103982732

IMPROVED CYBER SECURITY AWARENESS

2084 WORDS

RUBIE STANNARD

**Table of Contents**

1. [Executive Summary 2](#_Toc141109977)
2. [Perceptions and Awareness 3](#_Toc141109977)

2.1. [Basic Awareness 3](#_Toc141109979)

2.2. [Intermediate Awareness 3](#_Toc141109980)

2.3. [Advanced Awareness 4](#_Toc141109979)

1. Influencing [Factors 5](#_Toc141109997)

3.1. [Socioeconomic Status 5](#_Toc141109978)

3.2. [Personal Experience 5](#_Toc141109979)

3.3. [Knowledge and Education 5](#_Toc141109979)

3.4. Cultural and Moral Values [5](#_Toc141109979)

1. [Recommendations for Improvement 7](#_Toc141110001)
2. [Conclusion 8](#_Toc141110001)

[References 9](#_Toc141110025)

1. **Executive Summary**

The purpose of this report is to conduct a comprehensive literature review on the perceptions of Australian individuals towards cyber security, critically analyse the factors influencing these perceptions, and provide actionable recommendations to enhance awareness of cyber security among the Australian public.

This topic was chosen due to cyber security’s increasing relevance in today's digital landscape. With increased numbers of cyber threats and the growing dependency on digital technologies, understanding people's perceptions and how they influence behaviour is paramount. Because of this increasing relevance, I thought information would be highly available and easy to find, making this topic seem easier than the topic of having to investigate the strengths and possibilities of generative AI platforms to develop software.

The report will begin by analysing cyber security perceptions of Australian individuals and sorting awareness into three levels: basic, intermediate, advanced. Using my own opinion, and the Individual Competency Index, I will create criteria that determines how an individual is assigned to an awareness level. I will use statistics to try and vaguely show what percentage of the population is in each level.

Next, I will discuss the factors that shape these cyber security and cybercrime perceptions, including education and knowledge about the subject, previous personal experiences with cyber threats, economic considerations, and cultural and moral values.

By synthesizing information from literature, the report will end by identifying key challenges and opportunities in enhancing cyber security awareness. Although all of the recommendations may not be original, I will give my opinion on how existing strategies can be improved.

In conclusion, the report underscores the critical importance of collaboration, education, and proactive measures in enhancing cybersecurity resilience. By embracing these principles and implementing the recommended strategies, stakeholders can collectively contribute to creating a safer and more secure digital environment for all Australians.

1. **Perceptions and Awareness**

Perceptions are the “ability to notice and understand things,” (*Cambridge Dictionary, n.d.*), and perceptions result in awareness. In order to understand people’s perceptions of cyber security, one must understand people’s perceptions of cybercrime, since without cybercrime, there would be no cyber security. Cybercrimes are “crimes directed at computers or other information communications technologies, such as computer intrusions and denial of service attacks.” (*Australian Federal Police, n.d.*).

Some of the Australian communities’ perceptions of cybercrime include having their “personal information exposed to the public or used without their permission, their credit card or bank accounts used without their permission, a virus on their computer,” (*Cross et al, 2021, p. 49*), or someone hacking into their accounts. People can also think of cybercrimes as “malware, fake emails, or man-in-the-middle attacks.” (*Australian Federal Police, n.d.*).

Cyber security negates these perceptions as it’s used “to safeguard not only their computers and networks, but also to preserve the confidentiality, integrity and availability of their data.” (*Accenture, n.d.*). To understand how these perceptions can lead to different level of awareness, I’ll use my own opinion and the concept of the Individual Competency Index to “measure both conceptual and procedural knowledge needed by individuals,” (*BIM Dictionary, 2019*), in relation to cyber security.

**2.1. Basic Awareness**

People with a basic level of cyber security awareness “denote an understanding of fundamentals and some initial practical application,” (*BIM Dictionary, 2019*), and are capable of implementing basic cyber security measures, such as using antivirus software and setting up passwords.

Based on this information, “34% of Australians” (*Langit, 2021, p. 2*) are in this category and “are in high risk with little to no implementation of online safety measures.” (*Langit, 2021, p. 2*). This level can use the internet and general software easily but cannot “fix computer problems that arise.” (*Cross et al, 2021, p. 46*).

Older people would be the main demographic in this level as the Australian Competition and Consumer Commission identified that “older people suffered the greatest harm at the hands of scammers, with people over the age of 65 experiencing an increase in reported losses.” (*Australian Competition & Consumer Commission, 2024*).

**2.2. Intermediate Awareness**

People with and intermediate level of cyber security awareness “denote a solid conceptual understanding and some practical application,” (*BIM Dictionary, 2019*), and are capable of implementing basic cyber security measures and responding to common cyber threats effectively.

Based on this information, this level “checks that an email, text message or phone call isn’t a scam before providing their information and use unique passwords and do not share them with others.” (*OAIC, 2023*). This level thinks that “scammers trying to get their personal information” is the biggest problem they face,” (*OAIC, 2023*), therefore “71%” (*OAIC, 2023*) of Australians are in this category.

All demographics would make up this category since everyone is at an equal risk of being exposed to cybercrime. People in this demographic have a “mid-level of general computer skills, indicating that they can use a variety of software and fix some computer problems.” (*Cross et al, 2021, p. 46*).

**2.3. Advanced Awareness**

People with an advanced level of awareness of cyber security “denote significant conceptual knowledge and practical experience in performing a competency to a consistently high standard,” (*BIM Dictionary, 2019*), and are competent in performing complex cyber security tasks and mitigating advanced cyber threats effectively.

Based on this information, “17% of Australians” (*Langit, 2021, p. 2*) are in this category and have a “high awareness of cybersecurity and are actively implementing security measures.” (*Langit, 2021, p. 2*). People in this level are “very comfortable using a computer.” (*Cross et al, 2021, p. 46*).

This demographic would include people who have jobs in cybersecurity or cybercrime, students undertaking a degree resalted to technology, or people who have spent a lot of time teaching themselves about cyber security.

1. **Influencing Factors**

The perceptions individuals hold towards cyber security play a pivotal role in determining their attitudes, behaviours, and actions in navigating the digital landscape. From beliefs about personal vulnerability to cyber threats to perceptions of responsibility for digital security, these perceptions are influenced by a myriad of factors ranging from cultural norms and moral values to media framing and technological trust. Understanding these influencing factors is essential for developing effective cyber security education, awareness, and policy initiatives that resonate with diverse audiences and promote a culture of cyber resilience and responsibility.

**3.1. Socioeconomic Status**

Socioeconomic status impact individuals' ability to access and implement cyber security measures, since limited financial resources may hinder individuals from adopting robust cyber security measures, leading to increased vulnerability to cyber threats.

Economic factors such as income level, employment status, and access to technology shape individuals' ability to invest in cyber security. Geographic location can also affect individuals' exposure to cyber risks and their capacity to address them effectively.

**3.2. Personal Experience**

Previous personal experience with cyber threats can impact people’s perceptions about cyber security, as direct experiences with cyberattacks can heighten awareness and motivate individuals to do something to minimize the risk of it reoccurring. Conversely, people who have not had experience with cyberattacks may underestimate the importance of cyber security or believe that they are immune to cyber threats.

People’s level of digital engagement, and susceptibility to cyber risks based on online behaviours, and reactions to cyber incidents, such as the severity of impact and effectiveness of recovery measures, can shape their perceptions of cybersecurity.

**3.3. Knowledge and Education**

Education and technological knowledge significantly influence individuals' understanding of cybersecurity risks and best practices. “Individuals with higher education levels tend to have higher awareness levels.” (*SciSpace, n.d.*). Conversely, people with limited education and technological knowledge may contribute to misconceptions and ineffective cybersecurity behaviours.

Educational attainment, access to quality cyber security education and training programs, learning opportunities, digital literacy levels, familiarity with basic cyber security concepts and proficiency in using digital technologies, impact individuals' ability to navigate cyberspace safely, in turn impacting their cyber security knowledge and skills.

**3.4. Cultural and Moral Values**

Cultural and moral values shape individuals' perceptions of cyber security as someone’s sense of right and wrong, and the opinion of cyber threats in one’s culture, will influence their attitudes towards privacy, trust, and responsibility in the digital realm.

Cultures that prioritize online privacy may view cyber security as essential for protecting personal data and autonomy online. Moral values such as honesty, integrity, and respect for others' rights also influence perceptions of cyber security, with people who prioritize these values being likely to prioritize ethical cyber security practices and respect others' digital privacy.

1. **Recommendations for Improvement**

In an increasingly interconnected digital landscape, cyber security has become a paramount concern for individuals, organizations, and societies worldwide. Technology has brought unprecedented opportunities for innovation and collaboration, but it has also introduced new risks and vulnerabilities that threaten the confidentiality, integrity, and availability of sensitive information and critical systems. Addressing these challenges requires a proactive approach that encompasses technical solutions, policy frameworks, and human behaviour’s.

As the years go by, technology gets more advanced, insinuating that the future will have many uses of technology. If this is the case, being proactive and integrating cyber security education in school curriculum would be smart as it’ll emphasise digital literacy, online safety, and responsible digital citizenship. Introducing cyber security concepts early in education, schools can instil essential knowledge and habits in students, empowering them to navigate the digital world safely, and preparing future generations to address evolving cyber threats.

Many strategies are already in place to improve cybersecurity awareness, but people may not be aware of these initiatives. Improving the awareness of existing Australian Government campaigns such as ‘Learn the Basics’ where the government says “it’s easy to improve your cyber security! Take these simple steps today to protect yourself,” (*Australian Signals Directorate's, n.d.*), and ‘Cyber Security Awareness Month’ in October is a “reminder for all Australians to stay secure online.” (*Australian Signals Directorate's, n.d.*). Better advertising ensures that the government cyber security initiatives reach wider audiences across various demographics and geographic locations, educates the public about the available resources, tools, and guidance for improving cyber security, and having government-led cyber security initiatives carry inherent credibility and trust among the public.

In today's rapidly evolving technological threat landscape, maintaining up-to-date cyber security skills though continuous professional development programs by providing ongoing training and resources will enhance employee’s cyber security skills and knowledge is essential for workers across all sectors. Developing a skill will offer opportunities for ongoing learning, skill enhancement, and career advancement in cybersecurity fields, and allow organizations to strengthen their cyber security measures, reacting to cyber threats more efficiently.

There are many parts of technology that humans don’t understand, and many fiddly bits, which is why “human error is the main cause of 95% of cyber security breaches.” (*Ahola, 2022*). Human error can be reduced by ensuring users only have the necessary access they need to do their job, keep passwords safe and updated, and "address the lack of knowledge with training." (*Ahola, 2022*). Without human error security measures become more reliable and robust, and security policies and protocols are adhered to more strictly, reducing the likelihood of security breaches and incidents.

In conclusion, the evolving digital landscape presents both opportunities and challenges in the realm of cybersecurity. Addressing the multifaceted aspects of cyber security and embracing a collaborative and proactive approach enhances cyber security resilience, creating a safer and more secure digital environment.

1. **Conclusion**

In conclusion, the report underscores the importance of addressing cyber security in today's advanced digital landscape. As technology continues to advance, the risks and vulnerabilities associated with cyber threats also evolve, necessitating a proactive and multifaceted approach to cybersecurity.

Through an exploration of perceptions and awareness levels, the report highlights the varying levels of awareness and preparedness among individuals regarding cyber security. From basic awareness to advanced competency, it becomes evident that education, training, and access to resources play pivotal roles in shaping individuals' cyber security posture.

Furthermore, the report delves into the influencing factors that shape people's perceptions of cyber security, ranging from socioeconomic status and personal experiences to knowledge and education, as well as cultural and moral values.

Drawing upon these insights, the report offers a series of recommendations for improving cyber security awareness and preparedness. From integrating cyber security education into school curriculum to enhancing the visibility of government-led initiatives, these recommendations aim to empower individuals and organizations to navigate the digital landscape safely and responsibly.

In essence, the report underscores the importance of collaboration, education, and proactive measures in enhancing cyber security resilience. By embracing these principles and implementing the recommended strategies, stakeholders can collectively contribute to creating a safer and more secure digital environment for all.

**References**

Ahola, M. (2022, June 17). *The Role of Human Error in Successful Cyber Security Breaches*. usecure. <https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches>

Australian Competition and Consumer Commission. (2024, April 28). *Scam losses decline, but more work to do as Australians lose $2.7 billion.* Australian Competition and Consumer Commission. <https://www.accc.gov.au/media-release/scam-losses-decline-but-more-work-to-do-as-australians-lose-27-billion>

*Australian Community Attitudes to Privacy Survey.* OAIC. (2023, August). <https://www.oaic.gov.au/__data/assets/pdf_file/0025/74482/OAIC-Australian-Community-Attitudes-to-Privacy-Survey-2023.pdf>

Cross, C., Holt, T., Powell, A., & Wilson, M. (2021, August). *Responding to cybercrime: Perceptions and need of Australian police and the general community.* Australian Institute of Criminology. <https://www.aic.gov.au/sites/default/files/2021-08/ti635_responding_to_cybercrime.pdf>

*Cybercrime.* Australian Federal Police. (n.d.). <https://www.afp.gov.au/crimes/cybercrime#:~:text=this%20crime%20type-,About%20this%20crime,and%20denial%20of%20service%20attacks>

*Cyber Security Awareness Month.* Australian Signals Directorate’s. (n.d.-a). <https://www.cyber.gov.au/learn-basics/view-resources/cyber-security-awareness-month>

*Individual Competency Index (ICI).* BIM Dictionary. (2019, August 1). <https://bimdictionary.com/en/individual-competency-index/1#:~:text=The%20Individual%20Competency%20Index%20(ICI)%20measures%20both%20conceptual%20knowledge%20(,deliver%20a%20measurable%20outcome1>.

Langit, S. (2021, August). *Recommendation Paper for Australia’s National Cyber Security Strategy 2021.* Department of Home Affairs. <https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/sekar-langit.pdf>

*Learn the basics.* Australian Signals Directorate’s. (n.d.). <https://www.cyber.gov.au/learn-basics>

*Perception.* Cambridge Dictionary. (n.d.). <https://dictionary.cambridge.org/dictionary/english/perception>

*What are the factors that influence cyber security awareness?.* SciSpace. (n.d.). <https://typeset.io/questions/what-are-the-factors-that-influence-cyber-security-awareness-4s0kqakihy>

*What is Cybersecurity & Why is it important?.* Accenture. (n.d.). <https://www.accenture.com/au-en/insights/cyber-security-index>