

## Abstract

This dissertation contributes to the United Nations and World Health Organization's Healthy Ageing (2021–2030) initiative by addressing digital equity and cybersecurity challenges faced by older adults. As cyber threats become more sophisticated, older individuals remain particularly vulnerable due to gaps in cybersecurity awareness, digital literacy, and evolving online risks. Using a qualitative mixed Delphi method, this research engaged a panel of fifteen interdisciplinary experts in cybersecurity and aging to refine thirty-two cybersecurity competencies within the Identify, Protect, Detect, and Respond categories of the NIST Cybersecurity Framework (CSF). The study explored key questions regarding the essential cybersecurity skills needed by older adults, the barriers preventing their adoption of best practices, and how existing digital competency models can be adapted to enhance cybersecurity resilience among aging populations.

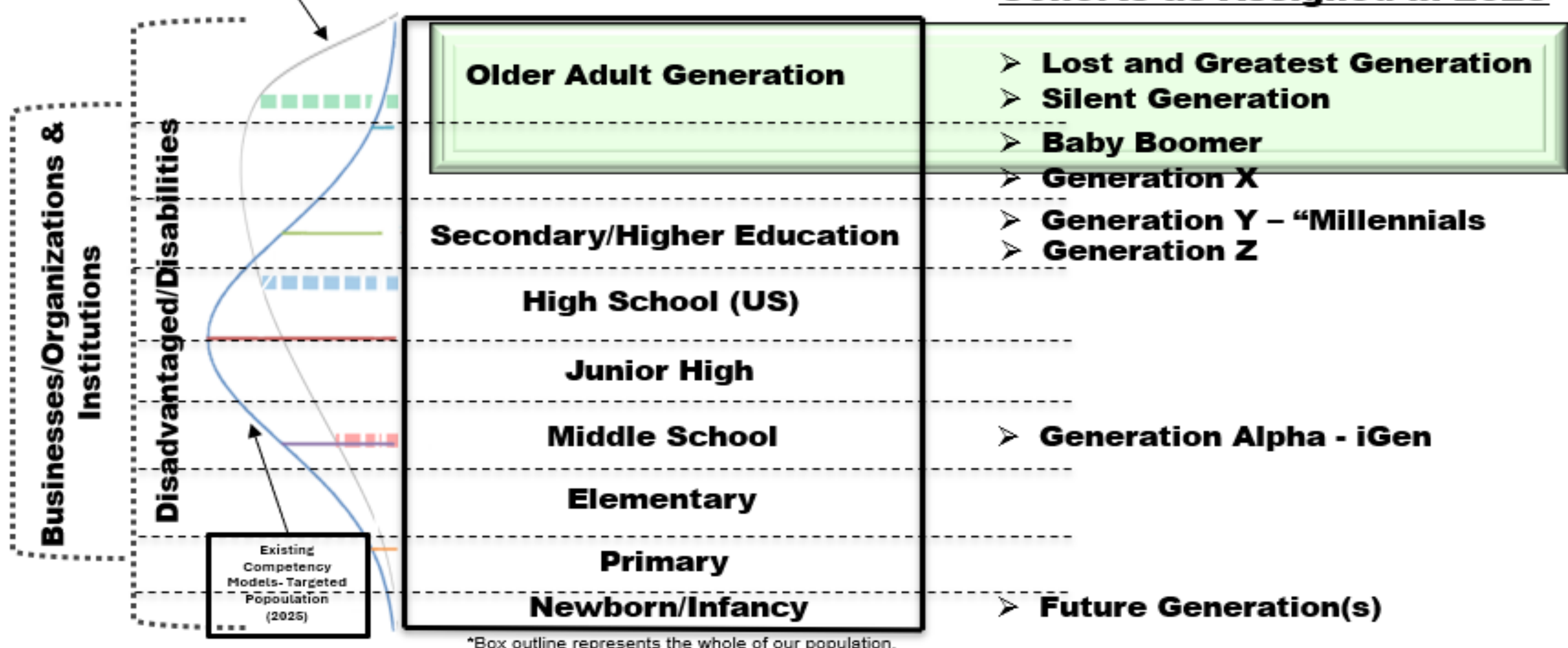
The findings revealed twenty-three critical gaps in older adults' understanding of core cybersecurity areas, including password security, phishing awareness, device protection, and online privacy. The Delphi panel emphasized the necessity of age-friendly cybersecurity education, incorporating simplified instructions, real-world scenarios, and interactive learning experiences to improve engagement. The study introduced the Cybersecurity Competency Model (CCM), grounded in Motivation, Awareness, Skills, and Knowledge (M.A.S.K.), reinforcing behavioral change through real-time feedback and cognitive adaptability. The research further aligns with Self-Determination Theory, Social Learning Theory, and Connectivism, emphasizing motivation, adaptability, and networked learning. Future research suggests that AI-driven cybersecurity training could enhance digital resilience, though human oversight remains crucial. This dissertation highlights the pressing need for structured, accessible cybersecurity education, advocating that an informed and proactive approach is the best defense against cyber threats, ultimately supporting the UN and WHO's global vision for healthy aging.

## Thesis Purpose:

### Cybersecurity Competency Model (CCM)

Cohort Distribution (Normal Curve and Targeted Distribution Curve)

Cohorts as Assigned in 2023



**Note:** This thesis researched traditional competency models by shifting the focus away from normal population distributions and addressed the unique needs of older adults outside of the working population, a group often overlooked in conventional models. Existing cybersecurity models are fragmented and do not adequately capture the diverse experiences, motivations and learning capacities of older adults. This research identified 32 competencies that better represent older adults' learning trajectories, cognitive adaptability, and technology adoption.



# CERIAS

## USING A MODIFIED DELPHI METHOD: IDENTIFY CYBER SECURE COMPETENCIES FOR OLDER ADULTS

The Center for Education and Research in Information Assurance and Security

