MULTI-GENERATIONAL CYBERSECURITY: UNDERSTANDING THE KNOWLEDGE, RISK PERCEPTION, AND RESPONSE BEHAVIOR OF SEVEN GENERATIONS

by

MELISA JOHNSON

B.S., Middle Georgia State University, 2013

M.S., Middle Georgia State University, 2019

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment for the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA
2026

Multi-generational cybersecurity: Understanding the knowledge, risk perception, and response behavior of seven generations

***Melisa Johnson**, Middle Georgia State University, melisa.johnson@mga.edu*

Abstract

In 2026, cybersecurity and cyber resilience are no longer optional; an individual's knowledge, risk perception, and incident-response behavior are more important than ever. This systematic literature review provides insight into how cybersecurity is interpreted across generational cohorts. Fourteen studies were analyzed using qualitative thematic synthesis in accordance with PRISMA guidelines. The interpreted results revealed that although younger cohorts held higher digital fluency, they demonstrated inconsistent security practices, while older cohorts were more structured in their actions and exhibited compliance-based behaviors. The Technology Acceptance Model (TAM) was embedded in this study to understand how cybersecurity acceptance across generations is mediated by perceived ease of use and perceived usefulness. The results emphasize that exposure to digital technology and perceived control shape generational differences, rather than age alone. In conclusion, this study implicates the need for targeted cybersecurity training and policy change.

Keywords: cybersecurity awareness, security behavior, risk perception, generational cohorts, Technology Acceptance Model (TAM)

Introduction

Before 1970, cybersecurity is not a socio-technical philosophy; computers are large, standalone, and disconnected systems locked away in secure environments, and modern forms of malicious software were not yet present. In the 1970s, technological advancements are just beginning, and ARPANET, the precursor to today's internet, enabled interconnections between computer systems (Mândraș, 2024). In their professional prime, the Silent Generation had limited computer skills and minimal awareness of cybersecurity knowledge, risks, or behaviors. In 1971, the first known computer virus, Creeper, was created, prompting the development of Reaper, the first program designed to remove viruses (Mândraș, 2024). These developments marked the beginning of a new era and a critical turning point, during which researchers began analyzing the unforeseen vulnerabilities inherent in interconnected systems (Warner, 2012).

Alternatively, modern society's cybersecurity exposure is significantly different, given an individual's constant internet connectivity and widespread exposure to personal computers (Silitonga, 2023). Constant exposure has changed the way that subsequent generations perceive risks and respond to cyber-attacks. This study explores how generational differences influence cybersecurity knowledge, risk perception, and response behaviors in today's highly interconnected digital environment.

As the world progresses, the transition between generations continues to drive ongoing changes in collective attitudes towards technology and cybersecurity risks. Concurrently, rapid technological advancements, including artificial intelligence (AI), machine learning, and the Internet of Things (IoT), introduce new, complex threats and vulnerabilities, increased complacency, and new security solutions. Although each generational cohort has different characteristics and experiences, understanding their responses to these threats, vulnerabilities, and risks will better prepare employers, teachers, organizations, policymakers, and businesses to effectively train and prepare individuals from all generations for inevitable cyber incidents (Bana, 2025). Despite the growing importance of this issue, little research has examined how generational differences affect cybersecurity knowledge, risk perception, and response behaviors.

The purpose of this study is to systematically review and synthesize existing literature on generational differences in cybersecurity knowledge, risk acceptance, and behavior, guided by the Technology Acceptance Model (TAM). This study examines the following generational cohorts: the Greatest Generation (GI Generation), the Silent Generation, the Baby Boom Generation, Generation X, the Millennial Generation (Generation Y), Generation Z, and Generation Alpha. These cohorts represent diverse developmental experiences, technological exposure, and sociocultural contexts that influence cybersecurity perceptions and practices. Examining generational differences provides a comprehensive understanding of how cybersecurity awareness and behaviors evolve across age groups and supports the development of targeted educational and risk management strategies.

RQ: What themes emerge from the systematic literature review regarding the seven generational cohorts varying levels of digital technology use differ in their understanding of cybersecurity, their perceptions of digital risks, and their approaches to responding to security incidents?

Literature Review

The Generations

Many researchers discuss and describe the characteristics of each generational cohort and their impact on Information Technology (IT). Still, there has been very little research on how generations respond to cybersecurity threats, vulnerabilities, and risks across all environments.

The Greatest Generation (1901-1927)

The Greatest Generation is born during a time of significant economic prosperity and cultural transformation, while their early life experiences were shaped by economic collapse, global instability, and large-scale conflicts (Thaariq, 2023). As a result, their security practices focus on physical data and documents rather than digital systems (Thaariq, 2023). Because modern-day cybersecurity threats do not exist during their formative years, their understanding of digital risks differs from that of younger generations. As one of the oldest living generational cohorts, they are particularly vulnerable to social engineering attacks, which have resulted in notable financial and personal consequences (Thaariq, 2023).

The Silent Generation (1928-1945)

The Silent Generation is witness to immense societal and technological changes, including the Great Depression, World War II, and the emergence of digital technologies (Lissitsa et al., 2022). Not growing up with the internet or smartphones has not stopped many of them from adapting to technology and embracing social media platforms, digital banking, and online shopping (Lissitsa et al., 2022). For this generation, there are uneven levels of technological proficiency, driven by socioeconomic status and education, and heightened susceptibility to cyber risks. As a result, the Silent Generation faces challenges with new technologies and navigating modern cybersecurity threats.

The Baby Boomers or Boomers (1946-1964)

Variations in technological exposure exist among Baby Boomers. This variance leads many of them to exhibit greater cyber awareness than preceding generations. However, Baby Boomers are segmented into two groups: individuals who were born between 1946 and 1955 are considered “the leading-edge baby boomers” and those born between 1956 and 1964 are considered “Generation Jones”, “late boomers” or “trailing-edge baby boomers” (Koman, 2016). Individuals born between 1946 and 1955 exhibit greater digital literacy gaps, lower cybersecurity awareness, inadequate password practices, and reduced trust in all forms of communication, which leads to social engineering attacks (Koman, 2016). As Baby Boomers age,

the technological world around them will become even more capable and complex, thereby creating a larger gap in understanding and inevitably placing this generation at greater risk of malicious hacking, digital theft, unnecessary surveillance, and targeted abuse (Koman, 2016).

Generation X or Gen X (1965-1980)

Generation X is commonly characterized as resourceful, independent, and tech-savvy while maintaining a strong emphasis on work-life balance (Lissitsa & Laor, 2021). As digital immigrants, they experience both pre- and post-internet environments, which fosters a strong awareness of cybersecurity practices and the use of strong passwords (Lissitsa & Laor, 2021). However, their self-reliant orientation may lead to top-down reductions in cybersecurity directives and put an organization at risk when individual judgment supersedes standardized security policies (Lissitsa & Laor, 2021). Overall, Generation X exhibits lower vulnerability to cyber threats than prior generations, but they remain at risk when institutional controls are not uniformly adopted.

Millennial Generation or Generation Y or Millennials (1981-1996)

Millennials currently represent the largest segment of the U.S. workforce and are the first generation of digital natives (Lissitsa & Laor, 2021). They are quick to adopt new technologies across every aspect of their daily lives, including smartphones, social media, and streaming entertainment. In their work environments, they're known for transforming companies worldwide (Yarnykah, 2021). Millennials desire to be safe online, but they prize the convenience and flexibility that technology enables; therefore, they may choose to accept cybersecurity risks rather than lose their technological advantage.

iGen or Generation Z or Gen Z (1997-2010)

Generation Z's characteristics are shaped by digital innovation, global connectivity, and social change. They have a financial focus, a desire to connect socially, and a drive to bring technology forward (Lissitsa & Laor, 2021). As the first "true" digital generation, Gen Z has grown up without privacy or a sense of control over their own lives (Mândraș, 2024). Even more than Millennials, Gen Z is more likely to choose convenience over privacy and security, thereby accepting cyber risks (Lissitsa & Laor, 2021). Their acceptance makes them more vulnerable to phishing and social engineering attacks, highlighting the need for specialized training and education tailored to these digital natives (Mândraș, 2024).

Generation Alpha (2010-2024)

Generation Alpha is the first generational cohort of artificial intelligence (AI) natives. From infancy, they grew up with AI being embedded into their daily lives (Ziatdinov & Cilliers, 2021). This generation has an intuitive understanding of AI and related technologies, which enables them to leverage innovations in ways previous generations could not. However, they are also more susceptible than prior cohorts to newer threats and vulnerabilities such as AI-enabled malware, automated attacks, deepfakes, and data exploitation (Ziatdinov & Cilliers, 2021). Starting early, Generation Alpha must receive targeted education beyond what our current educational system allows (Ziatdinov & Cilliers, 2021). To foster cyber-resilient digital citizenship, their education should focus on secure behavior, risk awareness, and responsible interaction with AI-enabled systems (Mândraș, 2024). Generation Alpha represents the beginning of a new digital era, as the first cohort fully immersed in technology from birth, positioning them as both highly capable and uniquely vulnerable in evolving cybersecurity environments (Ziatdinov & Cilliers, 2021).

Cybersecurity

Cybersecurity encompasses technologies and practices used to prevent or mitigate impacts from cyberattacks (Sadaghiani-Tabrizi, 2023). Cyberattacks can disrupt, damage, or destroy individuals, communities, and businesses (Sadaghiani-Tabrizi, 2023). The current workforce is focused on integrating cybersecurity into every aspect of the workplace through risk analysis. Previous generations lack an understanding of cybersecurity and struggle to incorporate it into their current, limited use of technology. The current workforce exhibits an extreme reliance on routine technology and may assume unnecessary risks. Generation Z and Generation Alpha have grown up with cybersecurity saturated in their everyday lives. However, this saturation leads to complacency, automation bias, and risk-accepting behaviors that increase the likelihood of minor catastrophic cyber incidents.

Cybersecurity Risks

Cybersecurity risks consist of vulnerabilities and threats. Risks can be a complex assault by an adversary (malware, virus infection, theft, etc.) or the physical destruction of an asset or a natural disaster. Pugnetti et al. define cybersecurity risks as risks that affect IT assets and that threaten the confidentiality, availability, and integrity of information systems (Pugnetti et al., 2024). Cybersecurity risks can pose a significant and growing threat to both individuals and organizations. Generation X and some of Generation Y had the opportunity to experience life before the influx of technology, making them the most cautious about accepting cybersecurity risks. However, Generation Z and Generation Alpha are more likely to exhibit automation complacency while prioritizing technological convenience over reducing cybersecurity risks.

Cybersecurity Challenges and Awareness

Researchers Dhungana et al. (2023) highlight increased cybersecurity risks for school-aged children that include cyberbullying and unsafe online behaviors (Dhungana et al., 2023). Implementing effective security controls at an early age, including specific online training, will help reduce risks for school-aged students. Proactive cybersecurity education, investment in necessary cybersecurity tools, teacher training, and institutional accountability will help promote effective risk reduction and ensure safe learning environments (Dhungana et al., 2023).

Redekop (2021) addresses a gap in research across generations and a lack of cybersecurity awareness training for different age groups (Redekop, 2021). The study emphasized that organizations needed to recognize and empower employees' cybersecurity awareness, since they are the first line of defense (Redekop, 2021). To summarize, IT security awareness programs cannot be a “one size fits all” approach, as it is unlikely to help the organization achieve its goals (Redekop, 2021).

Beyond awareness, emerging technologies create further cybersecurity challenges. Large language models (LLMs) complicate cybersecurity risks and amplify an already controversial relationship between humans and technology. LLMs are security guardians, security breachers, “unaware” enablers, and victims of cyber-attacks (Marulli et al., 2024). LLMs can be a two-edged sword, and as technology matures, researchers are actively examining new methods to mitigate cyber risks. These risk reductions and mitigations will use tools to create a more secure cybersecurity landscape.

Cybersecurity Training and Skills

Guided by the Technology Acceptance Model (TAM), cybersecurity training plays a critical role in shaping risk perception and improving the understanding of security behavior. When there is a lack of training across many professions, in particular criminal justice, it creates significant knowledge and skill gaps (Quintana et al., 2024). These gaps widened as digital technologies expanded rapidly during the COVID-

19 pandemic. Cybersecurity training is necessary to close these gaps and improve workforce readiness to adopt technology. Training should enhance employees' and students' ability to make well-informed cybersecurity risk decisions, especially among younger generations (Rahmat et al., 2024). However, research shows that current training practices and high technology use do not equate to stronger information security behaviors. These disparities highlight the need for ongoing, behavior-focused cybersecurity training across professions, amongst students, and throughout all generational cohorts. TAM informed that cybersecurity training will assist in reducing skills gaps, reducing vulnerabilities, and mitigating evolving cyber risks across generations and professions (Thaariq, 2023).

Shillair et al. (2022) examined over 80 countries and the impact that cybersecurity education, awareness, and training (CEAT) have on developing cybersecurity capabilities for education and training (Shillair et al., 2022). Grounded in the Cybersecurity Capacity Maturity Model (CMM), Shillair et al. (2022) found a strong significance for internet use and digital development for countries with more advanced CEAT programs (Shillair et al., 2022). These findings highlight the critical role of structured education and awareness efforts in shaping secure digital environments. Furthermore, the findings underscore the importance of cybersecurity education in influencing both knowledge and behavioral outcomes, suggesting that increased exposure to training and awareness initiatives can enhance users' ability to recognize and respond to cyber threats (Shillair et al., 2022). Ultimately, generational differences systematically create varying levels of access to and engagement with cybersecurity education. These differences contribute to disparities in cybersecurity knowledge, risk perception, and behavioral practices across cohorts.

Societal Impacts

Societal impacts are far-reaching when significant gaps in cybersecurity capacity exist throughout regions and nations (Mumford & Shires, 2023). Through their research, Mumford & Shires (2023) noted that cybersecurity maturity is important across all cultures, ethnicities, and countries, underscoring the need for inclusive and forward-thinking approaches to training and awareness (Mumford & Shires, 2023). From a decolonial perspective, Mumford & Shires (2023) consider coloniality primarily in the form of racialized stereotypes of intelligence and technological ability, but there is so much more that needs to be considered when talking about epistemic dominance (Mumford & Shires, 2023). Further analysis of gender and other forms of epistemic hierarchy is a necessary complement to this field of research (Mumford & Shires, 2023). Complimenting this perspective, Vo et al. (2025) examine demographic characteristics of Generation Z Vietnamese digital banking users, emphasizing factors such as gender, education, occupation, and income (Vo et al., 2025). Together, these findings demonstrate that cybersecurity capacity is shaped not only by technological exposure but also by social and structural inequalities. Equitable access to cybersecurity education across populations and regions is necessary, especially as vulnerabilities increase due to the convenience-driven adoption of technology.

Cybersecurity Human Factors (HF) and Behaviors

When it comes to data protection, humans are habitually the weakest link (Pollini et al., 2022). Therefore, to infiltrate data for pleasure or gain, adversaries exploit humans through targeted cyberattacks. The following cyber-attacks maximize human factor (HF) vulnerabilities: online fraud, DDoS (distributed denial of service), drive-by downloads, and other social engineering attacks (Pollini et al., 2022). In their study, Pollini et al. (2022) conclude that security culture often exposes organizations to potential human vulnerabilities as opposed to a lack of formal knowledge (Pollini et al., 2022). Organizations seeking cyber resilience invest time and resources in external and technical solutions for prevention rather than focusing on employee skills and behaviors (Warrington et al., 2022). In addition, generational cybersecurity skill gaps across the public and private sectors heighten cybersecurity risks, often due to insufficient management oversight of employee workloads and security behaviors (Silitonga, 2023). The rise of remote

and hybrid work environments requires organizations to trust multigenerational workers who bring diverse values, risk perceptions, and various levels of technological understanding.

Understanding an employee's moral reasoning, perceptions of moral intensity, and the moderating role of generational differences will assist organizations in implementing tailored training and hiring procedures (Akello et al., 2024). However, excessive cybersecurity training and awareness can overwhelm an individual, leading to cybersecurity fatigue, thereby reducing an individual's vigilance and increasing weak security behaviors. These behaviors include ignoring security warnings, reusing passwords, and choosing convenience over security. In addition, the sudden reliance on AI and automation tools challenges an individual's ability to engage in critical thinking in their daily activities, adding another layer of human dependence for data protection. Although increasing AI literacy and knowledge can help mitigate a lack of critical insight (Tian & Zhang, 2025), human factors (HF) continue to underscore the need for personalized training tailored to individual experience levels (Zierock et al., 2025).

Theoretical Framework: Technology Acceptance Model (TAM)

The TAM framework substantiates the findings on generational cohorts' ability to perceive, respond to, and accept the risks associated with learning and using new technologies. TAM supports the belief that technology adoption is driven by perceived ease of use and perceived usefulness (Sadaghiana-Tabrizi, 2023). This framework underscores how generational cohorts differ across multiple technology platforms in their understanding of cybersecurity. Furthermore, the advancement and reliance on AI influence a user's perceived ease of use by deducting both cognitive engagement and critical thinking (Tian & Zhang, 2025). However, if individuals, regardless of their cohort, perceive cybersecurity practices as worthwhile, they are likely to exhibit better cybersecurity behavior. And by establishing clear, easy-to-use security policies, individuals are more likely to adhere to them. However, too much trust in technology can lead to automation complacency and excessive cybersecurity training, and awareness can overwhelm an individual, leading to cybersecurity fatigue. Therefore, the TAM framework is critical for understanding and influencing human behavior and cybersecurity culture.

Literature Review Conclusion

The COVID-19 pandemic has accelerated the need for cybersecurity and cyber resilience at work and at home. As digital technologies continue to expand rapidly, cybersecurity permeates the current workforce and previous generations. There is existing literature on cybersecurity awareness, skill gaps, challenges, training, and behavior in these environments; however, several gaps remain. Limited analysis has examined multiple generational cohorts, as prior research has focused more on workplace environments and specific demographic groups. Multiple studies address cybersecurity knowledge, risk perception, and security behaviors independently, rather than examining how they together shape security decision-making. The rapid evolution of AI, digital environments, and technological mindsets demands integrative research that synthesizes how each generation's digital socialization molds their cybersecurity understanding, perceived risk, and behavioral response to security incidents. The following section outlines the systematic methodology observed throughout this study.

Methodology

The identified research gaps enabled this study to employ a systematic literature review using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework. PRISMA provides a rigorous and transparent synthesis of the literature on generational differences in cybersecurity knowledge, risk perception, and response behavior (Baumeister, 1997). The screening and eligibility process is illustrated in Figure 1.

By applying a structured search strategy and explicit inclusion criteria, selection bias is reduced, and it supports the systematic comparison of both qualitative and quantitative studies, ultimately offering greater consistency than narrative or thematic reviews.

By utilizing TAM, this research study provides a solid foundation for understanding how technology use influences each cohort's cybersecurity knowledge, risk perception, and response to security incidents. The inclusion of TAM in the methodology facilitates the systematic assessment of cybersecurity across all cohorts.

Research validity was improved by using multiple sources and only including peer-reviewed studies. The findings provide an understanding of the impact of technology on each generation from the turn of the 19th century.

Databases

- Google Scholar, EBSCO Host, IEEE Xplore, ACM Digital Library

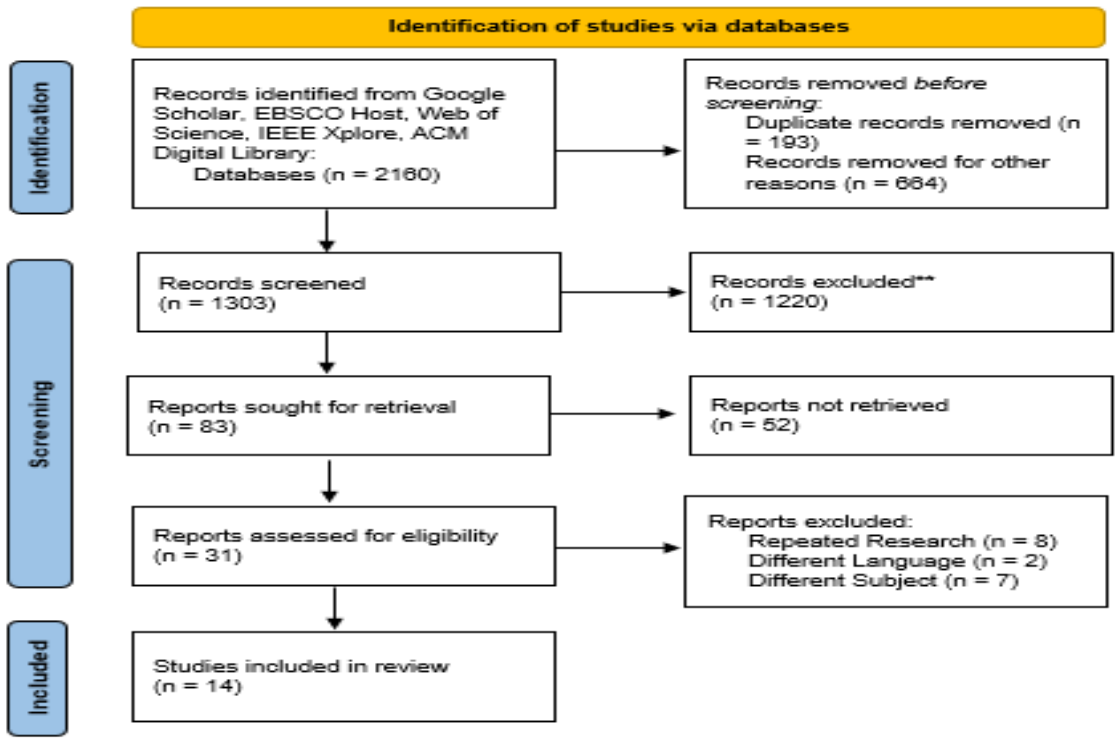
Search Strategy

Boolean operators and keywords were used to conduct comprehensive searches:

- ("Cybersecurity awareness" AND "generation" OR "information security behavior" AND "age" OR "employees"), ("Generation" OR "generational differences" OR "digital natives"), ("Cybersecurity risk perception" AND "demographic" OR "cybersecurity behavior"), ("Risk acceptance" AND "The Greatest Generation" OR "The Silent Generation" OR "Baby Boomers" OR "Generation X" OR "Generation Y" OR "Generation Z" OR "Generation Alpha")

Figure 1

PRISMA Flow Diagram



Note. 14 peer reviewed journal articles were included in this research study.

Coding

The screening process, guided by PRISMA, helped identify recurring patterns across the selected literature. Coding decisions were validated through an iterative review, in which the included articles were re-examined to ensure consistency and alignment with the study's objectives. Codes were developed inductively from the reviewed literature, allowing patterns to emerge naturally across studies. To enhance reliability, previously coded data were revisited and compared to ensure consistent interpretation.

Coding was organized using Microsoft Excel, where extracted findings were systematically recorded and grouped into higher-level categories. This process enabled structured tracking of coded concepts, cross-study comparisons, and the progressive refinement of themes.

Thematic synthesis was conducted using a two-step process. In the first step, recurring patterns across the studies were identified and assigned descriptive codes. In the second step, related codes were compared and grouped into broader conceptual categories. These categories were then reviewed and refined to ensure conceptual clarity and eliminate redundancy.

Following this process, the categories were consolidated into three overarching themes: cybersecurity knowledge, risk perception, and behavioral response. These themes were selected based on their recurrence across studies, relevance to the research questions, and their ability to capture meaningful generational differences. This systematic approach ensured that the final themes accurately reflected patterns identified across the included studies and strengthened the rigor and transparency of the analysis.

Results

After the screening and eligibility process, the final systematic review dataset included 14 studies. These results synthesize the studies analyzed to answer the research question: What themes emerge from the systematic literature review regarding the seven generational cohorts varying levels of digital technology use differ in their understanding of cybersecurity, their perceptions of digital risks, and their approaches to responding to security incidents?

The identified themes include cybersecurity knowledge, risk perception, and response behavior. Cybersecurity knowledge shapes an individual's ability to understand cyber risks when accessing various technological applications (Koman, 2016). Risk perception aligns with how an individual perceives digital risks (Debb et al., 2020). And the last theme, response behavior, isolates an individual's approach to responding to security incidents, being overly cautious or simply ignoring them (Akello et al., 2024). Both individually and collectively, these themes apply across cohorts to various degrees.

The generational differences identified in this review are understood and interpreted by TAM. Perceived usefulness links technology risk perceptions and behaviors, while perceived ease of use shapes technology knowledge and understanding. However, too much trust in technology can lead to automation complacency. While the fear of cyber threats, as well as an awareness of consequences, informs better individual risk perception and risk acceptance. And lastly, excessive cybersecurity training and awareness can overwhelm an individual, leading to cybersecurity fatigue.

Table 1

Included Studies

Author(s)	Year	Theme	TAM (Perceived)	Method	Population	Key Contribution
Akello et al.	2024	Response behavior	Usefulness	Mixed method	Employees	Shows generational shifts in a remote context
Bana et al.	2025	Response behavior	Usefulness	Quantitative	Organizations	Explains learning after incidents
Debb et al.	2020	Risk perception	Usefulness	Survey	Gen Y, Gen Z	Platform familiarity
Dhungana et al.	2023	Cybersecurity knowledge	Ease of use	Survey	Students	Cybersecurity understanding and awareness gaps
Hadlington	2017	Response behavior	Usefulness	Quantitative	Internet Users	Risky cybersecurity behavior and business behavior to internet addiction and impulsivity
Koman	2016	Cybersecurity knowledge	Ease of use	Quantitative	Older adults	Highlights age-related adoption gaps
Lissitsa et al.	2022	Cybersecurity knowledge	Ease of use	Quantitative	Older users	Explains generational tech gaps
Mândraş	2024	Cybersecurity Understanding	Ease of use	Mixed method	Gen Z, Alpha	Need for specialized training and education to ensure social success
Pollini et al.	2022	Response behavior	Usefulness	Mixed method	General users	Perceived threat severity to humans and organizations
Pugnetti et al.	2024	Risk perception	Usefulness	Mixed method	Mixed Cohorts	Mitigation of Behavioral Cyber Risk
Redekop	2021	Cybersecurity knowledge	Ease of use	Qualitative	Employees	IT Security Training and Awareness roles
Sadaghiana-Tabrizi	2023	Cybersecurity knowledge	Ease of use	Qualitative	Students/ Workforce	Shows contextual awareness changes
Warrington et al.	2022	Response behavior	Usefulness	Quantitative	Employees	Personality equals an employee's information security behavior
Zierock et al.	2025	Risk perception	Usefulness	Qualitative	Gen Z, Alpha	Technology has changed communication

Overview of Chosen Studies

The reviewed studies included peer-reviewed research spanning cybersecurity, information systems, behavioral psychology, risk behaviors, and technology understanding and adoption (Pollini et al., 2022; Pugnetti et al., 2024; Sadaghiana-Tabrizi, 2023). Research years incorporated early risk perception theory, along with cybersecurity research shaped by generational cohorts with varying levels of digital technology use throughout history (Zierock et al., 2025).

Qualitative and cross-sectional quantitative analyses were amongst the methodologies studied (Debb et al., 2020; Warrington et al., 2022; Redekop, 2021). Many of the studies included risk perception that was validated alongside qualitative inquiry (Koman, 2016; Dhungana et al., 2023).

Cohorts that were studied include the Greatest Generation, the Silent Generation, Baby Boomers, Generation X, Millennials, Generation Z, and Generation Alpha (Lissitsa et al., 2022; Debb et al., 2020). Studies involving the Greatest and Silent Generations, as well as Generation Alpha, were limited. Engagement frequency, diversity of platforms, environmental exposures, and measures of digital literacy were key in operationalizing digital technology usage (Bana et al., 2025; Lissitsa et al., 2022).

Thematic Findings

Thematic synthesis was used to examine the research question: in what ways do generational cohorts with varying levels of digital technology use differ in their understanding of cybersecurity, their perceptions of digital risks, and their approaches to responding to security incidents? Three themes were isolated: (1) cybersecurity knowledge, (2) risk perception variance, and (3) response behavior. The use of digital technology was highlighted across all themes, as referenced in Table 1 (Included Studies).

Cybersecurity Knowledge

Cybersecurity understanding, in both depth and breadth, differs across cohorts and can be interpreted through each cohort's perceived ease of use. Earlier cohorts perceive technology and security platforms as

easier to navigate (Debb et al., 2020; Dhungana et al., 2023). This understanding stemmed from environmental factors such as workplace training and exposure to identity theft (Koman, 2016). However, data reveal that an individual's perceived ease of use can lead to overconfidence due to a lack of awareness and consistent use of protective measures (Warrington et al., 2022; Pugnetti et al., 2024). Older cohorts perceive cybersecurity technologies as being overly burdensome, leading them to lean towards structured guidance and formal training (Redekop, 2021). Regardless of the specific cohort, the consistent and high-frequency use of digital technologies significantly shapes cybersecurity knowledge (Hadlington, 2017).

Risk Perception Variance

Differences in risk perception across cohorts align with perceived usefulness in the TAM. Older cohorts perceive the use of cybersecurity as highly useful for preventing financial loss, resulting in higher threat sensitivity (Koman, 2016). Younger cohorts perceive digital risk in terms of exposed privacy, damaged reputation, and consequences for social settings (Lissitsa et al., 2022; Debb et al., 2020). In addition, younger cohorts commonly associate cybersecurity with cumbersome regulations and less necessary perimeters. Risk normalization occurred after continuous digital immersion lowered vulnerability perceptions despite informed awareness (Mândraș, 2024). Studies indicated that perceived digital competence contributed to perceived control. With these variations across cohorts, data suggest that perceived usefulness is shaped by knowledge and digital experiences that influence how individuals prioritize and interpret cybersecurity risks (Pollini et al., 2022; Pugnetti et al., 2024).

Response Behavior

Throughout the study, identifiable patterns emerged, highlighting different approaches to security incidents. The behavioral response across cohorts further emphasizes the TAM constructs. Cybersecurity adoption primarily occurs when protective applications are seen as both useful and easy to implement (Koman, 2016; Redekop, 2021). Quick, accessible solutions are preferred by younger cohorts, who prioritize ease of use. However, older cohorts look to structured, organizationally supported responses that reflect perceived usefulness and trust (Lissitsa & Laor, 2021). Study findings revealed that knowledge was not the only factor in cybersecurity behavior; it also influenced the interaction among perceived effort, perceived benefit, and contextual trust (Debb et al., 2020).

Conceptual Synthesis

The synthesis suggests that generational cohorts indirectly influence cybersecurity outcomes through digital socialization, shaping both the perceived ease of use of technologies and their usefulness. Knowledge shapes the interpretation of the threat, thereby influencing risks and perceived vulnerabilities (Pollini et al., 2022). Response behaviors are reliant on institutional trust, perceived control, and ideal convenience (Warrington et al., 2022).

The differences in each generation's cybersecurity understanding, risk perception, and response behavior are explained by the intensity of use, the perceived ease of use, the usefulness of technology, and individuals' social awareness. Ultimately, the identity of a cohort aligns with a contextual structure rather than with the determining cause.

Discussion of findings

The findings for this study have several implications for cybersecurity training, human resource policy design, and individual security interventions. Applying a one-size-fits-all solution to cybersecurity training programs can no longer be the norm for corporations, governments, and educational institutions. Instead, a tailored approach should be adopted, starting with a cybersecurity training baseline based on an individual's needs. Generational perspectives should be used to emphasize training requirements as an indication of an individual's digital exposure and learning preferences.

For instance, younger cohorts may require input focused on behavioral consistency and risk awareness, while older cohorts may need additional assistance in navigating evolving digital environments and emerging threats. The development of training programs and business applications should also consider the perceived ease of use, as it plays a critical role in adherence and compliance across all cohorts.

Corporations, governments, and educational institutions should consider integrating cybersecurity education with specialized, targeted approaches that account for varying levels of digital knowledge and risk perception. It is also critical that training does not directly contradict the goal of protecting data. Therefore, the right amount of cybersecurity training and awareness should not introduce fatigue or complacency. Instead, it should command awareness and intertwine into the culture and the fabric of an individual's ability to understand, perceive, and respond to risks.

Furthermore, this study applies TAM in a generational context, thereby contributing to the cybersecurity and information systems literature. Perceived ease of use and perceived usefulness are shaped by digital experience and generational exposures. The application of TAM highlights how familiarity with technology, trust, and perceived control directly influence security behaviors. The results indicate the need for theoretical models that account for experiential variability and sociodemographic factors in cybersecurity decision-making.

Table 2 and Figure 2

Table 2 and Figure 2 were developed by accounting for differences in each cohort's knowledge, risk acceptance, and exposure to technology. These diagrams serve to identify differences in multi-generational technology use and cyber awareness.

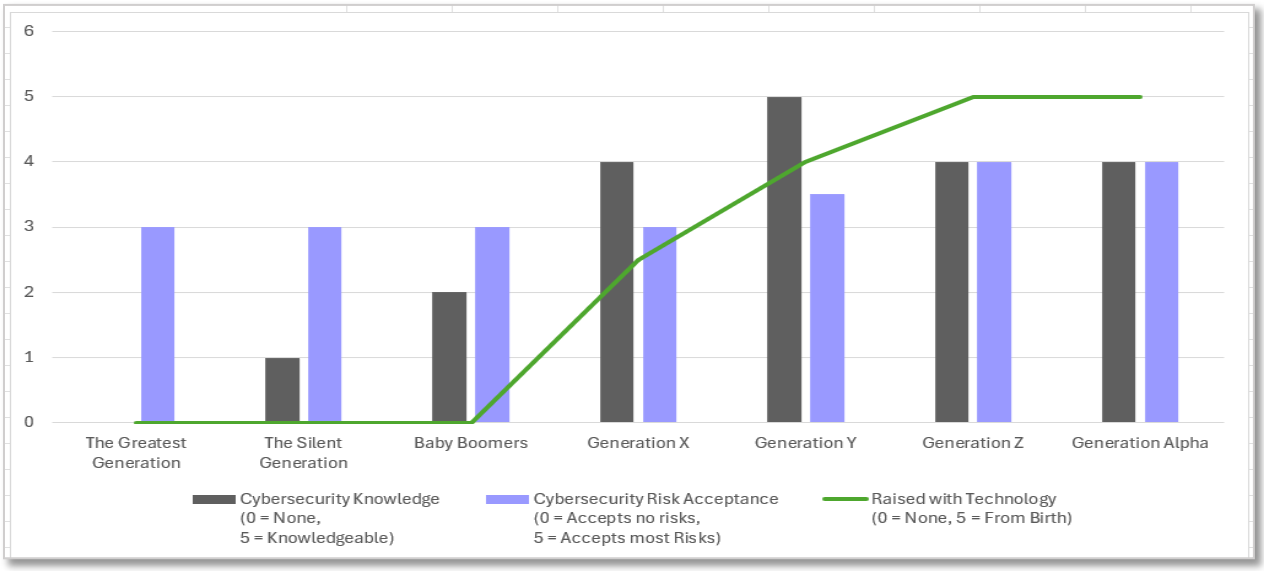
Table 2

Generational Cybersecurity Awareness

Generation	**Cybersecurity Knowledge** (0 = None, 5 = Knowledgeable)	**Cybersecurity Risk Acceptance** (0 = Accepts no risks, 5 = Accepts most Risks)	**Raised with Technology** (0 = None, 5 = From Birth)	**Study(s)**
The Greatest Generation	0	5	0	Thaariq, 2023
The Silent Generation	0.5	5	0	Lissitsa, et al., 2022
Baby Boomers	1.5	4	0	Koman, 2020
Generation X	4	3	2.5	Lissitsa & Laor, 2021
Generation Y	5	3	5	Lissitsa & Laor, 2021; Yarnykah, 2021
Generation Z	4	4	5	Mândraş, 2024; Rahmat, et al., 2024
Generation Alpha	4.5	4.5	5	Ziatdinov & Cilliers, 2021; Mândraş, 2024; Zierock et al., 2025

Figure 2

Multi-Generational Technology and Cybersecurity Awareness



Note. For the Silent Generation, the term cybersecurity knowledge should be interpreted within both historical and competorary contexts. First, although cybersecurity was not formally recognized as a distenct field until the latter half of the twenthieth centure, members of the Silent Generation engaged with foundataional security constructs such as information assurance, data protection, physical document security, and the safeguarding of early standalone or air-gapped computing systems. These experiences represent precursor forms of cybersecurity awareness rather than modern cybersecurity knowledge as currently defined..

Conclusion

This systematic literature review examined cybersecurity knowledge, risk perception, and response behavior across generational cohorts. The synthesis of findings from academic studies highlights patterns in digital exposure, technological knowledge, and empirical learning environments, emphasizing generational differences beyond individual age.

The findings indicate that cybersecurity response behavior is not predicated on higher levels of digital fluency and a broad awareness of platform-specific risks. Therefore, younger cohorts are more likely to accept risks, whereas older cohorts tend to favor structured, compliance-oriented security practices, thereby decreasing their likelihood of accepting risks.

It should be noted that TAM provides a theoretical explanation for these differences. Across cohorts, the study found that perceived ease of use and perceived usefulness suggested interactions with technology, beyond generational labels alone, that help shape cybersecurity risk and response behavior. While security fatigue is also a behavioral factor to consider, it can heighten cybersecurity risk by reducing user vigilance and increasing the likelihood of convenience-driven behaviors.

This study helps to pinpoint cybersecurity behavior as a multidimensional construct influenced by conceptual, behavioral, and environmental factors. Educators, policymakers, organizations, and governments must understand these dynamics and use them to design specific tools for necessary understanding.

Limitations of the Study

When interpreting the results of this study, several limitations should be considered. First, the included studies define the scope and quality of this systematic literature review. It should be noted that these variances in methodologies and sample populations may introduce inconsistencies.

Second, previous studies focused on age and merely mapped it onto generational cohorts, which leads to the oversimplification of the experiences and digital usage of each generation.

Finally, as technology continues to evolve and cybersecurity threats increase, the studies used are becoming outdated and may no longer be relevant.

Recommendations for Future Research

Future research should consist of the differences between generational identities and cybersecurity behaviors by incorporating extensive cross-cultural perspectives. Understanding how cybersecurity response behaviors historically develop within and across generations would help to pinpoint the role of continuous digital transformation and use.

Ultimately, future research should integrate multiple theoretical frameworks, including TAM and potentially the Protection Motivation Theory (PMT). This would help establish and isolate more complex models that account for conceptual, behavioral, and environmental factors in cybersecurity risk response and behavior.

The rapid advancement of technology sets the precedent for developing effective and inclusive security strategies that rely on comprehending generational experience, technological engagement, and cybersecurity behavior.

References

Akello, P., Firth, D., & Clouse, S. (2024). Moral dynamics in the age of remote work: Exploring the role of generational shifts in information security. *Association of Information Systems*, 1–11.

Bana, S. H. (2025). Human capital acquisition in response to data breaches. *MIS Quarterly, 49*(1)*,* 367–388. https://doi.org/10.25300/MISQ/2024/18352

Baumeister, R. F. (1997). Writing narrative literature reviews. *Review of General Psychology, 1*(3), 311–320. https://doi.org/10.1037/1089-2680.1.3.311

Debb, S., Schaffer, D., & Colson, D. (2020). A reverse digital divide: Comparing information security behaviors of Generation Y and Generation Z adults. *International Journal of Cybersecurity Intelligence & Cybercrime, 3*(1), 42–55. https://doi.org/10.52306/2578-3289.1052

Dhungana, R. K., Gurung, L., & Poudyal, H. (2023). Cybersecurity challenges and awareness of the multigenerational learners in Nepal. *Journal of Cybersecurity Education, Research, and Practice, 2*(5), 1–14. https://doi.org/10.32727/8.2023.17

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7)*,* e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Koman, V. P. (2016). *Age and the acceptance and use of cybersecurity: A quantitative survey of U.S. baby boomer mobile-device security practices* (Doctoral dissertation, Capella University). ProQuest Dissertations & Theses Global.

Lissitsa, S., & Laor, T. (2021). Baby boomers, generation X and generation Y: Identifying generational differences in effects of personality traits in on-demand radio use. *Technological Forecasting and Social Change, 64, 101526*. https://doi.org/10.1016/j.techsoc.2021.101526

Lissitsa, S., Zychlinski, E., & Kagan, M. (2022). The silent generation vs baby boomers: Socio-demographic and psychological predictors of the "gray" digital inequalities. *Computers in Human Behavior, 128*, 107098. https://doi.org/10.1016/j.chb.2021.107098

Mândraș, P. (2024). Exploring the security of the digital society: Focusing on the "phygital" space and advocating a novel educational model targeting Gen Z and Alpha. *Romanian Journal of Sociological Studies, 1*, 15–31.

Marulli, F., Paganini, P., & Lancellotti, F. (2024). The three sides of the moon: LLMs in cybersecurity: Guardians, enablers, and targets. *Computer Communications, 246*, 5340–5348. https://doi.org/10.1016/j.procs.2024.09.653

Mumford, D., & Shires, J. (2023). Toward a decolonial cybersecurity: Interrogating the racial-epistemic hierarchies that constitute cybersecurity expertise. *Security Studies, 32*(4–5), 652–655. https://doi.org/10.1080/09636412.2023.2230879

Pollini, A., Callari, T., & Tedeschi, A. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work, 24*, 371–390. https://doi.org/10.1007/s10111-021-00683-y

Pugnetti, C., Bjorck, A., Schonauer, R., & Casian, C. (2024). Towards diagnosing and mitigating behavioral cyber risks. *Risks, 12*(7), 116. https://doi.org/10.3390/risks12070116

Quintana, K., Sutton Chubb, C., Olson, D., & Kosloski, A. E. (2024). Cybersecurity skills, knowledge and abilities for criminal justice professionals: An exploratory study of practitioners' perspectives. *Journal of Cybersecurity Education, Research and Practice, 2024*(1), 1–10. https://doi.org/10.62915/2472-2707.1175

Rahmat, T., Ashshiddiqi, M. T., & Apriliani, D. (2024). Urgency of digital literacy to improving work readiness. *The Journal of Society and Media, 8*(1), 307–326. https://doi.org/10.26740/jsm.v8n1.p307-326

Redekop, B. D. (2021). IT security training and awareness in the multigenerational workplace. *International Journal of Information Security and Cybercrime, 10*(2), 9–15. https://doi.org/10.19107/ijisc.2021.02.01

Sadaghiani-Tabrizi, A. (2023). Revisiting cybersecurity awareness in the midst of disruptions. *International Journal for Business Education*, *163*(1), 2–16. https://doi.org/10.30707/ijbe163.1.1675491516.833197

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security, 119*, 102756. https://doi.org/10.1016/j.cose.2022.102756

Silitonga, M. S. (2023). The public sector's digital skills gap in Indonesia. *NIPA School of Administration Journal, 19*(1)*,* 1–11. https://doi.org/10.32834/gg.v19i1.585

Thaariq, Z. Z. (2023). Learner characteristics based on generational differences. *Jurnal Pendidikan Humaniora*, *11*(1), 10–20. https://doi.org/10.17977/um011v11i12023p32-42

Tian, J., & Zhang, R. (2025). Learners' AI dependence and critical thinking: The psychological mechanism of fatigue and the social buffering role of AI literacy. *Acta Psychologica*, *260*, 105725. https://doi.org/10.1016/j.actpsy.2025.105725

Vo, D. T., Thach, N. H., Pham Ngoc, K. K., Le Tran, B. H., & Pham Thi, K. T. (2025). Understanding Gen Z's digital banking loyalty: The role of switching costs and consumption values. *Journal of Organizational Behavior Research, 10*(1), 44–57.

Warrington, C., Syed, J., & Tappin, R. (2022). Personality and employees' information security behavior among generational cohorts. *Journal of Organizational Psychology*, *22*(3), 40–61. https://doi.org/10.33423/jop.v22i3.5647

Yarnykah, V. (2021). Media technologies in the corporate model of media education: Opportunities and prospects. *DESIDOC Journal of Library & Information Technology, 41*(4), 284–289. https://doi.org/10.14429/djlit.41.4.17140

Ziatdinov, R., & Cilliers, E. (2021). Generation alpha: Understanding the next cohort of university students. *European Journal of Contemporary Education, 10,* 783–789. https://doi.org/10.13187/ejced.2021.3.783

Zierock, B., Schulze, J., & Angar, S. (2025). From Gen Z to Generation Alpha: Navigating the evolution of communication in a digital age. *SCIREA Journal of Education, 10*(2), 69–80. https://doi.org/10.54647/education880581