Development of the Cybersecurity Skills Index (CSI): A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cybersecurity Skills

Yair Levy
Nova Southeastern University
Ft. Lauderdale, FL

Melissa Carlton
Florida State University
Panama City, FL

NSU NOVA SOUTHEASTERN UNIVERSITY

Overview

- Problem Statement
- Research Main Goal
- Research Questions
- Review of the Literature
- Methodology
- Results
- Contributions & Implications
- Future Research

Problem Statement

- The problem that this research addressed is the threats to organizational Information Systems (IS) due to vulnerabilities and breaches caused by employees (Hovav & Gray, 2014; Jensen et al., 2014; Peha, 2013)
- The protection of IS lie in the most vulnerable spot; that vulnerability usually rests in individuals (Hovav & Gray, 2014)
- Even with embedded Information Technology (IT) security tools working well, the non-IT user may still receive a social engineering message that can hook them into making mistakes due to low cybersecurity skills (Algarni et al., 2014; Axelrod, 2006; Winkler & Dealy, 1995)

Research Main Goal

Design, develop, and empirically test a set of hands-on tasks to measure the cybersecurity skills level of non-IT professionals

Main Research Question

What tasks will enable the validation of a hierarchical measure for observable cybersecurity skills of non-IT professionals?

Research Questions

RQ1: What are the specific subject matter experts (SMEs) identified set of *cybersecurity* ***skills*** of non-IT professionals, which address the most common organizational cybersecurity threats?

RQ2: What are the specific SMEs identified ***tasks*** that can be categorized, linked, and validated to the set of the identified cybersecurity skills?

RQ3: What are the specific SMEs identified ***weights*** of the tasks and skills that enable a validated hierarchical aggregation to the Cybersecurity Skills Index (CSI) benchmarking index?

Research Questions

RQ4: What are the ***scores*** of the CSI benchmarking index for the aggregated set of SMEs identified cybersecurity skills of a group of non-IT professionals?

RQ5: Are there any significant differences to CSI based on age, gender, educational level, job function, primary online activity, hours accessing the Internet, or experience with technology?

Review of the Literature

- Skills and Competencies
  - Skills Defined
  - Competence vs. Skills
  - Information Technology Skills
- Data Breaches
  - Social Engineering
  - Malware
  - Personally Identifiable Information
    - Phishing
    - Social Media
  - Work Information Systems Security
    - Confidential Information Exposure
    - Password Exploitations
- Cybersecurity
  - Cybersecurity Skills Shortage
  - Cybersecurity Risk Mitigation and Tools

Skills and Competencies

- Skills are defined as the combination of knowledge, experience, and ability to do something well (Boyatzis & Kolb, 1991)
- Cybersecurity skills are defined as an individual's technical knowledge, experience, and ability surrounding the hardware and software required to execute information security in protecting their IT against damage, unauthorized use, modification, and/or exploitation (Boyatzis & Kolb, 1991; Choi, Levy, & Hovav, 2014)

Skills and Competencies

- College coursework disseminates knowledge and is relevant to the competency level of a student (Eschenbrenner & Nah, 2014; Rubin & Dierdorff, 2009)
- Vital for an organization that relies on its employees to possess skills (i.e., knowledge, experience, & ability) to complete technical tasks (Downey & Smith, 2011)
- Information Technology (IT) skills are measured predominantly based on self-reported survey instruments (Levy, 2005; Torkzadeh & Lee, 2003)

Data Breaches

- Prior research identified the need for research to address the threats to organizational IS due to vulnerabilities and breaches caused by employees (Choi et al., 2013; Jensen et al., 2014; Peha, 2013)
- Since 2003, four of the top nine security incident patterns (e.g., miscellaneous errors, crimeware, insider misuse, & physical theft/loss) involved human error or misuse (Verizon Enterprise Solutions, 2015)
- Cyber threats and vulnerabilities are causing substantial losses for individuals, organizations, and governments around the world (Levy, Ramim, Furnell & Clark, 2011; Ramim & Levy, 2006)

Cybersecurity Skills Shortage

- Ponemon Institute (2014) found the IT security function understaffed at 70% of organizations surveyed
- People that want to use their cybersecurity skills for good and not evil are difficult to locate (Rastello & Smialek, 2013)
- People with good cybersecurity skills may be used in many related specialties; all do not obtain a computer science degree (Libicki et al., 2014)

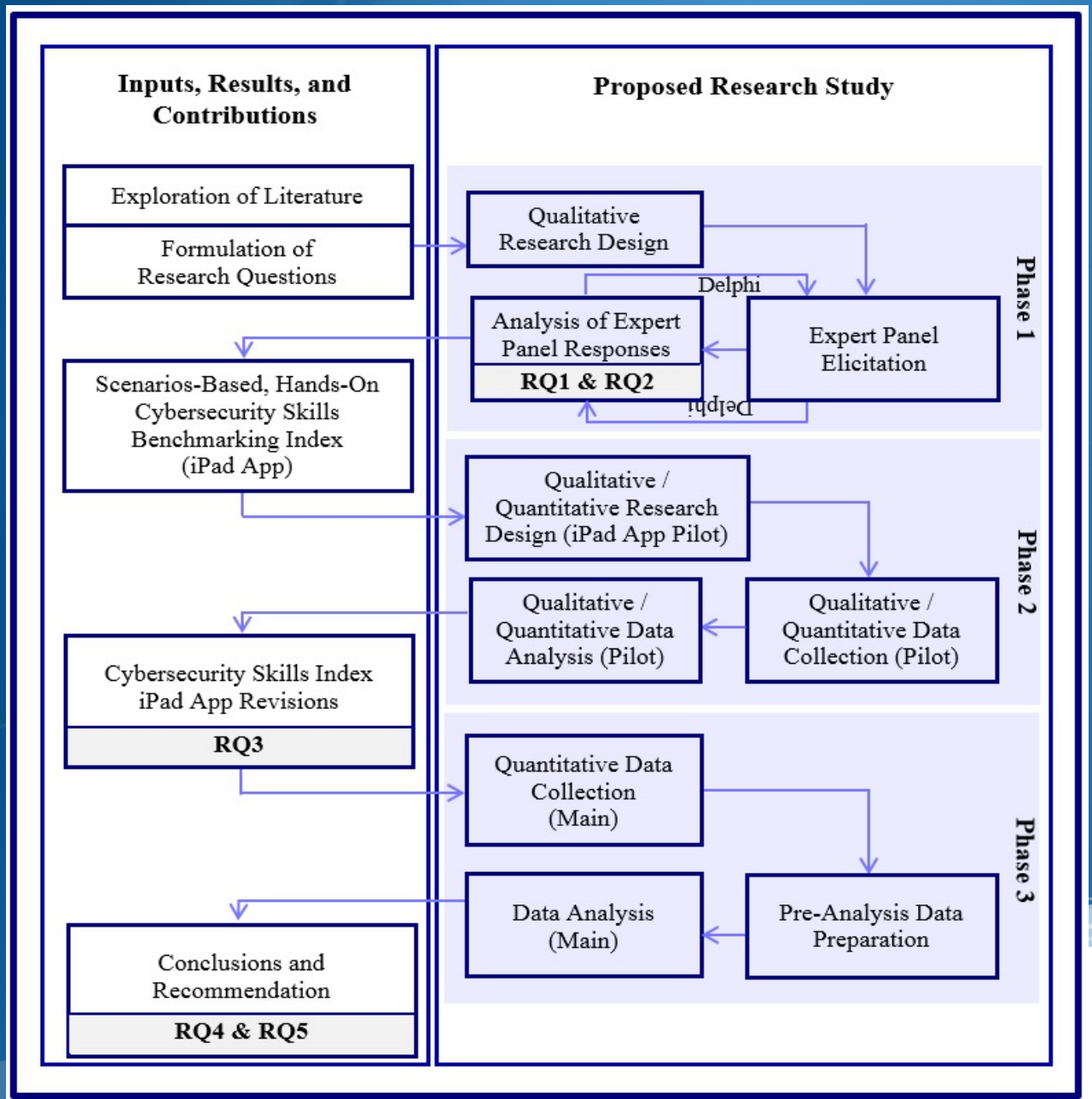
Cybersecurity Risk Mitigation and Tools

- Cybersecurity involves both technical and human ability “to protect or defend against cyber-attacks” (Committee on National Security Systems (CNSS), 2010, p. 22).
- According to Maxion and Reeder (2005), risk mitigation is necessary to protect IS systems as humans making mistakes compromise IS security.
- Executive Order 13,636 (2013) summons for the making of the ‘Cybersecurity Framework’ that includes “a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks” (p. 11741).

Methodology

- Development Research
  - Address the problem
    - Construct Cybersecurity Skills Index (CSI)
    - Operationalized into the MyCyberSkills™ iPad app prototype
- Sequential-Exploratory Design
  - Qualitative
  - Quantitative

Overview of the Research Design Process



Results

- Phase One
  - Survey of existing body of knowledge
    - Began with 12 cybersecurity threats
  - Delphi Technique - Round One
    - 18 Subject Matter Experts (SMEs)
      - Florida Chapter of the InfraGard
      - Government
      - Industry

Results (cont.)

- Phase One continues
  - Delphi Technique - Round Two
    - Previously identified independent cybersecurity threats
      - Seven-point Likert scale
        - ‘1’ – strongly disagree & ‘7’ – strongly agree
        - Valid to be included in core fundamental set
        - Each proposed matching skill is valid or not
        - Each proposed skill is independent of the others
        - Rank highest threat a ‘1’ and lessor threat a ‘10’
  - Consensus of SMEs’ opinion emerged

Results (cont.)

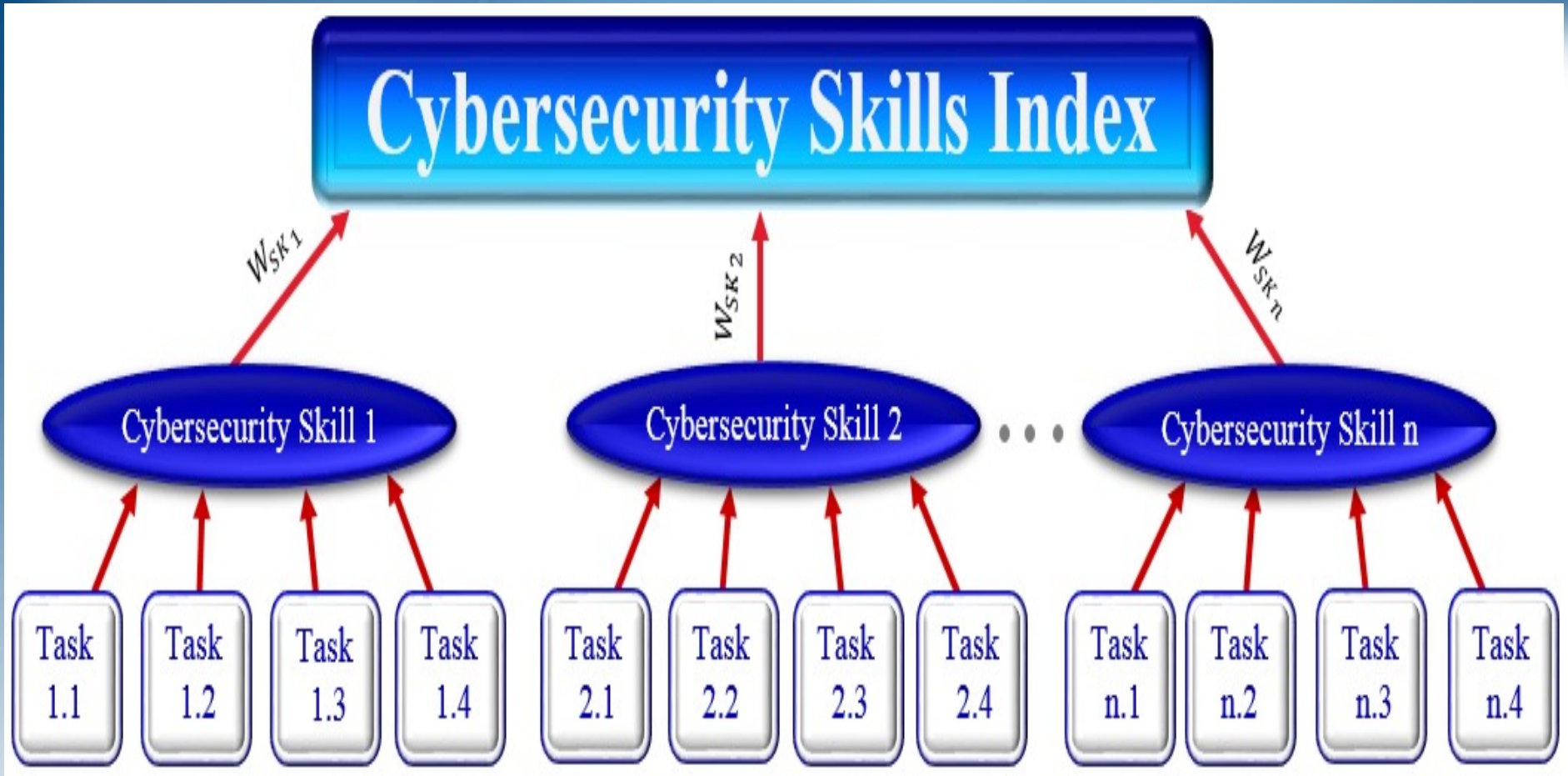
- Phase One continues
  - SMEs' identified top nine cybersecurity skills established the CSI
  - CSI operationalized into an iPad app prototype
    - 36 Scenario-based, hands-on tasks
    - Score 0 - 100

Results (cont.)

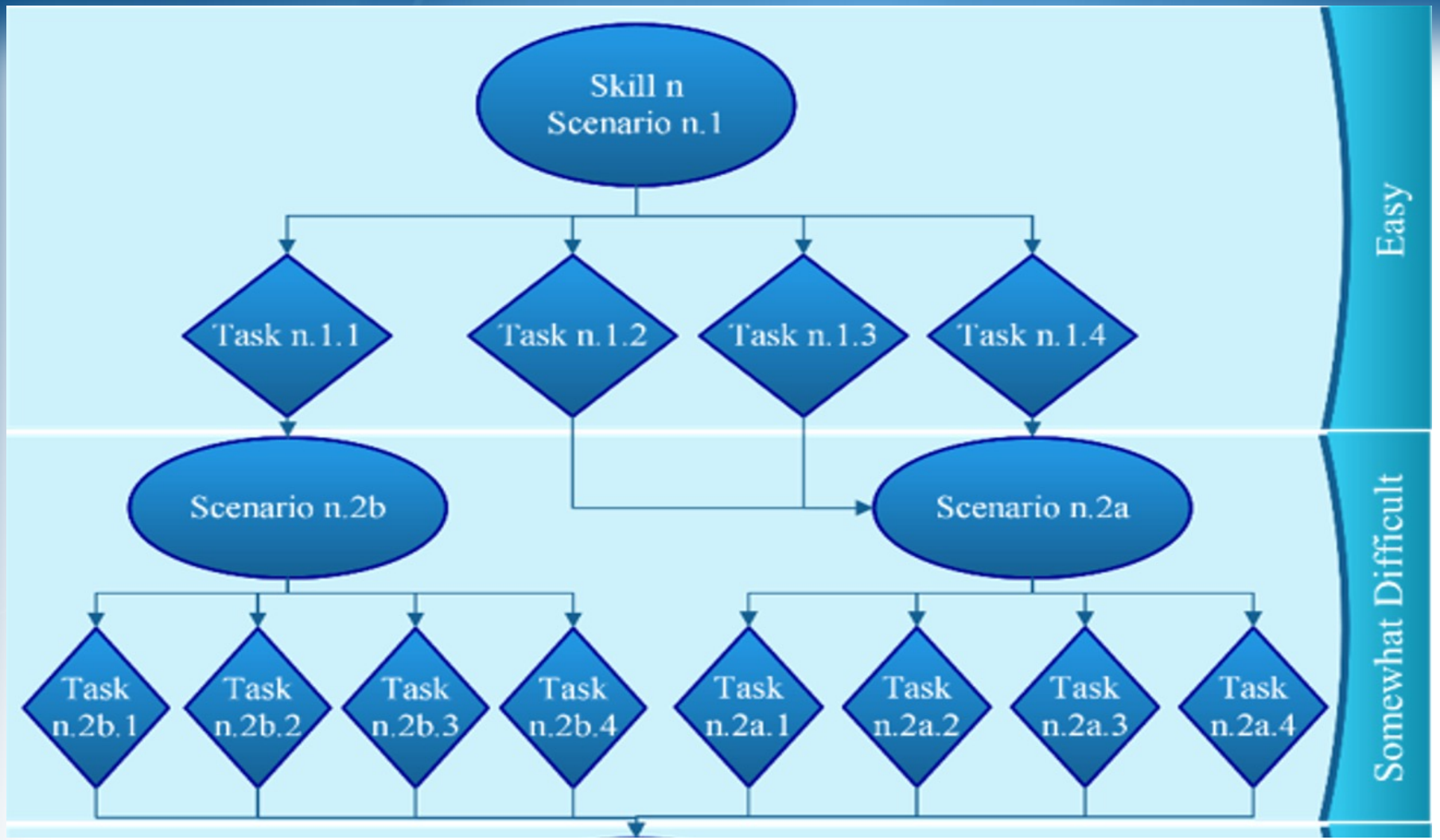
SMEs' Rankings of the Top Nine Cybersecurity Skills

Skills	Category	Individual SME Rankings										SME Response	Weighted Total	Weighted Average	Skill Importance Weight
		1	2	3	4	5	6	7	8	9	10				
1 - Preventing the leaking of confidential digital information to unauthorized individuals	Work Information Systems (WIS)	8	2	0	0	3	0	1	2	0	2	18	128	7.111	0.136
2 - Preventing malware via non-secure Websites	Malware	1	4	4	3	0	4	1	0	0	1	18	124	6.889	0.132
3 - Preventing personally identifiable information (PII) theft via access to non-secure networks	PII	4	1	2	3	2	2	2	0	2	0	18	120	6.667	0.127
4 - Preventing PII theft via e-mail phishing	PII	1	3	1	2	2	3	2	3	1	0	18	105	5.833	0.112
5 - Preventing malware via e-mail	Malware	2	0	6	1	2	0	2	0	3	2	18	103	5.722	0.109
6 - Preventing credit card information theft by purchasing from non-secured Websites	Malware	1	1	1	3	2	2	1	6	1	0	18	94	5.222	0.100
7 - Preventing information system compromise via USB or storage drive/device exploitations	WIS	0	3	1	2	1	2	3	3	2	1	18	91	5.056	0.097
8 - Preventing unauthorized information system access via password exploitations	WIS	1	0	1	4	3	2	1	1	3	2	18	89	4.944	0.095
9 - Preventing PII theft via social networks	PII	0	2	2	0	3	2	3	2	3	1	18	87	4.833	0.092
												Totals -->	941	52.278	1.000

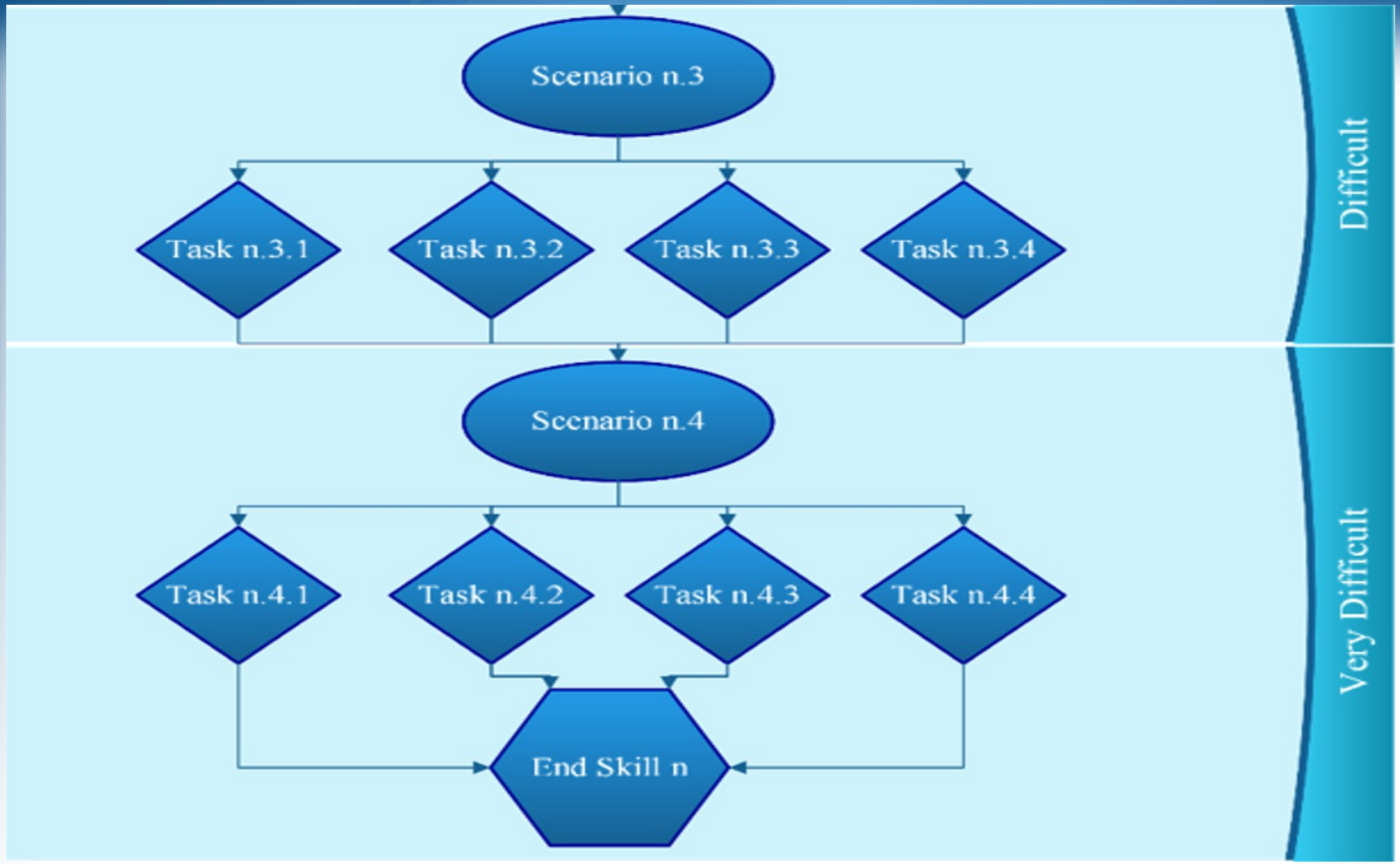
Conceptual Design of the CSI as an iPad App



Scenario-Based, Hands-On Task Skill Levels



Scenario-Based, Hands-On Task Skill Levels



MyCyberSkills™ Prototype

Designed Written Scenarios-based, Hands-on Tasks

Skill n – Preventing malware via non-secured Websites

Scenario n.1: A large architecture design firm hired Sarah a month ago as their Information Technology Analyst. After her first budget meeting, the CEO explained funds are limited and saving the company money is a priority.

Sarah's supervisor asks her to purchase 10 flash drives for the department.

Respective Developed MyCyberSkills™ Screen Shot

MyCyberSkills™ Prototype

Designed Written Scenarios-based, Hands-on Tasks

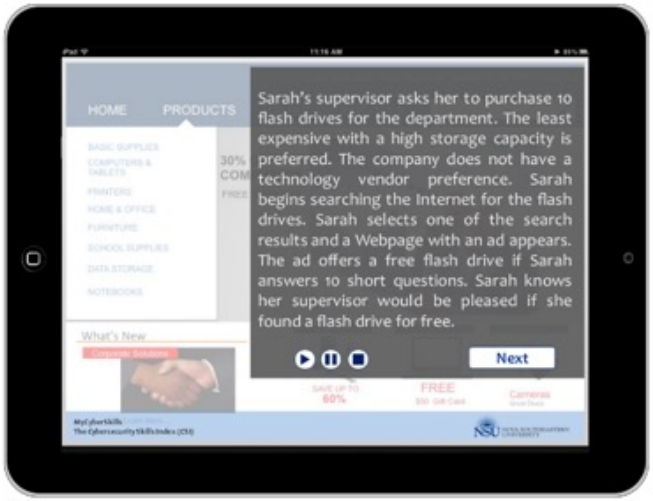
Skill n – Preventing malware via non-secured Websites

The least expensive with a high storage capacity is preferred. The company does not have a technology vendor preference. Sarah begins searching the Internet for the flash drives.

Sarah selects one of the search results and an ad on the Webpage appears. The ad offers a free flash drive if Sarah answers 10 short questions. Sarah knows her supervisor would be pleased if she found a flash drive for free.

Present the user with a Banner AD instructing people to answer 10 short questions and in return get a 128GB USB drive free

Respective Developed MyCyberSkills™ Screen Shot

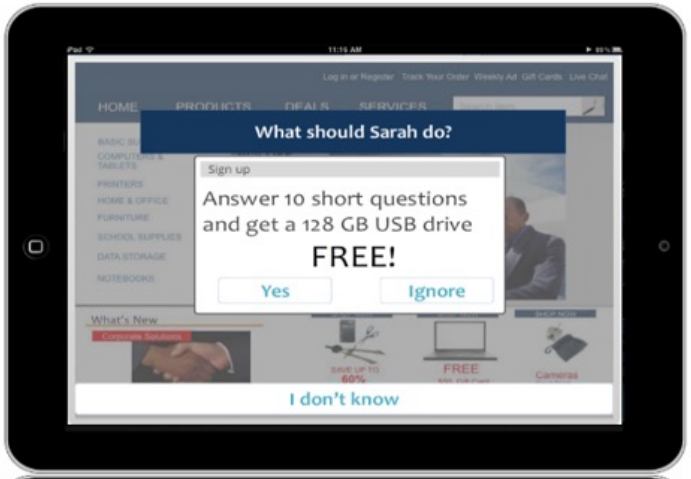


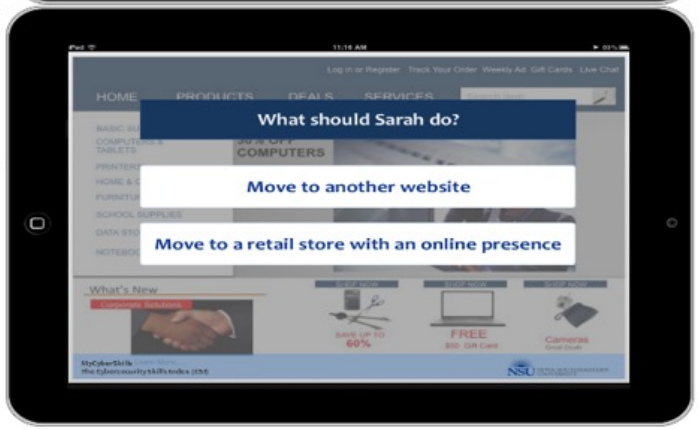
MyCyberSkills™ Prototype

Skill n – Preventing malware via non-secured Websites

Task: What should Sarah do?

Option	Framed Action	Description	What happens	Score
n.1.1	Yes	Click on the Banner Ad to proceed further	takes user to screen 2.2b	0
n.1.2	I don't know	Aborts the task	takes user to screen 2.2a	2
n.1.3	Ignore	• Move to a different website	takes user to screen 2.2a	6
n.1.4		• Move to a retail store with an online presence	takes user to screen 2.2a	10

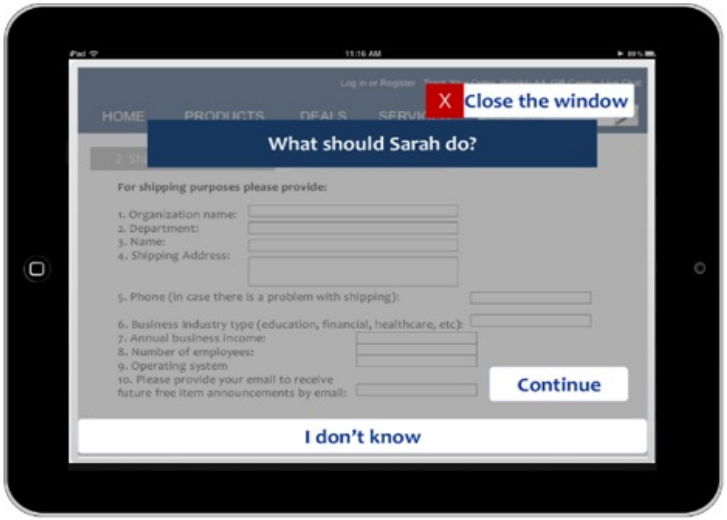




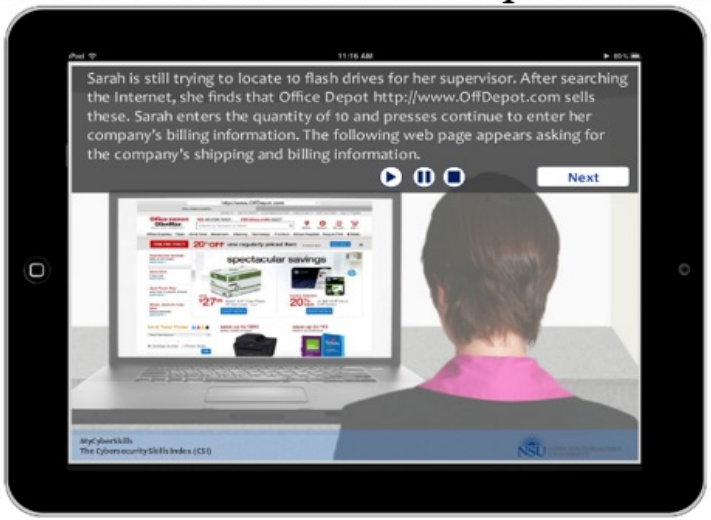
MyCyberSkills™ Prototype

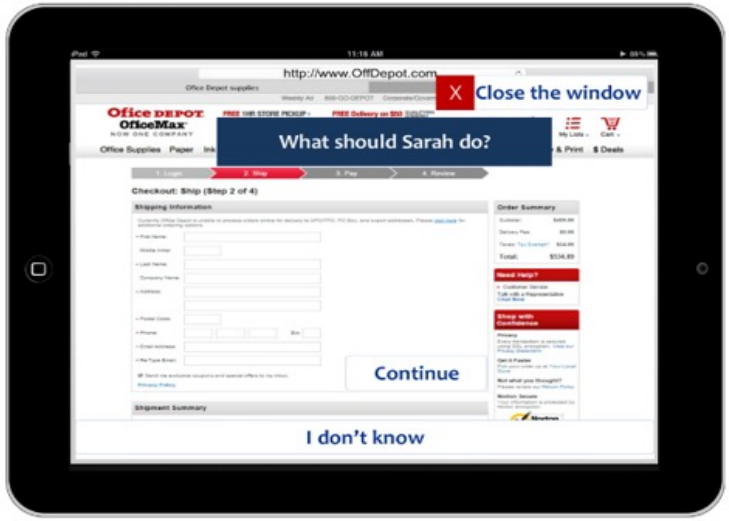
Skill n – Preventing malware via non-secured Websites

Move to another website screenshots



Move to a retail store with an online presence screenshots





Results (cont.)

- Phase Two
  - Expert Questionnaire
    - Eight SMEs validated the scenarios, tasks, and scores
  - Pilot Study
    - 21 (52.5%) non-IT professionals
    - Lab managers manually calculated participant's score, while the participant completed the iPad app prototype
    - The manual calculations were then compared to the internal scores captured by the prototype

Results (cont.)

- Phase Three
  - Research Study
    - Developed CSI operationalized as MyCyberSkills™
    - Community approach to recruitment
      - 975 non-IT professionals invited
        - 245 (25.1%) responded
        - 188 (19.3%) usable for data analysis

Data Analysis

ANOVA Results for Location

		ANOVA		
Item	**df**	**Mean Square between Groups**	**F**	**Sig.**
Malware (SK_2, SK_5, & SK_6)	1	0.000	0.046	0.830
PII (SK_3, SK_4, & SK_9)	1	0.000	0.000	0.987
WIS (SK_1, SK_7, & SK_8)	1	0.000	0.000	0.989
Overall CSI	1	0.000	0.005	0.942

* - $p<.05$, ** - $p<.01$, *** - $p<.001$

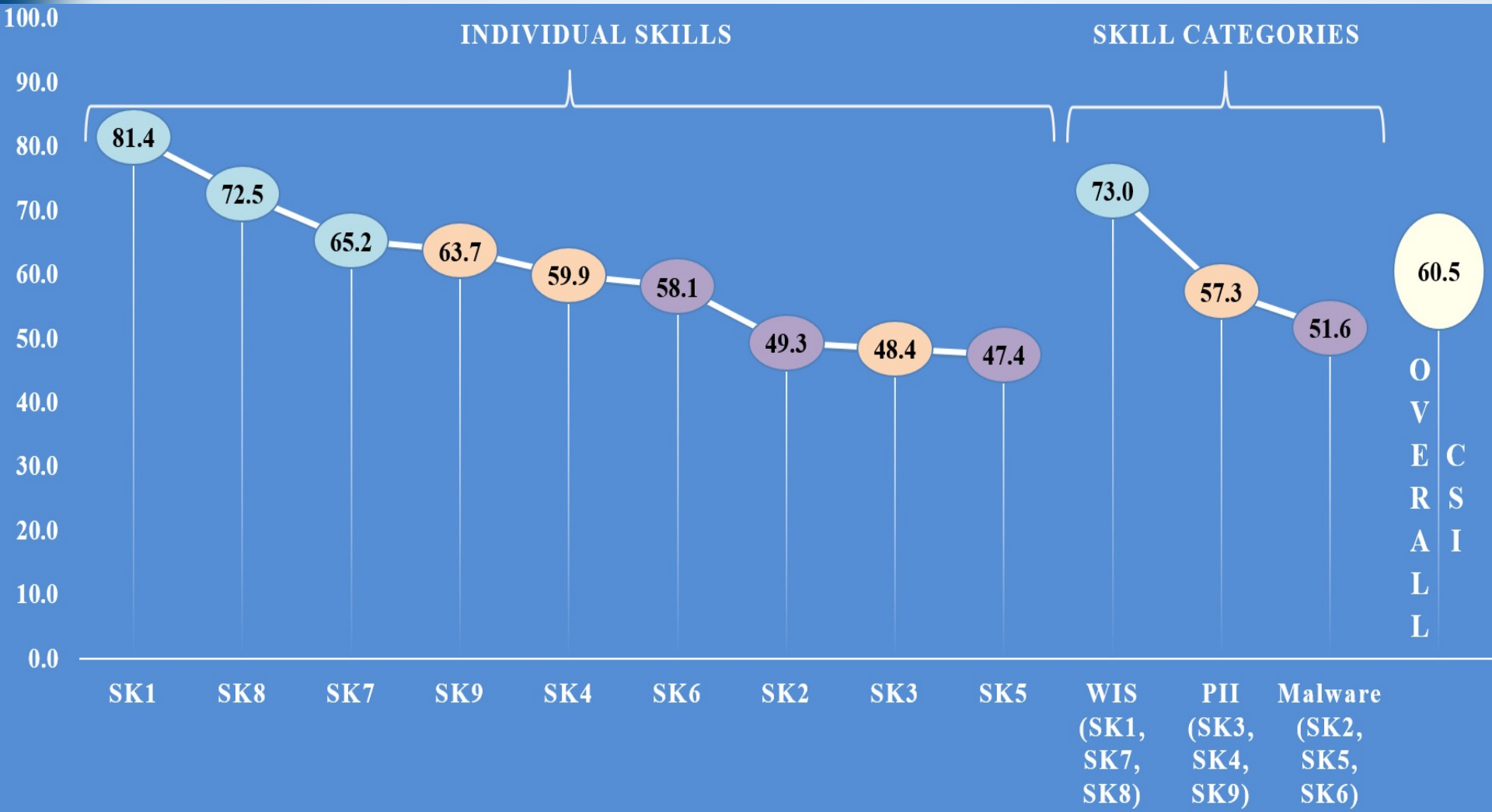
Data Analysis

Means and Standard Deviations for the Population (N=188)

	Item	Mean	Standard Deviation
Individual Skills	SK_1 Leak Confidential Info	0.814	0.142
	SK_2 Malware via Non-Secure Web	0.493	0.190
	SK_3 PII Theft via Non-Secure Web	0.484	0.298
	SK_4 PII Theft via email	0.598	0.198
	SK_5 Malware via email	0.474	0.185
	SK_6 Credit Card Theft via Non-Secure Web	0.581	0.159
	SK_7 USB Exploits	0.652	0.191
	SK_8 Password Exploits	0.725	0.175
	SK_9 PII Theft via Social Network	0.636	0.215
Categories	WIS (SK_1, SK_7, & SK_8)	0.730	0.119
	Malware (SK_2, SK_5, & SK_6)	0.516	0.116
	PII (SK_3, SK_4, & SK_9)	0.573	0.161
	Overall CSI	0.605	0.099

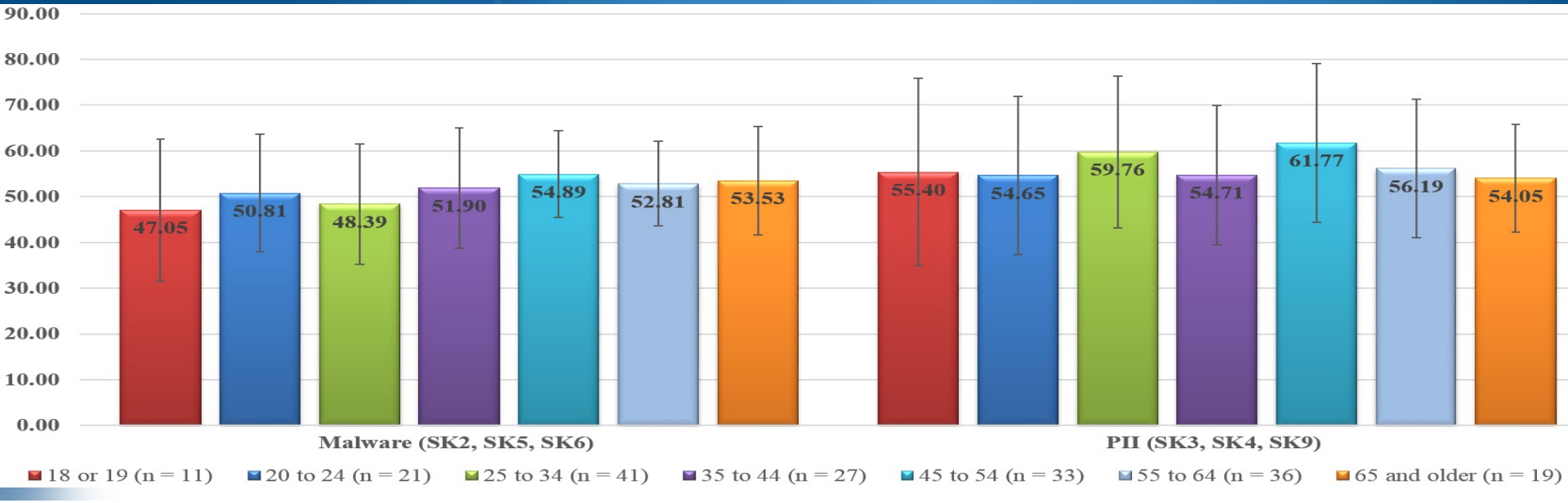
Data Analysis

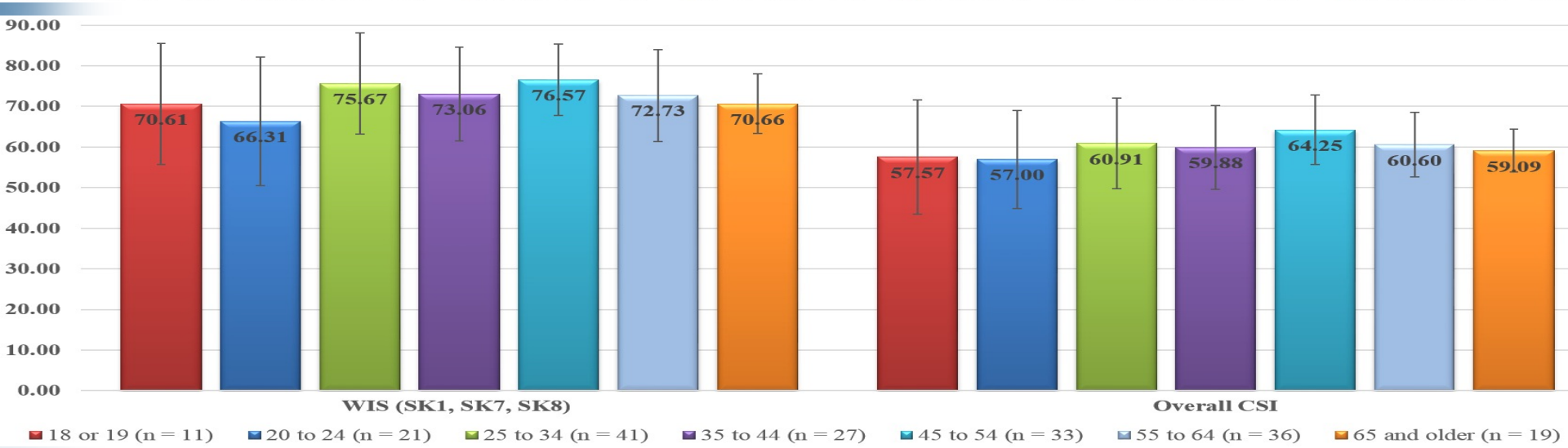
Means and Standard Deviations for the Population (N=188)



Data Analysis

Means and Standard Deviations for Age Group





Data Analysis

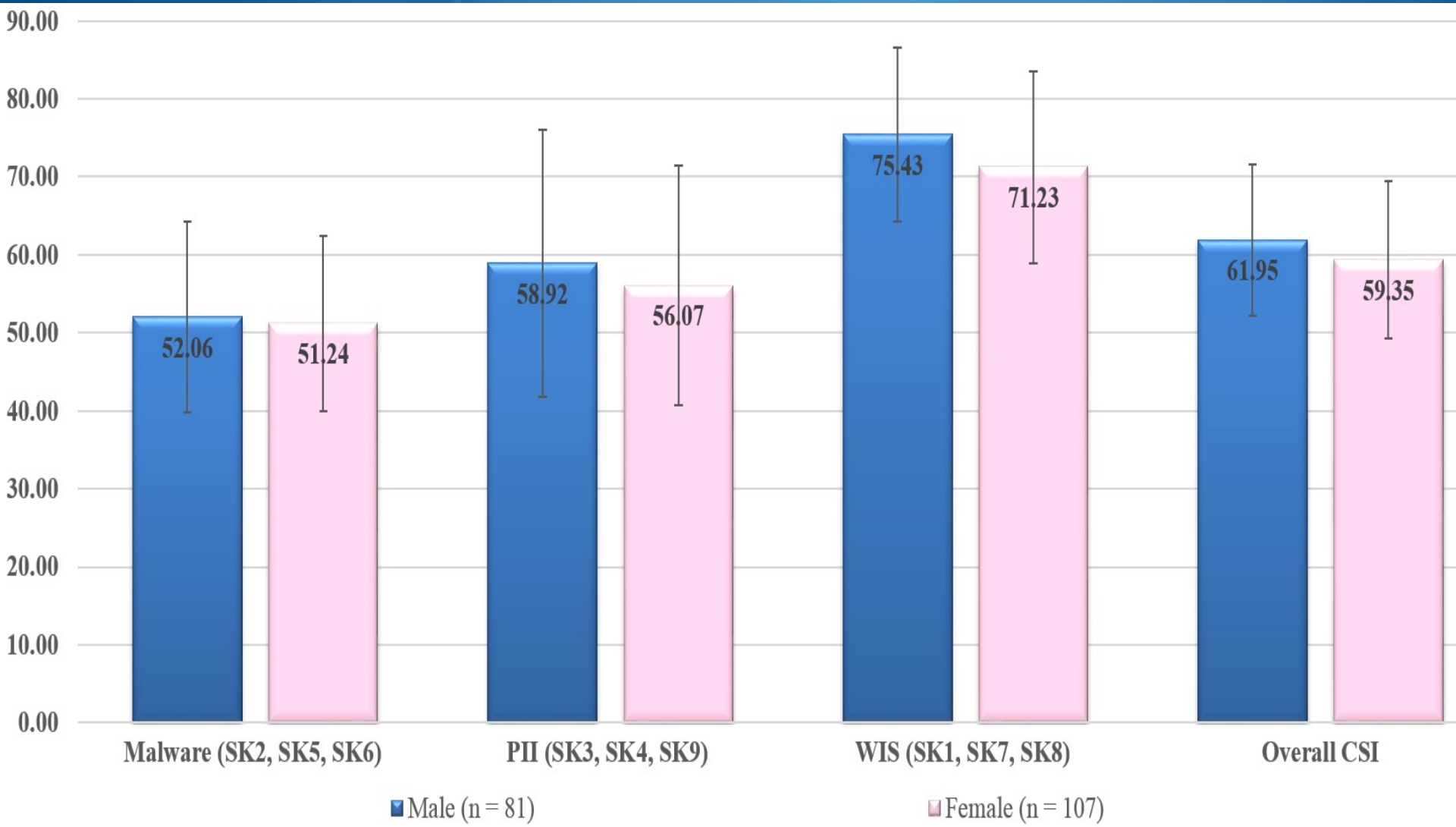
ANOVA Results for Age Group

			ANOVA		
Item	**df**	**Mean Square between Groups**	**F**	**Sig.**	
Malware (SK_2, SK_5, & SK_6)	6	0.019	1.422	0.208	
PII (SK_3, SK_4, & SK_9)	6	0.025	0.972	0.445	
WIS (SK_1, SK_7, & SK_8)	***6***	***0.030***	***2.218***	***0.043***	*
Overall CSI	6	0.014	1.478	0.187	

* - $p<.05$, ** - $p<.01$, *** - $p<.001$

Data Analysis

Means and Standard Deviations for Gender



Data Analysis

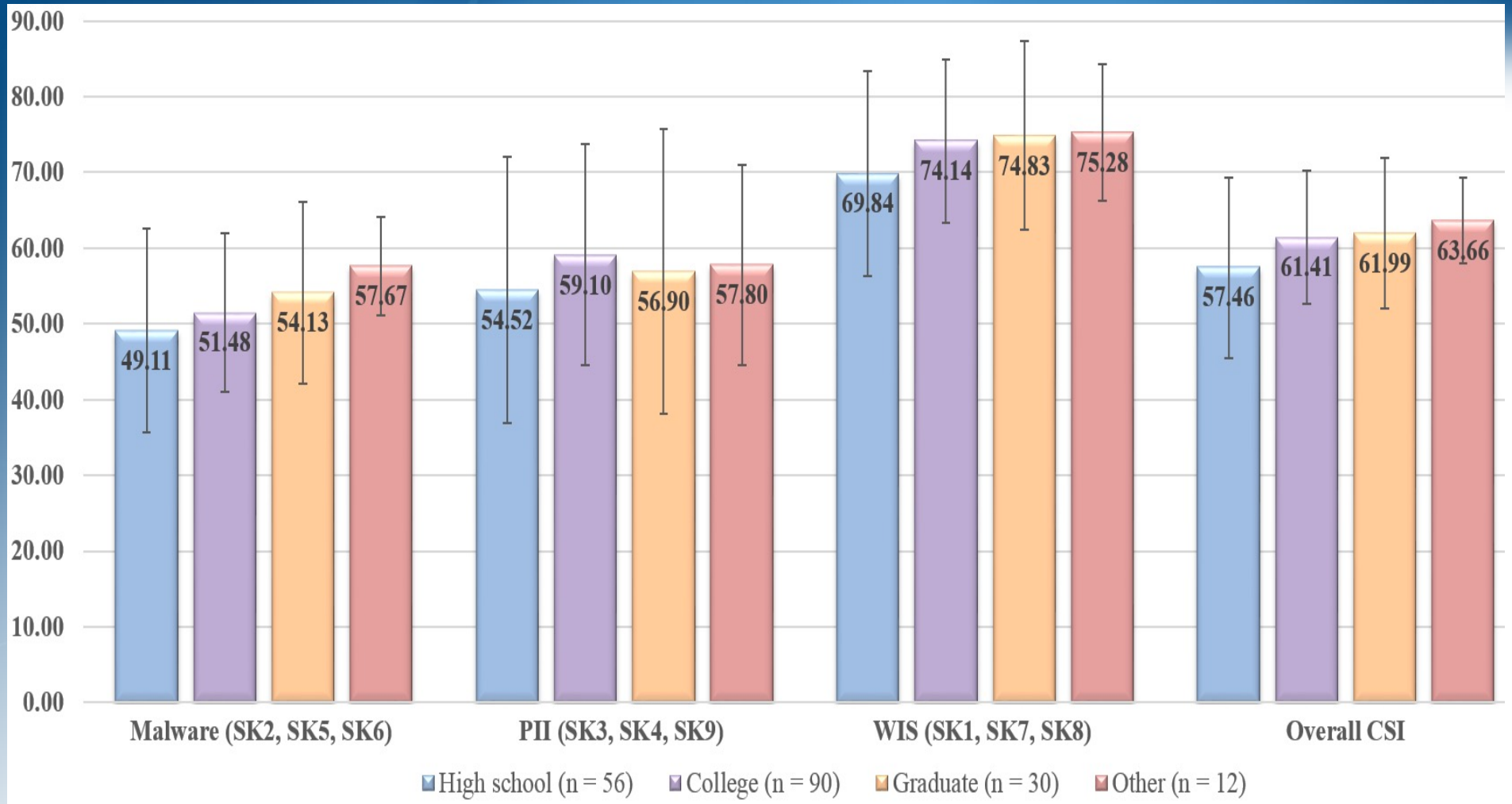
ANOVA Results for Gender

		ANOVA			
Item	**df**	**Mean Square between Groups**	**F**	**Sig.**	
Malware (SK_2, SK_5, & SK_6)	1	0.003	0.224	0.636	
PII (SK_3, SK_4, & SK_9)	1	0.037	1.442	0.231	
WIS (SK_1, SK_7, & SK_8)	***1***	***0.081***	***5.872***	***0.016***	*
Overall CSI	1	0.031	3.158	0.077	

* - $p<.05$, ** - $p<.01$, *** - $p<.001$

Data Analysis

Means and Standard Deviations for Education



Data Analysis

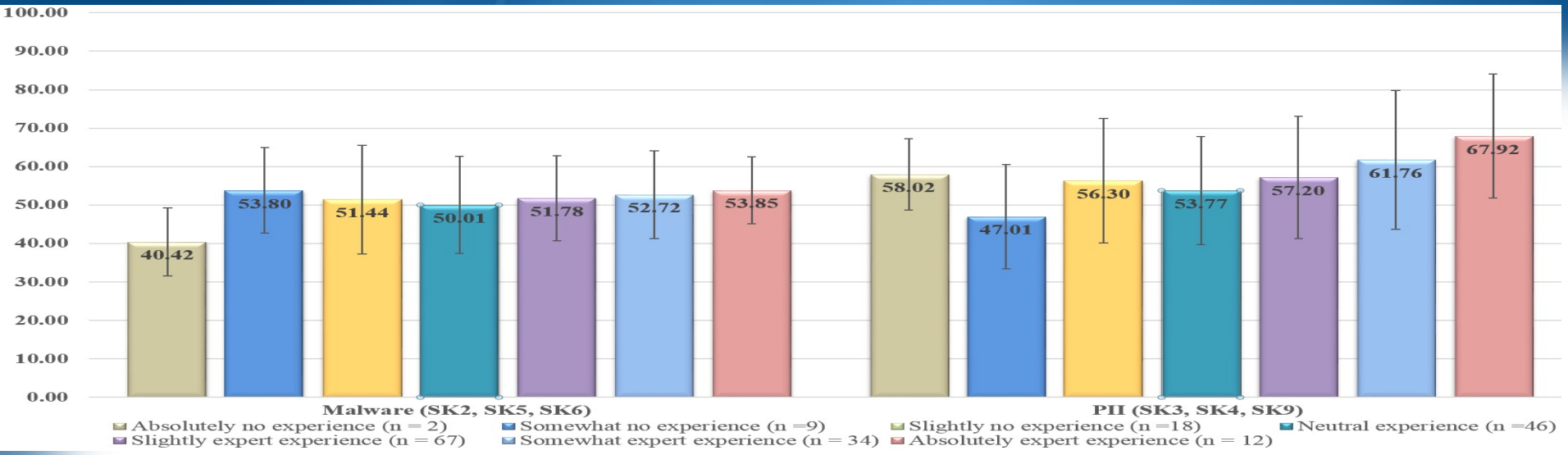
ANOVA Results for Education

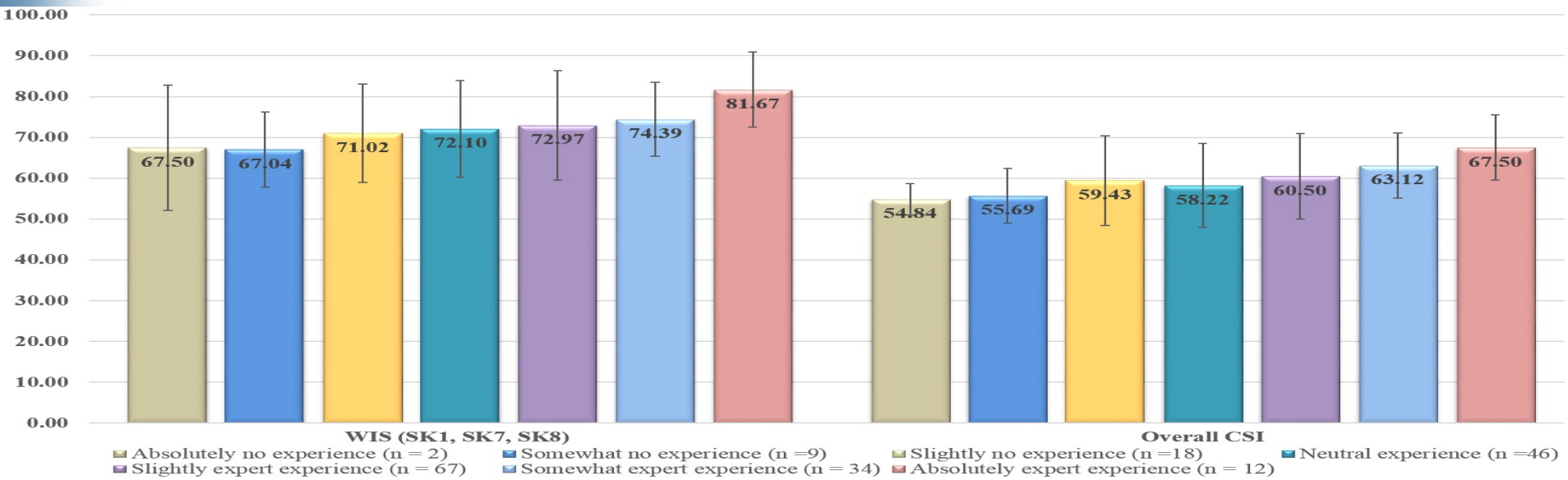
		ANOVA			
Item	**df**	**Mean Square between Groups**	**F**	**Sig.**	
Malware (SK_2, SK_5, & SK_6)	3	0.032	2.461	0.064	
PII (SK_3, SK_4, & SK_9)	3	0.024	0.937	0.423	
WIS (SK_1, SK_7, & SK_8)	3	0.028	2.000	0.115	
Overall CSI	***3***	***0.025***	***2.670***	***0.048***	*

* - $p<.05$, ** - $p<.01$, *** - $p<.001$

Data Analysis

Means and Std. Dev. for Experience Using Technology





Data Analysis

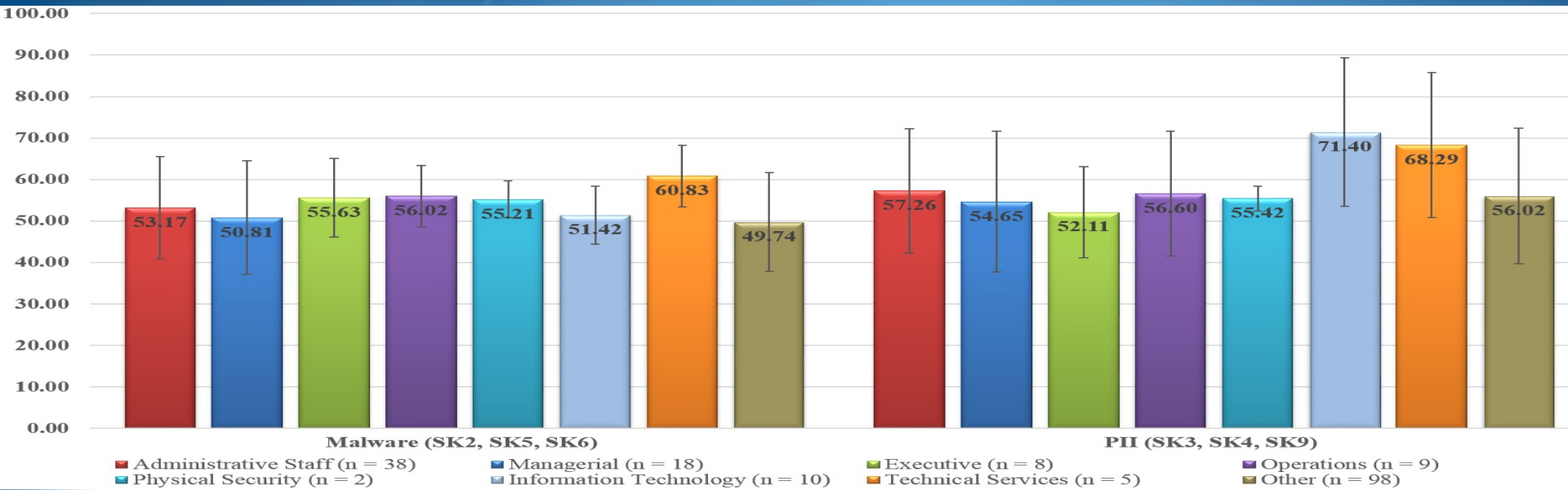
ANOVA Results for Experience Using Technology

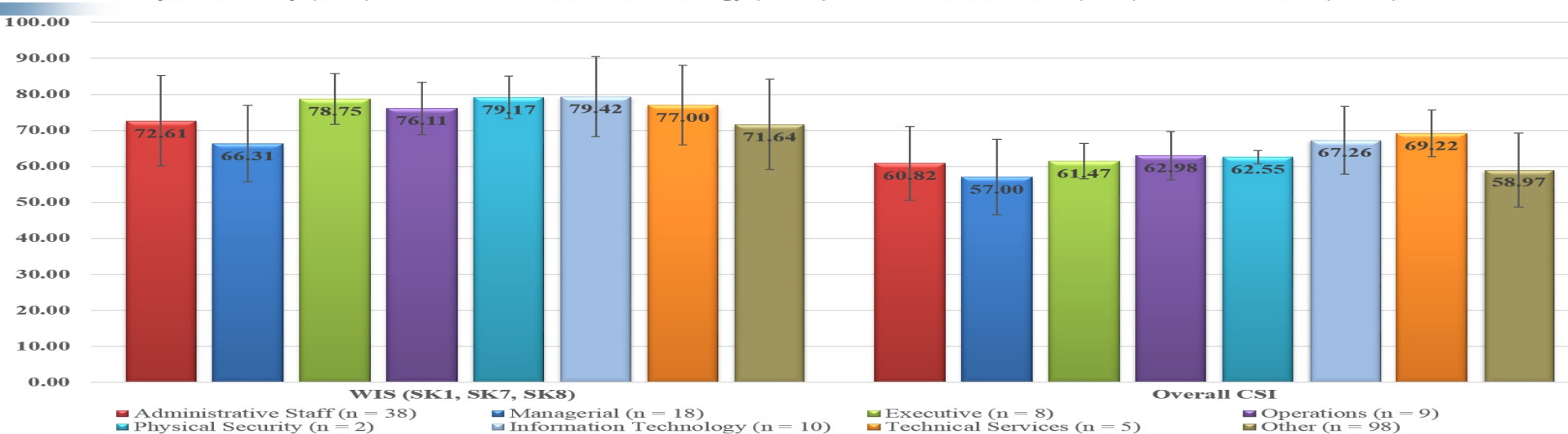
		ANOVA			
Item	**df**	**Mean Square between Groups**	**F**	**Sig.**	
Malware (SK_2, SK_5, & SK_6)	6	0.008	0.625	0.709	
PII (SK_3, SK_4, & SK_9)	***6***	***0.059***	***2.387***	***0.030***	*
WIS (SK_1, SK_7, & SK_8)	6	0.024	1.746	0.112	
Overall CSI	***6***	***0.022***	***2.361***	***0.032***	*

* - $p<.05$, ** - $p<.01$, *** - $p<.001$

Data Analysis

Means and Standard Deviations for Job Function





Data Analysis

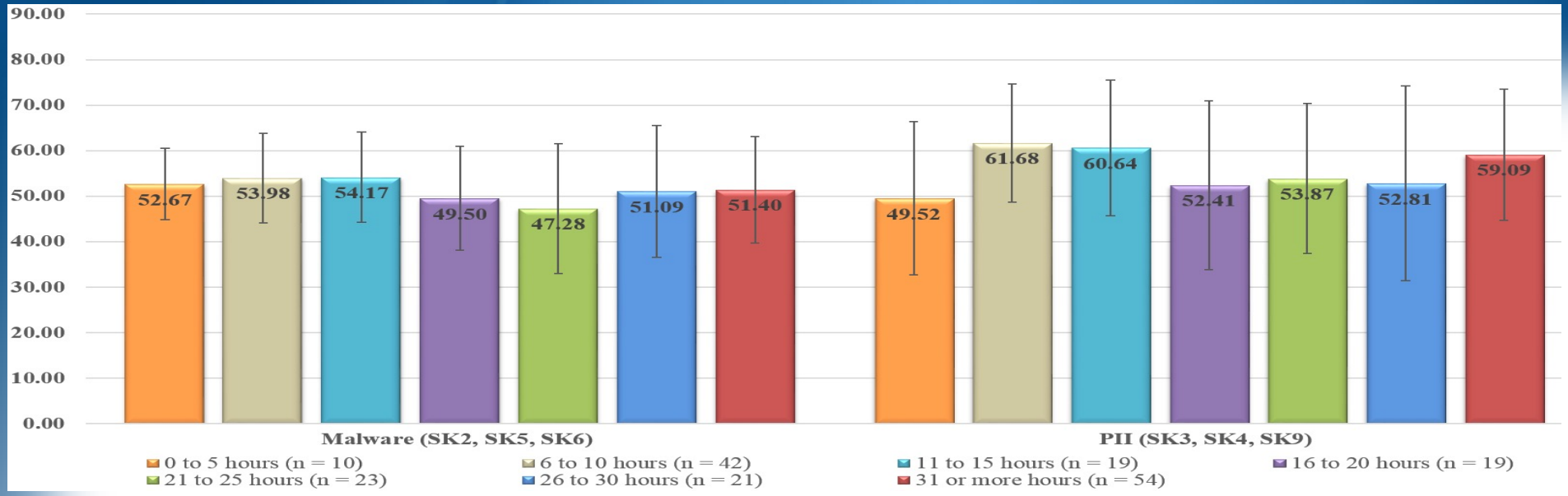
ANOVA Results for Job Function

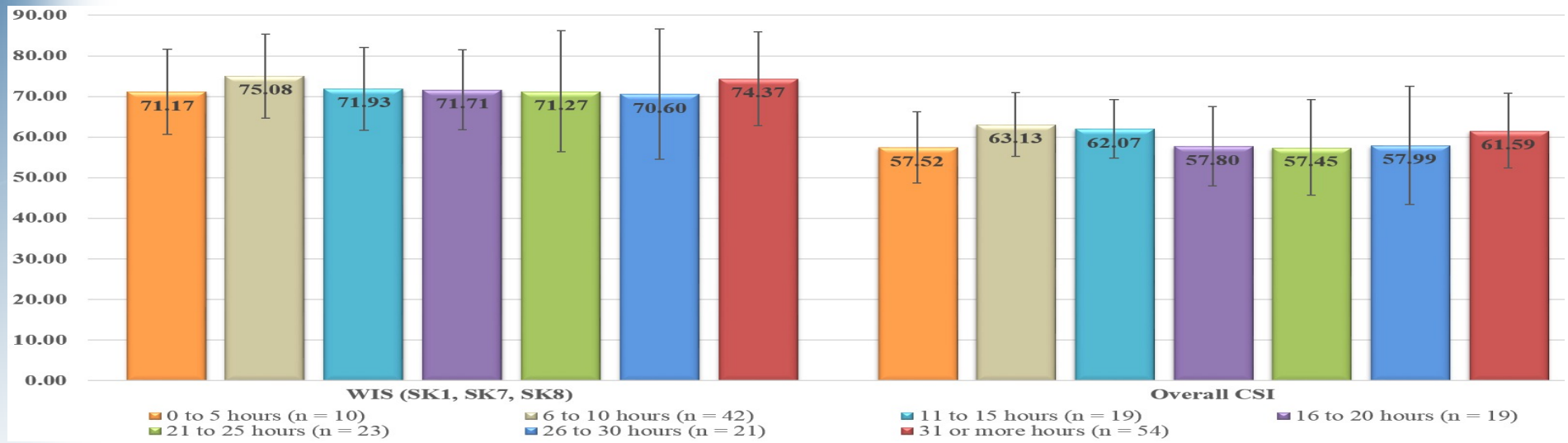
			ANOVA	
Item	**df**	**Mean Square between Groups**	**F**	**Sig.**
Malware (SK_2, SK_5, & SK_6)	7	0.017	1.262	0.271
PII (SK_3, SK_4, & SK_9)	7	0.042	1.683	0.115
WIS (SK_1, SK_7, & SK_8)	7	0.016	1.128	0.347
Overall CSI	7	0.016	1.690	0.113

* - $p<.05$, ** - $p<.01$, *** - $p<.001$

Data Analysis

Means and Std. Dev. for Hours Accessing the Internet





Data Analysis

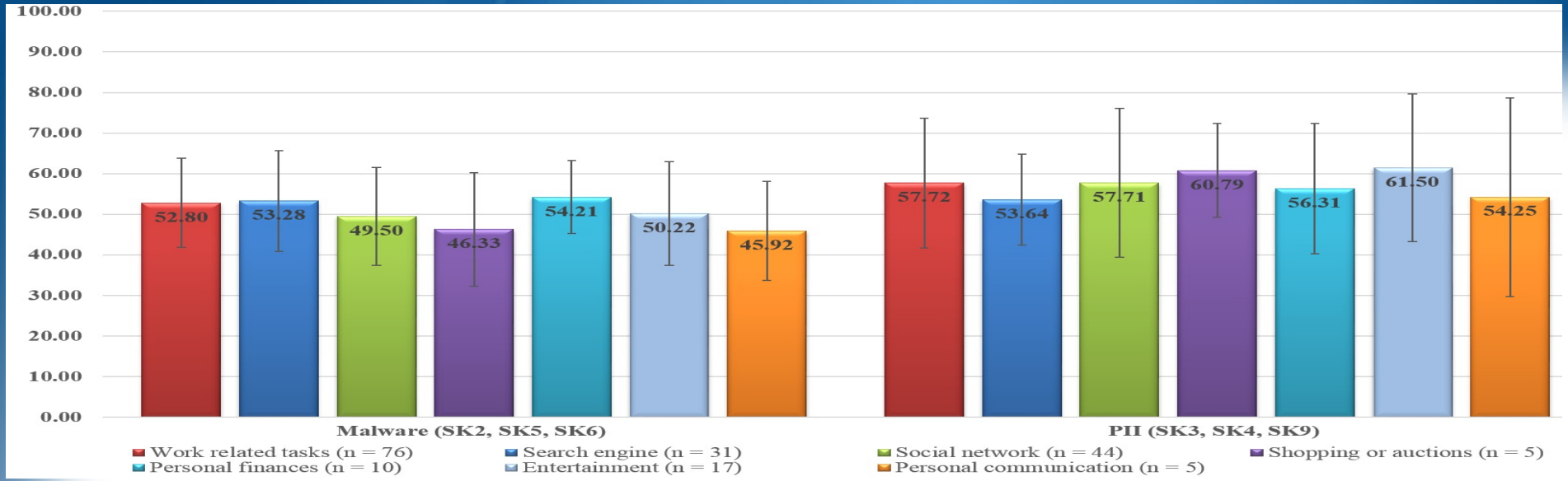
ANOVA Results for Hours Accessing the Internet

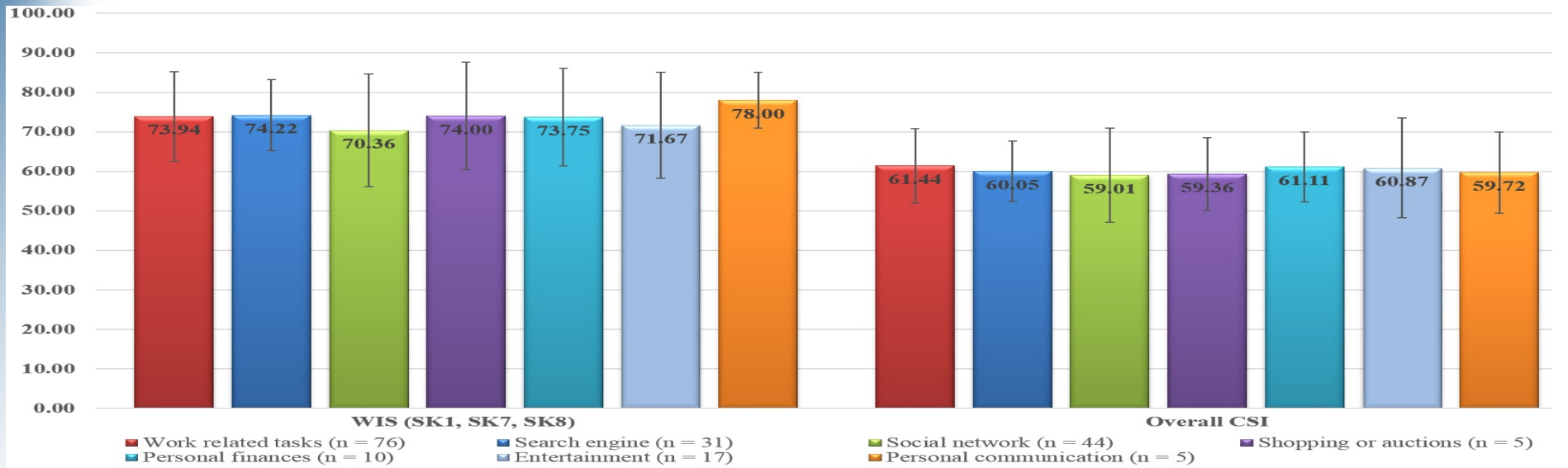
			ANOVA	
Item	**df**	**Mean Square between Groups**	**F**	**Sig.**
Malware (SK_2, SK_5, & SK_6)	6	0.014	1.099	0.364
PII (SK_3, SK_4, & SK_9)	6	0.049	1.939	0.076
WIS (SK_1, SK_7, & SK_8)	6	0.009	0.648	0.691
Overall CSI	6	0.016	1.663	0.132

* - $p<.05$, ** - $p<.01$, *** - $p<.001$

Data Analysis

Means and Std. Deviations for Primary Online Activity





Data Analysis

ANOVA Results for Primary Online Activity

			ANOVA	
Item	**df**	**Mean Square between Groups**	**F**	**Sig.**
Malware (SK_2, SK_5, & SK_6)	6	0.013	0.969	0.447
PII (SK_3, SK_4, & SK_9)	6	0.014	0.537	0.779
WIS (SK_1, SK_7, & SK_8)	6	0.009	0.678	0.667
Overall CSI	6	0.003	0.304	0.934

* - $p<.05$, ** - $p<.01$, *** - $p<.001$

Data Analysis

- RQ1: Literature review and expert panel
- RQ2: Literature review and expert panel
- RQ3: Validating CSI benchmarking index
  - Expert panel and pilot-test
- RQ4: Test the level of cybersecurity skills
- RQ5: Descriptive and one-way Analysis of Variance
  - Age
  - Gender
  - Education
  - Job function
  - Experience using technology
  - Primary activity
  - Hours online

Contributions & Implications

- Notable to the IS body of knowledge
- Provides insight for researchers and practitioners
  - Understanding an employee's cybersecurity skills level is critical to securing information and the systems that stores it
  - Assessing the cybersecurity skills level of non-IT professionals
  - Assist in the mitigation of threats due to vulnerabilities and breaches caused by non-IT professionals

Future Research

- Widen the recruitment community to increase generalizability
- Specific population to determine if the CSI level of a supervisor affects the CSI of a subordinate
- Organizational culture effects on CSI level of its employees
- Investigation of the effects of behaviors (i.e., curiosity, boredom, etc.) or emotions
- Replicated as a video presentation using an audience response system

Thank you . . .

Questions?

NSU NOVA SOUTHEASTERN UNIVERSITY