JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2025, tyaf029
https://doi.org/10.1093/cybsec/tyaf029

Research Paper

Consumer perceptions of personal cyber awareness, knowledge, and risk

Richard McGregor [1,*], Carmen Reaiche [1], Stephen Boyle [1], Graciela Corral de Zubielqui [2]

[1]College of Business, Law and Governance at James Cook University, Queensland 4811, Australia
[2]Adelaide Business School, Faculty of Arts, Business, Law and Economics, The University of Adelaide, South Australia 5005, Australia

*Corresponding author. 6 James Street, Blakehurst NSW 2221, Australia. E-mail: richard.mcgregor@my.jcu.edu.au

Received 19 August 2024; revised 14 August 2025; accepted 8 September 2025

Abstract

Despite the effectiveness and increasing proliferation of security controls designed to protect personal and sensitive information, there is increasing recognition that humans are susceptible to cyber exploitation and thus, individual users are deemed a causal element of personal cyber risk. Exposing personal perceptions and capabilities, such as cyber awareness and knowledge, is crucial to understanding personal cyber risks and allowing a holistic interpretation of an individual's cyber risk profile. This study uses a survey comprising $n = 263$ participants to explore to what extent awareness influences cyber knowledge and thereby impacts the level of personal cyber risk. We find that personal cyber awareness positively influences knowledge and personal cyber risk, whereas awareness independently fails to impact personal cyber risk, suggesting that knowledge acts as an influential mediator when determining an individual's personal cyber risk profile. Further, this paper acknowledges the importance of consistent definitions and addresses upfront a notable gap by defining personal cyberspace—a critical and foundational prerequisite to any research focused on the human cyber condition. The study contributes by proposing a unique definition of personal cyberspace, a conceptual model articulating an individual's personal cyber risk profile, and extending extant knowledge about relationships among personal cyber awareness, knowledge, and risk.

Keywords: personal cyberspace; cyber philosophy; personal cyber awareness; personal cyber knowledge; personal cyber risk; personal cyber risk profile

Introduction

Cyberspace is a contemporary and intricate phenomenon that imposes a complex socio-technical peril on individuals [1]. The rapid maturation of digitization, network interconnectedness, and the use of data—both in depth and breadth—has meaningfully augmented our productivity, our capabilities to process and communicate information at scale and at speed, and our ability to harness a technological eco-system to further drive advancement [2]. Whilst these refinements have notably and measurably improved standards of living and streamlined commercial transaction proficiencies, they have also introduced a plethora of cyber vulnerabilities and hazards at the individual, organizational, and national security levels [3]. To put these exponentially growing cyber threats into context, the World Economic Forum places cybercrime and cyber insecurity eighth on its list of most severe global risks anticipated by 2025 and also within the next decade, side-by-side with threats such as climate change, natural disasters, economic warfare, and involuntary migration [4].

Existing research within the cyber domain constitutes two preoccupations. The first is cybersecurity investigation, which is predominantly technical in nature and focused within computer sciences and/or engineering [5]. The second focus lies within the fields of social sciences and is centered on human and behavioural subjects such as cyber criminology, security legislation, cyber ethics, and privacy [6–8]. Although the cyber-themed extant literature is understandably extensive, there is significant emphasis on technical cybersecurity and research at the organizational level [9,10]. There is a relative dearth

of understanding and empirical evidence about individual awareness and knowledge of and within cyberspace, and how these may influence their personal cyber risk profile (PCRP). This paper aims to address this gap by exploring a priori what constitutes a definition of personal cyberspace, as this articulates fundamentally and logically the core baseline and scope upon which robust research and discussions within this domain are based. Once this genesis understanding is articulated, the study aims to examine the relationships between an individual's cyber awareness and knowledge and their consequent personal cyber risk (PCR) within the context of a PCRP model. The empirical component of the study then focuses on the relationships between personal cyber awareness, knowledge, and risk in support of the initial aims.

Thus, the key contributions of this paper to the literature on PCR and management are 3-fold. Specifically, the research seeks to answer the following research questions:

- (RQ1) How is personal cyberspace defined from the perspective of individual users?
- (RQ2) How do we leverage this definition to conceptualize a PCRP?
- (RQ3) Does personal cyber knowledge moderate the relationship between cyber awareness and PCR?

The paper is structured as follows. The following section presents a review of the literature on personal cyberspace that leads to the section 'A definition of personal cyberspace'. This is followed by an examination of the theoretical background, including a conceptual PCRP model, and the research hypotheses (section 'Theoretical background'). The research methodology is presented in the section 'Conceptual framework and hypotheses', including the design and procedures employed. The findings of the statistical analysis are tendered in the section 'Research methodology', which are subsequently discussed in the section 'Discussion'. The paper concludes (see the section 'Conclusion, limitations, and future research') with implications for individuals and practitioners, along with the study's limitations and suggestions for future research.

Literature review

A focus on personal cyberspace

The uplift in cyberspace engagement across society—in particular, with cyber security tools—has led to a growing accumulation of studies focused on personal cyber awareness and knowledge in recent years. Seungeun and Chua [6], for example, mapped variables influencing cybersecurity awareness and knowledge in US users (such as education, income, and gender), and Simonet and Teufel investigated the influence of social and personal factors on cyber awareness and behaviours specifically of home computer users [11], demonstrating a trend towards exploring human factors in cyberspace.

It is recognized, however, that such extant investigations gravitate towards specific population segments. For example, Karagiannopoulos et al. and Blackwood-Brown, both explored cohorts of elderly participants [12,13], and a study conducted by Limna et al. focused on mobile banking users in Thailand [14]. Or studies are role-based—for example, Khader et al. focused on cyber awareness amongst academics [15] and Alquhtani [2] and LeFebvre [16] specifically focused on factors affecting cybersecurity amongst university students. The authors recognize that collectively, such studies contribute meaningfully to the field of personal cyberspace, yet only a smaller constellation considers the wider implications of the personal cyber condition and how best to offer tangible, more holistic constructs to uplift individual cyber capability at scale (see, for example, [17–19]).

The extant literature offers extensive resources on enterprise- and SME-level cybersecurity research, but research regarding personal cyberspace—including human factors, cyber-psychology, and pragmatic mitigation options such as personal cyber insurance, amongst others—is still in its infancy [20]. The lack of investigation into the personal cyber condition is attributed to the availability of, and prioritization of, resources; namely, the very real need of organizations to implement robust cybersecurity for operational and regulatory purposes [21]. Thus, business and cybersecurity-related research [5] is extensive and correspondingly mature. It is also recognized that many foundational concepts within cyberspace are still ill-defined and inconsistent (such as cyber ethics [22,7], legislative principles [23], and governance [24,25]), thereby mitigating the benefits of authoritative guidance within such a dynamic and unique environment.

According to Liang and Xue (2010), threat appraisals (of perceived susceptibility and severity) and coping appraisals (of the effectiveness of safeguards and cost, and the principles of self-efficacy) were notable indicators of PCR avoidance behaviours [26]. Comprehensive exploration of home computer security and the personal cyber condition has not been subject to in-depth study [27]; however, COVID-19 pivoted focus to the widespread transformation from *in situ* work practices to teleworking and work-from-home (WFH) norms [28,29]. This resurgence of research interest has not only prompted investigation into the efficiency and technical cybersecurity of remote working and data security [30], but also an intense focus on how to materially improve user cyber awareness/knowledge and accelerate conscientious motivation to promote robust cyber behaviours [31].

It is imperative to emphasize the holistic and multidisciplinary complexion of PCR. The authors recognize that comparatively few studies have analysed the domain at the individual level, thus substantially supporting the rationale that investigation into the personal cyber condition presents an under-researched phenomenon. It is understood, however, that research within the commercial domain may provide direct or indirect insights and benefits analogous to extant and future knowledge of PCR and management.

A definition of personal cyberspace

Defining core terms and concepts in research is critical. Clarifying key definitions avoids confusion about and/or misinterpretation of (often subjective) concepts and ideas. Articulating definitions upfront ensures consistency between and comparability across research and establishes clear scope and focus, thereby ensuring that studies address the specific topics they propose to examine [32]. Considering the embryonic maturity of studies within personal cyber risk and management and the corresponding absence of scope definition (specifically attributable to personal cyberspace), we provide a pioneering examination of what constitutes personal cyberspace, thus providing a foundational baseline upon which the empirical analysis can be based.

The paradigm of personal cyberspace

The cyber domain attracts a diverse, disparate and often nebulous array of interpretations. *A priori*, it is necessary to first articulate the basic parameters of the personal definition of 'cyberspace'—a term frequently used by practitioners and users alike since the beginning of the digital age. The lack of standardized understanding commonly introduces semantic confusion as few articulate the true parameters

of the cyber domain in a standardized, widely accepted format [33]—and none specifically focus on the perspective of an individual user. To the best of our knowledge, this is the first study to propose a definition dedicated to personal cyberspace that extends beyond the technical or cognitive interpretations and highlights the importance of accommodating cyber human-centric elements. For the purposes of this study, 'cyberspace' and the phrase 'cyber domain' are considered synonyms. The authors support the notion proposed by Medeiros and Goldoni [34] p33, that:

> …The prefix "cyber" followed by nouns such as "war," "terrorism," or "space" induces in the reader's imagination the transposition of concepts represented by those nouns to a virtual arena. While this practice simplifies and transmits the message to the receiver, albeit crudely, it is analytically reductionist, as it does not consider conceptual aspects inherent in the cyber domain.

It is necessary to maintain a wider intellection when conceptualizing cyberspace, considering it as a distinctive yet heterogeneous domain. Thus, whilst employing the prefix 'cyber' enables meaning to be conveyed quickly and allows people to imagine such elements such as 'war' and 'terrorism' to be coupled with the digital environment, there is a danger that such attachments oversimplifies such concepts and misses key and/or specific instances wherein the prefix and noun are inappropriate or misrepresented. In such scenarios, definitions of terminology are essential to convey accurate meaning.

William Gibson originally coined the term 'cyberspace' in a short story in 1982, whereupon it was subsequently embraced as the ubiquitous phrase pertaining to the World Wide Web (www) or internet, or 'online' activities. An understanding of user behaviours in cyberspace and associated PCRs is logically premised on a clear and exact definition of cyberspace and what this means at the individual level.

Whilst not interpreting the nature of space itself, Karl Popper proposed meaningful abstractions representing the phenomenological universe. He speculated that human existence comprised three layers: (a) objectivity/physicality, (b) subjectivity of emotions, feelings and dreams, and (c) inter-subjectivity—a realm of real-world, material objects embodied by means of cross-fertilization of intellectualism (thoughts) and personal action [35]. To situate a definition of personal cyberspace, it is necessary to position the portraiture within the context of virtual space, which is logically ensconced within inter-subjectivity, wherein objects '…are patterns of ideas, images, sounds, stories, data… patterns of pure information'. Similar and parallel to the real world, digital landscapes require '…actors who construct through practices, contests, and interaction' [36]. In summary, Popper offers a conceptual framework within which to understand the overlaps among the physical, human, and digital domains, thereby identifying what constitutes those elements that are necessary to define personal cyberspace.

According to Lippert and Cloutier, 'Cyberspace is the domain where the electromagnetic spectrum is used to store, modify and exchange data' [33], and is '…clearly a system of systems (SoS)—a system composed of other systems'. Within the cyber domain, cyberspace is defined predominantly from the technical and theoretical facets of computer sciences and systems engineering [37–39]. Kuehl's definition typifies this focus:

> A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies. [40].

This is considered an apt description but it does not consider human involvement. The authors argue that whilst some consideration of human 'user' elements is intermittently incorporated within proposed definitions of cyberspace [41,42], these integral components are typically consigned to a subordinate lineage. Cohen [43] p216, concurs with this conceptual approach, stating that cyberspace should be considered '…as connected to and subsumed within an emerging, networked space that is inhabited by real, embodied users and that is apprehended through experience', thus emphasizing the importance of the individual experience for establishing an understanding of a user's definition of cyberspace.

Although traditional domain definitions emphasize the logical, systematic construct approach to defining cyberspace, closer inspection reveals ambiguity when incorporating an individual's characteristics and functioning. This is understandable insofar as defining a holistic cyber ecosystem is both challenging and complex (Lippert and Cloutier, 2021) and limiting the scope to quantified, well-understood segments can assist in managing the parameters and minimizing or simplifying assumptions. Ning et al. attempted to integrate the cyber technical and user by proposing a novel definition of cyberspace founded on traditional physical, social, and thinking spaces, existing in parallel with cyberspace [44] p1843, thus emphasizing the transition from considering cyberspace as a solely digital landscape to '…a completely new environment where cyber-related elements permeate all spaces and all aspects of our life, which we call General Cyberspace (GC)'. Similarly, Ventre [42] interpreted cyberspace as a context that transcends the traditional 'natural' domains. This implies that conceptual cyberspace is influenced by the user's experience of the digital landscape, thus suggesting that the 'peopleware' layer socializes the nature of cyberspace—aptly divorcing it from a strictly electronic or mechanistic perspective.

The increasingly intimate interrelationship and growing interdependency between the individual and the cyber domain stimulates social change at scale, thus presenting pragmatic challenges to our ways of working and daily life. Proposing a definition of cyberspace that relies extensively on technology without fully assimilating the human condition is circumscribed. To enable investigation into personal characteristics and *theorem* within cyberspace, it is crucial to establish a robust baseline definition of what is considered personal cyberspace, thus allowing insights to be consistently and equitably evaluated. Table 1 offers a sampler of cyberspace definitions, albeit no specific definitions for personal cyberspace were discovered in the literature.

The purpose of defining cyberspace from the perspective of an individual is to establish practical parameters relating to their lifestyle, digital and data experiences (Ning et al. 2018). The technological infrastructures, including devices, networked environments, interconnectivity, storage connectivity, the logical components that constitute services and support platforms, and the data properties/logicality, are integral and foundational aspects of cyberspace [38]. This study proposes the following definition of personal cyberspace, specifically intended to blend human cognitive characteristics, needs and motivations with cyber constituents to deliver a holistic schema that is paradigmatic and capable of acting as a common standard for future research:

> Contemporary personal cyberspace is defined by all individualistic user interfaces and digital touchpoints using secure independent devices or harnessing globally interconnected network infrastructures for the purposes of virtual personal communications, conducting or attending social engagements, controlling digitally enabled objects, performing data storage activities, or conducting commercial and/or other digital transactions.

Table 1. Exemplar of recent definitions of cyberspace within the literature.

Ref	Definition	Author	Source
1	Cyberspace is the domain where the electromagnetic spectrum is used to store, modify, and exchange data. It is characterized by logically networked systems that reside on physical infrastructure.	Lippert, K. J. Cloutier, R.	2021, Systems, Vol 9(48), https://doi.org/10.3390/systems9030048
2	A global domain within the information environment, consisting of an interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.	Medeiros, B.P. Goldoni, L. R. F.	Dictionary of Military and Associated Terms (DOD) of the Office of the Chairman of the Joint Chiefs of Staff (2019: 56) sourced from: 2020, Contexto Internatcional, Vol 42(1), The Fundamental Conceptual Trinity of Cyberspace http://dx.doi.org/10.1590/S0102-8529.2019420100002
3	Cyberspace is the domain in which cyber operations take place; cyber power is the sum of strategic effects generated by cyber operations in and from cyberspace.	Sheldon, J. B.	2011, Deciphering Cyberpower Strategic Purpose in Peace and War, Strategic Studies Quaterly Vol 5(2)
4	Cyberspace is 'a terra nullius in which social relations and laws have no historical existence and must be reinvented'.	Choucri, N.	2012, Cyberpolitics in International Relations, MIT Press, ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/jcu/detail.action?docID=3339542.
5	Cyberspace is the digital world created based on traditional physical, social, and thinking spaces.	Ning, H.	2018, General Cyberspace: Cyberspace and Cyber-Enabled Spaces, Vol 5(3)

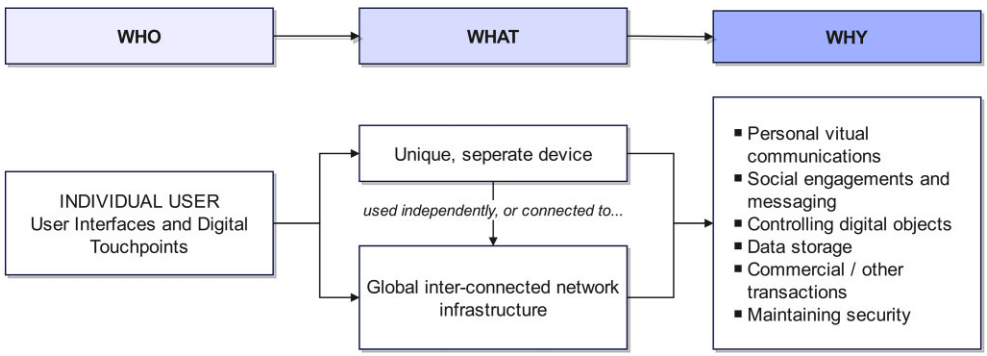

Figure 1. Visualization of the definition of 'personal cyberspace'.

This definition satisfies the aim of RQ1 and will be used as a baseline for this (and potentially future) study. It facilitates an understanding of what accurately constitutes personal cyberspace—avoiding conceptual definitions that are habitually embrace technocentric ambiguity [39,44 ,33], whilst embracing integration of individual users as an intrinsic element of the holistic concept of personal cyberspace. It is deemed essential also, to pivot towards a definition of cyberspace that excludes specificacy of organisational elements often targeted at use by entities (i.e. non-individual users) [45]. Such definitions are potentially inappropriate and misleading when employed within the context of 'personal cyberspace' as presented herewith.

Figure 1 provides a visual representation of this definition. Considering the multifaceted nature of personal cyberspace, the authors emphasize that the term cannot be limited to a narrow definition insofar as the condensed approach will minimize the depth and adequacy of a given definition [46]. It is important to note that user (personal) digital devices may be used either independently, offline (i.e. not connected to the internet—e.g. a vehicle dashcam) or online whilst connected to the internet or networked Wide Area Network (WAN) or Local Area Network (LAN). The nature of connectivity of each device meaningfully impacts the scope of PCR as discussed by [47] and [48], coupled with the use of the device (behaviour; such as the differential between personal virtual communications such as one-to-one messaging or email, vs social messaging which is a means to broadcast information) and capabilities enabled to mitigate potential cyber risk (mitigation).

Theoretical background

A unique distinction: our own PCRP

A key benefit to articulating the parameters of PCR is that it helps us delineate the difference between cyber safety and peril. The term 'risk' is a common and well-understood contemporary term that is employed extensively to articulate uncertainty at the individual and organizational levels. Instinctively, individuals are generally capable of perceiving unpredictability and conceptualizing heuristics to manage risk [49]. Conceptually, the abstract notion of risk is characterized '…as having the capacity to produce harm or loss and is measured in terms of likelihood of occurrence and severity of impact' [50]. Within the field of economics, Frank Knight, as cited in

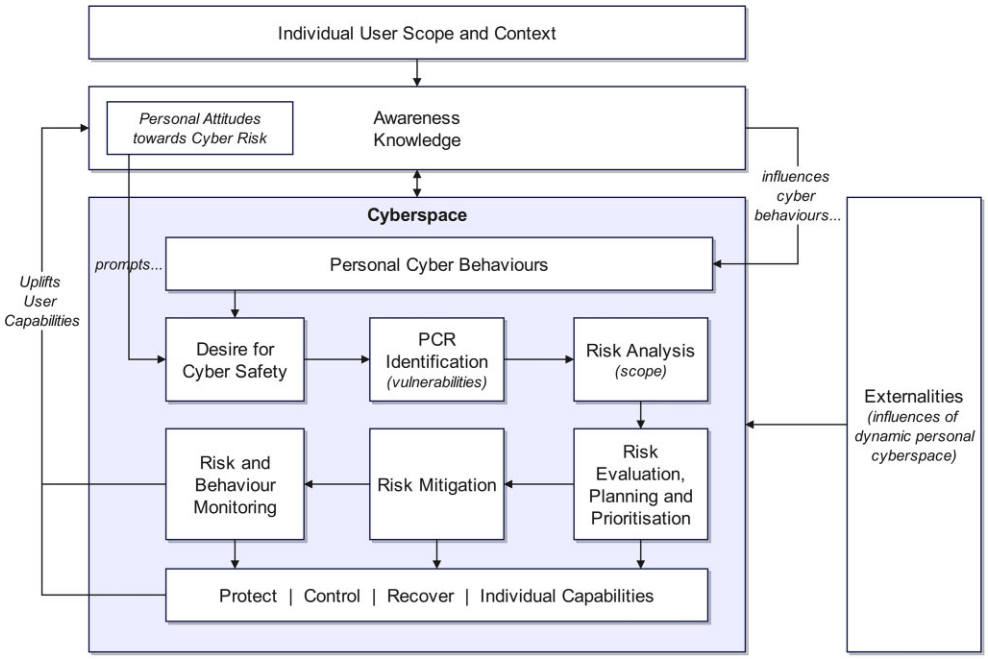

Figure 2. Constituent elements *in situ* within a Holistic Personal Cyber Risk Profile (adapted from ISO 310000 Enterprise Risk Management Frameworks (ISO31000:2018 Risk Management Process) and NIST Cybersecurity Risk Management Framework [51]).

LeRoy and Singell, (LeRoy and Singell 1987), differentiated the phenomenon of risk and uncertainty thus: 'Risk …referring to events subject to a known or knowable probability distribution, and uncertainty, as referring to events for which it was not possible to specify numerical probabilities'. Risk, therefore, pertains to circumstances whose future possibility can be inferred; in contrast, uncertainty means that it is simply not possible to predict future events.

The literature on risk and risk management is prodigious, with a multitude of conceptual definitions and perspectives, including cyber risk, although, as noted already, there is little on prescribing PCR. Considering this deficiency, the authors propose a definition of PCR as the probability that an individual user experiences data exposure, harm or other type of loss related to technical capabilities, psychological impacts or reputation resulting from an adverse cyber incident.

In line with the perpetual and exponential growth of personal cyberspace (as defined above), so too does the complexity and injurious nature of emergent PCR accelerate over time [51]. By leveraging an understanding of what constitutes both personal cyberspace and PCR, this article posits that we need to articulate how these phenomena influence cyber peril at the individual user level. In doing so, we can generate insights that empower a holistic assessment of the personal risk landscape and/or implications threatening an individual (comprising technical elements and personal comportment/behaviours). According to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework 2.0 [52], risk analysis of threat vectors and their characteristics, both qualitative and quantitative, may contribute to defining a risk profile for an organization, activity or individual [53].

Whilst the NIST definition of a risk profile is generic and heavily orientated towards enterprise-level applications, it can also be used to identify and analyse individualistic PCR. Therefore, we propose a PCRP whereby individual users can identify and articulate the breadth and scope of their cyber vulnerabilities, cyber safety and protection objectives, risk profile parameters and the level of personal investment they are prepared to execute in order to secure a satisfactory profile [54]. To place the PCRP within the context of an individual user's *milieu*, Fig. 2 presents the foundational elements and the sequential nature of analysis necessary to identify, manage and mitigate PCR. It is important to note that the PCRP is dynamic and depends on the idiosyncrasies of developments within cyberspace and cyber risks that are directly pertinent to the individual, and thus it continually morphs according to an individual's cyber vivacity (activities) and protectionist stance (risk acceptance) [55]. Similarly, the depth of PCR analysis necessary to establish meaningful insights will also differ per individual, insofar as the parameters and complexity of cyber engagement and transparency are unique to each person [56] warranting individualized approaches and divergent preconditions to identifying/mitigating PCRs.

Ganin et al. (2020) p183, explored the gap between risk assessment, encompassed by the PCRP, and risk management, thereby proposing a '…structure and transparent process of selecting risk management alternatives' [57]. The authors propose that the holistic PCRP model allows individual users to adopt an awareness-knowledge-risk (AKR) approach that offers objective measures and metrics tailored specifically to typical individual user cyber capabilities, to cyber risk management decision-making that is based on known and/or analysis of their specific PCRs, vulnerabilities and potential adverse consequences. Figure 2 clearly establishes the importance of individualistic variables—personal cyber awareness and knowledge—as the antecedent and necessary basis for understanding and ultimately managing PCR.

Conceptual framework and hypotheses

The above definition of personal cyberspace satisfies the initial aim of this paper and allows us to explore the conceptual PCRP model, presented in Fig. 2, which depicts the relationships between personal cyber awareness, knowledge, and PCR. Both the proposed definition of personal cyberspace and the PCRP model suggest a dependency on the foundational personal characteristics of personal cyber awareness

and knowledge. As such, we proffer a conceptual model and associated hypotheses. We hypothesize:

H1. Personal cyber awareness is positively associated with the mitigation of PCRs

A crucial element to understanding the personal cyber condition is personal cyber awareness, which refers to an individual user's extensive or peripheral exposure to and/or the extent of their perception of their unique personal cyberspace [6]. Rahim [58], p. 607, proposed a definition of cyber(security) awareness as follows: '…alerting Internet users of cybersecurity issues and threats, and enhancing Internet users' understanding of cyber threats so they can be fully committed to embracing security during Internet use'. Thus, for example, the level of user cyber awareness may necessitate an understanding of what constitutes malicious threats to a 'safe' website—such as SQL injection attacks or cross-site scripting—which are differentiated from a user's cyber knowledge actions such as employing Multi-Factor Authentication and ensuring that software is consistently updated. Howard and Cambria [59], p1, espoused the notion of 'situational awareness' (SA)—'…such as consistent tracking and extrapolation of objects in the user's environment'—as an essential capability for users wishing to achieve a unified view of their surrounding (cyber) environment and corresponding PCR. This axiom also supports the holistic linkages proposed within the PCRP, albeit the principle must simultaneously consider the multicentric nature of personal cyberspace (namely, the human–technical perspective) to be judicious.

It is posited that cyber awareness is the foundational personal trait necessary to reduce adverse cyber incidents experienced by individuals, as it allows them to comprehend prospective damages and motivates them to uplift understanding (knowledge) to mitigate PCR and any associated impacts (see, for example, [60,61] and [62]. The key relationship element between personal cyber awareness and PCR, is the level of vulnerability to adverse cyber incidents directly attributable to the individualistic competence to execute tasks that will mitigate PCR and improve their holistic PCRP [63]. There is a paradigm shift within the literature from utilitarian and systematic cyber security, towards a 'human centric security design' [64] that inherently considers the personal cyber condition, including how personal cyber awareness impacts PCR. This is appropriate, insofar that the landscape within which users operate and interact with in their personal cyberspace is perpetually morphing; thus, the connectivity between an individual's cyber awareness and their associated PCR at a point-in-time is constantly in flux—in which awareness of and the risk itself interact over time [65].

H2. Personal cyber awareness positively impacts personal cyber knowledge.

We propose that personal cyber awareness and knowledge enjoy a synergistic and paradoxically circular relationship, insofar that individuals require a precursory degree of cyber awareness as an essential antecedent to understanding the need for cyber knowledge—which in turn uplifts further cyber awareness, and so on. As society becomes increasingly dependent on digital technologies on a day-to-day basis, the scale of participation in personal cyberspace also soars exponentially [2]. Whilst increasing recognition of the need for and the importance of research focused on the human elements of cyberspace is emerging, it is widely discerned that knowledge of the necessary tools and skills amongst individual users necessary for personal protection against adverse cyber threats is languishing in comparison (see [66,67]).

Understanding that the individual user is both the point of success and failure—depending on their level of cyber awareness and knowledge—is pivotal when promoting the need to embed these personal capabilities and cognitive perceptions [61]. This will help us deliver a utilitarian norm that not only protects users from adverse cyber incidents but does so in unison with human behaviours and motivations [64]. This concept offers an opportunity to develop alternative methods—assuming an adequate user baseline cyber awareness and knowledge—that propose a balanced personal cyber approach that avoids a sole isolated point of failure. This could conceivably spread the PCR by amalgamating principles of cyber security and individual users, thereby leveraging a socio-cognitive-technical solution, as proposed by Grobler [64].

H3. Personal cyber knowledge positively impacts PCR

Erstwhile studies have focused on user security behaviours and/or intentions and privacy protection (e.g. [68,69]), but expended minimal attention on cyber knowledge. This is attributed to inconsistent definitions of these concepts, coupled with a lack of understanding about how to define the scope of personal cyberspace, as proposed earlier. This is a disturbing phenomenon, insofar as a multitude of studies confirm that human error is considered the dominant cause of data breaches—prompted by a lack of knowledge, lacklustre cyber hygiene activities and attitudes toward conscious cyber behaviours [70]. Individuals who exhibit elevated levels of cyber knowledge also reveal a preference or motivation for actively countering cyber threats [71,72]. Persons whose cyber knowledge and skills are perceived as minimal tend to underestimate PCR and the hazards that poor cyber behaviours/actions represent [68]. Such vulnerabilities are proven to be mitigated by means of cyber(security) awareness and proficiency education (see, for example, [73–75]).

A study performed by Zwilling (2020) indicated that most participants implemented only basic and insufficient activities (such as using antivirus software or strong password characteristics) [76]. A small minority used more elaborate protective mechanisms and tactics, such as regular network and computer security audits or avoiding publicly available WiFi networks (or similar, as presented by [77]) that necessitated a more sophisticated knowledge of cyberspace. Zwilling's findings indicated that respondents who displayed a greater level of computer knowledge, tended to have enhanced appreciation/implementation of cyber security (thereby mitigating their level of PCR)—a viewpoint shared by Ben-Asher and Gonzalez [78]. Paradoxically, Aytes and Connolly studied undergraduate students' self-perceptions of cyber expertise and found that 90% ranked themselves as knowledgeable or very knowledgeable [79]. It was discovered that regardless of the level of self-perceived expertise, risky behaviours were prevalent amongst the cohort. Such disparities within the literature suggest that other variables, such as regional, demographic or timing considerations, may influence the relevance of extant findings, and that there is a need to conduct further research to precisely determine the influence that knowledge has on PCR.

Knowledge as a mediator for awareness and PCR (indirect effect)

H4. Knowledge mediates the relationship between personal cyber awareness and PCR.

The inherent nature of cyberspace, including personal cyberspace, is that it is dynamic and increasingly interconnected. The desire of individual users to ensure cyber safety is highly dependent on their levels of cyber awareness, knowledge and behaviours—all of which

Table 2. Study test constructs.

Awareness	To what extent do you agree or disagree that the following are part of 'cyberspace'.
A1: Wireless home solutions	Your wireless home security and fire detection system
A2: Internet-connected car	Your internet-connected car
A3: Dark web	The 'dark web' (i.e. areas of the internet to which you don't have access)
A4: IoT devices	Any devices you own that are in the Internet of Things (IoT) (i.e. fridges, heaters or 'smart home' devices that are connected to the internet)
Knowledge	To what extent to you agree or disagree with the following statements about your personal cyber risk:
K1: Technology/data integration	The rapid integration of technology and data has increased my personal cyber risk profile
K2: Third party holding personal information	My personal cyber risk is significantly higher due to third party organisations holding my personal information (i.e. banks, electricity providers and your doctor)
Risk	What do you think the biggest challenges are that face personal cyber insurers?
R1: Cyberspace is dynamic	The fact that cyberspace changes all the time. It's never static
R2: Data grows continuously	The fact that the amount of data just keeps growing. More data equals more risk
R3: Interconnectivity	The fact that our technology is becoming more and more inter-connected. This means that the impact of adverse cyber events can spread at scale across networks of linked computers very quickly

influence their PCRP. Cyber knowledge, in particular, is shown in this study and previous research [76] to be pivotal in delivering a secure cyber experience. Cain et al. undertook an investigation analysing conceptual cyber knowledge and PCR and discovered statistically significant gender-wise variances in which male participants presented as more knowledgeable [80].

Arguably, knowledge within the cyber domain is a nebulous and ever-changing construct. Even users who may be perceived as being cyber knowledge mature, offer a variety of human vulnerabilities that contribute to lower awareness and consequently higher PCR. Moallem (2019), for example, conducted a study of students within California's Silicon Valley—a cohort that was considered cyber knowledge mature—and found that even '…when they were aware that their actions were being seen and tracked, college students were unaware that their data was not safely transported across university systems' [81]. Moallem also emphasized that cyber attackers constantly vary attack vectors and techniques, demonstrating the ongoing challenge for users to maintain their awareness of changes and trends within personal cyberspace, a view supported by Taha and Dahabiyeh [82]. It also demonstrates the need to perpetually invest in pursuing an adequate level of knowledge to guarantee cyber safety and deliver an acceptably secure PCRP standing.

Research methodology

Design

The study employed a self-reporting online survey distributed amongst $n = 263$ Australian consumers and administered via the internet-based survey platform Survey Monkey. All questionnaire constructs were measured using a 5-point Likert-type scale (plus an option for participants to select 'Prefer not to say or I don't know') as it affords better outcomes and offers a higher level of accurate variability than other scales [83]. The online survey avoided any opportunity to assess personal cyber skills and knowledge because employing self-reporting surveys to evaluate skills can simply result in an appraisal of an individual's percipience of their skill level rather than their actual skill [84].

Data collection

Subsequent to a survey review by dedicated behavioural science and academic professionals to ensure content reliability, validity and that the survey items adequately represented the construct domain, a specialist survey agency, 'Askable', was engaged to recruit a minimum cohort of 250 Australian-based participants. To ensure data validity and quality, 'Askable' provides AI fraud detection, verifies participant profiles and conducts screener/attention check questions. Participants were required to be at least 18 years old and have access to an internet-enabled device (thus exhibiting technical and cognitive capability to participate in the survey). All questions about personal cyber awareness, knowledge and risk were mandatory; thus, participation required full completion (100%) of all questions by participants. Of the 1200 prospective participants that were approached, 391 (32.5%) responded positively, indicating that they wished to complete the survey. The total number of respondents was $n = 263$ (slightly higher than the requested limit), representing the number of completed surveys submitted within a 24-h period.

Constructs

Research constructs are abstractions that represent phenomena that are not directly measurable, and thus must be implicitly presumed from other measurable variables. Survey instrument constructs are validated to ensure the instrument accurately measures the intended theoretical concepts. Pilot testing was conducted, administering a draft survey to a small sample (eight responses from ten individuals) representative of the target participants, allowing researchers to address question clarity, avoid ambiguity, and establish insights into the overall instrument performance. Table 2 presents the variables employed in this study. Personal perspectives on each question were answered using a 5-point Likert scale that ranged from 'Strongly disagree' through to 'Strongly agree'. In line with best practice, participants could also select 'Prefer not to say OR I don't know' [85]. Recognizing that every individual's personal cyber circumstances and digital environment are unique, the questionnaire offered participants a tailored selection of options that were constructed with the dual purpose of (a) ensuring the selections would be known to respondents, even if they only had a rudimentary knowledge of cyberspace, and (b) ensuring their appropriateness to the intent of each question.

It was recognized that participant responses are dependent on self-reported measures of cyber awareness and behaviours, thus introducing potential social desirability bias insofar that responses

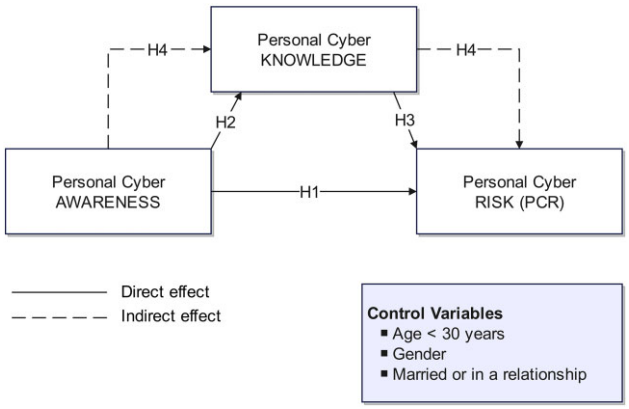

Figure 3. Conceptual model: personal cyber element relationships.

are provided in a manner perceived as favorable in lieu of being indicative of their actual awareness and behaviours. Questionnaires were adjusted to mitigate this bias by ensuring participants were aware that their responses were anonymized (thereby allowing participants to respond without feelings of self-incrimination) and that all questions were drafted in a neutral, non-judgmental tone, thus avoiding potential pressures to respond in a perceivably socially desirable manner.

Conceptual model

The conceptual model for the empirical component of the study is presented in Fig. 3. It reveals the hypothesized relationships between (internal) personal cyber awareness, personal cyber knowledge, and the associated influences of these variables on the level of personal cyber risk (thus, in consequence, impacting an individual's PCRP). Our research is predominantly focused on the internal capabilities of individual users, thus allowing insights into how these capabilities and hypotheses could impact the dual motivations to (a) uplift personal cyber capability by means of defining a PCRP and, thereby, (b) secure an opportunity to reduce cyber threats and vulnerabilities. Whilst most recent studies posit a direct relationship between cyber awareness and cyber risk (H1), the authors are interested in exploring the synergies between cyber awareness and knowledge insofar as proven dependencies will greatly influence the context, design, and adoption of tools or frameworks intended to mitigate PCR. The study acknowledges, however, that (H1) the influence of awareness on risk—as per Fig. 2—may present via more indirect means than direct.

Statistical analysis

The data analysis comprises two sequential stages. The preliminary stage involved conducting descriptive analysis, followed by a secondary stage that applied structural equation modelling (SEM) within STRATA v15 to analyse the structural models. The research hypotheses were also tested using SEM. The purpose of using SEM within this context was to assist in identifying which factors are most associated with the outcome and how different factors may interact to influence (mediate) the outcome [86]. Further, adopting SEM as an analysis method was appropriate insofar as this modelling technique accedes to multiple relationship analyses between variables and latent variables interacting with multiple observed variables [87]—a functional capability not offered by non-SEM modelling techniques. SEM allows measurement of the combined effect of variables and enables concurrently processing dependent links whilst differentiating between direct and indirect effects.

Descriptive analysis

Table 3 presents the study's descriptive statistics incorporating the mean, standard deviation, and correlation. All correlations have acceptable values, well below the 0.80 cut-offs recommended by [88], with the greater number indicating 0.63, indicating no multicollinearity problems. In addition, we assessed the reliability of the knowledge construct using a standard Alpha Cronbach with results of 0.78, 0.74, and 0.69 signifying internal consistency of the Likert questions. According to Griethuijsen et al. (2015) and Taber (2018), 'The accepted value of Cronbach's alpha is 0.7; however, values above 0.6 are also accepted'. Similarly, 'Pallant (2001) states Alpha Cronbach's value above 0.6 is considered high reliability and acceptable index (Nunnally and Bernstein, 1994). Whereas, the value of Alpha Cronbach is less than 0.6 considered low. Alpha Cronbach values in the range of 0.60–0.80 are considered moderate, but acceptable. While Alpha Cronbach in the ranges of 0.8 and up to 1.00 is considered very good.'

As depicted in Table 4, the population demographics for this study consisted of 263 participants comprising a younger cohort (67.3% being under 39 years) that presents a majority of female (68.8%) respondents. Over 70% were either married or in a 'relationship'. Similarly, the majority–83.3%—were in some form of full- or part-time employment.

Structural model

Using STATA 15, an SEM model was developed to test the hypotheses. We applied the maximum likelihood estimation coupled with the missing data and adapted the index to accept or reject the model. Based on this statistical adjustment index, the SEM result was accepted insofar that it met the minimum threshold proposed by [89]. Supplemental goodness-of-fit indices supported the model fit, including the structural model Chi-square, indicating 42.910 and a *P*-value of 0.199. The *P*-value of the Null Hypothesis (PCLOSE) is 0.912, with the Root Mean Square Error or Approximation (RMSEA) equaling 0.027, which is below the cut-off value of 0.05 as per [90]. The Tucker-Lewis index (TLI) = 0.989, which is above the acceptable value of 0.95 [91], whilst the comparative adjustment index (CFI) also exceeds the acceptable value of 0.95 [92], demonstrating good modelling adjustments. Considering these outcomes, the measurement model presented in Table 5 is well-adapted to the data.

Table 6 shows the results of the complete structural model. The model indicates to what extent the constructs of personal cyber awareness and knowledge affect PCR. Individual hypotheses have been tested and subsequently confirmed or rejected based on the importance/applicability of the relationships using Cohen's effect sizes interpretation, where small (S): $\beta \leq 0.1$, medium (M): $0.1 < \beta < 0.5$ and large (L): $\beta \geq 0.5$ [93].

The model was tested where H1, H2, and H3 represent the direct effects, and H4 represent the indirect effects (mediator) through knowledge. As presented in Table 5, H1 is rejected ($\beta = -0.085$, $P = 0.284$), whereas H2 and H3 are accepted ($\beta = 0.181$, $P = 0.016$, M) and $\beta = 0.336$, $P = 0.000$, M) respectively. The indirect effects of personal cyber awareness and PCR through personal cyber knowledge show that the indirect effect proffered by H4 is accepted ($\beta = 0.067$, $P = 0.048$, S).

Model robustness

H2 and H3 state that the effects of awareness of knowledge and knowledge on PCR are mediated by cyber knowledge. To ensure an acceptable level of robustness, the model was re-estimated using different sub-samples, including participants who identified as married

Table 3. Correlations.

	Mean	Std. Error	1	2	3	4	5	6	7	8	9	Age	Gender
A1: Wireless home solutions	4.030	0.068	1										
A1: Internet-connected car	4.034	0.061	0.6329	1									
A1: Dark web	4.340	0.067	0.3335	0.3711	1								
A1: IoT devices	4.051	0.067	0.6208	0.5877	0.3857	1							
K1: Technology/data integration	3.511	0.066	-0.0104	0.0309	0.2181	0.0525	1						
K2: Third party holding personal information	3.672	0.073	0.0855	0.0714	0.1606	0.0996	0.5162	1					
R1: Cyberspace is dynamic	4.528	0.044	0.0883	0.1280	0.1674	0.0974	0.1800	0.2140	1				
R2: Data grows continuously	4.434	0.048	0.0279	0.0779	0.0301	0.0272	0.1598	0.1733	0.4987	1			
R3: Interconnectivity	4.468	0.048	0.0546	0.0760	0.1338	0.0926	0.1816	0.1967	0.4778	0.4857	1		
Age	36.46	0.719	0.0681	0.0382	0.1298	-0.0304	0.1649	0.2020	0.1758	0.1652	0.2556	1	
Gender	1.332	0.031	0.1284	0.1579	-0.0138	0.0354	0.0193	0.0206	-0.0970	-0.0847	-0.0063	0.0593	1

Table 4. Survey participant demographics.

Ref	Characteristic	Frequency	Cumulative frequency	Percentage	Cumulative percentage
1	**Gender**				
	Male	82	82	31.2%	31.2%
	Female	181	263	68.8%	100.0%
2	**Age**				
	18–29 years	74	74	28.1%	28.1%
	30–39 years	103	177	39.2%	67.3%
	40–49 years	51	228	19.4%	86.7%
	50–59 years	21	249	8.0%	94.7%
	60 + years	14	263	5.3%	100.0%
3	**Relationship Status**				
	Single	78	78	29.7%	29.7%
	Married	140	218	53.2%	82.9%
	Relationship	45	263	17.1%	100.0%
4	**Work Status**				
	Full time employment	158	158	60.1%	60.1%
	Part time employment	61	219	23.2%	83.3%
	Not working	34	253	12.9%	96.2%
	Retired	10	263	3.8%	100.0%

Table 5. Structural model.

Fit Statistic	Value	Description/Commentary
Likelihood Ratio		
Chi-square X^2 MS (36)	42.910	Model vs Saturated
$P >$ Chi-square X^2	0.199	
Root Mean Square Error of Approximation (RMSEA) (∗)	0.027	Root mean squared error of approximation
P-value of the Null Hypothesis (PCLOSE)	0.912	Probability RMSEA ≤ 0.05
Baseline Comparison		
Comparative Fit Index (CFI)	0.989	
Tucker-Lewis Index (TLI)	0.983	

or in a relationship (model 1, β = Married or in a relationship), participants who were <30 years of age (model 2, $\beta \leq 35$ years old. The results presented in Table 7 reveal that the model fit index range is acceptable, meaning that the data fits the structural model and has valid value estimates. By employing alternate samples of the data within the model, the robustness of the model is established as it persists to produce valid results.

Discussion

The purpose of the empirical study was to explore the relationships between personal cyber awareness, knowledge, and PCR, and the extent to which these liaisons influence the individualistic—and all-pervasive—cyber condition. Our findings show that, overall, knowledge positively acts as a mediator between the constructs of personal cyber awareness and PCR, which is generally consistent with most

Table 6. Hypotheses test results.

Ref	Hypothesis	Descriptor	Model β (Sig)	Effect Size	Hypothesis Testing
1	**H1** Personal cyber awareness is positively associated with the mitigation of personal cyber risk	Personal Cyber Awareness influences Personal Cyber Risk (*increase in Awareness causes Cyber Risk to decline*)	-0.085 (0.284)		Rejected
2	**H2** Personal cyber awareness positively impacts personal cyber knowledge	Awareness influences Cyber Knowledge (*greater Awareness leads to greater Knowledge*)	**0.181 (0.016)**	**Medium** *Interpretation: Meaningful influence*	**Accepted**
3	**H3** Personal cyber knowledge positively impacts personal cyber risk	Knowledge influences Cyber Risk (*greater Knowledge causes Cyber Risk to decline*)	**0.336 (0.000)**	**Medium** *Interpretation: Strong Predicator*	**Accepted**
4	**H4** Knowledge mediates the relationship between personal cyber awareness and personal cyber risk	Knowledge is an exogenous variable that influences the relationship between personal cyber awareness and personal cyber risk (*Awareness no longer affects Cyber Risk after Knowledge has been controlled for*)	**0.067 (0.048)**	**Small** *Interpretation: Weak, but significant effect*	**Accepted**
		Age influences Personal Cyber Risk	0.178 (0.016)		
		Gender influences Personal Cyber Risk	0.034 (0.627)		
		Age influences Personal Cyber Knowledge	0.283 (0.000)		
		Gender influences Personal Cyber Knowledge	-0.139 (0.042)		

Table 7. Robustness tests.

Ref	Hypothesis	Descriptor	Model 1 β (Sig)	Model 2 β (Sig)
1	**H1** There is a positive relationship between awareness and cyber risk	Awareness *influences* Cyber Risk	**0.233 (0.007)**	-0.006 (0.956)
2	**H2** There is a positive relationship between awareness and cyber knowledge	Awareness *influences* Cyber Knowledge	0.084 (0.380)	**0.264 (0.013)**
3	**H3** There is a positive relationship between knowledge and cyber risk	Knowledge *influences* Cyber Risk	**0.442 (0.000)**	0.385 (0.001)
4	**H4** There is a positive relationship between awareness, knowledge and cyber risk	Awareness *influences* Knowledge and Cyber Risk	0.039 (0.860)	0.114 (0.082)
	Chi-square X^2 *(p- value)*		47.91 (0.088)	43.11 (0.1932)
	Root Mean Square Error of Approximation (RMSEA) (∗)		0.042	0.039
	P-value of the Null Hypothesis (PCLOSE)		0.631	0.638
	Comparative Fit Index CFI		0.973	0.974
	Tucker-Lewis Index (TLI)		0.959	0.961
	N		185	130

(∗) = values less than 0.05 are good, values between 0.05 and 0.08 are acceptable.

prior research (see [94,6,76]—with the condition that previous studies have offered different and/or specific participant cohorts (such as role-based) or have focused on enterprise-user environments vs typical home computer users; the personal condition has received comparatively scant attention [20]. The results also reveal that personal cyber awareness does not directly influence PCR, suggesting an antecedent dependency on an individual's cyber knowledge to enable identification and/or understanding of potential PCRs.

We highlight that the association between the constructs of personal cyber awareness, knowledge, and PCR is deemed to be only a partial effect, insofar that personal cyber safety is influenced by a pluralism of detrimental factors both internal and external to the individual. The level of cyber knowledge, all else being equal, influences the sophistication—and potential effectiveness—of personal cyber protection measures [68]. This may lead to a more robust PCRP, compared to persons whose level of cyber expertise may obfuscate their actual level of cyber safety, thus contributing to a significantly higher level of vulnerability and PCR. Importantly, personal cyber awareness or knowledge do not translate directly into an uplift in PCRP. Studies abound that stipulate the necessity of individualistic motivation as a prerequisite for delivering robust user security, as suggested by [95] and [94].

Methodologically, the differential modelling effects of personal user vis-à-vis enterprise user and/or cybersecurity/technological perspectives on PCR underscore the importance of disaggregating personal cyberspace into its constituent components [96]. This allows researchers to holistically and accurately understand the atmospherics of this dynamic and under-investigated environment.

Conclusion, limitations, and future research

Conclusion

Cyberspace is considered a domain constructed by humans in contrast to the other natural domains [34,97]. The cyber landscape is partly sequestered from tangibly physical space as it subsists within the electromagnetic spectrum, enabled by digital computers that act as nodes within an interconnected network of concatenated devices that facilitate the movement of logically constructed binary data between apparatus. Immersing the human condition within such a technological construct demands new ways of thinking and new mechanisms of engagement between cyberspace and its users [98]. By identifying key variables and affiliated relationships, and thereby contributing to the general understanding of cyberspace and individual cyber experiences, the structural model permits a theoretical–analytical reappraisal of the fundamental axiom of PCR from the individual user's perspective.

Against this landscape, this study has important implications for understanding and managing PCR. The findings indicate that cyber knowledge mediates the relationship between an individual's cyber awareness and their level of PCR (H4), and that (H1) cyber awareness does not directly or meaningfully impact PCR. These results suggest that to reduce PCR and build a comprehensive understanding of their holistic cyber capabilities and exposures, individuals are advised to actively and consistently maintain cyber awareness (H2) and uplift their cyber knowledge, creating the conditions necessary to attain meaningful and effective cyber safety (H3). This is essential, given that the findings show that in the absence of such knowledge, an individual's PCR intensifies. The results also underscore the necessity of employing standard mechanisms to identify, assess and mitigate PCR, such as the PCRP framework, designed to be employed at the individual user level and adapted specifically to accommodate personal cyberspace.

The AKR model discussed earlier is relevant in enhancing our understanding of the PCR environment within the context of modern cyberspace and contemporary cyber threats. The model simultaneously recognizes the precursors necessary for incentivizing personal motivation intended to deliver cyber safety. The research supports the argument that an individualistic, multidisciplinary and capaciously holistic approach is required, as recommended by Zimmermann and Renaud (2019), to build an understanding of those variables that impact personal cyber perspectives and the resultant PCRP [18]. To enable such an understanding of human cyber behaviours, including the motivations to adopt sub-standard personal cyber hygiene practices and personal cybersecurity missteps or transgressions, it is crucial to investigate the needs of the individual and clearly articulate their constraints (including awareness, knowledge, and consequential nocuous behaviours) to reduce any opportunities for conflict between personal cyber safety and the needs of an individual's digitally-enabled lifestyle. Such investigation may provide practical frameworks and/or tools through which individual users can advance their personal cyber 'safety'. This paper provides a baseline understanding upon which further studies that deliver pragmatic value-add models can be generated.

Limitations

Whilst this study makes meaningful theoretical and applied contributions, we acknowledge several limitations. Primarily, the research is conducted at a point in time, so insights are constrained by the dynamic and consistently transmuting nature of cyberspace. The authors anticipate that the findings and conceptual constructs will change over time and that the field of PCR and management would benefit from supplementary longitudinal studies, thereby mitigating any latent or actual retrospective bias potentially offered by a cross-sectional study. The limitation of examining variables at a single point in time may not account for temporal variations which have repercussions in terms of stability, replicability, and representativeness of the survey findings. Similarly, considering the study, data were collected at only one time point, the data set may not fully reflect the diversity or dynamics of the personal user population of cyberspace, thus mitigating the extent to which the results may be extrapolated thus introducing a potential inability to establish causality between personal cyber awareness, cyber knowledge, and associated cyber risk.

In addition, data collection was limited to a defined geography—Australia. Whilst Australia is considered to have a moderately well-established and distributed internet infrastructure (taking landmass and population size into account [99]), the survey participants may not compare equitably with other populations who do not enjoy similar internet capabilities or level of socioeconomic positioning (i.e. emerging economies) thereby presenting a risk of generalized findings to the entire Australian population. It is also important to consider that whilst Australia is a culturally diverse society, other geographies with distinct indigenous populations, linguistic differences, and alternative cultural contexts may present divergent perspectives to the survey participants that are under-represented in the study results. In addition, the survey over-represented female respondents (68.8% (Appendix 1) vs national average of female respondents within 2021 Census data indicating 50.7% response comparison), which may skew survey results if gender influences personal cyber perception.

The relatively smaller sample size may affect the robustness of conclusions drawn regarding PCR. To bolster understanding of the relationships between personal cyber awareness, knowledge and PCR, as well as extending understanding of the complexities of PCR across different population segments and user groups thereby improving the applicability of the PCRP, researchers could broaden data collection to include an extended participant cohort. It could be geographically and/or culturally diverse, and/or explore specific population segments deemed to be cyber vulnerable, such as the elderly or individuals with mental health challenges. Employing an extended variety of data collection instruments, such as face-to-face interviews or focus groups, could also be beneficial as could extending the scope of cyber behaviours studied which would widen the dimension of, and comprehensiveness of, individual cyber-risk profiles. This may mitigate potential self-reported bias which, despite survey data being anonymized, participants may overestimate their actual cyber hygiene practices stemming from a lack of awareness of potential threats, age, overconfidence in their digital skills, or simply a failure to keep up with the ever-evolving cyber landscape, as seen in prior studies [100,101].

Considerations pertaining to the wider context of personal cyberspace must be factored in, particularly in terms of temporal influences, insofar that cyberspace is a domain whereby technical, social, and behavioural changes consistently and rapidly, thereby this study's findings could become outdated posthaste as new trends, treats, and technologies emerge. Emerging threats such as AI-driven phishing capabilities may reshape individual risk profiles faster than standard cyber security awareness applications and cyber intelligence collection and analysis proficiencies adapt. Pragmatically, this demands a novel approach to determining PCRPs by means of a real-time, adaptive and holistic architecture that offers individuals a mechanism to assess and measure their cyber risk dynamically.

Future research opportunities

Given the study's limited scope, other variables may be considered in future research that extends the potential contributions from personal cyber awareness, knowledge, and risk specifically, through to exploring potentialities for and incentivization to adopt strategies to espouse personal cyber mitigation. In particular, the authors consider that further investigation into personal cyber behaviours, and their correlation and/or mediating influence on PCR would be beneficial. Some recent studies have focused on cyber risk behaviours (see [14,102,103] although most have investigated cyber behaviours of organizational users *in lieu* of generic, individual users. The practical importance of providing innovative and pragmatic frameworks/tools that may be applied day-to-day should prompt future studies into establishing standardized PCR assessment criterion and frameworks to assist individual users effectively and transparently manage their cyber capabilities. Such pioneering tools would provide individuals, at scale, the ability to attain an individualistically acceptable level of personal cyber safety.

Future research into personal cyberspace and risk could focus on additional variables such as habitual technology usage, online habits of individual users, and risk-taking tendencies such as repetitive password reuse practices or avoiding investment into cyber security applications and VPN usage—as well as cultural differences that influence perceptions and responses to personal cyber threats. These factors may prove to be important mediators or moderators in understanding PCR and resilience strategies. For instance, cultural norms pertaining to privacy, authority, and trust could materially impact an individual's cyber security behaviours and personal risk perceptions. In particular, replicating this study within regions that exhibit lower cyber maturity (in terms of infrastructure, cultural online norms, and user capabilities) would be insightful, and offer robust data to support government and/or employer usage of PCRP models to promote cyber (hygiene) awareness campaigns.

Longitudinal designs are necessary to test the relationship whether knowledge gains sustain risk reduction over time, especially given evolving threats such as deep-fake scams and AI-enabled tailored phishing campaigns. In particular, future studies should integrate clearly defined behavioural metrics such as audits of password strength and adaptation of personal cyber security applications (such as Nortons 360 or McAfee) to complement perceptual data regarding PCR. The value and fidelity of future research would benefit from adaptation of a mixed method methodology, particularly by pairing surveys and interviews to explore reasons for cyber knowledge gaps.

Incorporating these dimensions could enrich research and development of tailored frameworks for personal cyber safety, ensuring they are responsive to a diversity of behavioural and cultural contexts. This approach would augment insights into the complexities of personal cyber behaviours and improve the practical applicability of interventions across populations.

Author contributions

Richard McGregor (Conceptualization [lead], Data curation [lead], Formal Analysis [supporting], Investigation [lead], Methodology [lead], Project administration [lead], Visualization [lead], Writing – original draft [lead]), Carmen Reaiche (Supervision [supporting], Writing – review & editing [equal]), Graciela Corral de Zubielqui (Formal Analysis [supporting], Methodology [supporting], Supervision [supporting], Validation [lead], Writing – review & editing [equal])

Conflict of interest: The authors declare no conflict of interest.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

References

1. de Brulin H, Janssen M. Building cybersecurity awareness: the need for evidence-based framing strategies. *Govern Inform Quart* 2017;**34**:1–7. https://doi.org/10.1016/j.giq.2017.02.007
2. Alqahtani MA. Factors affecting cybersecurity awareness among university students. *Appl Sci* 2022;**12**:2–21. https://doi.org/10.3390/app12052589
3. McShane M, Eling M, Nguyen T. Cyber risk management: history and future research directions. *Risk Manage Insur Rev* 2021;**24**:93–125.
4. Zahidi S, Heading S. *The Global Risks Report 2023*. Switzerland: World Economic Forum, 2023, 1–98.
5. Lohrke FT, Frownfelter-Lohrke C. Cybersecurity research from a management perspective: a systematic literature review and future research agenda. *J Gener Manage* 2023;**0**:32–44.
6. Seungeun L, Chua YT. The role of cybersecurity knowledge and awareness in cybersecurity intention and behavior in the United States. *Crime Delinquency* 2023;**1**:1–28.
7. Pusey P, Sadera WA. Cyberethics, cybersafety, and cybersecurity. *J Digit Learn Teacher Edu* 2011;**28**:82–5. https://doi.org/10.1080/21532974.2011.10784684
8. Cains MG. Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Anal* 2022 1643–69, **42**. https://doi.org/10.1111/risa.13687.
9. Batra A. Cyber security management: creating governance, risk and compliance framework. *J Softw Engineer* 2020;**14**:27–33.
10. Yee CK, Zolkipli MF. Review on confidentiality, integrity and availability in information security. *J ICT Edu* 2021;**8**:34–42.
11. Simonet J, Teufel S. The influence of organizational, social and personal factors on cybersecurity awareness and behavior of home computer users. in *IFIP International Conference on ICT Systems Security and Privacy Protection*, In: Dhillon G., Editors. 2019, Springer. p. 194–208.
12. Karagiannopoulos DV. Cybercrime awareness and victimisation in individuals over 60 years: a Portsmouth case study. *Comput Law Secur Rev* 2021;**43**:105615. https://doi.org/10.1016/j.clsr.2021.105615
13. Blackwood-Brown C, D'Arcy J. Cybersecurity awareness and skills of Senior citizens: a motivation perspective. *J Comput Inform Syst* 2019;**61**:195–206. https://doi.org/10.1080/08874417.2019.1579076
14. Limna P, Kraiwanit T, Siripipattanakul S. The relationship between cyber security knowledge, awareness and behavioural choice protection among mobile banking users in Thailand. *Int J Comput Sci Res* 2022;**7**:1–19.
15. Khader M, Karam M, Fares H. Cybersecurity awareness framework for academia. *Information* 2021;**12**:417. https://doi.org/10.3390/info12100417
16. LeFebvre R. The human element in cyber security: a study on student motivation to act. in *Proceedings of the 2012 Information Security Curriculum Development Conference, 2012*. 2012. https://doi.org/10.1145/2390317.2390318
17. da Veiga A, Loock M, Renaud K. Cyber4Dev-Q: calibrating cyber awareness in the developing country context. *E J Info Sys Dev Countries* 2022;**88**:e12198. https://doi.org/10.1002/isd2.12198
18. Zimmermann V, Renaud K. Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. *Int J Hum Comput Stud* 2019;**131**:169–87, https://doi.org/10.1016/j.ijhcs.2019.05.005
19. Pollini A. Leveraging Human factors in cybersecurity: an integrated methodological approach. *Cogn Tech Work* 2022;**24**:371–90. https://doi.org/10.1007/s10111-021-00683-y
20. McGregor R. Cyberspace and personal cyber insurance: a systematic review. *J Comput Inform Syst* 2023:1–15.

21. Al-Sartawi A. Information technology governance and cybersecurity at the board level. *IJCIS* 2020;**16**:150–61. https://doi.org/10.1504/IJCIS.2020.107265
22. Finnemore M. Ethical dilemmas in cyberspace. *Ethics Int Aff* 2018;**32**:457–62. https://doi.org/10.1017/S0892679418000576
23. Kashani ES. Framing assumptions and cyberspace regulation: a critical reflection on differences among countries. *J Cyberspace Stud* 2019;**3**:109–18.
24. Shah MU. A comparative assessment of Human factors in cybersecurity: implications for cyber governance. *IEEE* 2023;**11**:87970–84.
25. Kharlamov A, Pogrebna G. Using Human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity. *Regulat Govern* 2021;**15**:709–24. https://doi.org/10.1111/rego.12281
26. Liang H, Xue Y. Understanding security behaviors in personal computer usage: a threat avoidance perspective. *J Ass Informat Syst* 2010.**11**.
27. Tsai HS. Understanding online safety behaviors: a protection motivation theory perspective. *Comput Secur* 2016;**59**:138–50. https://doi.org/10.1016/j.cose.2016.02.009
28. Mihailović A. Covid-19 and beyond: employee perceptions of the efficiency of teleworking and its cybersecurity implications. *Sustain (Switzerland)* 2021;**13**:6750.
29. Al-Qahtani AF, Cresci S. The COVID-19 scamdemic: A survey of phishing attacks and their counter-measures during COVID-19. *IET Inf Secur* 2022;**16**:324–45.
30. Lidong W, Alexander CA. Cyber security during the COVID-19 Pandemic. *AIMS Electron Electric Engineer* 2021;**5**:146–57.
31. Whitty MT, Moustafa N, Grobler M. Cybersecurity when working from home during COVID-19: Considering the Human factors. *J Cybersecur* 2024;**1**;1–11.
32. Van Mill FWF, Henman M. Terminology. the importance of defining. *Int J Clin Pharm* 2016;**38**;709–13.
33. Lippert KJ, Cloutier R. Cyberspace: a digital ecosystem. *Systems* 2021;**9**:48. https://doi.org/10.3390/systems9030048
34. Medeiros BP, Goldoni LRF. The fundamental conceptual trinity of cyberspace. *Contexto Int* 2020;**42**:31–54. https://doi.org/10.1590/s0102-8529.2019420100002
35. Popper KR. *Objective Knowledge: An Evolutionary Approach*. *Philosophia*. 1972, Oxford: Clarendon Press. Vol. **380**.
36. Gaitenby A. Law's mapping of cyberspace: the shape of new social space. *Technolog Forecast Soc Change* 1996;**52**:135–45. https://doi.org/10.1016/0040-1625(96)00050-9
37. Mareši NC. Information in cyberspace—actuality and challenges. *Strategic Impact* 2020;**76**:76–88.
38. Chen J, Ma T, Wei PJ. Study of cyberspace factors and description methods. *AMM* 2013;**427-429**:2477–80. https://doi.org/10.4028/www.scientific.net/AMM.427-429.2477
39. Liu HY, Huang R, Huang X. Research on development and key technologies of cyberspace. *AMM* 2014;**635–637**:1599–604. https://doi.org/10.4028/www.scientific.net/AMM.635-637.1599
40. Kuehl DT. From cyberspace to cyberpower: defining the problem. In: Starr SH, Wentz LK (eds), *Cyberpower and National Security*. USA: National Defence University Press, 2009, 24–42.
41. Clark D. *Characterising Cyberspace: Past, Present and Future*. USA: MIT CSAIL: MIT, 2010, 2016–28.
42. Ventre D. *Cyber Conflict: Competing National Perspectives*. Hoboken: John Wiley & Sons, 2012, 345. https://doi.org/10.1002/9781118562666
43. Cohen JE. *Cyberspace as/and Space*. USA: Georgetown University Law Centre, 2007, 210–56.
44. Ning H. General cyberspace: cyberspace and cyber-enabled spaces. *Internet of Things* 2018;**5**:1843–56.
45. Van 't Wout MC, Leenen L. Develop and maintain a cybersecurity organisational culture. In: *International Conference on Cyber Warfare and Security*. R.A.C.I. Limited, 2019, 457–XVI.
46. Strupczewski G. Defining cyber risk. *Saf Sci* 2021;**135**:105143. https://doi.org/10.1016/j.ssci.2020.105143
47. Cunneen M, Mullins M, Finbarr M. Artificial intelligence assistance and risk: framing a connectivity risk narrative. *AI Soc* 2020;**35**:625–34. https://doi.org/10.1007/s00146-019-00916-9
48. Williams PAH, Woodward AJ. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *MDER* 2015;**8**:305–16. https://doi.org/10.2147/MDER.S50048
49. Spikin IC. Risk management theory: the integrated perspective and its application in the public sector. *Estado Gobierno Gestión Pública* 2013;**21**:89–126.
50. Lyons B, Popov G. On the concept of risk, uncertainty and black swans. *J Am Soc Safe Profession* 2022;**67**;18–23.
51. Nobill M. DRIVERS: a platform for dynamic risk assessment of emergent cyber threats for industrial control systems. In: *2023 31st Mediterranean Conference on Control and Automation (MED)* Cyprus: IEEE, 2023. https://doi.org/10.1109/MED59994.2023.10185686
52. NIST. *NIST Cybersecurity Framework 2.0*. USA: US Department of Commerce, 2023, 1–52.
53. Melaku HM. Context-based and adaptive cybersecurity risk management framework. *Risks* 2023;**11**:1–22. https://doi.org/10.3390/risks11060101
54. King ZM. Characterizing and measuring maliciousness for cybersecurity risk assessment. *Front Psychol* 2018;**9**:113–45.
55. Aldasoro I. The drivers of cyber risk. *J Financ Stabil* 2022;**60**:100989. https://doi.org/10.1016/j.jfs.2022.100989
56. Mermoud A. To share or not to share: a behavioural perspective on Human participation in security information sharing. *J Cyber Secur (Oxford)* 2019;**5**:13.
57. Ganin AA. Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Anal* 2020;**40**:183–99. https://doi.org/10.1111/risa.12891
58. Rahim NHA. A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes* 2015;**44**:606–22. https://doi.org/10.1108/K-12-2014-0283
59. Howard N, Cambria E. Intention awareness: Improving upon situation awareness in human-centric environments. *Human-centric Comput Inform Sci* 2013;**3**:1–17.
60. D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Inf Syst Res* 2009;**20**:79–98. https://doi.org/10.1287/isre.1070.0160
61. White GL. Education and prevention relationships on security incidents for home computers. *J Comput Inform Syst* 2015;**55**:29–37. https://doi.org/10.1080/08874417.2015.11645769
62. Wolf M, Halworth D, Pietron L. Measuring an information security awareness program. *Rev Bus Inform Syst* 2011;**15**:9–22.
63. Yap SF, Xu Y, Tan LH. Coping with crisis: the paradox of technology and consumer vulnerability. *Int J Consumer Stud* 2021;**45**:1239–57. https://doi.org/10.1111/ijcs.12724
64. Grobler M, Raj G, Nepal S. User, usage and usability: redefining human centric cyber security. *Front Big Data* 2021;**4**:583723–. https://doi.org/10.3389/fdata.2021.583723
65. Young H, Van Vliet T, Van de Ven J. Understanding human factors in cyber security as a dynamic system. In: *Advanced in Intelligent Systems and Computing*. The Netherlands: Springer International Publishing, 2018.
66. Manap NA, Rahim AA, Taji H. Cyberspace identity theft: the conceptual framework. *Mediterr J Soc Sci* 2015;**6**:595–605.
67. Abawajy J. User preference of cyber security awareness delivery methods. *Behav Inform Technol* 2014;**33**:237–48. https://doi.org/10.1080/0144929X.2012.708787
68. Gratian M. Correlating Human traits and cyber security behavior intentions. *Comput Secur* 2018;**73**:345–58. https://doi.org/10.1016/j.cose.2017.11.015
69. Öğütçü G, Testik OM, Chouseinoglou O. Analysis of personal information security behavior and awareness. *Comput Secur* 2016;**56**:83–93.
70. Sawyer B, Hancock PA. Hacking the human: the prevalence paradox in cybersecurity. *Hum Factors* 2018;**60**:597–609. https://doi.org/10.1177/0018720818780472

71. Holt TJ, Turner MG. Examining risks and protective factors of on-line identity theft. *Deviant Behavior* 2012;**33**:308–23. https://doi.org/10.1080/01639625.2011.584050
72. Mohamed N, Ahmad IH. Information privacy concerns, antecedents and privacy measure use in Social networking sites: Evidence from Malaysia. *Comput Hum Behav* 2012;**28**:2366–75. https://doi.org/10.1016/j.chb.2012.07.008
73. Carlton M, Levy Y. Expert assessment of the top platform independent cybersecurity skills for Non-IT professionals. In: *Proceedings of the 2015 IEEE Southeast Con*. USA, 2015. https://doi.org/10.1109/SECON.2015.7132932
74. Venables A. Modelling cyberspace to determine cybersecurity training requirements. *Front Educ* 2021;**6**;45–66. https://doi.org/10.3389/feduc.2021.768037[CrossRef]
75. Zhang-Kennedy L, Chiasson S. A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Comput Surv* 2021;**54**:1–39. https://doi.org/10.1145/3427920
76. Zwilling M. Cyber Security awareness, knowledge and behavior: a comparative study. *J Comput Inform Syst* 2020;**62**:82–97. https://doi.org/10.1080/08874417.2020.1712269
77. Rajasekharaiah KM, Dule CS, Sudarshan E. Cyber security challenges and its emerging trends on latest technologies. *IOP Conf Ser: Mater Sci Eng* 2020;**981**:022062. https://doi.org/10.1088/1757-899X/981/2/022062
78. Ben-Asher N, Gonzalez C. Effects of cyber security knowledge on attack detection. *Comput Hum Behav* 2015;**48**:51–61. https://doi.org/10.1016/j.chb.2015.01.039
79. Aytes K, Connolly T. Computer security and risky computing practices: a rational choice perspective. *J Organiz End User Comput* 2004;**16**:22–40. https://doi.org/10.4018/joeuc.2004070102
80. Cain AA, Morgan E, Still JD. An exploratory study of cyber hygiene behaviours and knowledge. *J Inform Secur Appl* 2018;**42**:36–45.
81. Moallem A. *Cybersecurity Awareness among Students and Faculty*. Boca Raton: CRC Press, 2019. https://doi.org/10.1201/9780429031908
82. Taha N, Dahabiyeh L. College students infomraiton security awareness: a comparison between smartphones and computers. *Educ Inf Technol* 2021;**26**:1721–36. https://doi.org/10.1007/s10639-020-10330-0
83. Taherdoost H. Validity and reliability of the research instrument; how to test the validation of a questionnaire/survey in a research. *Int J Acad Res Manage* 2016;**5**:28–36.
84. Clarlton M, Levy Y. Expert assessment of the top platform independent cybersecurity skills for Non-IT professionals. In: *Proceedings of the 2015 IEEE SouthEastCon*. IEEE, 2015. https://doi.org/10.1109/SECON.2015.7132932
85. Glasgow PA. *Fundamentals of Survey Research Methodology*. Virginia, USA: MITRE Product, 2005, 1–28.
86. Kline RB. *Principles and Practice of Structural Equation Modeling*. 5th ed. USA: The Guilford Press, 2023, 494.
87. Klein A, Moosbrugger H. Maximum likelihood estimation of latent interaction effects within the LMS method. *Psychometrika* 2000;**65**:457–74. https://doi.org/10.1007/BF02296338
88. Berry WD, Feldman S. *Multiple Regression in Practice*. USA: Sage University Paper, 1985. https://doi.org/10.4135/9781412985208[CrossRef]
89. Hu L, Bentler PM. Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives. *Struct Equation Model Multidiscipl J* 1999;**6**:1–55. https://doi.org/10.1080/10705519909540118
90. Browne MW, Cudeck R. Alterative ways of assessing model fit. *Sociologi Methods Res* 1992;**21**:230–58. https://doi.org/10.1177/0049124192021002005
91. Bentler PM, Bonett DG. Significance tests and goodness of fit in the analysis of covariance structures. *Psychol Bull* 1981;**88**:588–606. https://doi.org/10.1037/0033-2909.88.3.588
92. Bentler PM. Comparitive fit indexes in structural models. *Psychol Bull* 1989;**107**:238–46. https://doi.org/10.1037/0033-2909.107.2.238
93. Cohen J. *Statistical Power Analysis for the Behavioural Sciences*. 2nd ed. New York, USA: Routledge, 1988, 567.
94. Ramlo S, Nicolas JB. The human factor: assessing individuals' perceptions related to cybersecurity. *ICS* 2021;**29**:350–64. https://doi.org/10.1108/ICS-04-2020-0052
95. Haney J. Users are not stupid: six cyber security pitfalls overturned. *Cyber Secur* 2023;**6**:230–41.
96. McKelvie A, Wiklund J, Brattström A. Externally acquired or internally generated? Knowledge development and perceived environmental dynamism in new venture innovation. *Entrepreneur Theory Pract* 2018;**42**:24–46. https://doi.org/10.1177/1042258717747056
97. Lambach D. The Territorialization of cyberspace. *Int Stud Rev* 2020;**22**:482–506. https://doi.org/10.1093/isr/viz022
98. Kioskli K. The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0. *Appl Sci* 2023;**13**:1–16.
99. Australian Government. *International Comparison of Fixed Broadband Performance*. Australia: Department of Infrastructure, Transport, Regional Development and Communications, 2020.
100. Rundenko Y. *Development of Youth Information Hygiene Skills: The Gap between the Self-Assessment and Real State*. In: Smyrnova-Trybulska E. (ed.), Switzerland: Springer, 2025.
101. Barakovic S, Barakovic Husic J. Cyber hygiene knowledge, awareness and behavioural practices of university students. *Inform Secur J* 3034;**32**:347–70.
102. Moustafa AA, Bello A, Maurushat A. The role of user behaviour in improving cyber security management. *Front Psychol* 2021;**12**:1–12. https://doi.org/10.3389/fpsyg.2021.561011
103. Blythe JM, Gray A, Collins E. *Human Cyber Risk Management by Security Awareness Professionals: Carrots or Sticks to Drive Behaviour Change?*In: Moallem A (ed.), Switzerland: Springer, 2020, 76–91.