

Improving National Digital Identity Systems Usage: Human-Centric Cybersecurity Survey

Malyun Hilowle, William Yeoh, Marthie Grobler, Graeme Pye & Frank Jiang

To cite this article: Malyun Hilowle, William Yeoh, Marthie Grobler, Graeme Pye & Frank Jiang (11 Sep 2023): Improving National Digital Identity Systems Usage: Human-Centric Cybersecurity Survey, Journal of Computer Information Systems, DOI: [10.1080/08874417.2023.2251452](https://doi.org/10.1080/08874417.2023.2251452)

To link to this article: <https://doi.org/10.1080/08874417.2023.2251452>



© 2023 The Author(s). Published with
license by Taylor & Francis Group, LLC.



Published online: 11 Sep 2023.



Submit your article to this journal [↗](#)



Article views: 1371



View related articles [↗](#)



View Crossmark data [↗](#)

Improving National Digital Identity Systems Usage: Human-Centric Cybersecurity Survey

Malyun Hilowle^{a,b}, William Yeoh^{a,b}, Marthie Grobler^{b,c}, Graeme Pye^{a,b}, and Frank Jiang^a

^aDeakin University, Melbourne, Australia; ^bCyber Security Cooperative Research Centre (CSCRC), Melbourne, Australia; ^cThe Commonwealth Scientific and Industrial Research Organisation (CSIRO)

ABSTRACT

National digital identity systems (NDIDs) are increasingly important for users' authentication and secure access to e-government services. However, there is insufficient research on human-centric cybersecurity (HCCS) that impacts the use of NDIDs. Drawing on the theory of planned behavior and technical formal informal model, this paper proposes and validates a research model that depicts how HCCS affect the use of NDIDs. Data were collected from 203 Australian residents and analyzed using structural equation modeling and multiple linear regression analysis. The findings revealed that security, privacy, perceived risk, usability, flexibility, and cultural and social interference significantly impact the use of NDIDs. Considering HCCS in NDIDs usage, especially in risk-conscious cultures, is crucial. Low cybersecurity awareness and trust impede NDIDs adoption, emphasizing the need for cybersecurity education and awareness. The insights benefit policy-makers, governments, and cybersecurity practitioners, providing a valuable understanding of human-centric cybersecurity influence on the use of NDIDs.

KEYWORDS

National digital identity systems; human-centric; cybersecurity; survey



Introduction

National digital identification systems (NDIDs) are security systems for managing digital identities. They allow users secure access to e-government services and ensure non-repudiation in transactions.¹ NDIDs provide secure digital signature and authentication capabilities and reduce the need for individuals to provide physical identification documents,² thus reducing instances of identity theft. Moreover, NDIDs help businesses save time and money by providing an interface between the business, consumers, and government services.³ Several countries have implemented NDIDs. For example, in Estonia, citizens use a government-issued smart card to access services such as healthcare and voting.⁴ In India, citizens use the Aadhaar system,⁵ which assigns a unique identification number to each citizen and allows them to access e-government services and welfare programs.

The slow adoption of NDIDs in Australia can be attributed to a variety of factors, such as concerns around data privacy and security, lack of awareness and education, and a fragmented identity verification landscape.⁶ To address these challenges, the Australian government introduced the Digital Transformation Agency (DTA) to oversee the development of digital identity solutions.⁷ However, as reported by the DTA in 2020, the adoption of digital

identity services in Australia remains low, with only about 1.5 million active users out of more than 21 million potential users. The use of NDIDs is a critical issue for governments and organizations worldwide. The European Union Agency for cybersecurity also highlights the European countries where self-sovereign identities technologies used in their digital identity systems are being considered or implemented to address privacy concerns and enhance digital identity security.⁸ This paper provides a comprehensive investigation of their combined impact on the adoption of NDIDs. By examining HCCS factors collectively, this research seeks to offer a holistic understanding of the complexities influencing NDID adoption. Moreover, the context of NDIDs is continually evolving, with advancements in technology and changes in user behaviors. Therefore, our research addresses the current landscape of digital identity systems and their adoption challenges around the world.⁶

Despite their enormous benefits, many Australians have rejected the use of NDIDs such as MyHealth record,⁶ a secure national digital health record system that allows users and their healthcare providers to view health records securely. Trust formation plays a pivotal role in the widespread adoption of NDIDs, as underscored by a survey conducted by the Australian Computer Society, which revealed that over 80% of respondents expressed concerns

CONTACT Malyun Hilowle  mmhilowle@deakin.edu.au  Department of Information Technology, Deakin University, Centre for Cyber Resilience and Trust (CREST), Cyber Security Cooperative Research Centre (CSCRC), 221 Burwood Highway, Burwood, Melbourne, Victoria 3125, Australia

© 2023 The Author(s). Published with license by Taylor & Francis Group, LLC.

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

about the security of their digital identity.⁹ Remarkably, only 12% exhibited trust in a government-issued digital identity credential. Achieving trust necessitates a comprehensive approach encompassing various HCCS factors, including security, privacy, usability, cultural and social interference, flexibility, cybersecurity awareness, and perceived risk. To instill trust, the Data Transformation Agency⁷ has demonstrated that implementing enhanced security measures, privacy protection, user-friendly interfaces, and cybersecurity awareness significantly influences users' confidence in e-government systems and online platforms. Additionally, cultural values, social norms, perceptions of institutional trust, and the adaptability of NDIDs play integral roles in trust formation. An essential strategy in building trust revolves around addressing digital identity systems from a human-centric perspective. By doing so, we can cultivate trust, thereby facilitating their broader acceptance and utilization.

Therefore, the primary focus of this study revolves around the cybersecurity perspective that places humans at the center and explores its implications for the adoption of NDIDs. The research question is: What is the impact of human-centric cybersecurity on the intention to use NDIDs? To address this question, Australia was selected as the case study for our research. A total of 203 Australian residents participated in an online survey, allowing us to investigate and identify the HCCS that play a role in shaping the usage of NDIDs.

Literature review

National digital identity systems

Research by National Institute of Standards and Technology¹⁰ in the United States highlighted the importance of developing HCCS strategies to enhance the use of NDIDs. Another study⁸ emphasized the need for user-centered methods of managing digital identities, such as NDIDs. There have been cases where the security and privacy of individuals and organizations have been compromised due to the challenges and risks associated with NDIDs. For example, the Korean Information Security Agency found that NDIDs were vulnerable to attack due to HCCS.¹¹ Additionally, a report by¹² highlighted the risks associated with the widespread adoption of NDIDs, including potential breaches of user privacy and the potential for government surveillance. HCCS is becoming a challenge for governments as users question the ability of governments and organizations to maintain data privacy such as the Myhealth record system used in Australia.¹³ For example, the process of setting up a myGov account in Australia requires providing identity documents that

have been targeted in recent data breaches like Optus and Medibank, emphasizing the importance of human-centric cybersecurity measures to protect users' personal information and prevent fraudulent activities in the use of digital identity systems.⁹

Furthermore, privacy concerns related to NDID systems have been a focal point of research. Studies have identified user apprehensions about data privacy, unauthorized access, and data misuse.¹⁴ For instance, El Haddouti¹⁵ delved into the challenges arising from fragmented identity verification landscapes and emphasized the necessity of interoperability among NDID systems. Additionally, Alenezi et al.² explored policy frameworks and regulatory aspects, shedding light on the governance and legal implications connected with digital identity systems.

Human-centric cybersecurity

HCCS is an approach that emphasizes the significance of the human element in designing, implementing, and managing cybersecurity systems.¹⁶ This approach involves understanding human behavior and designing systems that consider human factors. For instance, in healthcare information systems,¹⁷ several human factors that could affect the security of healthcare information have been identified, including user behavior, cognitive biases, and organizational culture. In terms of authentication and Internet of Healthcare Things (IoHT) devices, several human factors that can influence authentication security, such as user behavior, decision-making procedures, and the culture of using the devices.^{18,19} Employees were more inclined to adhere to cybersecurity policies if they understood the underlying reasoning for them.²⁰ These authors also found that employees were more likely to report security incidents if they felt confident that their actions would not result in punishment. These studies highlight the need to focus on the HCCS perspective when designing and introducing cybersecurity systems.

Research has revealed that the effectiveness of cybersecurity measures is influenced by human factors such as attitudes, beliefs, and behaviors.^{21–24} Consequently, an understanding of how individuals perceive and interact with cybersecurity measures, including NDIDs, is crucial. The key predictors of adoption and usage include perceived risk, utility, and convenience of use.²⁵ Additionally, trust, security, privacy, and social influence impact the use of mobile payment systems.²⁶ These studies highlight the crucial role of human behavior in cybersecurity and demonstrate how human-centric approaches can effectively improve cybersecurity outcomes. By understanding human behavior and

designing systems that incorporate HCCS, organizations can enhance their overall cybersecurity position. However, the existing research has mainly focused on the technical aspects of NDIDs, with little attention given to the human aspects. As such, this research addresses this gap by investigating the HCCS that impact the use of NDIDs, thereby enhancing NDID adoption among users.

Theoretical development

Theoretical background

This research employed the technical formal informal (TFI) model²⁷ and integrated it with the theory of planned behavior (TPB)²⁸ to investigate the factors affecting the adoption of NDIDs in the context of HCCS. The TFI model, originally introduced by Stamper et al., is a widely recognized theoretical framework used to gain insights into the adoption of technological systems like NDIDs. It offers flexibility and adaptability to suit the specific context of our study on HCCS and NDID adoption. An interdisciplinary approach is encouraged within the TFI model, taking into account factors from various domains, including technology, psychology, sociology, and information security. This perspective is essential for comprehending the intricate dynamics involved in NDID adoption, where technological, social, and psychological aspects interact.

In our study, the TFI model encompasses three primary dimensions: technology (security, usability, and flexibility), formal factors (cybersecurity awareness, privacy, and trust), and informal factors (culture and social interference and risk). To underscore the significance of the TFI model in information security research, Eibl²⁹ notably explored design criteria for e-learning systems to ensure security. Additionally, Samonas et al.³⁰ conducted a comprehensive review of the evolution of the CIA triad within the information security field.

The Theory of Planned Behavior (TPB) emphasizes the significance of personal beliefs and attitudes in shaping human behavior. In TPB intention represents the individual's subjective willingness to engage in a behavior in the future, while behavioral intention reflects their immediate readiness to perform the behavior at a given moment. The three primary factors that influence human behavior are attitudes toward behavior, subjective norms, and perceived behavioral control. Attitudes, about behavior, reflect an individual's evaluation, whether positive or negative, of a specific action. Subjective norms encompass the impact of social pressure on a person's inclination to either adopt or refrain from a particular behavior. The notion of perceived behavioral control relates to an individual's

confidence in their capacity to successfully execute a specific behavior.²⁸ Ajzen's²⁸ seminal work provides comprehensive insights into the theoretical underpinnings and empirical evidence supporting the distinction between these constructs.

As shown in Figure 1 below, to overcome these limitations, we combined the TFI and TPB to establish a theoretical foundation for this research on the HCCS that impact the use of NDIDs. The following subsection presents our hypotheses.

Hypothesis development

Security refers to the measures taken to prevent unauthorized access, tampering, or manipulation of data within cyber systems, including NDIDs.²⁴ Security concerns were a significant barrier to the adoption of NDIDs and that users were more likely to use NDIDs with strong security measures in place.³¹ In addition, the use of advanced security technologies, such as biometrics, has been shown to increase user acceptance and trust in NDIDs.³² For example, India's Aadhaar NDID, which uses biometric authentication, has been widely adopted and has become a crucial tool for accessing government services and financial products.³³ In summary, improved security measures play a critical role in building user trust and adoption of NDIDs, and are essential for the widespread use of digital identity systems.²⁵ The major challenges associated with the security of NDIDs are data confidentiality, data availability and data integrity for third-party organizations. The main concern with users is associated with user data security since they do not know how to protect themselves.²⁴ Security was a major concern for users in adopting electronic government services in.³⁴ In the realm of e-commerce, research by³⁵ investigated the impact of security and privacy concerns on online shopping behavior. The study found that security-related factors, such as secure payment mechanisms and secure communication channels, were significant predictors of online shopping adoption. Users were more likely to engage in online shopping when they perceived a high level of security in the transaction process. Furthermore, the role of security in users' acceptance and adoption of digital health technologies was explored.³⁶ The research findings highlighted that the security of their health information significantly influenced their willingness to adopt and use digital health systems. Therefore, we hypothesized that:

H1. *Security would positively influence users' use of NDIDs.*

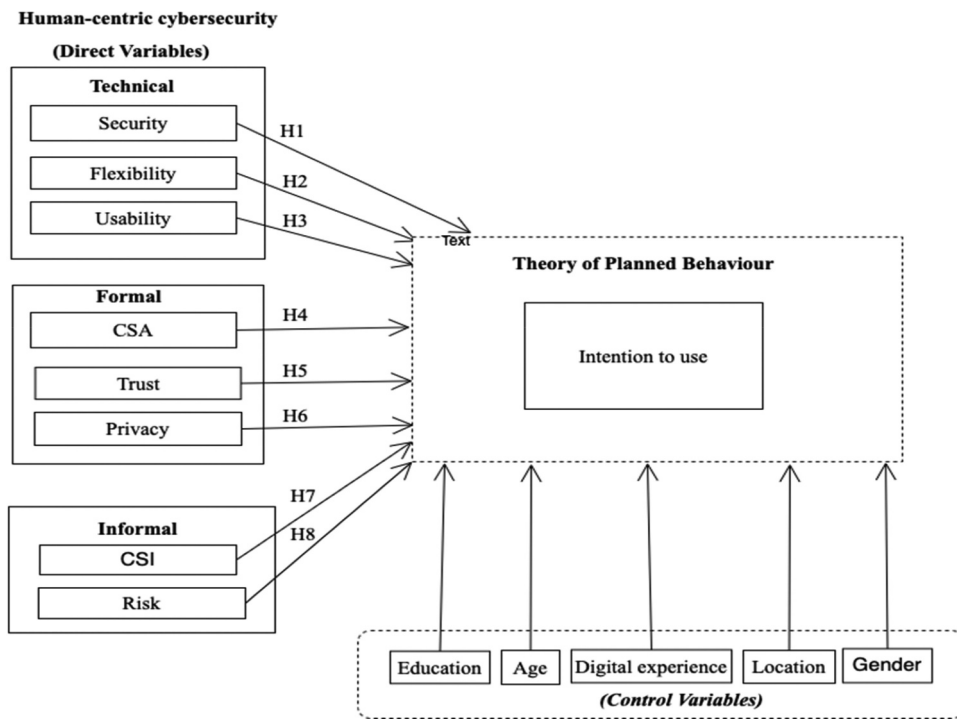


Figure 1. Research model.

Flexibility is defined as the ability of an NDID to adapt and facilitate the interoperability of e-government services.³⁷ The importance of flexibility cannot be overstated, as it allows NDIDs to adjust to changing conditions and meet evolving demands. Flexibility of digital identity systems enables the integration of new technology into existing processes effectively, leading to increased user acceptance.³⁸ Flexibility in NDIDs was discussed by Hodapp³⁹ and Hwang,²⁵ with these studies suggesting that the adaptability of an NDID allows for the exploration of new ideas and experimentation with novel approaches, resulting in increased use. In the context of e-learning platforms, the relationship between flexibility and user acceptance of these platforms revealed that users were more likely to engage with and utilize e-learning platforms when they perceived them to be flexible in terms of accommodating different learning styles.⁴⁰ Chong⁴¹ investigated the impact of the flexibility of the fingerprint scheme to verify users of cloud-based services. The study revealed that user's perception of the flexibility offered by cloud services, such as the ability to scale resources based on demand, access services from different devices, and choose from various service configurations, positively influenced their intention to adopt and use cloud services. Therefore, it was hypothesized that:

H2. *Flexibility would positively influence users' use of NDIDs.*

NDID usability is a measure of how easily users can interact with the system.⁴² This includes elements such as user control, consent, and interoperability. Given that users are more likely to avoid using systems that are difficult to use, usability is a key factor in NDID design and implementation.² Both individuals and government organizations can benefit from an easily navigable and usable system, which allows users to complete tasks efficiently and with minimal effort.⁴³

Studies have demonstrated that users tend to engage more with technology that is easy to learn, use, and remember.¹⁶ Factors that impact usability, such as navigation, layout, and visual design, can also influence user satisfaction, engagement, and loyalty.⁴⁴ Additionally, improving usability has been found to decrease user frustration, anxiety, and uncertainty, leading to a more positive user experience.¹⁶ Additionally, the influence of system usability on users' intention to use information systems was discussed in.² The research findings highlighted that users' perception of system usability significantly influenced their intention to adopt and use these systems. When users found the system easy to use, clear in its functionalities, and requiring minimal effort to perform tasks, they were more likely to engage with the system. Furthermore, Chen⁴⁵ explored the role of usability in users' acceptance and use of mobile banking applications. The research findings indicated that user's perception of the usability of mobile banking

applications, such as ease of use, intuitive design, and clear navigation, significantly influenced their intention to adopt and use these applications. Users were more likely to engage with and utilize mobile banking applications when they found them user-friendly and efficient. Therefore, designing NDIDs with good usability can increase user acceptance, usage, and satisfaction. Accordingly, we hypothesized that:

H3. *Usability would positively influence users' use of NDIDs.*

Cybersecurity awareness refers to the understanding and actions taken to safeguard information assets.²⁶ The awareness of cybersecurity in the context of electronic identification (eID) and the utilization of self-sovereign identity emphasizes the importance of understanding potential online threats and protective measures when managing and controlling one's own digital identity.⁴⁶ For example, users who are aware of phishing attacks and malware are more likely to adopt secure password practices and install antivirus software.²⁵ Moreover, users who are aware of cybersecurity risks are more likely to use systems that have adequate cybersecurity measures in place, such as two-factor authentication and encryption.⁴⁷ Similarly, users who are aware of privacy risks associated with online platforms are more likely to adjust their privacy settings and avoid sharing sensitive information.²⁴

High cybersecurity awareness has been shown to have a positive and negative impact on user behavior.⁴⁸ Furthermore, it is demonstrated that individuals well-informed about risks are less likely to adopt new technologies,⁴⁹ while conscious users are less prone to adopting certain technologies.⁵⁰ Additionally, users knowledgeable about cybersecurity issues perceive higher security risks, leading to cautious online behaviors.⁵¹ Despite this consistent literature has shown high cybersecurity awareness can enhance the user experience by reducing user anxiety and uncertainty and increasing user confidence in technology.⁵² Therefore, promoting cybersecurity awareness through education and training can help organizations improve user acceptance and use of technology while mitigating cybersecurity risks. Therefore, we hypothesized that:

H4. *Cybersecurity awareness would positively influence users' use of NDIDs.*

Trust is the user's belief in the reliability, truthfulness, and effectiveness of NDIDs. The level of trust users

have in NDIDs is a significant factor in their willingness to adopt new technologies.⁵³ With the shift from paper-based to electronic-based NDIDs, user trust in NDIDs must be established for their successful use. Also, the relationship between trust and electronic identity with users' worries about identity theft.³ The research findings indicated that users' trust in the system's security, data protection measures, and privacy controls significantly influenced their intention to adopt and use digital identity technologies. The impact of trust on users' intentions to share and disclose personal information was revealed in that users' trust, data handling practices, and protection of personal information, positively influenced their willingness to disclose personal information. Furthermore, the influence of trust on users' acceptance and use of e-government services highlighted that users' trust in the government, including trust in the security measures, data protection practices, and reliability of e-government systems, significantly influenced their intention to adopt and use these services.³⁴ Therefore, we proposed that:

H5. *Trust would positively influence users' use of NDIDs.*

Privacy pertains to the capability of NDID users to regulate and handle their personal information.⁵⁴ Growing user concerns regarding the privacy of their data underscore the significance of privacy protection in fostering user trust and adoption.³⁶ The study by Chong¹⁷ has demonstrated that privacy concerns influence the adoption of mobile health applications, with users more inclined to use systems that assure the security of their personal health information. Similarly, research on mobile payment systems indicates that users prefer and utilize platforms that offer privacy-enhancing features.³⁶ These findings emphasize the importance of addressing privacy concerns in NDID systems to positively impact user behavior. Prioritizing the implementation of privacy-enhancing features and effectively communicating these measures to users can build trust and encourage adoption.⁴⁸ By ensuring robust privacy measures, NDIDs can offer a more positive user experience, thus promoting wider adoption of this technology.⁴⁹ Therefore, our hypothesis is as follows

H6. *Privacy would positively influence users' use of NDIDs.*

The cultural and social context of a user is an important factor that influences their acceptance and use of

information systems.⁵⁵ Social cognitive theory suggests that users' behaviors and interactions affect their preferences for a system.⁵⁶ The use of IT systems is influenced by cultural characteristics, according to theoretical, empirical, and anecdotal research.⁵⁷ Cultural variables fundamentally impact how digital identity concerns develop.⁵⁸ Cultural and social interference can hinder the adoption and use of technology.⁵⁹ Thompson et al.⁵⁹ discovered that technology adoption and usage are significantly impacted by culture, influencing people's perceptions of technology and their willingness to utilize it. Additionally, social factors, including pressure to conform to social norms and expectations, have detrimental effects on the acceptance and utilization of IS.⁶⁰ Additionally, the influence of cultural factors on individuals' acceptance and use of e-government services indicated that cultural beliefs and values, such as concerns about privacy, trust in government institutions, and skepticism toward technology, can act as barriers to the adoption and use of e-government services.⁶¹ Social interference can lead to resistance against the adoption of IS, especially if they are not widely accepted by a person's social circle. Hence, we hypothesized that:

H7. *Cultural and social interference would negatively influence users' use of NDIDs.*

Perceived risk is crucial as it reflects the user's belief that using the system could result in a loss, such as an emotional, physical, mental, or financial loss.⁶² The level of perceived risk a user experiences can significantly impact their motivation to use a system.³² Perceived risks can be divided into functional risks (i.e., the system not meeting the user's expectations), social risks (i.e., the user feeling embarrassed by the system), and financial risks (i.e., the user being worried about losing money by using the system).²⁵ Studies such as Hansen²⁵ indicate that individuals are cognizant of the cybersecurity risks linked to online systems. Also, the impact of perceived risk on users' acceptance and adoption of identity management systems revealed that users' perception of risks, including concerns about the security and privacy of personal information, affected their willingness to adopt and utilize identity management systems.¹² These risks stem from the possibility that user data may be compromised through hacking, shared with unauthorized parties, used without the user's knowledge or consent, or even compromised due to human error.⁵⁵ Several previous studies have revealed a connection between risk and system use.⁴² Given the heightened risks associated with

NDIDs, if users perceive less risk associated with using NDIDs, they are more likely to accept them. Therefore, we hypothesized that:

H8. *Perceived risk would negatively influence users' use of NDIDs.*

Materials method

Survey design

The questionnaire adopted in this study was designed to capture eight main HCCS factors that may impact the intention to use NDIDs. The questionnaire comprised of multiple sections. The initial section encompassed screening questions, followed by section 2, which included demographic information. Section 3 of the questionnaire focused on the HCCS with the intent to use NDID. The questionnaire underwent verification by industry experts and practitioners from the Commonwealth Scientific and Industrial Research Organisation (CSIRO), as well as the research supervisory team within the faculty. Approval for this study was granted by the university's human ethics advisory board.

Data collection

The survey was created and deployed by Qualtrics software and was distributed online to social media groups. A total of 263 anonymous respondents commenced the survey. Sixty responses were not valid and, hence, were removed; these respondents were removed because they did not complete all of the questions in the survey. The target respondents were Australian residents. The two primary inclusion criteria were: (1) Australian resident with either citizenship, permanent residence, or on an Australian visa, and (2) aged ≥ 18 years. The level of digital skills of the respondents was defined according to three levels i.e., basic, intermediate, and advanced.

Measurement model

This study measured the HCCS factors and categorized them into two groups: reflective and formative. The reflective factors comprised security, trust, and privacy, while the formative factors included flexibility, usability, cultural and social interference, and cybersecurity awareness. Subsequently, we grouped the HCCS into the three dimensions of the TFI model and integrated them into the TPB theory by substituting the subjective norms. Figure 1 depicts the HCCS factors across the technical, formal, and informal dimensions that influence the intention to use

NDID. As part of the context of structural equation modeling (SEM) or path analysis, studies such as Pirouz⁶³ utilize multiple linear regression (MLR) to estimate the relationships between latent constructs and observed variables. By estimating the regression coefficients, the strength of the connections between the latent constructs and the observed variables can be determined. This integration of MLR analysis within SEM enabled a comprehensive evaluation of the structural model and facilitated the examination of the hypothesized relationships. Considering its ability to handle multi-path research, it was deemed the most suitable approach for testing the structural model.

Apart from the aforementioned HCCS factors, users' intentions to use NDIDs are also influenced by other important indirect variables such as gender, age, location, education, and level of digital skills. Existing research suggests that women may exhibit more risk-averse behavior, potentially impacting their attitudes toward adopting new technologies like NDIDs.⁴⁵ Age can also play a role, with older individuals being less familiar with digital technologies, leading to potential hesitancy in using NDIDs.⁴³ Additionally, location can influence individuals' access to digital infrastructure and resources, affecting their ability to adopt NDIDs.¹³ Education and digital skills can further shape perceptions of the ease of use and benefits associated with NDID adoption.⁵⁰ Addressing these indirect variables will allow us to gain insights into NDID use and adoption of NDIDs.

Demographic information

A total of 203 participants completed the survey. As shown in Table 1, the respondents were from various regions: 81% lived in metropolitan areas in Australia, 11% lived in regional areas in Australia, and 8% lived overseas. Most of the respondents were female.⁶⁴ The largest age group was those aged between 18 and 30 years (34%). Regarding the level of education, the largest group of respondents was those with a bachelor's degree,⁶⁵ followed by a diploma (25%), and a master's degree (23%). Most respondents had an intermediate level of digital skills,⁶⁶ followed by a basic level of digital skills (38%).

Analysis and results

Item loading

The properties of the data were evaluated before analysis. The estimated means approach was used to assign values to any missing data. The structural models were tested by estimating the variance, minimum, maximum, and mean

Table 1. Demographic information.

Variable	Category	Percentage
Age	18–30	34%
	31–40	27%
	41–50	25%
	51–60	11%
	>61	3%
Gender	Male	45%
	Female	55%
Level of education	High school qualification	12%
	Certificate or diploma	25%
	Bachelor certificate	40%
	Master certificate and above	23%
Level of digital skills	Basic	38%
	Intermediate	41%
	Advanced	21%
Location	Metropolitan area	81%
	Regional area	11%
	Overseas	8%

values, and the standard deviation. The purpose of this was to demonstrate the relationships between the variables and the degree to which the independent variables accounted for the variance in the dependent variable. Significant findings were observed in security, usability, privacy, flexibility, cultural and social interference, and risk, indicating their positive impact on the intention to use NDIDs. However, cybersecurity awareness and trust showed a negative influence on the use of NDIDs. Table 2 displays the significance of the items and the performance of the model. These findings confirm that the HCCS significantly influence the intention to use NDIDs by users in Australia.

Reliability test

The purpose of conducting a reliability test is to ensure that the responses given by the participants are consistent.⁶³ Table 3 displays the composite reliability and Cronbach's alpha values associated with the different variables examined in the study. Composite reliability serves as a more suitable indicator of internal consistency when the items exhibit non-equivalence, whereas Cronbach's alpha assesses the reliability of a scale or test, providing insights into its accuracy in measuring the intended construct.⁶⁷

The examination indicated that all variables exhibited reasonably high composite reliability values, ranging from 0.724 to 0.879. This suggests that the items within each variable consistently measure the same underlying concept. The Cronbach's alpha values were also relatively high, ranging from 0.711 to 0.895, indicating that the scales used are dependable and consistent. Collectively, these findings suggest that the measurements employed in this study possess reliability and consistency, thereby enhancing the accuracy and credibility of the study's results.

Table 2. Item loadings of variable.

HCCS	Variable	Mean	Standard Deviation	Variance	Statistically Significant
Security	SEC1	3.81	1.42	2.01	Yes
	SEC2	3.96	1.21	1.47	Yes
	SEC3	3.07	1.51	2.27	Yes
	SEC4	3.17	1.53	2.33	Yes
Flexibility	FLX1	2.85	1.44	2.07	No
	FLX2	2.99	1.49	2.22	No
	FLX3	3.18	1.44	2.08	Yes
	FLX4	3.16	1.51	2.28	Yes
Usability	USB1	3.79	1.21	1.47	Yes
	USB2	4.02	0.96	0.92	Yes
	USB3	3.70	1.17	1.37	Yes
	USB4	3.91	1.05	1.11	Yes
CSA	CSA1	4.55	0.83	0.69	Yes
	CSA2	2.70	1.42	2.01	No
	CSA3	2.84	1.47	2.17	No
	CSA4	2.76	1.47	2.15	No
Trust	TRS1	2.66	1.48	2.20	No
	TRS2	3.21	1.46	2.14	Yes
	TRS3	2.62	1.44	2.08	No
	TRS4	2.75	1.42	2.03	No
Privacy	PRV1	4.06	1.13	1.27	Yes
	PRV2	4.17	1.07	1.13	Yes
	PRV3	4.08	1.12	1.26	Yes
	PRV4	3.28	1.57	2.48	Yes
CSI	CSI1	4.10	1.15	1.33	Yes
	CSI2	3.67	1.30	1.68	Yes
	CSI3	4.00	1.05	1.10	Yes
	CSI4	4.30	0.96	0.92	Yes
Risk	RSK1	3.99	1.17	1.37	Yes
	RSK2	4.20	0.93	0.86	Yes
	RSK3	4.21	0.96	0.92	Yes
	RSK4	4.14	1.06	1.13	Yes

Legend: USB = usability; CSI = cultural and social interference; SEC = security; PRV = privacy; FLX = flexibility; TRS = trust; CSA = cybersecurity awareness; RSK = risk.

*See appendix for further explanation of item numbers.

Table 3. Assessment of composite reliability and cronbach's alpha.

Variable	Composite Reliability	Cronbach Alpha
SEC	.873	.779
FLX	.826	.722
USB	.803	.753
CSA	.879	.835
TRS	.862	.846
PRV	.765	.734
CSI	.854	.895
RSK	.724	.711

Correlation analysis among variables

The model was evaluated according to previous studies on IS that employed second-order formative variables. To establish convergent validity, each construct's extracted average variance should exceed 0.50. Discriminant validity can be confirmed by ensuring that the square root of the average variance extracted for each latent variable is higher than the correlations between variables.⁶⁷ In this preliminary examination of the first-order measurement model, all the requirements were met, as shown in Figure 2.

The study's findings support the claim that a greater intention to use more digital identity services in the future is positively correlated with the safeguarding of

online identities (P-value of 0.000). Most of the participants showed confidence in the security and reliability of NDIDs and were convinced that such systems offer a secure way to manage their online identity. Furthermore, the results revealed that cultural background positively influences NDIDs usage intentions (P-value of 0.003). Privacy (PRV1 to PRV4) was also found to be strongly correlated with security (SEC1 to SEC4). However, trust (TRS3 and TRS4) were not correlated with cybersecurity awareness (CSA1). The usability (USB1 to USB4) of NDIDs was found to be correlated with the cultural and social interference (CSI1) of users, indicating that people's social and cultural perceptions affect the perceived usability of NDIDs.

Robustness check

Linear regression

To further enhance our analysis, linear regression was conducted to investigate the linear relationships between the variables.⁶⁸ As indicated in Table 4, security, privacy, risk, usability, flexibility, and culture and social interference demonstrated significant associations with the intention to use NDIDs. However,

	SEC1	SEC2	SEC3	SEC4	PRV1	PRV2	PRV3	PRV4	TR51	TR52	TR53	TR54	RSK1	RSK2	RSK3	RSK4	CSA1	CSA2	CSA3	CSA4	USB1	USB2	USB3	USB4	FLX1	FLX2	FLX3	FLX4	CS11	CS12	CS13	CS14
SEC1	0.64																															
SEC2	0.965	0.618																														
SEC3	0.564	0.481	0.68																													
SEC4	0.786	0.685	0.935	0.693																												
PRV1	0.947	0.986	0.508	0.676	0.63																											
PRV2	0.965	0.996	0.418	0.647	0.974	0.551																										
PRV3	0.958	0.993	0.504	0.685	0.998	0.984	0.596																									
PRV4	0.806	0.698	0.823	0.88	0.754	0.663	0.743	0.651																								
TR51	0.058	-0.09	0.805	0.614	-0.026	-0.154	-0.042	0.582	0.376																							
TR52	0.605	0.583	0.942	0.856	0.649	0.515	0.631	0.852	0.693	0.716																						
TR53	-0.062	-0.197	0.747	0.522	-0.131	-0.263	-0.148	0.482	0.992	0.637	0.269																					
TR54	-0.016	-0.109	0.804	0.601	-0.092	-0.177	-0.095	0.384	0.91	0.652	0.922	0.305																				
RSK1	0.942	0.983	0.599	0.747	0.988	0.963	0.989	0.76	0.05	0.716	-0.051	0.033	0.722																			
RSK2	0.909	0.967	0.567	0.693	0.989	0.945	0.985	0.747	0.032	0.72	-0.063	-0.003	0.993	0.699																		
RSK3	0.928	0.975	0.563	0.702	0.995	0.955	0.991	0.764	0.031	0.709	-0.068	-0.017	0.995	0.999	0.675																	
RSK4	0.957	0.996	0.495	0.68	0.997	0.987	0.9996	0.727	-0.059	0.621	-0.164	-0.102	0.989	0.983	0.99	0.612																
CSA1	0.967	0.951	0.34	0.62	0.914	0.971	0.93	0.652	-0.183	0.391	-0.303	-0.251	0.885	0.852	0.875	0.933	0.432															
CSA2	-0.053	-0.15	0.779	0.573	-0.134	-0.217	-0.137	0.355	0.911	0.62	0.926	0.999	-0.01	-0.047	-0.06	-0.144	-0.285	0.358														
CSA3	0.233	0.148	0.933	0.769	0.18	0.076	0.173	0.605	0.914	0.833	0.897	0.961	0.294	0.265	0.252	0.164	-0.013	0.949	0.527													
CSA4	0.061	-0.067	0.735	0.636	-0.111	-0.112	-0.094	0.313	0.782	0.49	0.777	0.927	0.02	-0.055	-0.059	-0.094	-0.125	0.929	0.864	0.209												
USB1	0.806	0.871	0.703	0.737	0.916	0.826	0.903	0.77	0.229	0.859	0.153	0.216	0.946	0.962	0.951	0.8997	0.691	0.172	0.466	0.094	0.83											
USB2	0.757	0.86	0.507	0.551	0.92	0.825	0.901	0.671	0.037	0.731	-0.033	-0.012	0.918	0.957	0.945	0.898	0.686	-0.055	0.249	-0.166	0.965	0.74										
USB3	0.696	0.812	0.587	0.589	0.865	0.766	0.848	0.631	0.117	0.79	0.06	0.137	0.893	0.927	0.907	0.846	0.598	0.093	0.374	-0.023	0.977	0.979	0.743									
USB4	0.737	0.838	0.561	0.582	0.901	0.797	0.881	0.684	0.103	0.777	0.037	0.066	0.909	0.947	0.933	0.877	0.648	0.023	0.321	-0.099	0.977	0.997	0.99	0.701								
FLX1	0.167	0.11	0.887	0.668	0.186	0.03	0.164	0.616	0.918	0.868	0.913	0.902	0.279	0.282	0.265	0.151	-0.088	0.888	0.96	0.706	0.509	0.34	0.45	0.412	0.492							
FLX2	0.396	0.324	0.96	0.813	0.393	0.25	0.374	0.782	0.884	0.948	0.834	0.474	0.469	0.459	0.361	0.15	0.814	0.947	0.671	0.652	0.483	0.564	0.543	0.97	0.563							
FLX3	0.561	0.554	0.958	0.876	0.58	0.485	0.574	0.734	0.667	0.959	0.62	0.74	0.682	0.664	0.648	0.57	0.351	0.709	0.884	0.64	0.811	0.643	0.746	0.698	0.857	0.919	0.679					
FLX4	0.604	0.539	0.829	0.89	0.469	0.506	0.495	0.567	0.487	0.671	0.424	0.658	0.585	0.505	0.505	0.501	0.466	0.636	0.743	0.786	0.556	0.333	0.436	0.373	0.559	0.653	0.819	0.522				
CS11	0.971	0.989	0.488	0.684	0.995	0.985	0.997	0.761	-0.042	0.608	-0.153	-0.121	0.977	0.97	0.981	0.995	0.948	-0.161	0.149	-0.109	0.876	0.876	0.81	0.852	0.138	0.356	0.539	0.475	0.931			
CS12	0.845	0.902	0.729	0.798	0.911	0.862	0.91	0.736	0.205	0.831	0.124	0.256	0.961	0.954	0.945	0.911	0.738	0.213	0.491	0.205	0.977	0.909	0.938	0.922	0.474	0.626	0.837	0.694	0.881	0.907		
CS13	0.83	0.908	0.601	0.667	0.951	0.873	0.939	0.735	0.102	0.782	0.021	0.072	0.963	0.984	0.976	0.936	0.747	0.028	0.334	-0.04	0.989	0.987	0.976	0.987	0.386	0.543	0.719	0.472	0.916	0.96	0.946	
CS14	0.966	0.991	0.423	0.64	0.987	0.993	0.992	0.71	-0.12	0.542	-0.231	-0.189	0.965	0.956	0.968	0.992	0.965	-0.229	0.076	-0.155	0.842	0.853	0.781	0.824	0.057	0.279	0.479	0.448	0.996	0.855	0.892	1

Figure 2. Correlations among variables. *Correlation tests examine the relationship between variables to determine if the values of one variable increase, decrease, or remain unchanged when the values of another variable change.

Table 4. Linear regression test among variables for intention to use NDIDs.

Variable	R squared	Statistical Significance
SEC	0.611	Strong
FLX	0.768	Strong
USB	0.739	Strong
CSA	0.229	Not Strong
TR5	0.126	Not Strong
PRV	0.982	Strong
CSI	0.846	Strong
RSK	0.857	Strong

cybersecurity awareness and trust did not exhibit significant associations to use NDIDs. This implies that the respondents' levels of trust and cybersecurity awareness are low, which reduces the influence of these characteristics on their intentions to utilize NDIDs.

Ranked ANOVA

Similar to the standard analysis of variance,⁶⁹ the ranked ANOVA determines if two variables are statistically connected.⁶⁹ When evaluating the significance of results and deciding whether to reject the null hypothesis, both the F value and the P-value should be taken into consideration. A high F value, exceeding the critical F value, along with a low P-value, indicates statistical significance. The F statistic is used to assess the overall impact of all HCCS. The null hypothesis should only be rejected when the P-value is below the predetermined alpha level.⁷⁰

The ranked ANOVA test results indicated that the variables security, privacy, risk, usability, flexibility, and culture and social interference were significantly associated

with the intention to use NDIDs, while trust and cybersecurity awareness were not. The F-value measures the overall significance, and the P-value indicates the significance level of each variable. Since every variable had an F-value higher than the F-critical value, each can be considered to significantly affect the intention to use NDIDs. Security, privacy, risk, usability, flexibility, and culture and social interference all had P-values <.05, indicating that these variables have substantial impacts. Conversely, the P-values for trust and cybersecurity awareness were greater than 0.05, indicating that these variables do not have significant impacts. Therefore, it can be concluded that have significant impacts on the intention to use NDIDs, while trust and cybersecurity awareness do not.

Table 5 shows the statistical significance of the HCCS with P-values <.05 about the intentions of users. Usability confirms that users' needs can be met by NDIDs. They will use more NDIDs in the future, and they believe that the use of NDIDs allows them to access services that they could not access otherwise. Culture

Table 5. Ranked ANOVA test between variables and the intention to use NDIDs.

Variable	F value	P value	F critical value
SEC	11.2639872	.00020082	3.05556828
FLX	15.8596138	.00024901	3.47804969
USB	41.3223140	.00301144	7.70864742
CSA	0.00120213	.99993897	3.49029482
TR5	0.07176697	.10122345	3.48804970
PRV	13.8972239	.00043151	3.47804969
CSI	15.1272074	.00332692	4.75706266
RSK	24.6812933	.00089504	4.75706266

Table 6. Hypothesis testing.

Variable Relations	Hypothesis	B	Beta	CV	Sig.	VIF	Accept Hypothesis
<i>Security → intention to use</i>	H1	2.186	2.24	0.202	0.001	1.2	Yes*
<i>Flexibility → intention to use</i>	H2	0.34	0.3	0.190	0.00001	1.6	Yes*
<i>Usability → intention to use</i>	H3	2.5595	2.16	0.285	0.00001	2.45	Yes*
<i>Cybersecurity awareness → intention to use</i>	H4	0.1245	0.15	0.292	0.2295	1.6	No
<i>Trust → intention to use</i>	H5	2.4538	0.1325	0.287	0.202	1.8	No
<i>Privacy → intention to use</i>	H6	1.579	1.33	0.249	0.00001	1.06	Yes*
<i>Cultural & social interference → intention to use</i>	H7	-0.6488	-0.548	0.254	0.03	1.2	Yes*
<i>Perceived risk → intention to use</i>	H8	-3.490	-2.84	0.325	0.00001	1.9	Yes*

R² = 0.756, Adjusted R² = 0.712, Model fit (AIC = 424), CI = 95%.

* $p < .01$.

R² for intention to use = 0.756 ($R^2 \geq 0.5$) and ($p < .01$ (significant)).

and social interference indicate that users find it easier to use NDIDs to access online services because of the effects of social media. Finally, the security indicates that NDIDs offer security in managing online identities, and users feel that NDIDs may be more secure than traditional authentication systems.

Hypothesis testing

The results of the hypothesis testing in Table 6 indicate that several factors have a significant influence on the intention to use NDIDs. Security, flexibility, usability, and privacy all have a positive and statistically significant relationship with the intention to use NDIDs. Additionally, perceived and cultural & social interference, risk negatively impact the intention to use NDIDs and also show a statistically significant relationship with intention to use NDIDs. However, cyber security awareness and trust do not show a significant influence on the intention to use NDIDs. The overall model explains 75.6% of the variance in intention to use NDIDs, with a good model fit based on the AIC value and a 95% confidence interval. This suggests that the model fits the data well, and the independent variables can explain a significant amount of variance in the dependent variable, which was the intention to use NDIDs. All hypotheses, except for H3 and H4, were accepted.

Discussion

The results of this study indicate new findings that show that there is a lack of trust in the use of NDIDs and poor levels of cybersecurity awareness. This is evidenced by the low standardized path coefficient for the relationships between the intention to use NDIDs and both cybersecurity awareness (0.15) and trust (0.1325). There may be several reasons for the low levels of cybersecurity awareness and trust in NDIDs found in this study. Firstly, NDIDs are still a relatively new technology, and users may not be familiar with the security measures and standards implemented to protect their data.⁶ Furthermore, there has been an increase in

security incidents and data breaches due to the changing work practices during the pandemic and post-pandemic era. This has garnered significant attention and may have resulted in a loss of trust in online services and platforms among users. Finally, users indicate that they don't fully understand the potential risks and threats associated with NDID cybersecurity and they are not aware of the best practices for protecting their personal information.¹⁹

It becomes evident that security factors play a crucial role in shaping users' intention to adopt national digital identity systems (NDIDs). The positive beta coefficient of 2.24 suggests that users who perceive NDIDs as secure, and having data integrity are more likely to adopt them aligns with^{19,26,37} emphasizing the significance of security as a key driver for technology adoption. The results reinforce the importance of instilling trust and confidence in the security features of NDIDs to enhance user acceptance. However, the study acknowledges that the relationship between security factors and technology adoption is not a straightforward one. Other factors like perceived digital skills, location of users and cybersecurity awareness of users' decisions lead to variations in adoption intentions across studies and contexts.^{18,66} This highlights the complexity of the interplay between different elements in shaping users' attitudes toward NDIDs and emphasizes the need for a more nuanced understanding of security perceptions.

Furthermore, cultural and social interference (CSI) factors have a negative influence on the adoption of NDIDs. These results provide new insights by highlighting the significance of users' perceptions regarding the alignment of NDIDs with their cultural values and social interactions, which can impact their intention to use these systems.^{20,57} Moreover, the study demonstrates that perceived risk factors strongly affect users' intention to adopt NDIDs, in line with the research of.^{25,36} This provides new insights by identifying specific risk factors, such as the fear of managing online identity and potential fraud, as crucial concerns influencing users' decisions. Therefore, the adoption and use of NDIDs may be limited by the perceived high risks associated with their use,

especially for those who value their privacy and information security.³⁴ Furthermore, cultural and social interference, such as societal norms, preferences, or resistance to change, have a detrimental impact on individuals' willingness to adopt NDIDs. The statistically significant P-value of 0.03 indicates that this relationship is unlikely to have occurred by chance. Therefore, it is important to address cultural and social concerns and potential barriers to promote the adoption of NDIDs effectively.⁵⁹

Additionally, previous the role of flexibility in technology adoption highlights the importance of a flexible operating environment, dynamic resource scaling, and accessibility from various client devices.³⁸ However, variations in findings across studies suggest that contextual factors and user preferences may interact with flexibility considerations in shaping adoption intentions.⁷¹ From our results, users also have mixed opinions about their ability to use NDIDs. Respondents felt that they could access NDIDs easily, with a mean score of 2.99. On the other hand, they felt that they lacked the necessary digital skills and knowledge to use these systems, with a mean score of 2.89. Finally, the need for assistance when using these systems highlights the importance of user-friendly interfaces and training programs.²⁴

Contributions

Theoretical contributions

This paper significantly contributes to theory and research by introducing a novel HCCS model for understanding the adoption of NDIDs. This study addresses the adoption of NDIDs from an HCCS perspective. By integrating both the TPB and TFI, a comprehensive research model was developed and tested to investigate the HCCS influencing users' intentions to use NDIDs. Notably, this model stands apart from existing ones as it combines insights from existing literature with empirical data collected from a survey of 203 Australian residents. The study's findings validate the proposed research model, offering valuable insights that can guide future researchers in this domain.

Secondly, This study extensively evaluated the intention to use within the context of HCCS influencing the use of NDIDs. This contributes to ongoing interdisciplinary methodological discussions. The findings highlight a significant intention and use gap, with a substantial disconnect between the two. This result supports the claim⁷² on studying intentions correlates with human traits. By utilizing the combined research model in our study design, we were able to effectively investigate the transferability of intention studies to the influence of HCCS on the use of NDIDs.

Lastly, our study fulfills the requirement for investigating NDIDs concerning emerging users during the pandemic era, as previously highlighted.⁷³ By presenting empirical evidence for our research assumptions, we make a significant contribution to the expanding literature on NDIDs, also focusing on increased online dependency on e-government services during the pandemic and post-pandemic era of using digital identity systems. Our findings are in line with our theoretical framework and offer valuable insights into the intention to use within this distinct context.

Implications for practice

First, existing cases have demonstrated the significant influence of human-centered cybersecurity factors, particularly cultural beliefs, on users' beliefs and behaviors related to NDIDs. Case studies^{20,57} have explored how cultural values and social norms influence users' perceptions of privacy and security of technology systems. Our findings further highlight the importance of considering these human-centered cybersecurity factors when implementing NDIDs, as users' cultural beliefs can impact their intention to adopt and utilize such systems. Policymakers and governments must recognize these influences to develop successful and inclusive NDID strategies. By acknowledging the impact of cultural characteristics on NDID use, policies can be tailored to align with users' cultural values, fostering greater acceptance and trust in these identity systems. Our research emphasizes the need for investments in human-centered cybersecurity measures that respect and accommodate users' cultural beliefs, thereby enhancing the overall adoption and success of NDIDs.

Second, Our study emphasizes the importance of cybersecurity training to address trust issues and overcome cybersecurity challenges related to NDID usage. The relationship between trust and cybersecurity awareness is complex and multifaceted. Trust can be misplaced or eroded, and other factors such as location, level of education and digital skills of users as shown from the results may also play a role in shaping users' perceptions and behaviors, and other factors may also influence users' perceptions and behaviors. Therefore, our study provides valuable demographic and behavioral insights, highlighting the significance of cybersecurity awareness, especially for users with high levels of Cultural and Social Interference (CSI). To enhance NDIDs adoption, cybersecurity training programs should target users, including those in rural areas. Governments should allocate resources to cybersecurity awareness education, employing digital campaigns and short videos to promote NDID usage

and improve cybersecurity awareness. By adopting these measures, policymakers and stakeholders can effectively tackle trust-related concerns and cybersecurity challenges, facilitating the successful implementation of NDIDs.

Third, this study has shed light on the crucial role of human cognition and social behavior in security breaches, emphasizing the need for more effective security systems that account for users' thought processes and interactions. As a result, there has been a growing emphasis on user-centered design in the context of NDIDs, to create systems that are user-friendly and easy to comprehend. By collaborating with policymakers, this approach seeks to enhance frameworks for NDID usage, ultimately increasing user adoption and compliance with security protocols. The insights gained from this research can significantly contribute to the design and implementation of digital identity systems worldwide, promoting greater security and user satisfaction.

Conclusion

This paper investigated the HCCS factors that impact the intention to use NDIDs. A comprehensive survey of 203 Australian residents was conducted and a research model that identified HCCS that impact intention to use NDIDs was developed and validated. The findings suggest that a set of HCCS factors impact the use of NDIDs. The results also highlight the importance of HCCS in decision-making for users with diverse cultural backgrounds and an online social presence. The findings suggest that low levels of cybersecurity awareness and trust among users hinder the use of NDIDs. Taken together, these results imply that users should receive cybersecurity education and training to enhance their knowledge and awareness, thereby increasing their trust in and use of NDIDs. These findings contribute to the NDID and HCCS literature and have important implications for practice.

While this study provides valuable insights into the HCCS factors influencing NDID use and adoption, there are limitations to be addressed and opportunities for future research. First, one limitation is that the study exclusively focused on Australian residents. Future studies could test the proposed model in other countries to compare the findings across different cultures and contexts. Second, the use of an online survey may have limited the study's sample to digitally literate internet users, potentially impacting the generalizability of the study's findings to those who do not use the internet.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme.

References

1. Banihashemi S, Homayounvala E, Talebpour A, Abhari A. Identifying and prioritizing evaluation criteria for user-centric digital identity management systems. *Int J Adv Comput Sci Appl*. 2016;7(7). doi:10.14569/IJACSA.2016.070707.
2. Alenezi H, Tarhini A, Sharma SK. Development of quantitative model to investigate the strategic relationship between information quality and e-government benefits. *Transforming Gov*. 2015;9(3):324–51. doi:10.1108/TG-01-2015-0004.
3. Dubey A, Saquib Z, Dwivedi S. Electronic authentication for e-government services - a survey. Bristol (UK): Institution of Engineering and Technology; 2015.
4. E-estonia. 2023 [accessed 2023 Mar]. <https://e-estonia.com/solutions/e-identity/id-card/>.
5. Government of India. E-pramaan: framework for e-authentication. 2014.
6. The Guardian. My health record opt-out doubles to 2.5 million people. Australia: The Sunday Morning Herald; 2019. [accessed 2022 Feb 18].
7. Digital Transformation Agency. Trusted digital identity framework. 1.2. 2018.
8. European Union. Regulation (eu) no 910/2014 of the European parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec. 2014.
9. ACS Information Age. ATO pays \$500m to cyber criminals. Highlights flaws in the myGov ID system. 2023 [accessed 2023 Aug]. <https://ia.acs.org.au/content/ia/article/2023/ato-pays-500m-to-cyber-criminals.html?ref=newsletter&deliveryName=DM18850>.
10. National Institute of Standards and Technology. Digital identity guidelines. 2017.
11. Srinivas J, Das AK, Kumar N. Government regulations in cyber security: framework, standards and recommendations. *Future Gen Comput Syst*. 2019;92:178–88. doi:10.1016/j.future.2018.09.063.
12. Marta I. Digital identity as a key enabler for e-government services. London (UK): GSMA; 2016.
13. Sule M-J, Zennaro M, Thomas G. Cybersecurity through the lens of digital identity and data protection: issues and trends. *Technol Soc*. 2021;67:101734. doi:10.1016/j.techsoc.2021.101734.
14. ACS Information Age. Australian defence force database hacked. Australia; 2020 [accessed 2022 Feb 3]. <https://ia.acs.org.au/article/2020/australian-defence-force-database-hacked.html>.
15. El Haddouti S, Kettani M. Towards an interoperable identity management framework: a comparative study. *Int J Comput Sci Iss*. 2015;12(6):1694–0784.

16. Grobler M, Gaire R, Nepal S. User, usage and usability: redefining human centric cyber security. *Front Big Data*. 2021;4. doi:10.3389/fdata.2021.583723.
17. Chong AYL, Blut M, Zheng S. Factors influencing the acceptance of healthcare information technologies: a meta-analysis. *Inf Manage*. 2022;59(3):103604. doi:10.1016/j.im.2022.103604.
18. Mamdouh M, Awad AI, Khalaf AAM, Hamed HFA. Authentication and identity management of ioh devices: achievements, challenges, and future directions. *Comput Secur*. 2021;111:102491. doi:10.1016/j.cose.2021.102491.
19. Neigel AR, Claypoole VL, Waldfogle GE, Acharya S, Hancock GM. Holistic cyber hygiene education: accounting for the human factors. *Comput Secur*. 2020;92:101731. doi:10.1016/j.cose.2020.101731.
20. Sharma S, Aparicio E. Organizational and team culture as antecedents of protection motivation among it employees. *Comput Secur*. 2022;120:102774. doi:10.1016/j.cose.2022.102774.
21. Kortjan N, Solms R. A conceptual framework for cyber security awareness and education in sa. *South Afr Comput J*. 2014;52. doi:10.18489/sacj.v52i0.201.
22. Heartfield R, Loukas G. Detecting semantic social engineering attacks with the weakest link: implementation and empirical evaluation of a human-as-a-security-sensor framework. *Comput Secur*. 2018;76:101–27. doi:10.1016/j.cose.2018.02.020.
23. Pollini A, Callari TC, Tedeschi A, Ruscio D, Save L, Chiarugi F, Guerri D. Leveraging human factors in cybersecurity: an integrated methodological approach. *Cogn Technol Work*. 2021;24:371–390. doi: 10.1007/s10111-021-00683-y.
24. Hu S, Hsu C, Zhou Z. Security education, training, and awareness programs: literature review. *J Comput Inf Syst*. 2021;62:1–13.
25. Hansen JM, Saridakis G, Benson V. Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions. *Comput Human Behav*. 2018;80:197–206. doi:10.1016/j.chb.2017.11.010.
26. Mondego DY, Gide E. Exploring the factors that have impact on consumers' trust in mobile payment systems in australia. *J Inf Syst Technol Manage*. 2020. doi:10.4301/S1807-1775202017009.
27. Stamper R, Liu K, Hafkamp M, Ades Y. Understanding the roles of signs and norms in organizations - a semiotic approach to information systems design. *Behav Inf Technol*. 2000;19(1):15–27. doi:10.1080/014492900118768.
28. Ajzen I. From intentions to actions: a theory of planned behavior. 1991.
29. Eibl CJ, Schubert SE. Development of e-learning design criteria with secure realization concepts. Berlin Heidelberg: Springer Berlin Heidelberg; 2008. p. 327–36. doi:10.1007/978-3-540-69924-8_30.
30. Samonas S, Coss D. The cia strikes back: redefining confidentiality, integrity and availability in security. *J Inf Syst Secur*. 2014;10:21–45.
31. Identification for development practitioner's guide. The world bank. 2022 [accessed 2022 Feb 5]. <https://id4d.worldbank.org/guide/types-id-systems>.
32. Ioannou A, Tussyadiah I, Lu Y. Privacy concerns and disclosure of biometric and behavioral data for travel. *Int J Inf Manage*. 2020;54:102122. doi:10.1016/j.ijinfomgt.2020.102122.
33. Mishra U, Fatmi SN. E-readiness of India with reference to national e-governance plan. *Int J Comput Appl*. 2015;123(8):21–26. doi:10.5120/ijca2015905424.
34. Alharbi NS, Papadaki M, Dowland P. The impact of security and its antecedents in behaviour intention of using e-government services. *Behav Inf Technol*. 2017;36(6):620–36. doi:10.1080/0144929X.2016.1269198.
35. Selsikas P. Managing identities: from government E-commerce to national security. 2009.
36. Fernández-Alemán JL, Señor IC, Lozoya PÁO, Toval A. Security and privacy in electronic health records: a systematic literature review. *J Biomed Inform*. 2013;46(3):541–62. doi:10.1016/j.jbi.2012.12.003.
37. Ngwenyama O, Henriksen HZ, Hardt D. Public management challenges in the digital risk society: a critical analysis of the public debate on implementation of the Danish nemid. *Eur J Inf Syst*. 2021;32(2):1–19. doi:10.1080/0960085X.2021.1907234.
38. Ramaraj P. Information systems flexibility in organizations: conceptual models and research issues. *Global J Flexible Syst Manage*. 2010;11(1):1–12. doi:10.1007/BF03396574.
39. Hodapp D, Hanelt A. Interoperability in the era of digital innovation: an information systems research agenda. *J Inf Technol*. 2022;02683962211064304.
40. Hwang G-J, Wu C-H, Kuo F-R. Effects of touch technology-based concept mapping on students' learning attitudes and perceptions. *J Edu Technol Soc*. 2013;16:274–85.
41. Chong KW, Kim YS, Choi J. A study of factors affecting intention to adopt a cloud-based digital signature service. *Information*. 2021;12(2):60. doi:10.3390/info12020060.
42. Alwahaishi S, Snasel V. Modeling the determinants affecting consumers' acceptance and use of information and communications technology. *Int J E-Adoption*. 2013;5(2):25–39. doi:10.4018/jea.2013040103.
43. Bruun A, Jensen K, Kristensen D. Usability of single- and multi-factor authentication methods on tabletops: a comparative study. Berlin Heidelberg: Springer Berlin Heidelberg; 2014. p. 299–306. doi:10.1007/978-3-662-44811-3_22.
44. Tamilmani K, Rana NP, Dwivedi YK. Consumer acceptance and use of information technology: a meta-analytic evaluation of UTAUT2. *Inf Syst Front*. 2021;23(4):987–1005. doi:10.1007/s10796-020-10007-6.
45. Chen C. Perceived risk, usage frequency of mobile banking services. *Managing Serv Qual*. 2013;23(5):410–36. doi:10.1108/MSQ-10-2012-0137.
46. Pöhn D, Grabatin M, Hommel W. Eid and self-sovereign identity usage: an overview. *Electronics*. 2021;10(22):2811. doi:10.3390/electronics10222811.
47. Ardito C, Desolda G, Di Nocera F, Khamis M, Marrella A. Human-centered cybersecurity. Bari (Italy): ACM Press; 2019.
48. Evans M, Maglaras LA, He Y, Janicke H. Human behaviour as an aspect of cybersecurity assurance. *Secur Commun Netw*. 2016;9(17):4667–79. doi:10.1002/sec.1657.

49. De Bruijn H, Janssen M. Building cybersecurity awareness: the need for evidence-based framing strategies. *Gov Inf Q*. 2017;34(1):1–7. doi:10.1016/j.giq.2017.02.007.
50. Hong WCH, Chi C, Liu J, Zhang Y, Lei V-L, Xu X. The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Educ Inf Technol*. 2023;28(1):439–70. doi:10.1007/s10639-022-11121-5.
51. Daengsi T, Pornpongtechavanich P, Wuttidittachotti P. Cybersecurity awareness enhancement: a study of the effects of age and gender of Thai employees associated with phishing attacks. *Educ Inf Technol*. 2022;27(4):4729–52. doi:10.1007/s10639-021-10806-7.
52. Liaropoulos A. A human-centric approach to cybersecurity: securing the human in the era of cyberphobia. *J Inf Warfare*. 2015;14:15–24.
53. Office of the Victorian Information Commissioner. Victorian protective data security framework. 2020.
54. Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. *J Comput Syst Sci*. 2014;80(5):973–93. doi:10.1016/j.jcss.2014.02.005.
55. Goutas L, Hess B, Sutanto J. If erring is human, is system use divine? Omission errors during post-adoptive system use. *Decis Support Syst*. 2020;130:113225. doi:10.1016/j.dss.2019.113225.
56. Barriers to electronic government citizens' adoption: a case of municipal sector in the emirate of abu dhabi. *IEEE*; 2011.
57. Halevi T, Memon N, Lewis J, Kumaraguru P, Arora S, Dagar N, Aloul F, Chen J. Cultural and psychological factors in cyber-security. In: *iiWAS '16: Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services*. Singapore: ACM; 2016 Nov. p. 318–324. doi:10.1145/3011141.3011165.
58. Tolah A, Furnell SM, Papadaki M. An empirical analysis of the information security culture key factors framework. *Comput Secur*. 2021;108:102354. doi:10.1016/j.cose.2021.102354.
59. Thompson N, McGill T, Bunn A, Alexander R. Cultural factors and the role of privacy concerns in acceptance of government surveillance. *J Assoc Inf Sci Technol*. 2020;71(9):1129–42. doi:10.1002/asi.24372.
60. Dinev T, Goo J, Hu Q, Nam K. User behaviour towards protective information technologies: the role of national cultural differences. *Inform Syst J*. 2009;19(4):391–412. doi:10.1111/j.1365-2575.2007.00289.x.
61. Henshel D, Sample C, Cains M, Hoffman B. Integrating cultural factors into human factors framework and ontology for cyber attackers. Springer International Publishing; 2016. p. 123–37.
62. Australian Cyber Security Growth Network. United States government's cyber security maturity model certification. 2020 [accessed 2021 May 16]. <https://www.austcyber.com/news-events/united-states-government-cyber-security-maturity-model-certification>.
63. Pirouz D. An overview of partial least squares. *SSRN Electron J*. 2006. doi:10.2139/ssrn.1631359.
64. Rajapakse J. E-government adoptions in developing countries. *Int J Electron Gov Res*. 2013;9(4):38–55. doi:10.4018/ijegr.2013100103.
65. Swanson EB. Information systems innovation among organizations. *Manage Sci*. 1994;40(9):1069–92. doi:10.1287/mnsc.40.9.1069.
66. Camp LJ. Digital identity. *IEEE Technol Soc Mag*. 2004;23(3):34–41. doi:10.1109/MTAS.2004.1337889.
67. Chin W, Marcoulides G. The partial least squares approach to structural equation modeling. London: Modern Methods for Business Research; 1998. p. 8.
68. Kumari K, Yadav S. Linear regression analysis study. *J Pract Cardiovasc Sci*. 2018;4(1):33. doi:10.4103/jpcs.jpcs_8_18.
69. Wang H, Akritas M. Rank tests for anova with large number of factor levels. *J Nonparametr Stat*. 2004;16(3–4):563–89. doi:10.1080/10485250310001624774.
70. Aydin S, Cam H, Alipour N. Analyzing the factors affecting the use of digital signature system with the technology acceptance model. *J Econ Bibliography*. 2018;5(4):239–252.
71. Danila R, Abdullah A. User's satisfaction on e-government services: an integrated model. *Procedia Soc Behav Sci*. 2014;164:575–82. doi:10.1016/j.sbspro.2014.11.148.
72. Gratian M, Bandi S, Cukier M, Dykstra J, Ginther A. Correlating human traits and cyber security behavior intentions. *Comput Secur*. 2018;73:345–58. doi:10.1016/j.cose.2017.11.015.
73. Golinelli D, Boetto E, Carullo G, Nuzzolese AG, Landini MP, Fantini MP. Adoption of digital technologies in health care during the COVID-19 pandemic: systematic review of early scientific literature. *J Med Internet Res*. 2020;22(11):e22280. doi:10.2196/22280.

Appendix

Item Numbers

This section defines item numbers used in [Table 2](#): item loading variables.

Items	Definition
SEC1	Digital identity systems offer security for managing my online identity.
SEC2	I feel that digital identity systems may be more secure than traditional authentication systems
SEC3	I feel confident my data is secure when using digital identity systems.
SEC4	I feel digital ID systems have the integrity to secure my personal information.
PRV1	I'm afraid that digital ID systems are collecting too much personal data about me.
PRV2	Digital identity systems should disclose to users how data is collected, processed, and stored.
PRV3	I feel a loss of privacy if the data stored in digital identity systems is shared between government agencies.
PRV4	Digital identity systems maintain the privacy and confidentiality of my data.
TRS1	I feel that digital identity systems are reliable and can be trusted.
TRS2	I trust the process of digital identity verification.
TRS3	I trust my personal information will be used correctly on digital ID systems.
TRS4	Digital identity system providers with good credibility and reputation are available.
RSK1	It would be risky to use a digital identity system to manage and control my online identity.
RSK2	Using a digital identity system exposes my online identity to the risk of being hacked.
RSK3	Using a digital identity system exposes my online identity to potential fraud.
RSK4	Using digital identity systems exposes me to potential financial risk when conducting online transactions.
CSA1	I believe cybersecurity training is important to improve cyber security awareness amongst users
CSA2	I can recognize a phishing scam when using digital identity systems
CSA3	I am aware of steps I can take to safeguard my personal information when using digital identity systems
CSA4	Overall, I am satisfied about the level of my knowledge on cyber security
USB1	My user needs can be met by digital identity systems.
USB2	I will use more digital identity services in the future.
USB3	Digital identity services are compatible with my values and goals as a user.
USB4	The use of digital identity systems will allow me to access services that I could not access before.
FLX1	I am satisfied with the flexibility of services provided between digital identity systems.
FLX2	Digital ID systems provide flexible options for online verification, i.e., biometrics, PINS, and passwords.
FLX3	It is flexible for me to access e-government services on my mobile phone.
FLX4	It is flexible for me to verify myself using a mobile phone or laptop.
CSI1	I believe my cultural background affects how I use digital identity systems.
CSI2	I find it easier to use digital identity systems to access online services.
CSI3	I believe digital identity systems increase online social activities through online verification of users.
CSI4	My social perception affects how I use digital identity systems.