding of health insurance. *J. of Health Econ.*, 32(5):850–862, 2013.

[27] Florian Schütz, Florian Rampold, Andre Kalisch, and Kristin Masuch. Consumer cyber insurance for risk transfer: A coverage analysis. *Procedia Computer Science*, 219:521–528, 2023.

[28] Daniel W Woods, Ioannis Agrafiotis, Jason RC Nurse, and Sadie Creese. Mapping the coverage of security controls in cyber insurance proposal forms. *Journal of Internet Services and Applications*, 8(1):8, 2017.

[29] Jason R.C. Nurse, Louise Axon, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith, and Sadie Creese. The data that drives cyber insurance: A study into the un-

derwriting and claims processes. In *2020 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. IEEE, 2019.

[30] Omer F Keskin, Kevin Matthe Caramancion, Irem Tatar, Owais Raza, and Unal Tatar. Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. *Electronics*, 10(10):1168, 2021.

[31] Sazzadur Rahaman, Gang Wang, and Danfeng Yao. Security certification in payment card industry: Testbeds, measurements, and recommendations. In *Proc. of the Conf. on Computer and Communications Security*, pages 481–498. ACM, 2019.

[32] Kenneth S Abraham. A theory of insurance policy interpretation. *Michigan Law Review*, 95:531, 1996.

[33] Joseph E Stiglitz. Monopoly, non-linear pricing and imperfect information: the insurance market. *The Review of Economic Studies*, 44(3):407–430, 1977.

[34] Rob Thoyts. *Insurance theory and practice*. Routledge, 2010.

[35] Martin Eling and David Antonius Pankoke. Systemic risk in the insurance sector: a review and directions for future research. *Risk Management and Insurance Review*, 19(2):249–284, 2016.

[36] Yannis Bakos, Florencia Marotta-Wurgler, and David R Trossen. Does anyone read the fine print? consumer attention to standard-form contracts. *The Journal of Legal Studies*, 43(1):1–35, 2014.

[37] Daniel Schwarcz. Coverage information in insurance law. *Minn. L. Rev.*, 101:1457, 2016.

[38] Daniel W Woods and Jessica Weinkle. Insurance definitions of cyber war. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 45(4):639–656, 2020.

[39] Daniel W Woods. Personal identity insurance: Coverage and pricing in the US. *Journal of Financial Transformation*, 57:36–45, 2023.

[40] Cori Faklaris, Laura A Dabbish, and Jason I Hong. A self-report measure of end-user security attitudes (SA-6). In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 61–77, 2019.

[41] Verena Distler, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Lorrie Faith Cranor, and Vincent Koenig. A systematic literature review of empirical methods and risk representation in usable privacy and security research. *ACM Trans. on Comp.-Human Inter.*, 28(6):1–50, 2021.

[42] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symp. on Sec. and Privacy (SP)*, pages 1326–1343. IEEE, 2019.

[43] Jenny Tang, Eleanor Birrell, and Ada Lerner. Replication: How well do my results generalize now? the external validity of online privacy and security surveys. In *18th Symp. on Usable Priv. and Sec. (SOUPS 2022)*, pages 367–385, 2022.

[44] Gergely Biczók and Pern Hui Chia. Interdependent privacy: Let me share your data. In *Int. Conf. on Fin. Crypto. and Data Sec.*, pages 338–353. Springer, 2013.

[45] Mathias Humbert, Benjamin Trubert, and Kévin Huguenin. A survey on interdependent privacy. *ACM Computing Surveys (CSUR)*, 52(6):1–40, 2019.

[46] Casey Breen, Cormac Herley, and Elissa M Redmiles. A large-scale measurement of cybercrime against individuals. In *Proc. of the 2022 CHI Conf. on Human Factors in Computing Systems*, pages 1–41, 2022.

[47] Daniel W Woods and Lukas Walter. Reviewing estimates of cybercrime victimisation and cyber risk likelihood. In *2022 IEEE Euro. Symp. on Sec. and Priv. W. (EuroS&PW)*, pages 150–162. IEEE, 2022.

[48] Carin MM Reep-van den Bergh and Marianne Junger. Victims of cybercrime in Europe: a review of victim surveys. *Crime Science*, 7(1):1–15, 2018.

[49] Timothy D Wilson, Christopher E Houston, Kathryn M Etling, and Nancy Brekke. A new look at anchoring effects: basic anchoring and its antecedents. *Journal of Experimental Psychology: General*, 125(4):387, 1996.

[50] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (Un)informed consent: Studying GDPR consent notices in the field. In *Proc. of the 2019 Conference on Computer and Communications Security*, pages 973–990, 2019.

[51] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. Smart, useful, scary, creepy: perceptions of online behavioral advertising. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, pages 1–15, 2012.

[52] Maximilian Hils, Daniel W. Woods, and Rainer Böhme. Privacy preference signals: Past, present and future. *Proc. on Privacy Enhancing Technologies*, 2021(4):249–269, 2021.

[53] Rainer Böhme and Galina Schwartz. Modeling cyber-insurance: Towards a unifying framework. In *Workshop on the Economics of Information Security*, 2010.

[54] Markus Riek and Rainer Böhme. The costs of consumer-facing cybercrime: an empirical exploration of measurement issues and estimates. *J. of Cybersecurity*, 4(1), 2018.

[55] Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Dürmuth, Yixin Zou, and M Angela Sasse. Digital security–a question of perspective. a large-scale telephone survey with four at-risk user groups. In *Proc. of the Symp. on Sec. and Privacy*. IEEE, 2024.

[56] Sowmya Karunakaran, Kurt Thomas, Elie Bursztein, and Oxana Comanescu. Data breaches: User comprehension, expectations, and concerns with handling exposed data. In *Fourteenth Symp. on Usable Privacy and Security (SOUPS 2018)*, pages 217–234, 2018.

[57] Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, et al. Design and evaluation of a data-driven password meter. In *Proc. of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 3775–3786, 2017.

[58] Shayak Sen, Saikat Guha, Anupam Datta, Sriram K

Rajamani, Janice Tsai, and Jeannette M Wing. Bootstrapping privacy compliance in big data systems. In *IEEE Symp. on Sec. and Priv.*, pages 327–342, 2014.

[59] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "my data just goes everywhere" User mental models of the internet and implications for privacy and security. In *Eleventh Symp. on Usable Priv. and Sec. (SOUPS 2015)*, pages 39–52, 2015.

[60] Nicole Meng, Dilara Keküllüoğlu, and Kami Vaniea. Owning and sharing: Privacy perceptions of smart speaker users. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–29, 2021.

[61] Angelica Marotta, Fabio Martinelli, Stefano Nanni, Albina Orlando, and Artsiom Yautsiukhin. Cyber-insurance survey. *Computer Science Review*, 24:35–61, 2017.

[62] Martin Eling. Cyber risk and cyber risk insurance: Status quo and future research. *The Geneva P. on Risk and Ins.-Issues and Prac.*, 43:175–179, 2018.

[63] Savino Dambra, Leyla Bilge, and Davide Balzarotti. SoK: Cyber insurance—Technical challenges and a system security roadmap. In *Proc. of the Symp. on Security and Privacy*, pages 293–309. IEEE, 2020.

[64] Aggeliki Tsohou, Vasiliki Diamantopoulou, Stefanos Gritzalis, and Costas Lambrinoudakis. Cyber insurance: state of the art, trends and future directions. *International Journal of Information Security*, pages 1–12, 2023.

[65] GuyCarpenter. Through the lookin glass: Interrogating the key numbers behind today's cyber market, 2023.

[66] SwissRe. Personal cyber insurance: Protecting our digital lives, 2019.

[67] Dirk Wrede, Tino Stegen, and Johann-Matthias Graf von der Schulenburg. Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the german insurance market. *The Geneva P. on Risk and Ins.-Issues and Prac.*, 45(4):657–689, 2020.

[68] Daniel W Woods, Tyler Moore, and Andrew C Simpson. The county fair cyber loss distribution: Drawing inference from insurance prices. In *Workshop on the Economics of Information Security*, 2019.

[69] Anna Cartwright, Edward Cartwright, Jamie MacColl, Gareth Mott, Sarah Turner, James Sullivan, and Jason RC Nurse. How cyber insurance influences the ransomware payment decision: theory and evidence. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 48(2):300–331, 2023.

[70] Ulrik Franke. The cyber insurance market in Sweden. *Computers & Security*, 68:130–144, 2017.

[71] Louise Axon, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith, and Sadie Creese. Analysing cyber-insurance claims to design harm-propagation trees. In *Int. Conf. on Cyber Situ. Aware., Data Analytics and Assess.* IEEE, 2019.

[72] Jonathan Haidt. *The anxious generation: How the great rewiring of childhood is causing an epidemic of mental illness*. Random House, 2024.

TABLE 3. SUMMARY STATISTICS OF THE SA-6 ITEMS.

Item	Mean	Std. dev.	Correlation w/ index
I seek out opportunities to learn about security measures that are relevant to me.	3.37	1.10	0.804
I am extremely motivated to take all the steps needed to keep my online data and accounts safe.	3.94	0.99	0.774
Generally, I diligently follow a routine about security practices.	3.58	1.05	0.792
I often am interested in articles about security threats.	3.37	1.14	0.754
I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.	3.79	0.94	0.731
I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.	3.32	1.07	0.692

Cronbach's α is 0.851. Threshold 0.70; original scale validation study 0.84 [40].

TABLE 4. STATISTICS OF THE SA-6 SECURITY AWARENESS INDEX.

Moments	Mean	Std. dev.
Total	3.56	0.79
Breach victims	3.66^{***}	0.77
US	3.49^{*}	0.85
UK	3.63^{*}	0.73
Correlation with variables of the threat definition task	τ with perc. difficulty	τ with similarity
Cyber attack	-4.12^{***}	4.59^{***}
Cyber extortion	-4.41^{***}	3.24^{**}
Online fraud	-3.62^{***}	4.90^{***}
Data breach	-3.37^{***}	4.16^{***}
Identity theft	-2.76^{**}	2.14^{*}
Cyberbullying	-0.96	1.79

Statistical significance levels: $^{*} \leq 0.05$, $^{**} \leq 0.01$, $^{***} \leq 0.001$

[73] Bruce Schneier. Insurance and the computer industry. *Communications of the ACM*, 44(3):114–114, 2001.

[74] Elissa M Redmiles, Miraida Morales, Lisa Maszkiewicz, Rock Stevens, Everest Liu, Dhruv Kuchhal, and Michelle L Mazurek. First steps toward measuring the readability of security advice. In *The 2018 IEEE Security & Privacy Workshop on Technology and Consumer Protection (ConPro)*, 2018.

[75] Miranda Wei, Jaron Mink, Yael Eiger, Tadayoshi Kohno, Elissa M Redmiles, and Franziska Roesner. Sok (or solk?): On the quantitative study of sociodemographic factors and computer security behaviors. In *USENIX Security Symposium*, 2024.

TABLE 5. DESCRIPTIVE STATISTICS OF THE ONLINE SURVEY.

Variable	US	UK	Total	Breach victims
Age				
18–29 years old	20.6	23.6	22.1	21.4
30–39 years old	32.7	31.0	31.9	32.5
40–49 years old	17.8	18.0	17.9	18.3
50–59 years old	16.7	18.0	17.3	17.0
60 or older	12.1	9.5	10.8	10.8
Gender				
Female	47.7	63.0	55.4	52.0
Male	49.8	36.3	43.0	46.7
Non-binary / third gender	1.4	0.7	1.1	0.9
Education				
Primary School / Elementary School	0.0	0.4	0.2	0.0
Secondary School / High school / Sr. High School	12.1	15.1	13.6	15.5
Some college/assoc./tech. deg.	29.5	22.9	26.2	26.6
Bachelor's degree	38.4	41.9	40.2	38.7
Master's degree	14.2	16.9	15.6	15.2
Doctorate degree	5.3	2.5	3.9	3.7
Other (please specify)	0.4	0.4	0.4	0.3
Occupation				
Disabled	2.1	2.5	2.3	2.2
Employed full time	55.9	48.9	52.4	52.6
Employed part time	11.7	18.3	15.0	13.6
Retired	8.2	4.9	6.5	6.8
Self employed	10.7	8.8	9.7	11.1
Student	2.1	5.3	3.7	3.4
Unemployed looking for work	5.3	4.6	5.0	5.3
Unemployed not looking for work	3.9	6.7	5.3	5.0
Annual household income				
Up to $25,000/£20,000	11.0	15.1	13.1	13.3
$25,000 to $49,999 / £20,000 to £39,999	23.8	38.4	31.2	29.4
$50,000 to $74,999 / £40,000 to £59,999	18.9	22.9	20.9	20.7
$75,000 to $99,999 / £60,000 to £79,999	14.6	12.3	13.5	12.1
$100,000/£80,000 or more	31.7	11.3	21.4	24.5
Last victimization experience				
never	34.2	51.4	42.8	0.0
in last 1 month	5.7	4.2	5.0	8.7
between 1 month to 6 months ago	13.9	10.6	12.2	21.4
between 6 month to 1 year ago	11.0	6.7	8.8	15.5
over 1 year ago	35.2	27.1	31.2	54.5
Type of experience (coded from text description)				
Cyber attack	4.3	4.2	4.2	7.4
Cyber extortion	1.1	1.1	1.1	1.9
Identity theft	3.2	1.8	2.5	4.3
Financial fraud	23.1	16.9	20.0	35.0
Data breach	27.0	13.0	20.0	35.0
Phishing	1.8	4.2	3.0	5.3
Online account compromise	16.0	16.2	16.1	28.2
Insurance coverage for cybercrime				
Do not know	14.9	22.5	18.8	18.9
No	82.2	77.1	79.6	78.6
Yes	2.8	0.4	1.6	2.5
Number of cases N	281	284	565	323

TABLE 6. REGRESSIONS FOR CYBER ATTACK.

Cyber attack	Dependent variable			
	Expected frequency (ordered probit)		Estimated impact ($\log_{10}$ US$)	
Loss experience	0.56**	0.58**	0.51	0.47
Security awareness	0.07	0.06	0.16*	0.17*
Perceived difficulty	−0.04	−0.04	0.01	−0.00
Controls				
US		0.08		0.05
Female		−0.02		0.10
30–39 years old		0.07		−0.45*
40–49 years old		0.22		−0.35
50–59 years old		0.22		−0.10
60 or older		0.32		−0.14
Low income		−0.02		−0.23
Tertiary education		0.13		0.09
Pseudo / R^2 (adjusted)	0.02	0.02	0.01	0.01

Statistical significance levels: $^{*}p \leq 0.05$, $^{**}p \leq 0.01$, $^{***}p \leq 0.001$

TABLE 7. REGRESSIONS FOR CYBERBULLYING.

Cyberbullying	Dependent variable			
	Expected frequency (ordered probit)		Estimated impact ($\log_{10}$ US$)	
Loss experience	0.21*	0.22*	−0.11	−0.09
Security awareness	−0.03	−0.02	0.22*	0.22*
Perceived difficulty	−0.11*	−0.07	0.34***	0.33***
Controls				
US		0.00		0.00
Female		−0.03		0.12
30–39 years old		−0.21		−0.29
40–49 years old		−0.24		−0.18
50–59 years old		−0.35*		0.14
60 or older		−0.55**		−0.14
Low income		0.03		−0.12
Tertiary education		0.18		0.16
Pseudo / R^2 (adjusted)	0.02	0.03	0.04	0.03

Statistical significance levels: $^{*}p \leq 0.05$, $^{**}p \leq 0.01$, $^{***}p \leq 0.001$

TABLE 8. REGRESSIONS FOR CYBER EXTORTION.

Cyber extortion	Dependent variable			
	Expected frequency (ordered probit)		Estimated impact ($\log_{10}$ US$)	
Loss experience	0.03	0.01	0.90	0.68
Security awareness	0.18**	0.15*	0.07	0.08
Perceived difficulty	0.01	0.02	0.12*	0.12
Controls				
US		−0.09		0.10
Female		−0.22*		0.04
30–39 years old		0.04		−0.41*
40–49 years old		0.13		−0.56*
50–59 years old		0.25		−0.20
60 or older		0.22		−0.17
Low income		0.02		−0.37*
Tertiary education		0.08		0.27
Pseudo / R^2 (adjusted)	0.02	0.02	0.00	0.02

Statistical significance levels: $^{*}p \leq 0.05$, $^{**}p \leq 0.01$, $^{***}p \leq 0.001$

TABLE 9. REGRESSIONS FOR IDENTITY THEFT.

Identity theft	Dependent variable			
	Expected frequency (ordered probit)		Estimated impact ($\log_{10}$ US$)	
Loss experience	0.16	0.16	0.32	0.18
Security awareness	0.15**	0.14*	0.06	0.11
Perceived difficulty	0.04	0.04	0.01	0.03
Controls				
US		0.14		0.28**
Female		0.03		0.28**
30–39 years old		0.15		−0.05
40–49 years old		0.39**		−0.13
50–59 years old		0.51***		−0.03
60 or older		0.51**		−0.05
Low income		−0.01		−0.34***
Tertiary education		−0.07		−0.11
Pseudo / R^2 (adjusted)	0.01	0.04	−0.00	0.03

Statistical significance levels: $^{*}p \leq 0.05$, $^{**}p \leq 0.01$, $^{***}p \leq 0.001$

TABLE 10. REGRESSIONS FOR ONLINE FRAUD.

Online fraud	Dependent variable			
	Expected frequency (ordered probit)		Estimated impact ($\log_{10}$ US$)	
Loss experience	0.23*	0.22*	0.03	0.07
Security awareness	0.09	0.05	0.03	0.04
Perceived difficulty	0.05	0.05	0.09	0.06
Controls				
US		−0.03		0.00
Female		−0.05		0.26*
30–39 years old		0.10		−0.08
40–49 years old		0.48***		−0.06
50–59 years old		0.66***		0.11
60 or older		0.66***		0.15
Low income		−0.02		−0.24*
Tertiary education		0.10		0.12
Pseudo / R^2 (adjusted)	0.01	0.06	0.00	0.01

Statistical significance levels: $^{*}p \leq 0.05$, $^{**}p \leq 0.01$, $^{***}p \leq 0.001$

TABLE 11. REGRESSIONS FOR DATA BREACH.

Data breach	Dependent variable			
	Expected frequency (ordered probit)		Estimated impact ($\log_{10}$ US$)	
Loss experience	0.60***	0.57***	0.06	0.01
Security awareness	−0.03	−0.04	0.21*	0.24**
Perceived difficulty	0.03	0.02	0.05	0.06
Controls				
US		0.19*		0.17
Female		0.12		0.16
30–39 years old		0.29*		−0.34
40–49 years old		0.37**		−0.32
50–59 years old		0.49***		−0.11
60 or older		0.20		−0.32
Low income		0.02		−0.27*
Tertiary education		0.15		0.02
Pseudo / R^2 (adjusted)	0.05	0.07	0.01	0.01

Statistical significance levels: $^{*}p \leq 0.05$, $^{**}p \leq 0.01$, $^{***}p \leq 0.001$

Appendix A. Seed Sample of Insurers

To identify US insurers, we used the following list:

- Top 100 U.S. Property and Casualty Insurance Companies, available: https://www.reinsurancene.ws/top-100-u-s-property-casualty-insurance-companies/

To identify UK insurers, we used the following lists:

- The top 50 UK insurers, available: https://www.insurancetimes.co.uk/top-50-uk-insurance-groups-and-companies/.
- Top UK insurers by 2022 brand awareness, available: https://www.statista.com/statistics/1112741/insurance-brand-recall-in-the-united-kingdom-uk/.
- Best home insurance in 2022, available: https://moneyfacts.co.uk/insurance/best-home-insurance/.
- Top UK insurance companies in 2022 based on market cap, available: https://www.propertycasualty360.com/2022/05/23/top-uk-insurance-companies-of-2022-based-on-market-cap/.
- Top UK insurance companies based on number of employees in 2021, available: https://www.propertycasualty360.com/2021/06/07/the-u-ks-largest-insurance-companies-in-2021/.

Appendix B. Codebooks

We used the follows themes and sub-themes to analyze the cyber insurance policies:

- Cyber Attack
  - Data recovery
  - System restoration
  - Cyber disruption services
  - Other
- Cyber Extortion
  - Ransom payment
  - Professional assistance
  - Generic costs
- Online Fraud
  - Direct financial loss
- Identity Theft
  - Re-filling application costs
  - Notarizing affidavits and other communication costs
  - Costs for credit reports
  - Attorney fees and expenses
  - Lost wages
  - Childcare and eldercare expenses
  - Monitoring services
  - Generic costs
- Data Breach
  - Legal professional assistance
  - IT professional assistance
  - Services to affected individuals
  - Notification costs
  - Generic costs
- Cyber Bullying
  - Mental health services
  - IT and other professional assistance
  - Educational expenses
  - Relocation expenses
  - Lost salary
  - Legal expenses
  - Childcare and eldercare expenses
  - Purchase of support software

We used the following codes to classify the free-text responses to the question "*Please provide additional details about the most recent breach of security you experienced.*"

- Kind of attack (Non-exclusive categories)
  - cyber attack
  - cyber extortion
  - online fraud - financial fraud
  - online fraud - identity theft
  - data breach
  - online account compromised
  - phishing
- vague or insufficient information

Appendix C. Meta-Review

The following meta-review was prepared by the program committee for the 2025 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

C.1. Summary

This paper presents an exploratory study of the supply and demand sides of the personal cyber insurance market.

First, the authors analyze 24 personal cyber insurance policies, finding that they cover a diverse set of incidents spanning security, privacy, fraud, and social media abuse.

Then, they study the demand side via a survey distributed to 584 participants in the US and the UK, introducing the concepts of risk uncertainty and coverage uncertainty, finding both are prevalent for personal cyber insurance. As for coverage uncertainty, the authors discover a gap between insurers and participants, whereas, for risk uncertainty, they discovered that in the aggregate users are relatively well calibrated regarding the frequency of different incidents.

C.2. Scientific Contributions

The paper presents a novel study on personal cyber insurance, an under-studied area, addressing both the supply side (insurance policies) and the demand side (user perceptions).

C.3. Reasons for Acceptance

The program committee appreciated the paper's timeliness and valuable contributions.

C.4. Noteworthy Concerns

A few concerns were raised during the review process related to the lack of a detailed analysis of/focus on: 1) policy implications and regulatory influences, 2) correlations between perceptions and participants' (demographic) characteristics, and 3) participants who have actually purchased cyber insurance.

Appendix D. Response to the Meta-Review

The first noteworthy concern is outside the scope of our exploratory research study. We hope that future work can address the policy implications of personal cyber insurance.

The second noteworthy concern could have been answered with analyses that we have already conducted. For example, the regressions in the Appendix control for demographic factors, and therefore show the correlations between risk perceptions and demographic variables. However, we did not report on these results because this was not an initial research goal. This follows recommendations on exploring sociodemographic factors in computer security research [75].

The third noteworthy concern is a fascinating direction, but it may have to wait for adoption to increase. Just 1.5% of our respondents had cyber insurance coverage, and this was mostly via home insurance policies.