Taylor & Francis
Taylor & Francis Group

Journal of Computer Information Systems

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ucis20

Cyberspace and Personal Cyber Insurance: A Systematic Review

Richard McGregor, Carmen Reaiche, Stephen Boyle & Graciela Corral de Zubielqui

To cite this article: Richard McGregor, Carmen Reaiche, Stephen Boyle & Graciela Corral de Zubielqui (2023): Cyberspace and Personal Cyber Insurance: A Systematic Review, Journal of Computer Information Systems, DOI: 10.1080/08874417.2023.2185551

To link to this article: https://doi.org/10.1080/08874417.2023.2185551

Published online: 05 Apr 2023.

JOURNAL OF COMPUTER INFORMATION SYSTEMS
https://doi.org/10.1080/08874417.2023.2185551

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS Check for updates

Cyberspace and Personal Cyber Insurance: A Systematic Review

Richard McGregor[a], Carmen Reaiche[a], Stephen Boyle[a], and Graciela Corral de Zubielqui[b]

[a]James Cook University, Townsville, Queensland, Australia; [b]The University of Adelaide, Adelaide, South Australia, Australia

ABSTRACT

As individuals become increasingly digitally dependent, cyber threats and cyber insurance to mitigate them gain relevance. This literature review conceptualizes a framework for siting Personal Cyber Insurance (PCI) within the context of cyberspace. The lack of empirical research within this domain demonstrates a need to identify and define the scope of PCI in order to allow cyber insurers to understand customer needs, and to conduct effective management and distribution of PCI products and services. We conducted a systematic literature review of 229 articles that were clustered into three meta-level themes: cyberspace, personal cyber risk, and PCI. The literature review indicates a significant paucity of research related to PCI particularly as it is influenced by antecedent risk externalities, the nature of cyberspace itself, the PCI market and operations, and post-cyber event support. The paper concludes with a proposal for a future research agenda.

KEYWORDS

Cyberspace; personal cyber risk; personal cyber insurance; cyber insurance; systematic literature review

Introduction

Cyberspace has provided significant improvement to the quality of social connectivity and productivity during the past few decades and allowed enormous capability uplift of information sharing and communication between people and communities.[1] Conversely, cyber technologies have simultaneously caused an increase in personal digital dependency and a reliance on digital technologies which furnish opportunities for adverse events such as data breaches and cyberattacks.[2] These technologies also introduce an insidious threat of omnipresent cyber risk,[3,4] that introduces peril into everyday digital activities, reduces user confidence and productivity.

There has been a significant increase in the number, scale, sophistication, and effectiveness of malicious cyber incidents in recent years is significant,[5] particularly since the advent of the COVID-19 pandemic and the widespread adoption of "work-from-home" practices.[6] The extent of privacy breaches, the proliferation of cyber-criminal activity, and the acuteness of financial consequences has been punishing.[7] Cyber incidents are a persistent and costly cause of business interruption.[3] Furthermore, as entire industries undertake digital transformation, vulnerabilities localized within online connection points that may contribute to a breach also multiply due to escalating interdependencies.[8] Individuals and businesses alike are adversely impacted by cyber incidents, prompting efforts to investigate strategies and tactics to mitigate cyber risk, including cyber insurance.[9] However, cyber insurers face substantial challenges. The lack of historical cyber threat data makes it difficult for insurers to accurately predict the future of customer cyber risk. This is exacerbated by the inherently dynamic nature of cyberspace and the possibility of large cascading loss events due to system interconnectivity.

Until recently, cyber insurance as a product and type of peril was heavily invested within the commercial domain, especially within the United States, which currently holds an estimated 90% of all cyber insurance policies,[10] driven predominantly by regulatory obligations designed to mitigate financial losses and property damage instigated by system failure or malicious cyber events. Cover for cyber liability, cyber extortion and business interruption are also primary drivers for procuring cyber insurance, contributing to a market premium of US$7 billion in 2022 and a market segment that enjoys an annual compound growth rate of 15%.[11] This market is forecast to hit US$22 billion in premium by 2025.[12] According to Lloyd's in 2017, cyber insurance is the ". . . fastest growing line of business in the insurance industry"[13] p. 492] prompted by the increasing scale of total global economic loss due to cybercrime which was recently estimated by MunichRE at US$6 trillion in 2021.

CONTACT Richard McGregor richard.mcgregor@iag.com.au Insurance Australia Group (IAG), 201 Sussex Street, Sydney, NSW 2000, Australia

It is argued that, *ceteris parabus*, the nature of cyberspace intrinsically provides characteristic peculiarities that pose significant and bespoke challenges to cyber insurers, often incongruent with risk attributes commonly associated with traditional personal line insurance products. These challenges include, *inter alia*, a paucity of historical claim/loss data for underwriting and pricing purposes,[14,15] interdependencies of cyber architecture promoting higher cyber risk, difficulties in evaluating cyber risk,[16] intangibility of risk assets (such as data, reputation), lack of standardization across the industry,[17] high and undetermined tail risks, and moral hazard among others. Whilst these challenges are reflected within both the commercial and personal cyber insurance (PCI) domains, each market segment exhibits unique idiosyncrasies. Furthermore, cyberspace itself as a discrete peril and the core source of cyber risk is ill-defined for cyber insurers,[18] and it is postulated that the traditional general insurance customer journey and business model are ill-suited for the peculiarities of cyberspace.[19]

As a consequence of the limitations outlined above, this research aims to fulfill the gaps by surveying the existing literature across three key topic areas: cyberspace, personal cyber risk and PCI. This study contributes to the literature by summarizing previous research by scholars, proposing a framework of research *foci* of extant studies, and identifying avenues for further research.

This article begins with a summary background to the research and an outline of the methodology employed to conduct this literature review, followed by a critique of the literature by “key topic” (namely cyberspace, cyber risk, and cyber insurance) intended to elicit insights for discussion. This framework reflects the sequential dependencies of each key topic, with each section contributing to the baseline knowledge necessary to explore the subsequent key topic. The final section concludes by proposing avenues for future research.

Methodology

The literature review was undertaken using two different review processes. Initially, a narrative literature review was completed as an *a priori* exploration to confirm the research parameters. A subsequent review process was then conducted employing the Preferred Reporting Items for Systematic reviews and Meta-Analysis (PRISMA) framework.[20] To ensure accuracy and transparency, the systematic review of the literature was completed employing a five-stage sequence,[21] as per Figure 1.

Initially, the research problem and the purpose of the literature review were established (Stage 1). This was intentionally broad to reflect the breadth of key topics and comprehensively appraise the range of interpretation, ideation and theory across these domains. The research questions, presented below, were developed at this point to guide the literature review.

- **Research Question 1 (RQ1)**: How has previous research considered the relationships between cyberspace, cyber risk and personal cyber insurance?
- **Research Question 2 (RQ2)**: What aspects of cyberspace, personal cyber risk and personal cyber insurance have not secured any/inadequate attention from researchers?

By addressing the initial contextual research question, “How has previous research considered the relationships between cyberspace, cyber risk and personal cyber insurance?,” the authors provide a baseline knowledge from which the research can answer the second exploratory question, “What aspects of cyberspace, personal cyber risk and personal cyber insurance have not secured any/inadequate attention from researchers?” In general, the existing literature largely overlooks the importance of PCI in preference to commercial cyber insurance and is consequently under-scrutinized.

A framework for analysis was crafted in line with Crossan and Apaydin[22] to define categories for analysis, including type of publication, authors, year of publication, specific keywords (within title, abstract and/or keywords), and linkage(s) to the research questions. The initial collection of records was completed using a Boolean search per key topic as presented in Table 1 (Stage 2).

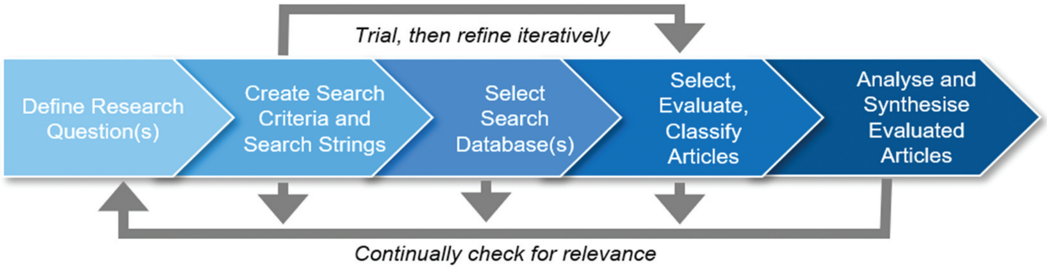
Trial, then refine iteratively
Define Research Question(s)
Create Search Criteria and Search Strings
Select Search Database(s)
Select, Evaluate, Classify Articles
Analyse and Synthesise Evaluated Articles
Continually check for relevance

Figure 1. Staged approach to systematic literature review (adopted from Denyer and Tranfield (2009)).

Table 1. Search terms, strings and results per database (PRISMA all records identified).

	Search Terms, Strings and Results						
Domain	Cyberspace	Qty	Cyber Risk	Qty	Cyber Insurance	Qty	TOTAL
Keywords	Cyberspace, cyber space, definition		Cyber risk, insurance cyber risk, personal cyber risk		Cyber insurance, personal cyber insurance		
Scopus	(TITLE-ABS-KEY (“cyberspace”) OR TITLE-ABS-KEY (“cyber space”) AND ALL (“definition”))	1,131	(TITLE-ABS-KEY (“Cyber Risk”) OR ALL (“Insurance Cyber Risk”) OR ALL (“Personal Cyber Risk”))	1,169	(TITLE-ABS-KEY (“Cyber Insurance”) OR ALL (“Personal Cyber Insurance”))	306	2,606
Emerald	(content-type:article) AND (title:“Cyberspace” OR (title:“Cyber space”) AND (“Definition”))	98	(content-type:article) AND (“Cyber Risk” OR (“Insurance Cyber Risk”) OR (“Personal Cyber Risk”))	169	(content-type:article) AND (“Cyber Insurance” OR (“Personal Cyber Insurance”))	33	300
IEEE	(“All Metadata:”Cyberspace) OR (“All Metadata:”Cyber Space) AND (“All Metadata:”Definition) (Journals)	1,107	(“Publication Title:”Cyber Risk) OR (“Publication Title:”Insurance Cyber Risk) OR (“Publication Title:”Personal Cyber Risk) OR (“Abstract:”Cyber Risk) OR (“Abstract:”Insurance Cyber Risk) OR (“Abstract:”Personal Cyber Risk) (Journals)	304	(“Document Title:”Cyber Insurance) OR (“Document Title:”Personal Cyber Insurance) OR (“Abstract:”Cyber Insurance) OR (“Abstract:”Personal Cyber Insurance) OR (“Author Keywords:”Cyber Insurance) OR (“Author Keywords:”Personal Cyber Insurance)	218	1,629
ScienceDirect	Title, abstract: “Cyberspace” OR “Cyber Space” AND “Definition”	771	“Cyber Risk” OR “Insurance Cyber Risk” OR “Personal Cyber Risk”	180	“Cyber Insurance” OR “Personal Cyber Insurance”	37	988
SubTOTAL		3,107		1,822		694	5,523

Four databases were selected for the literature review: Scopus, Emerald Insight, IEEE and ScienceDirect (Stage 3). These sources provided comprehensive results for each key topic area over the selected ten-year research period (beginning 2012 to end 2021) and all records were imported into EndNote 20.4.1 for de-duplication and subsequent screening as per the PRISMA framework (Stage 4). The inclusion and exclusion criteria for the search are presented in Table 2.

The initial search performed on 5th September 2022 on all three key focus domains returned 5,523 articles. Duplicate papers were identified and removed ($n = 374$), other papers were eliminated ($n = 5{,}049$) as they failed to meet the inclusion criteria (see Table 2). The exclusion criteria needed to be stringent insofar that the authors were aware that the repertoire of references for personal cyber risk/insurance is not large, therefore the search criteria/keywords employed in the search strings were intentionally generic/high level (namely, cyberspace, cyber risk, cyber insurance and so forth) to ensure that an adequate and representative coverage was reached that could subsequently be narrowed by exclusion. The “interdisciplinary context” exclusion criteria was interpretive in nature—namely, any article that was not directly related to the key domains of cyberspace, cyber risk or cyber insurance was removed ($n = 1{,}560$). Another significant number of exclusions ($n = 1{,}795$) were prompted by either the title, abstract or keywords missing key search “terms.” Subsequent to this screening process, an analysis of the remaining screened articles was conducted independently by the researchers and 100 were deemed eligible for review. In-depth quality assurance reduced this number by three (including mislabeled articles causing duplicates) ($n = 97$) which was added to the studies ($n = 132$) identified during the narrative literature review, presenting a final total of 229 articles. Figure 2 provides a summary of the search and analysis process within the PRISMA construct.

Table 2. Inclusion and exclusion criteria and rationale.

Inclusion/Exclusion Criteria and Rationale		
Inclusion Criteria	Exclusion Criteria	Rationale
Publications in peer-reviewed journals	Articles <5 pages	Quality benchmark
Industry organization reports and conferences papers	Books/book section, white papers, magazine articles, websites	Industry insights not available elsewhere
Selected databases (x4)	Any other databases	Comprehensive coverage of existing literature sources
Timeframe: 2012 to 2022	Articles prior to 2012 unless unique work/significant domain classified “not available”	Coverage of latest studies within last decade
English language artefacts	Non-English artefacts and/or full text articles whose status is classified “not available”	Facilitated comprehension and accessibility
Interdisciplinary context	Non-domain subject focus	Appropriateness of context
Keywords in title/abstracts	No keywords in title/abstract	Ensure relevance

Analysis and results

Finally, the key topic results were further categorized into an ontology of subcategories also represented within the EndNote "group" framework. This facilitated the overview of studies within the context of the research questions, allowing the researchers to focus on predominant themes for review and synthesis (Stage 5). The researchers independently reviewed the articles by means of a 20-article pilot test with the intent to establish inter-rater reliability (degree of agreement amongst raters).[23] The results were collected within an MS Excel spreadsheet using a three-group ranking (Excellent .76 to 1, Fair to Good .4 to .75, Low 0 to .4 as defined by Joseph Fleiss in 1981) and the percentage of inter-reliability was subsequently calculated by means of the "joint probability of agreement" which estimates the percentage that raters agree on within a nominal or categorical rating framework. The inter-rater reliability was calculated at 86.7%. By extracting the data into MS Excel, the researchers were able to generate insights into the literature status, themes, and connections (see Figure 7) and identify existing gaps in research within each key topic.

Database source results

Of particular interest is the notable volume growth of Studies Included In Report (SIIR) key topic articles over the specified research time frame (2012 to 2021) – a 15× increase since the beginning of 2012, as demonstrated in Figure 3.

The volume spread of articles per stage of the PRISMA process presented in Figure 4 reflects the maturity (or otherwise) of the key topic within the literature. "Cyber" references appertaining to cyberspace and cyber risk are significantly more volumetric and established than the cyber insurance research domain that materialized only comparatively recently, although research outputs within cyber insurance have grown materially since 2015 (Figure 3).

Database sources employed during PRISMA reflect key capabilities of the source, and also

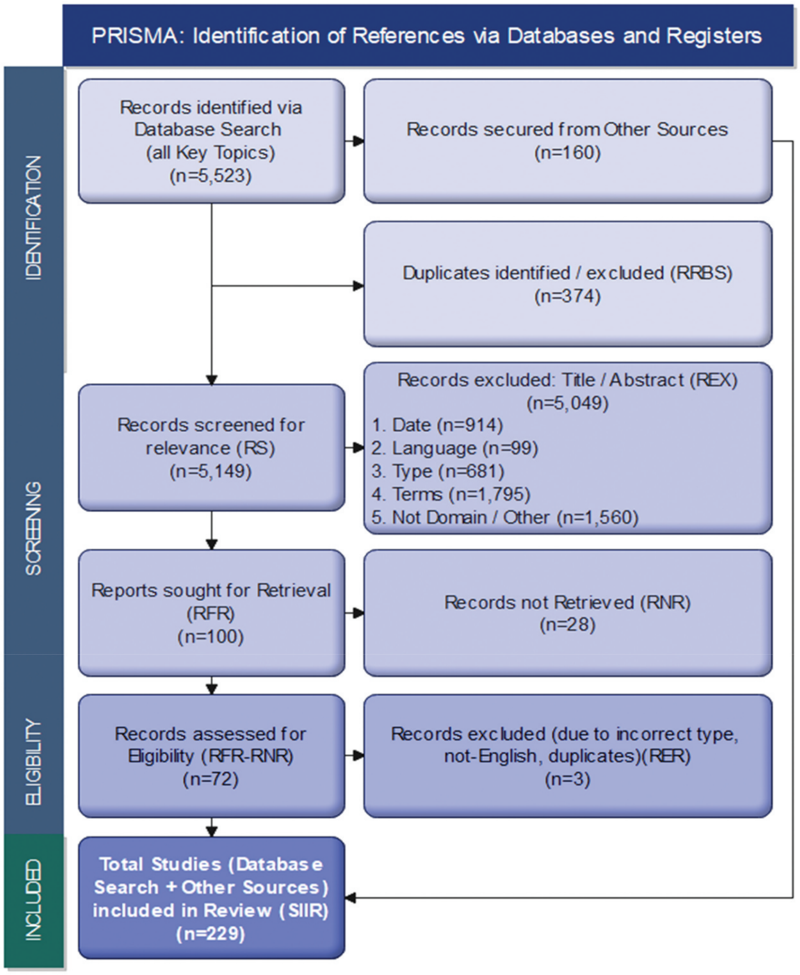
PRISMA: Identification of References via Databases and Registers
IDENTIFICATION
SCREENING
ELIGIBILITY
INCLUDED
Records identified via Database Search (all Key Topics) (n=5,523)
Records secured from Other Sources (n=160)
Duplicates identified / excluded (RRBS) (n=374)
Records screened for relevance (RS) (n=5,149)
Records excluded: Title / Abstract (REX) (n=5,049)
1. Date (n=914)
2. Language (n=99)
3. Type (n=681)
4. Terms (n=1,795)
5. Not Domain / Other (n=1,560)
Reports sought for Retrieval (RFR) (n=100)
Records not Retrieved (RNR) (n=28)
Records assessed for Eligibility (RFR-RNR) (n=72)
Records excluded (due to incorrect type, not-English, duplicates)(RER) (n=3)
Total Studies (Database Search + Other Sources) included in Review (SIIR) (n=229)

Figure 2. PRISMA search and analysis process and outcomes.

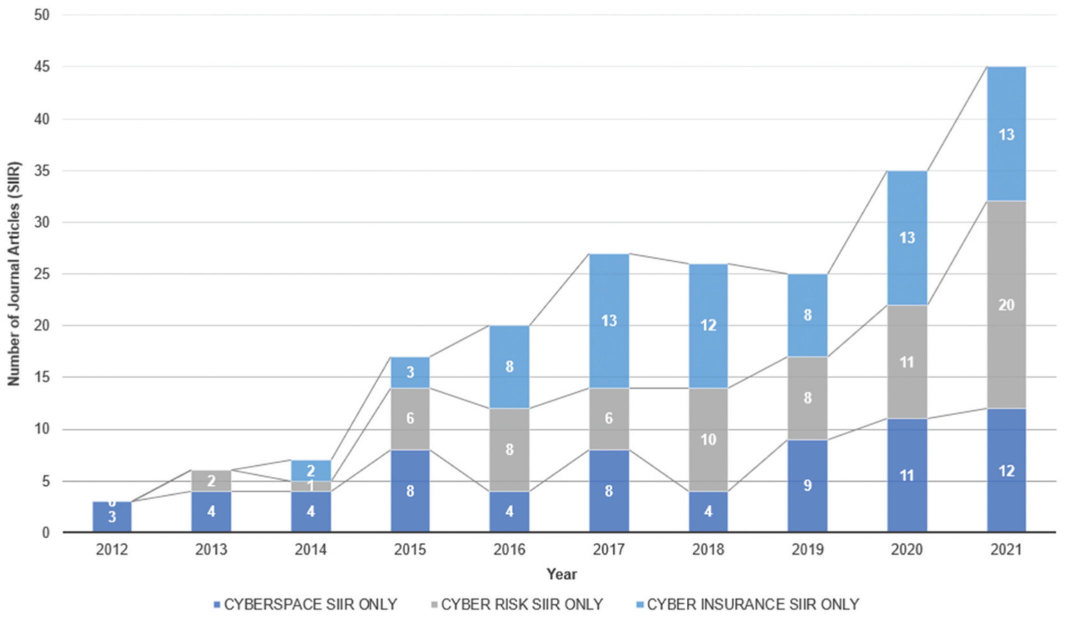

Figure 3. Numbers of studies per key topic over time (2012 through 2021).

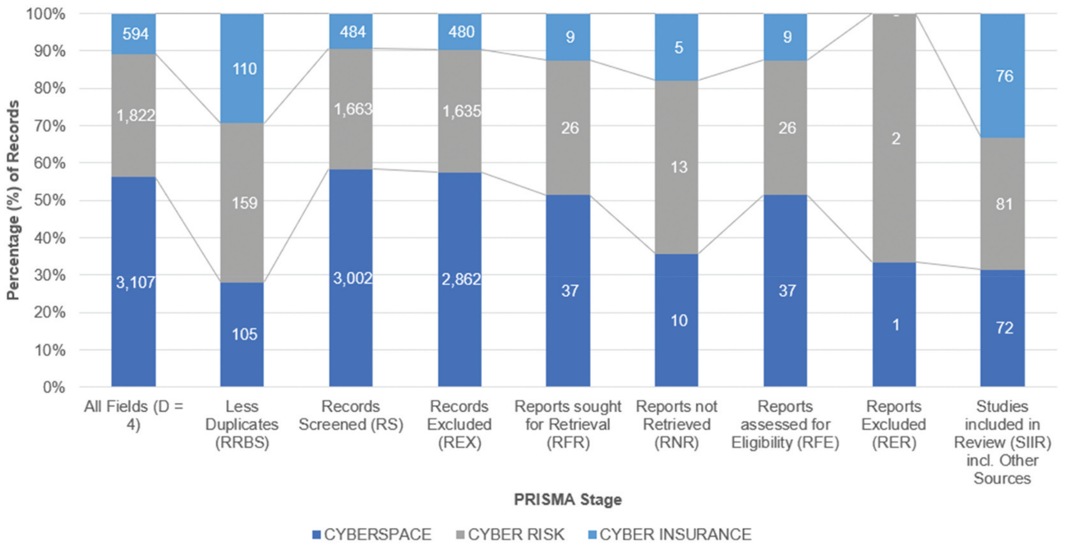

Figure 4. Search results by PRISMA stage, by key topic.

support the insight provided by Figure 4 insofar that the volume of references identified within each database reflects the maturation of that domain. Figure 5 illustrates that Scopus consistently generates appreciably greater record volume in all key topics. IEEE offers meaningful proficiency within cyberspace, although the authors note that the search term "cyberspace" appeared to be interpreted more generically by databases than the (more specific) terms used for the other key topic domains (namely, cyber risk and cyber insurance) which would have induced a higher record return rate, as clearly indicated in Figure 5.

To establish a conceptual scope of the key topic domains, the authors conducted a keyword co-occurrence employing VOSViewer (see Figure 6).[24] The analysis parameters included a total of 376 keywords from all SIIR articles; 66 keywords met the 2× minimum threshold for consideration, generating four clusters and 77 links, with a total link strength of 140. Overall, the color-coding of the keyword co-occurrence network supports the PRISMA analysis insofar that cybersecurity appears a more mature and established domain, with interest in insurance and network security emerging from 2018, cumulating in a focus on cyber insurance (and associated

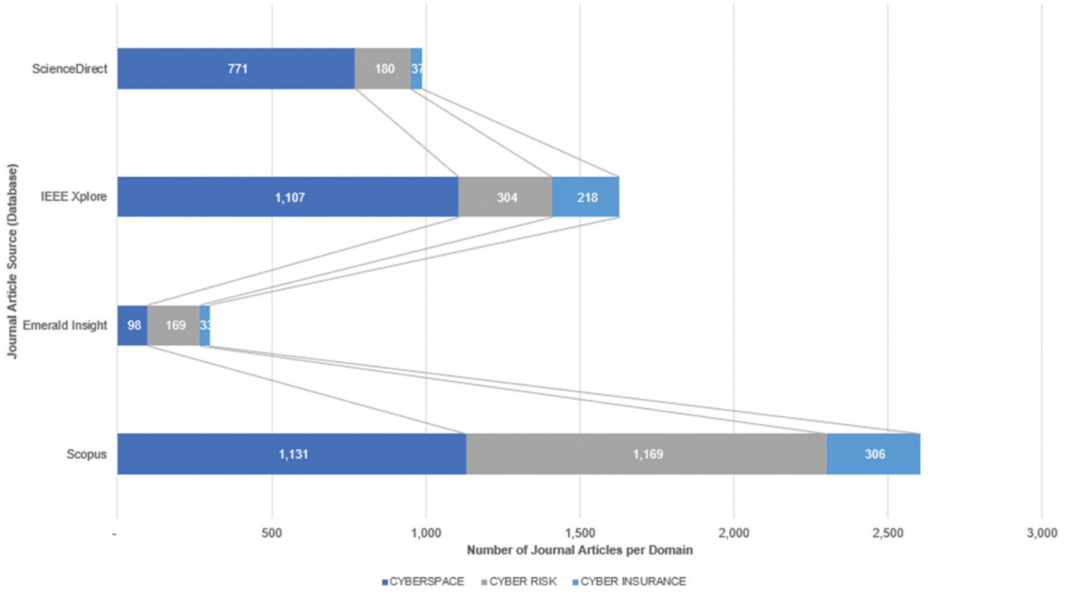

Figure 5. Key topic results (RS) by database source.

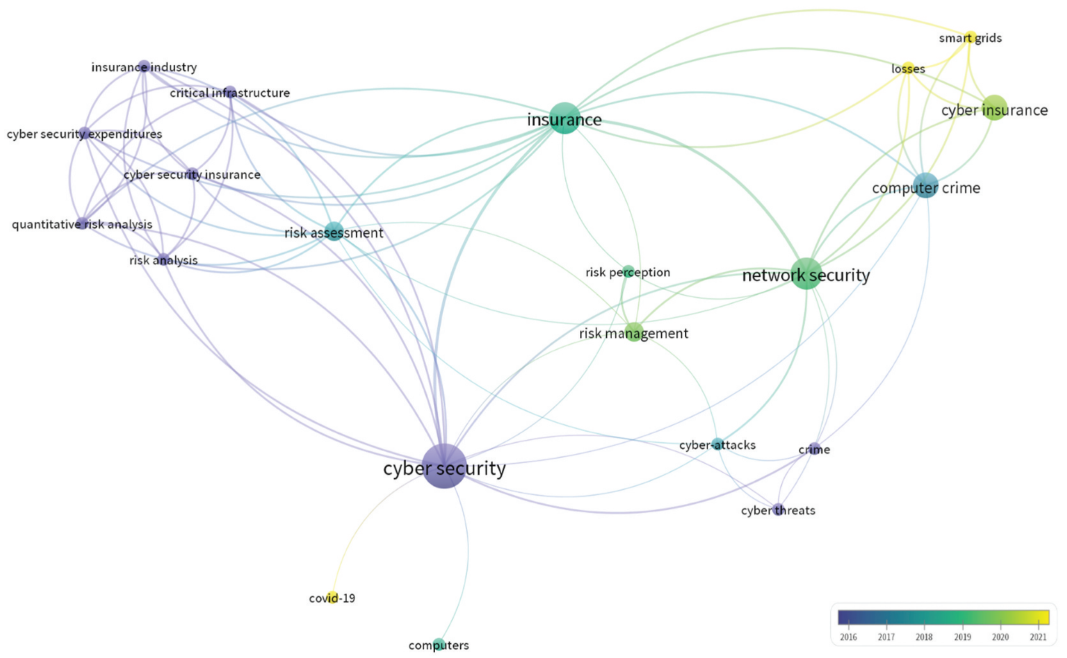

Figure 6. Keyword co-occurrence Network.

losses), COVID-19 and smart technologies over the past few years. The keyword co-occurrence network also provides a stratum for the analysis *foci* offered by the following sections.

Reviewing the knowledge domain

The theme of modern society rapidly becoming increasingly digitally dependent is a consistent *communiqué*, largely taking place within the boundaries of cyberspace.[25] This study challenges the notion that cyberspace within the context of personal cyber risk and PCI are currently well understood and argues that the general insurance business model and current insurer “ways of working” are thereby ill-suited to the provision of PCI.[26] To explore the status quo effectively and judiciously and to conceptualize a potential new paradigm for personal cyber insurers requires the identification of extant and future research *foci* for each key topic.

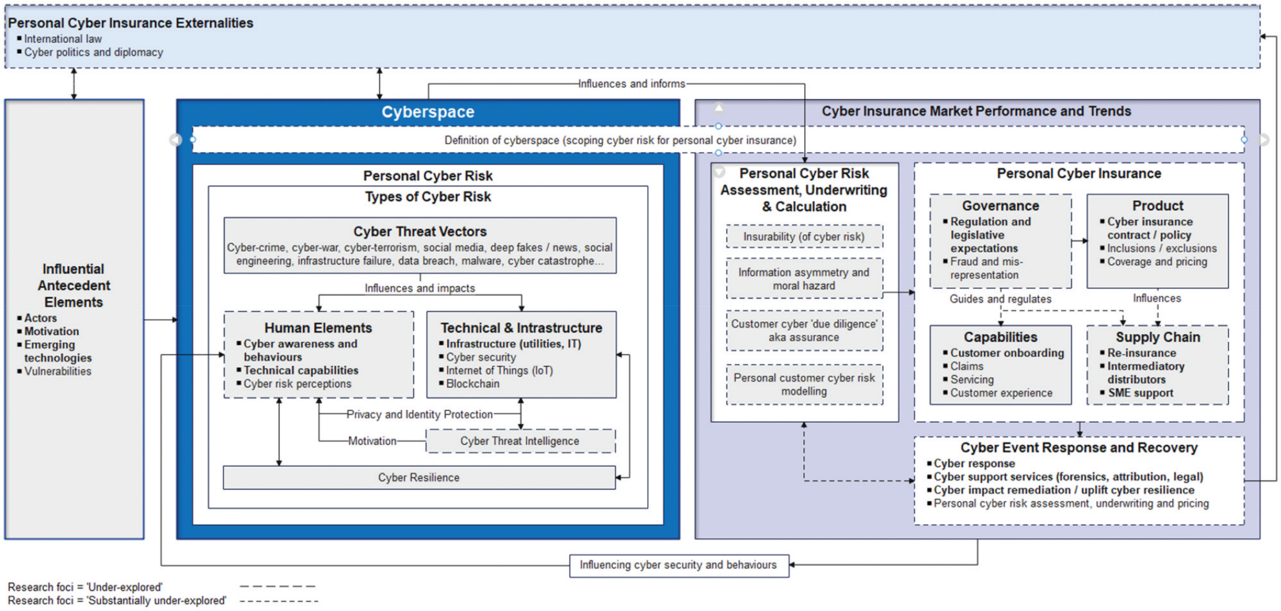
Personal Cyber Insurance Externalities
▪ International law
▪ Cyber politics and diplomacy
Influences and informs
Influential Antecedent Elements
▪ Actors
▪ Motivation
▪ Emerging technologies
▪ Vulnerabilities
Cyberspace
Definition of cyberspace (scoping cyber risk for personal cyber insurance)
Personal Cyber Risk
Types of Cyber Risk
Cyber Threat Vectors
Cyber-crime, cyber-war, cyber-terrorism, social media, deep fakes / news, social engineering, infrastructure failure, data breach, malware, cyber catastrophe...
Influences and impacts
Human Elements
▪ Cyber awareness and behaviours
▪ Technical capabilities
▪ Cyber risk perceptions
Technical & Intrastructure
▪ Infrastructure (utilities, IT)
▪ Cyber security
▪ Internet of Things (IoT)
▪ Blockchain
Privacy and Identity Protection
Motivation
Cyber Threat Intelligence
Cyber Resilience
Cyber Insurance Market Performance and Trends
Personal Cyber Risk Assessment, Underwriting & Calculation
Insurability (of cyber risk)
Information asymmetry and moral hazard
Customer cyber 'due diligence' aka assurance
Personal customer cyber risk modelling
Personal Cyber Insurance
Governance
▪ Regulation and legislative expectations
▪ Fraud and mis-representation
Product
▪ Cyber insurance contract / policy
▪ Inclusions / exclusions
▪ Coverage and pricing
Guides and regulates
Influences
Capabilities
▪ Customer onboarding
▪ Claims
▪ Servicing
▪ Customer experience
Supply Chain
▪ Re-insurance
▪ Intermediatory distributors
▪ SME support
Cyber Event Response and Recovery
▪ Cyber response
▪ Cyber support services (forensics, attribution, legal)
▪ Cyber impact remediation / uplift cyber resilience
▪ Personal cyber risk assessment, underwriting and pricing
Influencing cyber security and behaviours
Research foci = 'Under-explored'
Research foci = 'Substantially under-explored'

Figure 7. Framework summarizing extant and future research foci, based on PRISMA SIIR results (adapted from Guckenbiehl, 2021).

Cyberspace

"Cyberspace" is a widely used term that attracts a wide variety of definitions. Although cyberspace has become an intrinsic element to our daily lives, there is a lack of clarity or consistency on what it actually comprises within the literature.[27] Understanding what exactly constitutes cyberspace is incipient and concepts are typically full of technocentric ambiguity.[28]

Although the Internet is the primary conduit for cyber threats (as a public domain resource), cyberspace is generally considered all networks that connect IT systems[29] (including network environments such as LAN and WAN) where " … information is stored and communication takes place"[30] p. 77]. This highly technical interpretation is similarly supported by the United States Department of Defense Dictionary of Military and Associated Terms[31] p. 64], which defines cyberspace as "… a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems and embedded processors and controllers." Considering cyberspace as a solely technological domain is a common theme within current literature; however, in recent years cyberspace and associated definitions has spread to a myriad of disciplines ranging (non-exhaustively) from information and national security, international law and cybercrime, the social-political domains, Internet governance, and even cyber-geography.[32] As stated by Lambach in his essay, "The Territorialization of Cyberspace," "… cyberspace can no longer be conceived as separate from the 'off-line world'"[33] p. 483]. It is evident, *ergo*, that the definition of cyberspace requires a holistic approach that facilitates generic understanding, regardless of domain or scenario.

The approach proposed by Clark in 2010 on behalf of the US Office of Naval Research offers a descriptive architecture that couples both the technical layers of information processing and the human element. Clark's[34] four-layer model includes the *physical* layer (the physical devices on which cyberspace is built), the *logical* layer (a framework upon which new capabilities are created), the *information* layer (the data created, captured, stored or processed in cyberspace) and the *people* layer (the active users who contribute to and experience the cyberspace ecosystem). This model is framed in a manner that integrates both technical and human constituent parts, emphasizing the "inter-connectiveness" of each layer. Bolpagni supports this notion[35] p. 1644] by proposing a "sociotechnical composite index" that considers "… human, social, organizational, economic, and technical factors, as well as the complex interaction between them;" and also supported by.[36] The model provides an embryonic framework unmatched in the literature, and one that offers a baseline to a more holistic and pragmatic definition of cyberspace. It is suggested that the model could be further developed by incorporating a layer of governance to facilitate and control future cyberspace development, attribution, international law and sovereignty.

The definition of cyberspace can be seen from the above analysis as necessarily broad in scope, whilst also technically specific if appropriate. The consequence on the provision of cyber insurance is significant, as this directly influences the defined scope of cyber risk to be covered by insurers. Thus, it is imperative to clarify the term "cyberspace" *a priori* to any subsequent discussion related to cyber insurance and/or cyber risk.

Cyber threats and vectors

Technology is rapidly evolving and pushing the boundaries of consumer "digital dependency" within cyberspace, driven by social media, online and automated transactions, social networks, the adoption of cloud computing and storage services.[37] As cyberspace becomes society's new preoccupation, adverse cyber events are becoming increasingly common[38,39]; IT infrastructure failures impact core online services and cybercriminals develop neoteric attack types, tools and techniques ("T&T") that open access to increasingly sophisticated and secure environments, increase their ability to perform large-scale damage, secure material quantities of personal data and/or intellectual property (IP), and mitigate attempts at attribution.

The scope and multifariousness of cyber threats within the personal digital landscape is punitive for consumers. Threats vary from simple automated ransomware algorithms leased by the month on the dark web by amateur hackers through to complex theft of sensitive medical and personal details by State-sponsored actors. Recent examples of data breaches that have affected people include Uber's 2016 data breach (which released private data belonging to 47 million drivers and riders) and the 2017 Equifax breach that revealed financial details of 145.5 million US citizens (approximately 40% of the US population).[40] Li and Liu suggest that the specific nature and technique of each malicious cyber event are defined by the purpose of the attack (such as financial (monetization), political, theft of IP or personal/sensitive data, psychological),[5] although this assertion depends on the assumption that adequate resources are available to the attacker to initiate target reconnaissance, compile algorithms, launch and monitor/adjust the attack cadence as necessary.

Cybersecurity

Cybersecurity is defined by Craigen[41] p. 13] as "… the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from events that misalign *de jure* from *de facto* property rights." Whilst this definition relies on a legal standpoint, this perspective does not limit considering cybersecurity as an interdisciplinary framework employing a variety of roles, models, and processes.[42] Therefore, the purpose of cybersecurity is intent on "… restraining and mitigating negative outcomes [emanating from cyberspace] …" as proposed by Etschemaier[43] p. 140]. In 2019, Etschemaier proposed a "rational, holistic framework"[43] p. 91] to counter what is perceived as disparity in the scope of cybersecurity, which currently encourages differences in approaches, methods, objectives, and users' responsibilities within cyberspace. This rationale supports Craigen's earlier study in 2014[41] p. 13] that concluded that there is an "… absence of a concise and universally acceptable definition that captures the multidimensionality of cybersecurity," although his commentary is oriented toward the theme that distinct disciplines should act in congruence to address "… the growing and complex threats to cyberspace and cyberspace-enabled systems."

The authors contend that the conventional approach to seeking technological solutions to all cybersecurity challenges in cyberspace is circumscribed, and that this paradigm may deviate focus from the actual causes of the problems[43] which lie within the interdependencies between both technical and human contexts. Cybersecurity has typically adopted a technocentric approach, oft with minimal knowledge or appreciation of the individual end user cognitive capabilities, motivations[44] or nontechnical cyber countermeasures. Consequently, cybersecurity has traditionally prioritized technical responses (such as firewalls, antivirus applications, intrusion detection systems) to mitigate cyber threats,[45] while Corradini[46] and Gallegos-Segovia *et al.*[47] contend that social engineering cyberattacks are considered the cybersecurity top threat, as they target the "weak link," manipulating individual users to divulge personal information by exploiting social and cognitive (psychological) vulnerabilities. In support of Craigen *et al.* and Etschemaier's perspective above, recent investigations into cybersecurity advocate for an intrinsically holistic approach to contest the cybersecurity landscape.[48]

Nature of cyber risks

Cyber risk can be characterized as "any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, integrity, or availability of data or services"[49] p. 658]. It is important to note that cyber risks may evolve naturally due to, for example, a natural disaster or power surge impacting hardware, or be prompted by man-made actions arising from human error, cybercriminals, cyberwar, or terrorism.[29] As a threat vector, cyber risk includes an expansive catalog of perils, the most obvious to an individual being data breaches that include disclosure of their personal information, insertions of malware, or identity theft[50] and several studies have attempted to establish an ontology of cyber risk.[51] However, the interconnectedness of cyberspace also raises a spectrum of third-party cyber risks[52] that are often not within the congruence of the consumer but obfuscated by the interdependent nature of cyberspace. For instance, a telecommunications network failure could impact thousands of Internet users, or an insider-instigated data breach could release quantities of sensitive medical data from a health provider, neither instance of which would typically allow a consumer prior knowledge or provide an opportunity to conduct any form of additional preventative measures.[53]

Personal cyber risk

Although attention to cyber risk has grown substantially in the literature over the past decade, only few researchers have focused on this subject from the perspective of business, economics[54] or the experience of the individual. PCI provides risk mitigation for cyber risks emerging from cyberspace; it is therefore pivotal to understand what personal cyber risks are, where they emanate from, and how to best identify robust and simple countermeasures that are easily implemented by individuals. In their research, Kovačević *et al.* conducted an exploratory study to analyze personal factors that influence cybersecurity awareness such as socio-demographics, cybersecurity perceptions, IT usage, experience of previous cyberattacks and generic IT knowledge.[55] Kovačević *et al.* contend that humans are "… the central figures in cybersecurity and the way to reduce risk in cyberspace is to make people more security aware"[55] p. 125140], thus suggesting that personal accountability and effort is necessary to mitigate personal cyber risk. The outcomes were insightful, and although the participants were students, and thus could be considered technically competent digital natives and not representative of society in general, they were typically found not to behave securely and not enjoy adequate knowledge to protect themselves in cyberspace. These results are supported by similar research conducted by Parsons *et al*,[56] although a study carried out by Alquahtani[57] found that increasing knowledge of personal security parameters (such as passwords) increased the level of cybersecurity awareness of students.

The implications of lower levels of information security awareness within cyberspace contribute directly to a higher degree of personal cyber risk and the impact is amplified by individual's online behaviors.[58] Personal cyber risk is universal amongst digitally engaged individuals, as online capabilities have propelled common, transcultural societal behaviors to change, enabled by ubiquitous mobile devices—in 2019 IoT Analytics estimated that there were 17 billion Internet-connected devices worldwide and this number is anticipated to expand by an annual growth rate of 10%.[59] Consumers routinely establish more online accounts, rely on more systemic inter-connectivity and store more personal and sensitive data than any time previously, thus augmenting their personal cyber risk profile. Studies report that whilst consumers concurrently display significant anxiety about threats stemming from cyberspace, they typically invest minimal effort in an attempt to uplift their personal cybersecurity and safety.[40]

Personal cyber risk diverges from commercial or infrastructure risk insofar that whilst many cyber threats are analogous between both scenarios (such as malware, phishing, or ransomware), frequently the nature of cyber events, for example, cyber bullying or stalking, at the personal level are unique to an individual and are not applicable to other circumstances. *Ceteris parabus*, this would suggest that the needs of individuals to prevent and protect their "digital selves" within cyberspace, as well as the ability to identify and engage specialist cyber services support, is pivotal to securing a safe online experience, but that these capabilities are often not evident or available. Pavel and Gafni[60] provide an excellent exploration into the "invisible hole" of cyber services offered by insurers within the commercial domain, but no studies furnish insights at the personal level. This dilemma is exacerbated by customers typically underestimating the probabilities and impact of cyber events,[61] induced predominantly by a knowledge and expectation gap by both consumers and the providers of cyber support services.

Personal cyber insurance

Cyber insurance as a research topic has been studied for more than two decades[62]p1] with initial studies exploring a novel and distributed "system application of insurance to the internet." Whilst the literature provides a breadth of domain subject matter that offers in-depth analysis which contributes to a solid foundation of knowledge, at the meta level the research displays common traits that limit the potential of these investigations. In particular, numerous studies employ conceptual and/or mathematical models to propose insights (such as[63,64] which are beneficial within specific scenarios or circumstances but oft lack a holistic or interdisciplinary perspective.[65] These studies typically concentrate on a single entity (insurer, risk type and customer) whereas in reality, cyberspace and the claims process are highly dynamic with in-depth and on-going interactions. As noted by Liu *et al*,[66] whilst there is an extensive repertoire of research into the theoretical elements of the cyber insurance ecosystem, very few researchers have employed real data or engaged the expertise of system security specialists and/or business architects—an observation compounded by Allodi *et al.*, who intimated that in other domains risk assessment is nominally based on quantitative estimates, whereas cyber risks are computed employing qualitative metrics that are contingent on the opinion of subjective experts.[67] All the aforementioned limitations impede attempts by researchers to integrate the influence of cyberspace and cyber risks with the needs of customers, and the authors suggest that these challenges are also contrary to cyber insurer current "ways of working." The following section sites cyber insurance within the wider context of cyberspace.

Cyber insurance market

Since its inception as a global phenomenon, cyberspace has materialized as an interdependent domain capable of challenging the *status quo* of the contemporary general insurance paradigm due to idiosyncrasies which escape the traditional premises upon which insurance products and services are based. Cyber insurance emerged at scale as a distinct product segment during the late 1990s[10] in an attempt by general insurers to provide a traditional risk transfer option to commercial customers facing an emerging and ubiquitous digital peril.[17] Increasingly, in recent years insurers are methodically removing any indirect coverage for cyber events (alias, "silent cyber") within other lines of insurance (such as property and general liability)[68] allowing the industry to focus on issuing specialist (dedicated) first- or third-party cyber policies.

The introduction of PCI is a recent phenomenon, prompted by public realization that individuals are more vulnerable to cyber events than organizations as they typically have less resources and expertise to augment their cyber defense capabilities[69] and are often the inadvertent victims of third-party data breaches. In their study, Papatsaroucha *et al*. proposed the concept of a "user susceptibility profile" which could provide a baseline against which an individual's cyber stance could be determined by a cyber insurer before issuing a PCI policy (namely, during the initial "assurance" stage).[70] This concept is further supported by Dodel and Mesch[71] p. 75] in a study that supports the notion that "... the best predictor of cyber-safety behaviors are digital safety skills" and that by focusing on specific "cyber-safety" skills these may improve an individual's cyber stance and lower their risk profile.

Personal cyber insurance... a non-traditional peril type

Similarly, the PCI market offers a dynamic growth opportunity for the insurance industry, with SwissRE claiming that premiums in the United States have reached 25% that of the commercial sector[4] currently estimated by MunichRE at US$9.2 billion (beginning of 2022).[12] MunichRE assert that like commercial cyber insurance, risk awareness and levels of underinsurance within individual consumers indicate greater discrepancies—even amongst those considered to be "digital natives"[55] and despite a third of consumers with connected technology having previously experienced identify theft.[72]

PCI is analogous to commercial lines insofar that individuals share many similar cyber risks to organizations. Personal cyber risks and impacts depend on the context of the individual; namely, the extent of exposure to cyberspace, cybersecurity measures and behaviors, and each policy holder is heterogenous thus attracting a unique cost and effort to reinstate pre-cyber event status.[73] The type and personalization of cyber support services needed by PCI customers vs commercial organizations are therefore tangibly different, necessitating distinctive skillsets, responses and remedial support services unique to each product domain, although the authors are unaware of any specific studies exploring this divergence.

Within the general insurance industry, cyber policies —especially *PCI* – is a nascent peril type and product.[74] The need for a personal line cyber product has arisen seemingly as a consequence of the more established commercial cyber insurance market, whereby individual consumers recognize that they also require an option to mitigate cyber threats originating from cyberspace that pose risks to themselves at an individual level.[4] The unique idiosyncrasies of cyberspace inherently influence the nature, type and impact of the peril against which the policyholder is covered and contribute to an insurance product that is atypical of those commonly included within the general insurance portfolio.[75] Consequently, the support required by individuals within the context of an adverse cyber event is often wider than financial remediation and may extend to a variety of pre- and post-cyber event activities such as pre-approval assurance services to uplift a customer's technical cyber resiliency (predominantly a service employed within the commercial cyber insurance domain),[76] specialist cyber forensic services to attribute identify theft and associated unlawful withdrawal of funds and/or fraud, or delivering counseling for emotional and psychological harm induced by cyberbullying, mobbing or stalking.[4] In a study conducted by SwissRE in 2019, less than 10% of surveyed consumers indicated that they were only interested in financial cover vs additional specialist cyber services,[4] which strongly suggests that consumers are not confident in their capabilities to protect themselves adequately or successfully navigate the aftermath of a cyber event. The 2022 Symantic Norton Cyber Security Insights Report supports this assertion, having surveyed 10,030 adults in ten countries – 53% of participants admitted that they were unaware of how to protect themselves from cybercrime.[77]

Cyber threats and vectors are in a state of continual and dynamic motion, seemingly generating a persistent succession of new cyber threats that influence existing, or create entirely new, use cases for which personal cyber insurers must adapt.[27] Traditional products such as motor or property exhibit tangible characteristics that remain relatively static,[78] whereas there are an increasing number of studies in the literature exploring specific risk use cases such as cyberattacks on electric vehicle charging stations,[79] cyber-enabled burglary of smart homes[80] and cyber threats faced by autonomous and connected vehicles.[81] The authors argue that these non-traditional and still-emerging risks offer challenges to personal cyber insurers as the boundaries of such novel use cases have yet to be defined. For instance, in the event of the theft of an electric vehicle employing a cyber-initiated attack from the driveway of a private property, would coverage be offered by the policy holder's home, motor or PCI? Defining the use case parameters between the coverage of different product types is pivotal to ensure transparency and confidence between insurers and customers and is considered a priority within the literature,[18] although at this point no studies have specifically targeted this need.

Theoretical framework for extant and future research within key foci

There has been much emphasis in this systematic review on the unique character of cyberspace, and how cyber risks emanating from the digital landscape offer particular challenges to personal cyber insurers that are quite different from traditional general insurance perils and products.[82] This study aimed to offer a systematic review of the literary contextual relationships between, and the extant nature of the literature exploring key themes of, cyberspace, personal cyber risk and insurance. Extrapolating insights secured during the PRISMA analysis, the authors conceptualized a framework that identifies the various *foci* and relationships of extant studies and identified underexplored topics and capabilities for future research initiatives in a manner adapted from.[83] The summary framework in Figure 7 presents the core elements and associated linkages within the key topics of cyberspace, personal cyber risk and cyber insurance, along with the heterogeneous levels of existent research, represented by the intensity of dotted lines. Thematically, the schema posits an egregious structural congruence between commercial and PCI in terms of components but clearly demonstrates that elements necessary to provide cyber coverage tailored for *individuals* (including human elements, assurance, pricing, governance, capabilities and cyber response and remediation *inter alia*) are typically under-researched.[26]

Examining the PCI landscape at the meta level (Figure 7) offers key insights into the categorizations and constructs employed in the literature and offers a blueprint of their associated relationships in a manner adapted from Guckenbiehl.[84] Preeminently, the model clearly differentiates cyberspace and the unique idiosyncrasies of personal cyber risk from the cyber insurer operational framework, thus emphasizing the holistic and multidisciplinary nature of the domain. Very few studies analyzed across all *foci* considered implications for the individual (compared to impacts or use cases associated with commercial cyber insurance), thus providing substance for the widespread assertion presented within the model that this domain presents a substantially underexplored status—although it is recognized that studies within commercial cyber insurance may provide substance for research and insights into PCI. The authors also contend that the knowledge and research link between cyberspace and cyber insurance industry is immature, requiring researchers and practitioners to excogitate holistically across the PCI domain thereby materially adding to the body of knowledge of the domain and influencing variables. Figure 7 offers some assistance in identifying future research opportunities by illustrating substantially underexplored constituents.

Avenues for future research

Despite its status as a relative newcomer to the insurance industry, cyber insurance has attracted intensifying attention from academic researchers in recent years. Whilst there has been a profusion of theoretical investigation into pertinent and influential subjects such as (cyber) asymmetric information,[85] cyber risks[86,87] and cyber-legal frameworks,[88] there is a clear need to extend attention in empirical research, as recommended by Böhme and Schwartz[89] who observed that research conducted in general and cyber insurance differed insofar that studies in the former domain focused on existing business approaches, whereby cyber investigation tended toward conceptualizing theory first in anticipation of establishing a real-world outcome.[90] Influential researchers Eling and Schnell support this assertion, stating that further investigations are required in this field, both within the demand and supply side.[91]

Continued investigation into the nucleon of contemporary cyber insurance topics will inevitably continue apace, but novel mechanisms to materially improve the capability of PCI should also be pursued, including avant-garde cross-disciplinary models such as behavioral-dependent pricing, continuous and dynamic underwriting and holistic personal "digital self" cyber monitoring. Future studies should explore more deeply customer needs for cyber insurance across the customer journey, and how cyber insurers should orientate their architecture and business models[26] to best protect their customers effectively, and ensure profitability.

Disclosure statement

Richard McGregor is an employee of Insurance Australia Group (IAG) and a PhD Candidate at James Cook University, Australia.

Funding

This paper was supported by The Firemark Collective, a wholly owned entity of Insurance Australia Group (IAG).

Author contributions

Richard McGregor (conceptualization, methodology, original draft), Associate Professor Carmen Reaiche and Professor Stephen Boyle, Associate Professor Graciela Corral de Zubielqui (review and editing). All authors and Insurance Australia Group (IAG) have read and agreed to the published version of this article.

References

1. Carter DM. Cyberspace and Cyberculture. In: Kobayashi A, editor. International encyclopedia of human geography. 2nd ed. Elsevier: Oxford; 2020. p. 143–47.
2. Shanker AK, Usha G. Cyber threat landscape in cyber space. 2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA); 2017; Coimbatore, India. Institute of Electrical and Electronics Engineers Inc. doi:10.1109/ICECA.2017.8203709.
3. Dobie GEA. 2021 Allianz Risk Barometer. Germany: ALLIANZ Global Corporate and Specialty SE; 2021. https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2021.html.
4. Willi F, Bundt M. Personal cyber insurance: protecting our digital lives. Zurich, Switzerland: Swiss Reinsurance Company Ltd; 2019. https://www.swissre.com/dam/jcr:68e4d8fb-509c-4182-a219-c803f7d23af1/ZRH-18-00632-P1_Personal_cyber_insurance_Publication_WEB.pdf.
5. Li Y, Liu Q. A comprehensive review study of cyber attacks and cyber security; emerging trends and recent developments. Energy Rep. 2021;7:8176–86. doi:10.1016/j.egyr.2021.08.126.
6. Lallie HS, Shepherd LA, Nurse JRC, Erola A, Epiphaniou G, Maple C, Bellekens X. Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comput Secur. 2021;105:102248. doi:10.1016/j.cose.2021.102248.
7. Agrafiotis I, Nurse JRC, Goldsmith M, Creese S, Upton D. A taxonomy of cyber-harms: defining the impacts of cyber attacks and understanding how they propogate. J Cybersecur (Oxford). 2018;4(1):4. doi:10.1093/cybsec/tyy006.
8. Süzen AA. A risk assessment of cyber attacks and defense strategies in industry 4.0 ecosystem. Int J Comput Netw Inf Secur. 2020;1(1):1–12. doi:10.5815/ijcnis.2020.01.01.
9. Khaliligarekani M. Incentive Mechanisms for Managing and Controlling Cyber Risks: The Role of Cyber Insurance and Resource Pooling. USA: University of Michigan; 2020. https://deepblue.lib.umich.edu/bitstream/handle/2027.42/155236/khalili_1.pdf?sequence=1&isAllowed=y
10. Kalinich K, Foord-Kelcey L. Global Cyber Market Overview (AON): Uncovering the Hidden Opportunities. Chicargo, USA: AON Inpoint; 2017. https://www.aon.com.au/australia/insights/reports-and-whitepapers/2017/global-cyber-market-overview-inpoint-report.pdf.
11. Parrant M. Cyber Insurance Market Insights Q3 2018. Australia: AON; 2018 https://aoninsights.com.au/cyber-insurance-market-insights-q3-2018/.
12. Kreuzer M, von Dem Knesebeck A. MunichRE Global Cyber Risk and Insurance Survey 2022. Germany: Münchner Rückversicherungs-Gesellschaft; 2022.
13. Strupczewski G. Current State of the Cyber Insurance Market. 10th Economics & Finance Conference; 2018; Rome, Italy.
14. (ENISA), E.N.a.I.S.A., R. N, and R. Europe. Incentives and barriers of the cyber insurance market in Europe. Resilience and CIIP Program. Greece: European Network and Information Security Agency (ENISA); 2016.
15. Tøndel I, Seehusen F, Gjære EA, Moe ME. Differentiating cyber risk of insurance customers: the

insurance company perspective. International Conference on Availability, Reliability, and Security; 2016; Salzburg, Austria. p. 175–90.
16. Dambra S, Bilge L, Balzarotti D. SoK: cyber insurance - technical challenges and a system security roadmap. In: IEEE Symposium on Security and Privacy (SP) San Francisco, CA, USA; 2020. p. 1367–83. doi:10.1109/SP40000.2020.00019.
17. Granato A, Polacek A. The growth and challenges of cyber insurance. In: Essays on issues. Chicago, USA: The Federal Reserve Bank of Chicago; 2019. p. 1–6.
18. Friedman S, Thomas A. Demystifying cyber insurance coverage. In: Demystifying cyber insurance coverage. USA: Deloitte Touche Tohmatsu Limited; 2017. p. 2-17.
19. Meland PH, Tøndel IA, Solhaug B. Mitigating risk with cyberinsurance. IEEE Secur Privacy. 2015;13(6):38–43. doi:10.1109/MSP.2015.137.
20. Sarkis-Onofre R, Catalá-López F, Aromataris E, Lockwood C. How to properly use the PRISMA statement. Syst Rev. 2021;10(1). doi:10.1186/s13643-021-01671-z.
21. Denyer D, Tranfield D. Chapter 39: *Producing a systematic review*. In: Buchanon D, Bryman A, editors. The SAGE handbook of organizational research methods. United Kingdom: SAGE Publishing; 2009. p. 671–89.
22. Crossan MM, Apaydin M. A multi-dimensional framework of organizational innovation: a systematic review of the literature. J Manage Stud. 2010;47(6):1154–91. doi:10.1111/j.1467-6486.2009.00880.x.
23. Ping W. The inter-rater reliability in scoring composition. Engl Lang Teach. 2009;2(3):39–43. doi:10.5539/elt.v2n3p39.
24. Orduña-malea E, Costas R. Link-based approach to study scientific software usage: the case of VOSViewer. Scientometrics. 2021;126(9):8153–86. doi:10.1007/s11192-021-04082-y.
25. Eling M, Lehmann M. The impact of digitalization on the insurance value chain and the insurability of risks. Geneva Pap Risk Insur. 2017;43(3):359–96. doi:10.1057/s41288-017-0073-0.
26. Tøndel IA, Meland PH, Omerovic A, Gjære EA, Solhaug B. Using cyber insurance as a risk management strategy: knowledge gaps and recommendations for further research. Norway: SINTEF Digital; 2015.
27. Medeiros BP, Goldoni LRF. The fundamental conceptual trinity of cyberspace. Contexto Int. 2020;42(1):31–54. doi:10.1590/s0102-8529.2019420100002.
28. Eggenschwiler J. Accountability challenges confronting cyberspace governance. Internet Policy Rev. 2017;6(3). doi:10.14763/2017.3.712.
29. Eling M, Hendrick Wirfs J. Cyber risk: too big to insure? Risk transfer options for a mercurial risk class. Switzerland: University of St. Gallen; 2016. p. 1–174. 978-3-7297-2006-0.
30. Mareši NC. Information in cyberspace - actuality and challenges. Strategic Impact. 2020;76:76–88.
31. Defence, U.S.D.o. United States department of defence dictionary of military and associated terms. 2021. p. 360.
32. Gao C, Guo Q, Jiang D, Wang Z, Fang C, Hao M. Theoretical basis and technical methods of cyberspace geography. J Geogr Sci. 2019;29(12):1949–64. doi:10.1007/s11442-019-1698-7.
33. Lambach D. The territorialization of cyberspace. Inter Stud Rev. 2020;22(3):482–502. doi:10.1093/isr/viz022.
34. Clark D. Characterising cyberspace: past, present and future. USA: MIT CSAIL: MIT; 2010. p. 2016–28.
35. Bolpagni M. Cyber risk index: a socio-technical composite index for assessing risk of cyber attacks with negative outcome. Qual Quant. 2022;56(3):1643–59. doi:10.1007/s11135-021-01199-3.
36. Gandhi R, Sousan W, Laplante PA. Dimensions of cyber attacks: cultural, social, economic and political. IEEE Technol Soc Mag. 2011;2011(1):28–38. Spring doi:10.1109/MTS.2011.940293.
37. Bendovschi A. Cyber-attacks – trends, patterns and security countermeasures. 7th International Conference on Financial Criminology 2015; 2015; Oxford, United Kingdom. p. 24–31.
38. Aldasoro I, Gambacorta L, Giudici P, Leach T. The drivers of cyber risk. J Financ Stab. 2022;60:100989. doi:10.1016/j.jfs.2022.100989.
39. Singh A, Sharma VK, Chauhan S. 5th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud). A hybrid model for cyberspace security; 2021; Palladam, India. doi: 10.1109/I-SMAC52330.2021.9640951.
40. Kostyuk N, Wayne C. The microfoundations of state cybersecurity: cyber risk perceptions and the mass public. J Global Secur Stud. 2021;6(2). doi:10.1093/jogss/ogz077.
41. Craigen D, Diakun-Thibault N, Purse R. Defining cybersecurity. Technol Innovation Manage Rev. 2014;4(10):13–21. doi:10.22215/timreview/835.
42. Etschmaier MM. A purposeful systems design approach for cybersecurity. EPiC Ser Comput. 2019;63:90–100.
43. Etschmaier MM. Critical issues of cybersecurity: solutions beyond the technical. Inter J Comput Appl. 2019;26:140–53.
44. Pollini A, Callari TC, Tedeschi A, Ruscio D, Save L, Chiarugi F, Guerri D. Leveraging human factors in cybersecurity: an integrated methodological approach. Cognit Technol Work. 2022;24(2):371–90. doi:10.1007/s10111-021-00683-y.
45. Mouton F, Leenen L, Venter HS. Social engineering attack examples, templates and scenarios. Comput Secur. 2016;59:186–209. doi:10.1016/j.cose.2016.03.004.
46. Corradini I. Refining the approach to cybersecurity. In: Kacprzyk J, editor. Building a cybersecurity culture in organizations Switzerland: Springer Nature AG; 2020. p. 49–62. doi:10.1007/978-3-030-43999-6_3.
47. Gallegos-Segovia PL, Bravo-Torres JF, Larios-Rosillo VM, Vintimilla-Tapia PE, Yuquilima-Albarado IF, Jara-Saltos JD. Social engineering as an attack vector for ransomware. 2017 Chilean Conference on Electrical, Electronics Engineering, Information and Communication Technologies; 2017; Pucon, Chile.
48. Al-Darwish AI, Choe P. A framework of information security integrated with human factors. International Conference on Human-Computer Interaction; 2019; Orlando, USA. doi:10.1007/978-3-030-22351-9_15.

49. Wrede D, Stegen T, Graf von der Schulenburg JM. Affirmative and silent cyber coverage in traditional insurance policies: qualitative content analysis of selected insurance products from the German insurance market. Geneva Pap Risk Insur. 2020;45 (4):657–89. doi:10.1057/s41288-020-00183-6.
50. Falco G, Eling M, Jablanski D, Weber M, Miller V, Gordon LA, Wang SS, Schmit J, Thomas R, Elvedi M, et al. Cyber risk research impeded by disciplinary Barriers. Science. 2019;366(6469):1066–69. doi:10.1126/science.aaz4795.
51. Merah Y, Kenaza T. Ontology-based cyber risk monitoring using cyber threat intelligence. The 16th International Conference on Availability, Reliability and Security (ARES 2021); 2021; Vienna, Austria. doi:10.1145/3465481.3470024.
52. Batra A. Cyber security management: creating governance, risk and compliance framework. J Software Eng. 2020;14(4):27–33. doi:10.26634/jse.14.4.17403.
53. Wheatley S, Hofmann A, Sornette D. Addressing insurance of data breach cyber risks in the catastrophe framework. Geneva Pap Risk Insur. 2020;46(1):53–78. doi:10.1057/s41288-020-00163-w.
54. Eling M, Wirfs J. What are tHe actual costs of cyber risk events? Eur J Oper Res. 2018;272(3):1109–19. doi:10.1016/j.ejor.2018.07.021.
55. Kovačević A, Putnik N, Tošković O. Factors related to cyber security behavior. IEEE Access. 2020;8:125140–48. doi:10.1109/ACCESS.2020.3007867.
56. Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Comput Secur. 2014;42:165–76. doi:10.1016/j.cose.2013.12.003.
57. Alqahtani MA. Factors affecting cybersecurity awareness among university students. Appl Sci. 2022;12 (5):2589. doi:10.3390/app12052589.
58. Cox EB, Zhu Q, Balcetis E. Stuck on a phishing lure: differential use of base rates in self and social judgments of susceptibility to cyber risk. Compr Results Social Psychol. 2020;4(1):25–52. doi:10.1080/23743603.2020.1756240.
59. Rejeb A, Suhaiza Z, Rejeb K, Seuring S, Treiblmaier H. The internet of things and the circular economy: a systematic literature review and research agenda. J Clean Prod. 2022;350:131439. doi:10.1016/j.jclepro.2022.131439.
60. Pavel T, Gafni R. The invisible hole of cybersecurity insurance services. Online J Appl Knowl Manage (IIAKM). 2020;8(2):1–16. doi:10.36965/OJAKM.2020.8(2)1-16.
61. Grotto AJ, Makridis CA. Perception of digital risks: evidence from 54 countries. 2022.
62. Kesan JP, Majuca RP, Yurcik WJ. The evolution of cyberinsurance. In: National Center for Supercomputing Applications (NCSA) editor. Department of economics. Illinois (USA): University of Illinois at Urbana-Champaign; 2005. p. 1–16.
63. Khalili MM, Naghizadeh P, Mingyan L. Designing cyber insurance policies: the role of pre-screening and security interdependence. IEEE Trans Inf Forensics Secur. 2018;13(9):2226–39. doi:10.1109/TIFS.2018.2812205.
64. Dou W, Tang W, Wu X, Qi L, Xu X, Zhang X, Hu C. An insurance theory based optimal cyber insurance contract against moral hazard. Inf Sci. 2020;527:576–89. doi:10.1016/j.ins.2018.12.051.
65. Kjartan P, Gudmundsson S, Shetty S. Analysis of the impact of cyber events for cyber insurance. Geneva Pap Risk Insur. 2020;45(4):564–79. doi:10.1057/s41288-020-00171-w.
66. Liu Y, Sarabi A, Zhang J, Naghizadeh P, Karir M, Bailey M, Liu M. Cloudy with a chance of breach: forecasting cyber security incidents. In: 24th USENIX Security Symposium Washington (USA): USENIX The Advanced Computing Systems Association; 2015.
67. Allodi L, Massacci F. Security events and vulnerability data for cybersecurity risk estimation. Risk Anal. 2017;37(8):1606–27. doi:10.1111/risa.12864.
68. Mishina R, Tanimoto S, Goromaru H, Sato H, Kanai A. Risk management of silent cyber risks in consideration of emerging risks. In: 10th International Congress on Advanced Applied Informatics (IIAI-AAI). Niigata (Japan): Institute of Electrical and Electronics Engineers Inc.; 2021. doi:10.1109/IIAI-AAI53430.2021.00126.
69. Cain AA, Edwards ME, Still JD. An exploratory study of cyber hygiene behaviors and knowledge. J Inf Secur Appl. 2018;42:36–45. doi:10.1016/j.jisa.2018.08.002.
70. Papatsaroucha D, Nikoloudakis Y, Kefaloukos I, Pallis E, Markakis EK. A survey on human and personality vulnerability assessment in cybersecurity: challenges: approaches, and open issues. ACM Comput. Surv. 2021;1–39.
71. Dodel M, Mesch G. An integrated model for assessing cyber-safety behaviors: how cognitive, socioeconomic and digital determinants affect diverse safety practices. Comput Secur. 2019;86:75–91. doi:10.1016/j.cose.2019.05.023.
72. Kevelighan S, Lynch J, McGregor J, Pieffer D. Helping customer understand the value of cyber insurance. New York (USA): Insurance Information Institute (III); 2018.
73. Pal R, Golubchik L, Psounis K. Improving cyber security via profitable insurance markets. Perform Eval Rev. 2018;45(4):7–15. doi:10.1145/3273996.3273999.
74. Falk R, Brown AL. Underwritten or oversold? How cyber insurance can hinder (or help) cyber security in Australia. Australia: Cyber Security Cooperative Research Centre; 2021.
75. Toregas C, Zahn N. Insurance for cyber attacks: the issue of setting premiums in context. United States: The George Washington University; 2014. p. 1–20.
76. Sun N, Li C-T, Chan H, Islam MZ, Islam MR, Armstrong W. How do organizations seek cyber assurance? Investigations on the adoption of the common criteria and beyond. Comput Sci. 2022;10:71749–63. doi:10.1109/ACCESS.2022.3187211.
77. Analytics HI. 2021 Norton cyber security safety insights report global results. 2021.
78. Manap NA, Abdul Rahim A, Taji H. Cyberspace identity theft: an overview. Mediterr J Social Sci. 2015;6:290–99.
79. Acharya S, Mieth R, Konstantinou C, Karri R, Dvorkin Y. Cyber insurance against cyberattacks on electric vehicle charging stations. IEEE Trans Smart Grid. 2022;13(2):1529–41. doi:10.1109/TSG.2021.3133536.

80. Hodges D. Cyber-enabled burglary of smart homes. Comput Secur. 2021;110:102418. doi:10.1016/j.cose.2021.102418.
81. Parkinson S, Ward P, Wilson K, Miller J. Cyber threats facing autonomous and connected vehicles: future challenges. IEEE Trans Intell Transp Syst. 2017;18(11):2898–915. doi:10.1109/TITS.2017.2665968.
82. Flaco GEA. A research agenda for cyber risk and cyber insurance. In: The 2019 Workshop on the Economics of Information Security (WEIS). Boston (USA): Stanford Center for International Security and Cooperation; 2019. https://cisac.fsi.stanford.edu/publication/research-agenda-cyber-risk-and-cyber-insurance-0 .
83. Khan A, Krishnan S, Dhir A. Electronic government and corruption: systematic literature review, framework and agenda for future research. Technol Forecasting Social Change. 2021;167:120737. doi:10.1016/j.techfore.2021.120737.
84. Guckenbiehl P, Corral de Zubielqui G, Lindsay N. Knowledge and innovation in start-up ventures: a systematic literature review and research agenda. Technol Forecasting Social Change. 2021;172:121026. doi:10.1016/j.techfore.2021.121026.
85. Bandyopadhyay T, Mookerjee VS, Rao RC. Why IT managers don't go for cyber insurance products. Commun ACM. 2009;52(11):68–73. doi:10.1145/1592761.1592780.
86. Organisation for Economic Co-Operation. Enhancing the role of insurance in cyber risk management. Paris (France): Organisation for Economic Co-Operation, Development (OECD) Publishing; 2017. Report Number: 978-92-64-28214-8. doi:10.1787/9789264282148-en.
87. Waters M. The current state of cyber insurance as a risk transference option. Nashville (USA): Lipscomb University; 2015.
88. Nieuwesteeg B, Visscher L, de Waard B. The law and economics of cyber insurance contracts: a case study. Eur Rev Private Law. 2021;26(3):371–420. doi:10.54648/ERPL2018027.
89. Bohme R, Schwartz G. Modeling cyber-insurance: towards a unifying framework. In: Workshop on the Economics of Information Security (WEIS). USA: Harvard; 2010.
90. Bahsi H, Franke U, Langfeldt Friberg E. The cyber insurance market in norway. Inf Comput Secur. 2019;28(1):54–67. doi:10.1108/ICS-01-2019-0012.
91. Eling M, Schnell W. What do we know about cyber risk and cyber risk insurance? J Risk Finance. 2016;17(5):474–91. doi:10.1108/JRF-09-2016-0122.