College of Computing
and Engineering
NOVA SOUTHEASTERN UNIVERSITY | **NSU** Florida

Challenges and future path for valid research in the human factor of cybersecurity

Dr. Yair Levy, Professor of IS & Cybersecurity

Department of Computing

Director, Center for Information Protection, Education, and Research (CIPhER) (https://infosec.nova.edu/)

College of Computing and Engineering (https://computing.nova.edu/)

2025 CAE Community Symposium

Research on the 'Human Factor' in Cybersecurity

- Types of research on 'Human Factor' in Cybersecurity
  - Theoretical research
  - Applied research (developmental research & experimental research)
- Challenges in conducting research on Human Factor in Cybersecurity
  - Actual measures
  - Actual data
- Research validity

Direct vs. Indirect Measures in 'Human Factor' of Cybersecurity

College of Computing and Engineering
NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

Thermometer

Pyrometer

vs.

2025 CAE Community Symposium

Research on the Human Factor in Cybersecurity (Cont.)

College of Computing and Engineering
NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

- ***AVOID *** "Intention to X" studies!
- "Behavioral compliance intentions with ISP" or "Intention to comply with X" or "Computer misuse intentions"
    1. *"I would follow the advice in the corporate message to reduce my risk of private information theft*
    2. *I would pay closer attention to similar instructions to prevent information theft*
    3. *I would take the steps necessary to protect myself to avoid private data theft"* (Zhang & Borden, 2019)

Zhang, X. A., & Borden, J. (2019). How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises. *Journal of Risk Research*, 22(1), 1–17.

Publisher: Routledge Taylor & Francis

Research on the Human Factor in Cybersecurity (Cont.)

College of Computing and Engineering
NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

Item	Original Construct Items	DL Adjusted Items by Levy
1.	"I would follow the advice in the corporate message to reduce my risk of private information theft"	"I would follow the advice in the DMV handbook to reduce my risk of car accidents"
2.	"I would pay closer attention to similar instructions to prevent information theft"	"I would pay closer attention to similar instructions to prevent car accidents"
3.	"I would take the steps necessary to protect myself to avoid private data theft"	"I would take the steps necessary to protect myself to avoid car accidents"

Research on the Human Factor in Cybersecurity (Cont.)

Item	Original Construct Item	Adjusted Items by Levy
1.	"I would follow the advice ... the corporate ... to ... reduce my risk ... private ... information ... ft"	I would ... llow the advice in the ... DMV ha... ok to reduce my risk ... ca... ...ts"
2.	"I would pay ... oser attenti... similar instru... ons to pr... information t..."	...uld pay ... ser attention to ... ...n instr... ons to prevent car ...id...ts"
3.	"I would take th... ps necessary to prot... ... to avoid private data the..."	...ould ... e the steps necessary ... r... ...t myself to avoid car ...nts"

Levy CyLAB

The research in our laboratory focuses on the *human-centric* lens of all three cybersecurity pillars with increased emphasis on addressing the following key research areas and their interconnections:

- Cybersecurity threat mitigation
- Social-Engineering/Human Factor in Cybersecurity
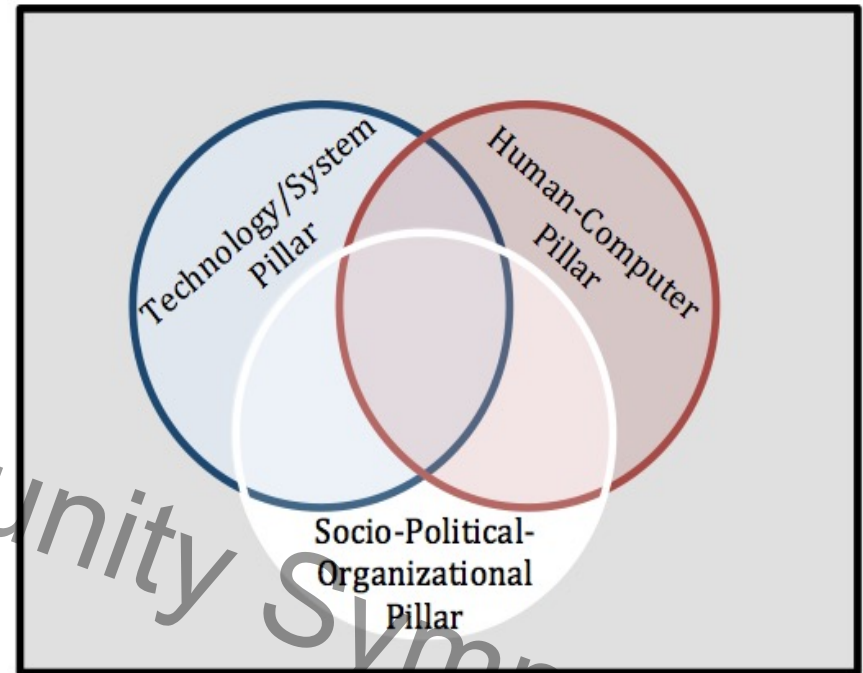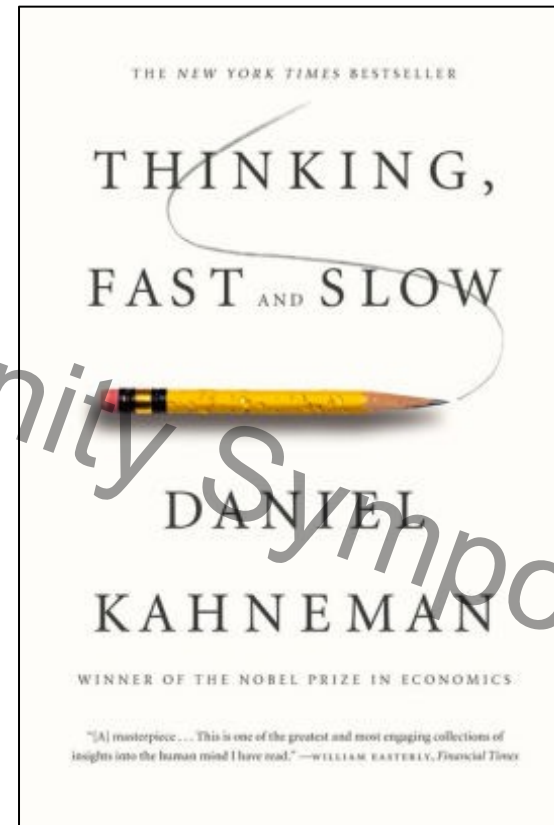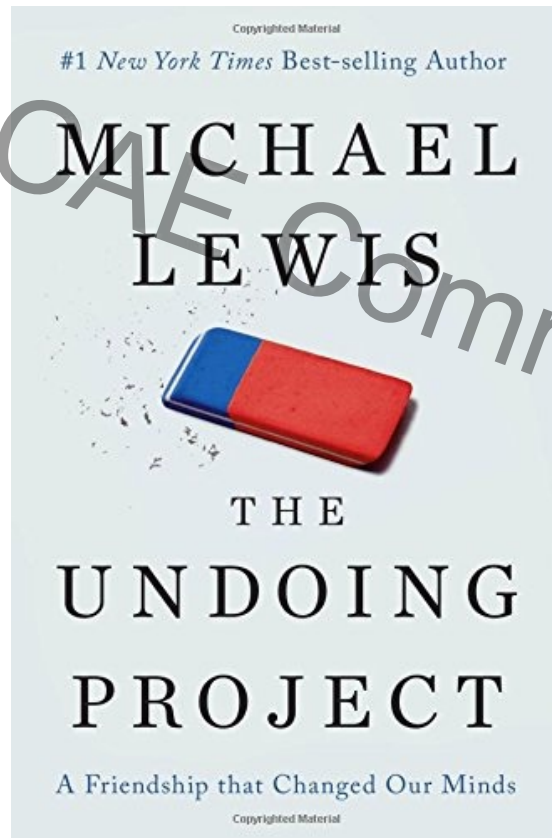- User-authentication

Figure 1: The Cybersecurity Landscape

https://infosec.nova.edu/cylab/

Human-Centric "lens" of Cybersecurity?

Some Theoretical Foundation:

College of Computing
and Engineering
NOVA SOUTHEASTERN UNIVERSITY | **NSU** Florida
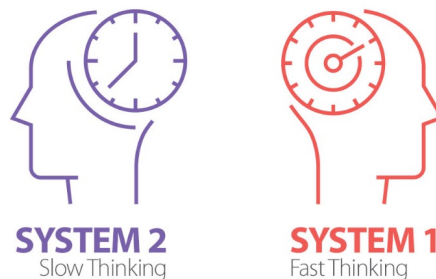
Dr. Daniel Kahneman

An Israeli-American psychologist notable for his work on the psychology of judgment and decision-making, as well as behavioral economics, for which he was awarded the **2002 Nobel Prize in Economic Sciences** (shared with Vernon L. Smith). His empirical findings challenge the assumption of human rationality prevailing in modern economic theory. With **Amos Tversky** and others, Kahneman established a cognitive basis for common human errors that arise from heuristics and biases.
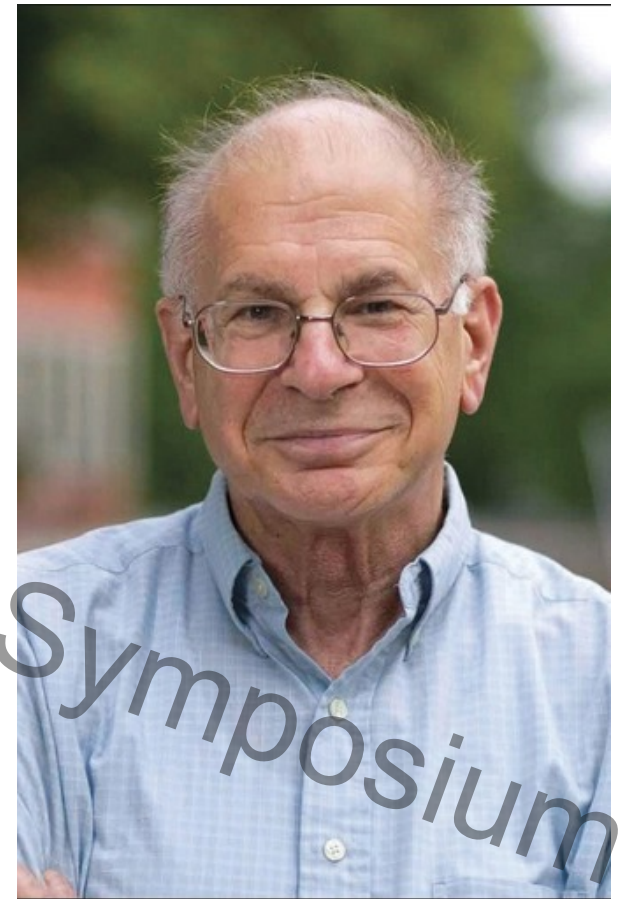
1934-2024
Princeton University

SYSTEM 2 Slow Thinking

SYSTEM 1 Fast Thinking

College of Computing
and Engineering
NOVA SOUTHEASTERN UNIVERSITY

NSU
Florida

System 1 vs. System 2 Thinking

System 1 vs. System 2 Thinking
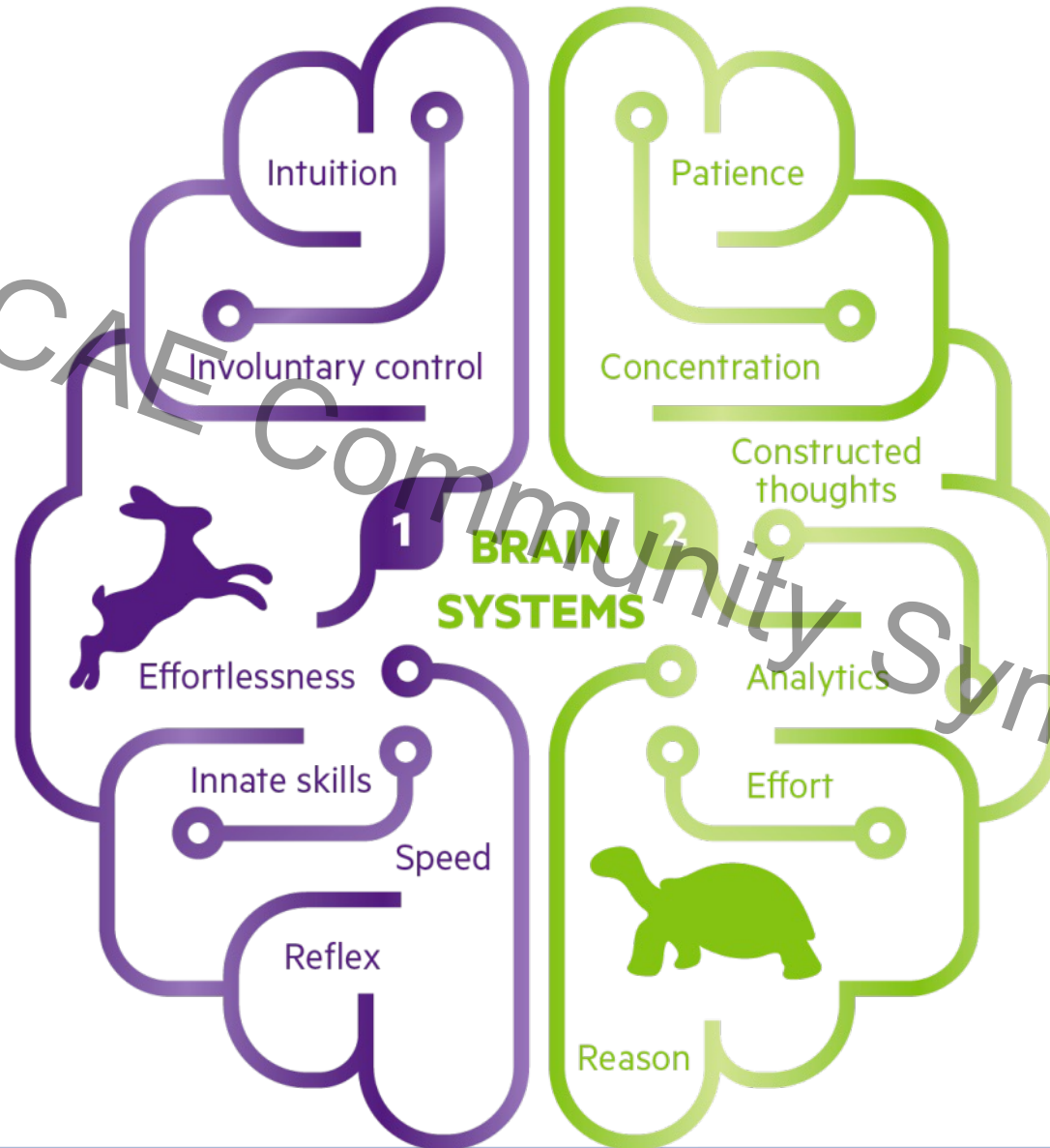
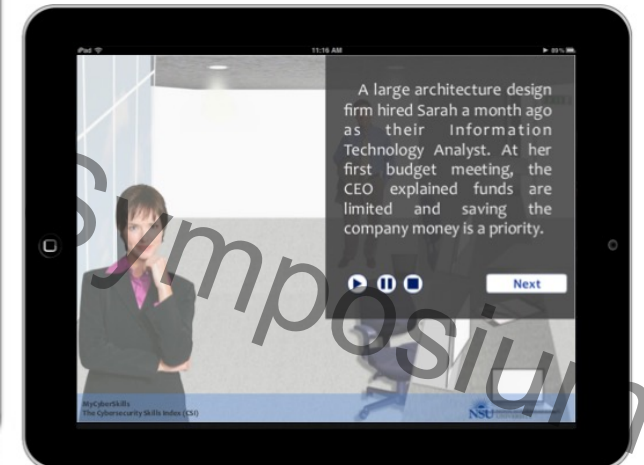# Measuring Cybersecurity Skills

College of Computing and Engineering
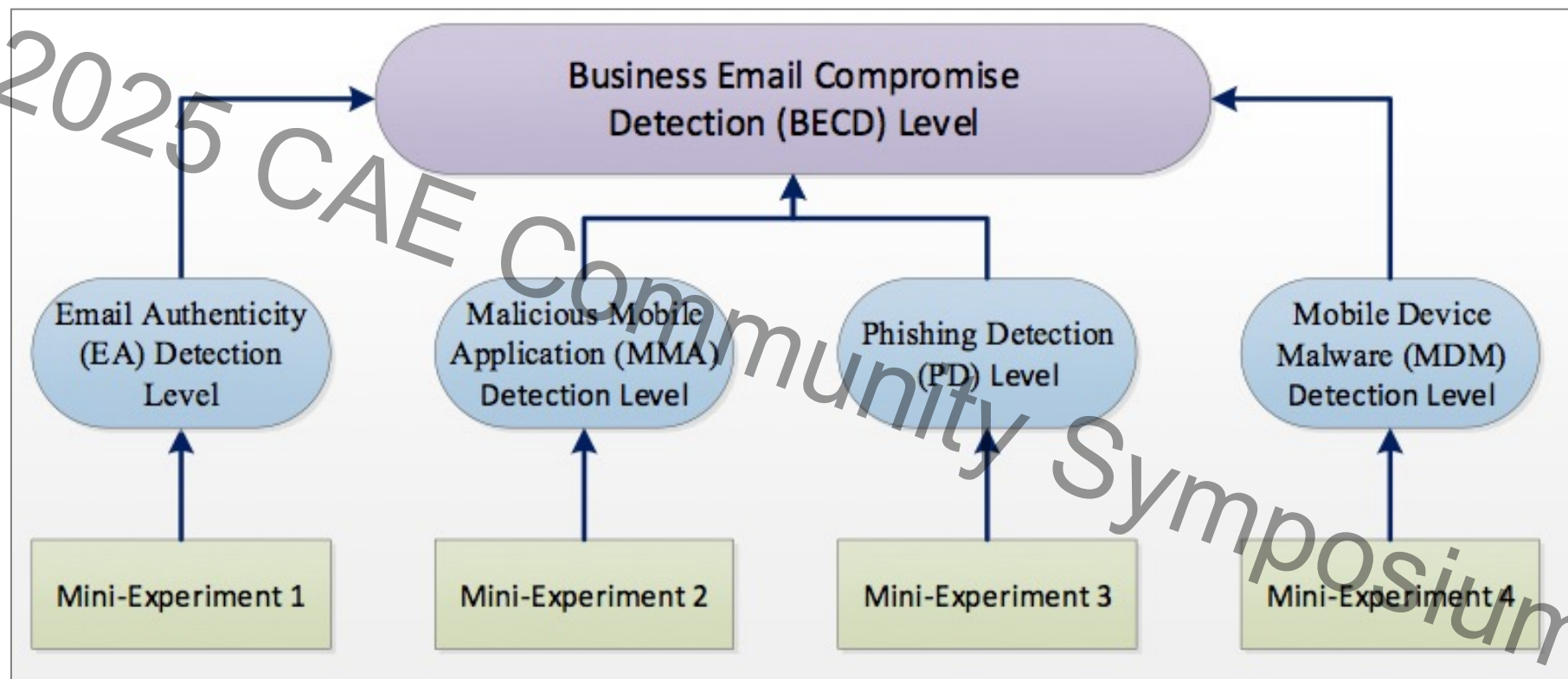NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

Melissa Carlton, Ph.D. - Huston Buptist University - Assistant Professor
Dissertation title (2016): *"Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills"*

Detecting Business E-mail Compromise (BEC)

College of Computing and Engineering
NOVA SOUTHEASTERN UNIVERSITY | **NSU** Florida

http://becd.app/

Business Email Compromise Detection (BECD) Level

Email Authenticity (EA) Detection Level

Malicious Mobile Application (MMA) Detection Level

Phishing Detection (PD) Level

Mobile Device Malware (MDM) Detection Level

Mini-Experiment 1

Mini-Experiment 2

Mini-Experiment 3

Mini-Experiment 4

Shahar (Sean) Aviv, Ph.D. - ExcelNet.com
Dissertation title (2019): *"An Examination of User Detection of Business Email Compromise Amongst Corporate Professionals"*

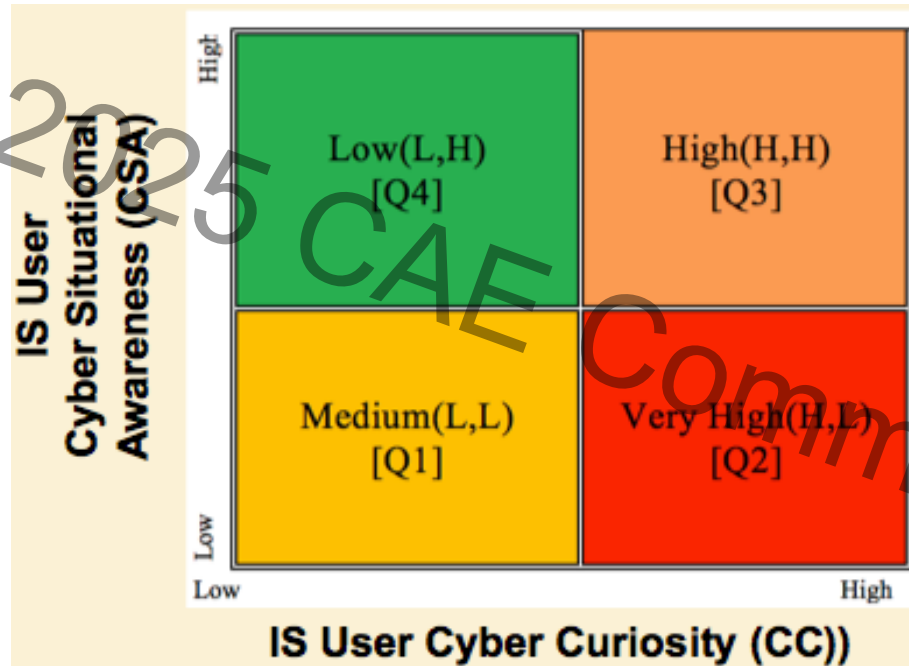# Cyber Situational vs. Curiosity as Measure of Risk

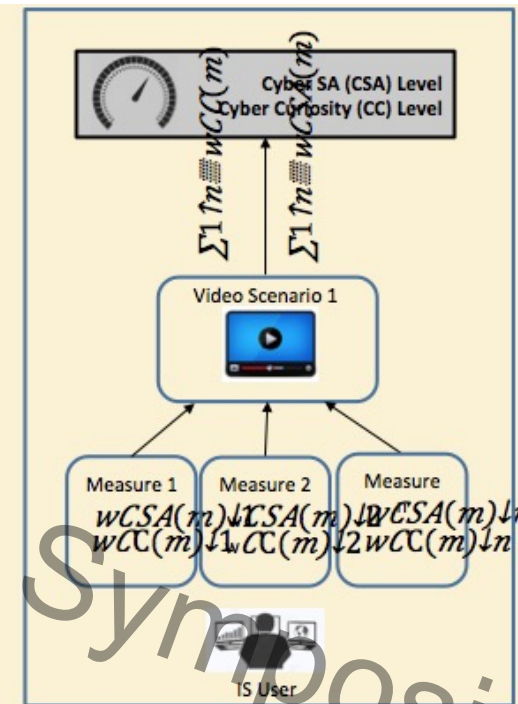Figure 3 User cyber SA and cyber curiosity cyber risk taxonomy

Figure 4. Conceptual design of the cyber SA and cyber curiosity measurement approach

Guillermo (Will) Perez, Ph.D. - Royal Caribbean Cruises

Dissertation title (2019): "*Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry*"

Types of Human Error in Large Data Breaches

OH SHOOT!

Price Waterhouse Coopers database

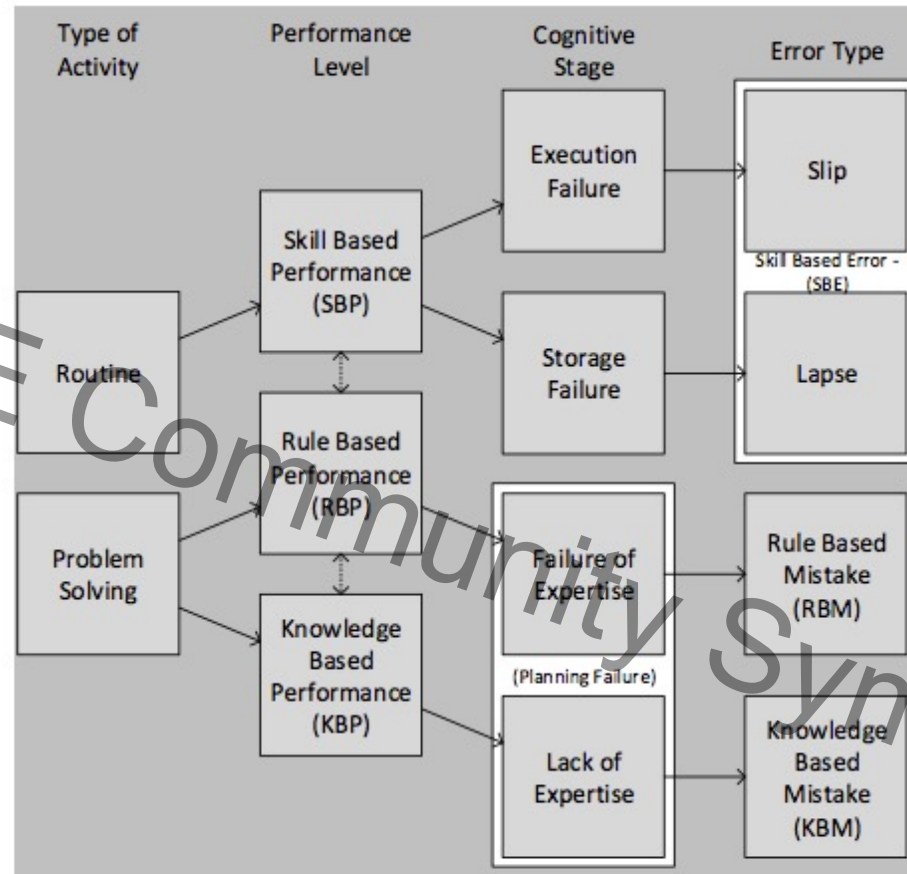Figure 1: Generic Error-Modeling System (GEMS) adapted from Reason (1990)

Type of Activity → Performance Level → Cognitive Stage → Error Type

- Routine → Skill Based Performance (SBP) → Execution Failure → Slip
- Skill Based Performance (SBP) → Storage Failure → Skill Based Error - (SBE) → Lapse
- Problem Solving → Rule Based Performance (RBP) → Failure of Expertise → Rule Based Mistake (RBM)
- Problem Solving → Knowledge Based Performance (KBP) → (Planning Failure) → Lack of Expertise → Knowledge Based Mistake (KBM)
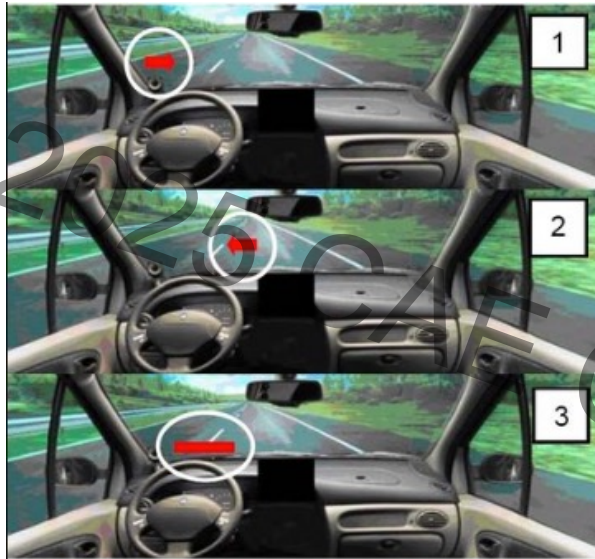
Gabriel Cornejo, Ph.D. - DoD
Dissertation title (2021): *"Human Errors in Data Breaches: An Exploratory Configurational Analysis"*

Audio, Visual, and Haptics Alerts and Warnings

Molly Cooper, Ph.D. - Associate Professor - Ferris State University
Dissertation title (2021): "*Assessment of Audio and Visual Warnings to Mitigate Risk of Phishing Attacks*"

Pause for a Cybersecurity Cause

The single-use timer that will wholesale for about a dollar is designed to make a nurse's life easier. Photo: David Tenenbaum

NSU Security WARNING: This is an external email. Do not click links or open attachments unless you recognize the sender and know that the content is safe.

OH SHOOT!

Amy Antonucci, Ph.D. - Western Governors University
Dissertation title (2021): *"Pause for a Cybersecurity Cause: Assessing the Influence of a Waiting Period on User Habituation in Mitigation of Phishing Attacks"*

Judgment Errors: Environment & Device Type

OH SHOOT!

Social Engineering Attack Type

Phishing

PMSER

	Environment		
Device	**Mobile Phone**	Distracting: Distracted via Mobile Phone	Non-Distracting: Not Distracted via Mobile Phone
	Computer	Distracted via Computer	Not Distracted via Computer

	Environment		
Device	**Mobile Phone**	Distracting: Distracted via Mobile Phone	Non-Distracting: Not Distracted via Mobile Phone
	Computer	Distracted via Computer	Not Distracted via Computer

Figure 1. Proposed 2x2x2 Experimental Design Taxonomy of Device (Mobile Phone/Computer) vs. Environment (Distracting/Non-Distracting) vs. Social Engineering Attack Type (Phishing/PMSER)

Tommy Pollock, Ph.D. - National Defense University (NDU)
Dissertation title (2022): "*Experimental Study to Assess the Role of Environment and Device Type on the Success of Social Engineering Attacks: The Case of Judgment Errors*"

Comparing social engineering prevention methods

OH SHOOT!

KnowBe4
Human error. Conquered.

Randomized Quasi-Experimental Groups

|		Phishing Campaign Method	
		Industry-standard phishing campaign	Red Team phishing campaign
Phishing Training Method	An annual industry-standard phishing awareness training	30 end user random sample for pilot study	30 end user random sample for pilot study
	Continuous customized social engineering focused training	30 end user random sample for pilot study	30 end user random sample for pilot study
	No training - Control	30 end user random sample for pilot study	30 end user random sample for pilot study

Jackie (Chris) Scott, Ph.D. - AirSculpt Technologies
Dissertation title (2023): "*Comparing social engineering prevention methods and their role on successful malicious emails in corporations*"

Remote Workers' Cyberslacking and Computer Security Posture
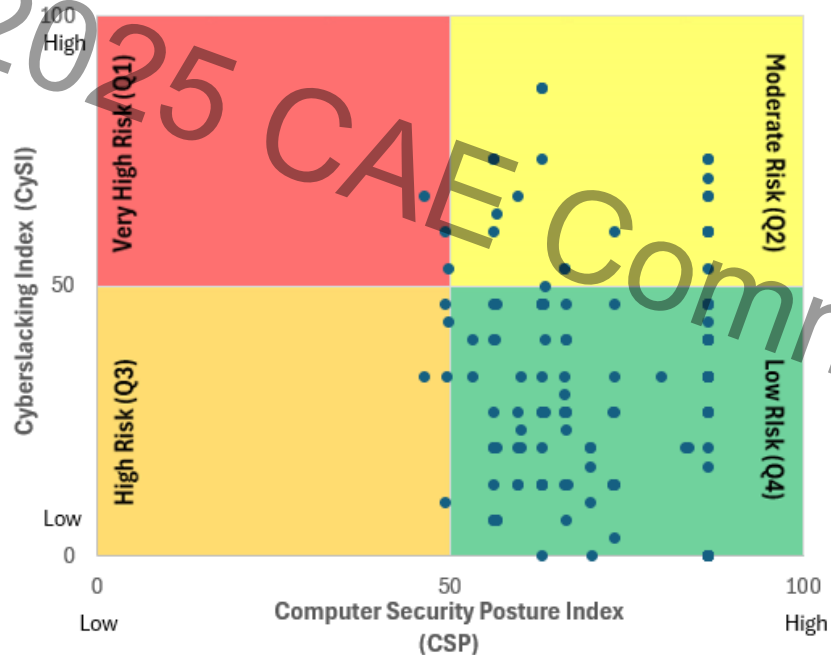
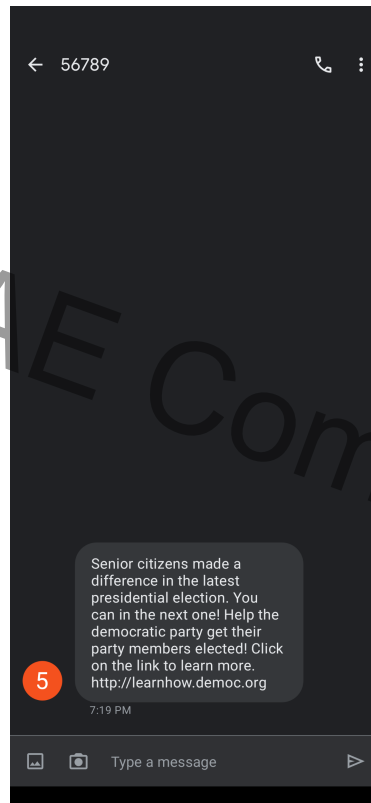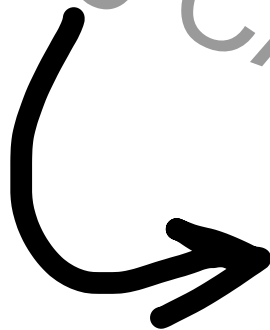| PMID	Indicator
CSP01	Operating System Version
CSP02	Operating System Patching (systems are up to date)
CSP03	Antivirus/Malware Detection programs
CSP04	Antivirus/Malware signature updates
CSP05	Software Updates
CSP06	Disk Encryption Enabled
CSP07	Firewall Enabled
CSP08	VPN Update
CSP09	Collection of security logs
CSP10	End Point Protection

Ariel Luna, Ph.D. - Microsoft
Dissertation title (2024): *"Empirical Assessment of Remote Workers' Cyberslacking and Computer Security Posture to Assess Organizational Cybersecurity Risks"*
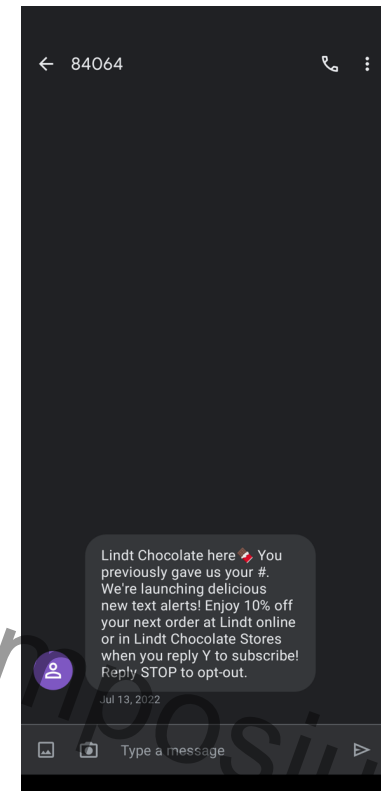
Senior Citizen's Susceptibility to SMiShing

SMiShing
(Social Proof)

Legitimate

> 56789
>
> Senior citizens made a difference in the latest presidential election. You can in the next one! Help the democratic party get their party members elected! Click on the link to learn more. http://learnhow.democ.org
>
> 7:19 PM

> 84064
>
> Lindt Chocolate here 🍫 You previously gave us your #. We're launching delicious new text alerts! Enjoy 10% off your next order at Lindt online or in Lindt Chocolate Stores when you reply Y to subscribe! Reply STOP to opt-out.
>
> Jul 13, 2022

Brian Bisceglia, Ph.D. - Worcester Police Department & FBI Boston
Dissertation title (2024): "*An Empirical Assessment on the Role of Persuasion Principles and Cybersecurity Skills Training on Senior Citizens' SMiShing Susceptibility*"

Cybersecurity Competencies Through Human-Guided Generative Artificial Intelligence (GenAI)

College of Computing and Engineering
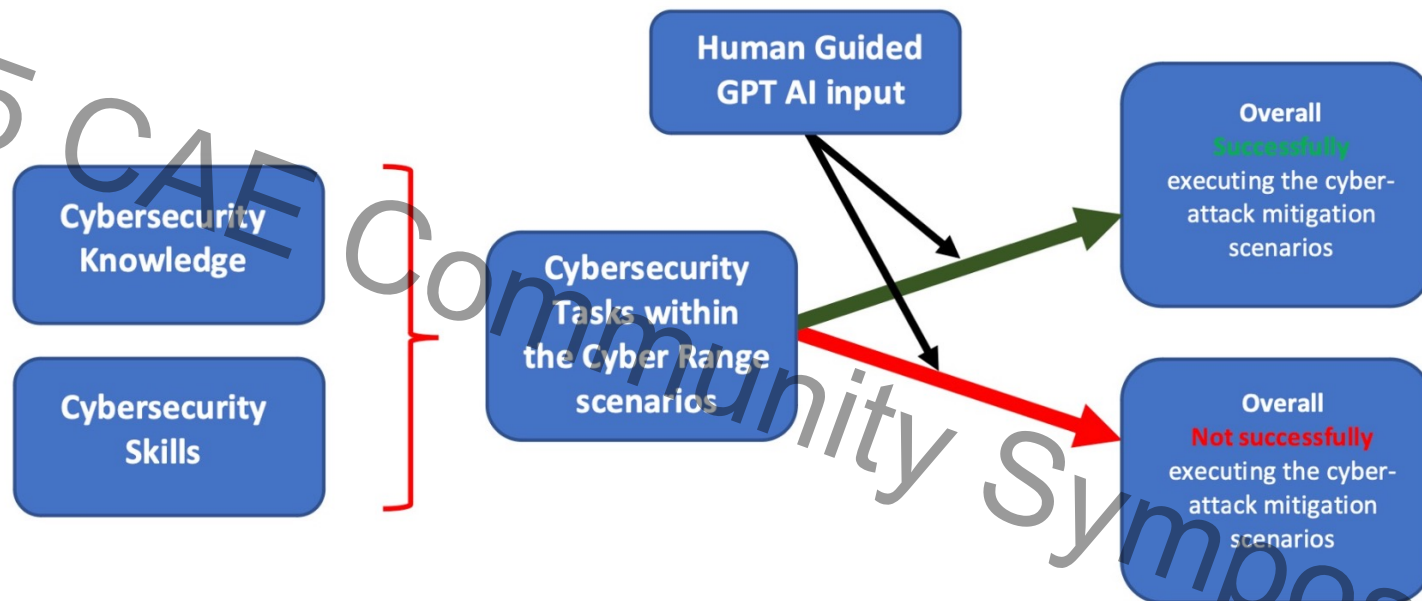NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

Figure 1. Conceptual Model for the Intervening Effect of Human-Guided GPT AI Input on Foundational Cybersecurity Competencies

Dariusz Witko, Ph.D. Student
Dissertation title: *"Empirical Assessment of Cybersecurity Competencies Through Human-Guided Generative Artificial Intelligence (GenAI)"*
dw1272 AT mynsu.nova.edu

- Questions?
- Discussion

CYBERSECURITY
Everyone's job!