IISE ANNUAL CONFERENCE & EXPO 2024

Understanding the Impact of Poll Worker Cybersecurity Behaviors on U.S. Election Integrity

Abigail Kassel[1], Isabella Bloomquist[1], Natalie M. Scala[1], **Josh Dehlinger**[2]

[1]*Department of Business Analytics & Technology Management*
[2]*Department of Computer & Information Sciences*
Towson University

About Us

- Empowering Secure Elections Research Lab at Towson University
  - Non-partisan, interdisciplinary research lab focused understanding the risks to election processes and developing mitigations to the cyber, physical, and insider risks that can arise
  - Partnered with Maryland Boards of Elections to develop targeted, poll worker training modules to develop awareness of threats in elections processes and equipment
  - 2020 U.S. Elections Assistance Commission Clearinghouse Award for Outstanding Innovation in Election Cybersecurity and Technology
  - Analyzed risks to mail-based voting processes, updated the EAC's attack tree, and were the first to develop a relative risk assessment for U.S. elections (Scala et al., 2022)
    - Demonstrated that mail-based voting increases voter access and disincentivizes attacks from adversaries

Motivation

How do we ensure their votes count as they intended?

How do we ensure elections are secure?

Motivation

Election day vote counts have fallen in key races; officials cite human error

Emily Sullivan 5/17/2024 3:07 p.m. EDT, Updated 5/17/2024 5:10 p.m. EDT

Motivation and Context

- Senate Intelligence Committee (2019): Election systems in all 50 states targeted in 2016
- Robert S. Mueller, III (2019): Interference ongoing
- Director of National Intelligence (2020): Iran and Russia obtained US voter registration information
- Little election security research at the local level
- Inventories of vulnerabilities and known incidents
- Poll workers as a trusted insider threat not addressed
- Election infrastructure designated as national critical infrastructure (2017)

Who are the People at a Polling Place?

Poll workers *are* *trusted insiders!*

Investigation Questions

Goal: Examine the efficacy of poll worker training to mitigate election threats and understand the relationship between training results and poll worker personal security behaviors.

1. How does personal cybersecurity behavior (i.e., cyber hygiene) for a poll worker predict training outcome?
2. Are the predictions and corresponding strength moderated by demographics?
3. What are the election security policy implications of these results?

Training Modules

- Iteratively developed, validated and piloted seven training modules specific to election judge processes:
  - **Pollbook, Scanning Unit, and Provisional voting**
- Online education/training modules have been shown to be:
  - An easy and effective means to integrate new knowledge into existing courses/training
  - Appropriate learning tools for diverse learners
  - A re-usable and extensible resource that can be used/adapted in other precincts/states

Research Approach

Poll workers in a large mid-Atlantic county were sent the SeBIS survey.

Poll workers were then sent three training modules: Scanning Units Module, Electronic Pollbooks Module, and Provisional Voting Module

Poll workers were then sent a quiz after completing each training module.
The quiz they received was based on their respective training module and knowledge that was covered in the module.

Completed an analysis of SeBIS survey results and quiz scores to determine the relationship between poll workers' security behavior and training.

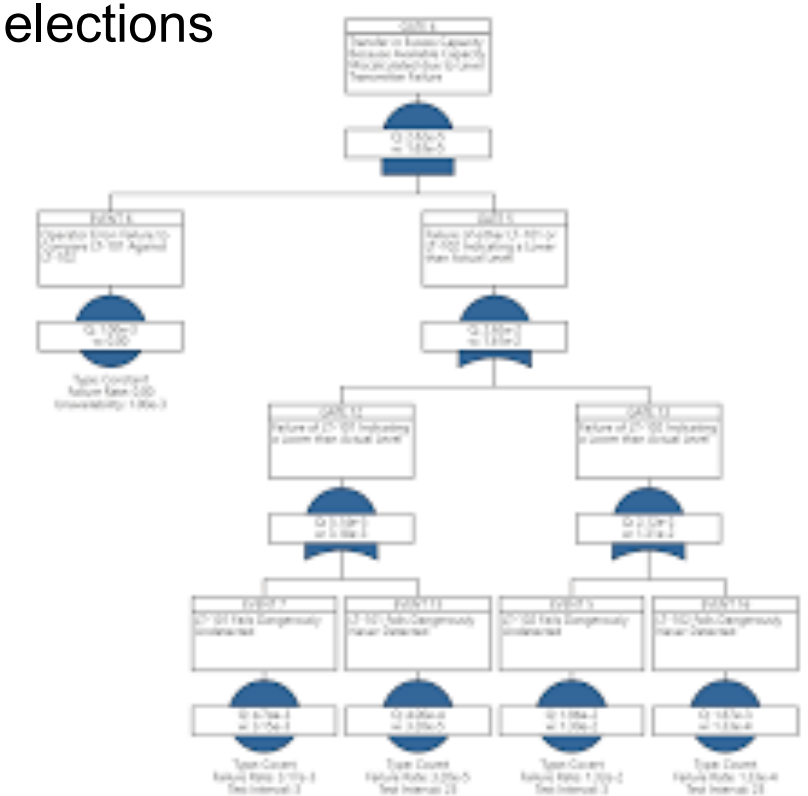
Security Behaviors and Intentions Scale Inventory

SeBIS Inventory Questions	
Device Securement	
F1	I set my computer screen to automatically lock (i.e., sleep) if I don't use it for a prolonged period of time.
F2	I use a password/passcode to unlock my laptop or tablet.
F3	I manually lock my computer screen when I step away from it.
F4	I use a PIN or passcode to unlock my mobile phone.
Password Generation	
F5	I do not change my passwords, unless I have to.
F6	I use different passwords for different accounts that I have.
F7	When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.
F8	I do not include special characters in my password if it's not required.
Proactive Awareness	
F9	When someone sends me a link, I open it without verifying where it goes.
F10	I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.
F11	I submit information to websites without first verifying that it will be sent securely (e.g., SSL, https, a lock icon).
.F12	When browsing websites, I mouse over links to see where they go, before clicking them.
F13	If I discover a security problem, I continue what I was doing because I assume someone else will fix it.
Updating	
F14	When I'm prompted about a software update, I install it right away.
F15	I try to make sure that the programs I use are up-to-date.
F16	I verify that my anti-virus software has been regularly updating itself.

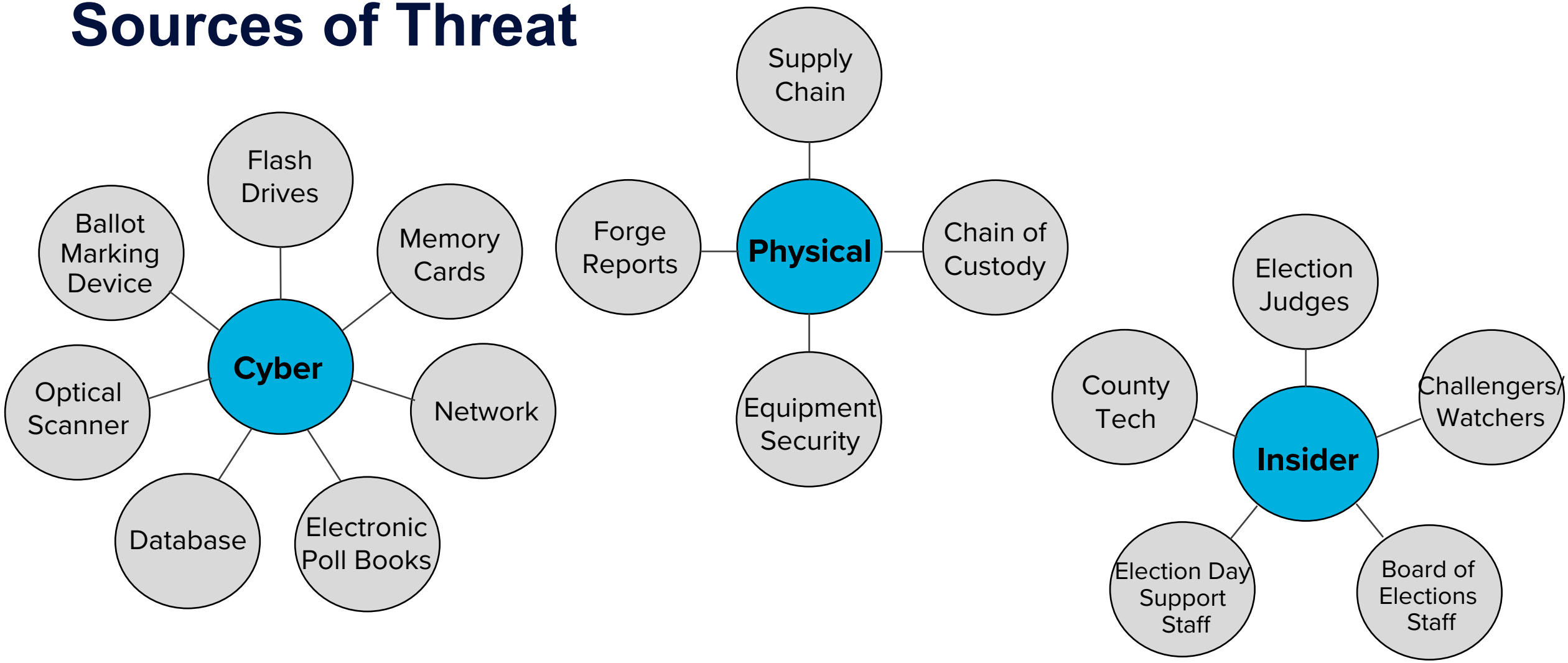
- Validated and accepted by the usable security community to create characterizations based on the respondents' level of cyber and computer security knowledge and savvy
- Measures participant intentions related to security and how those intentions may vary between individuals; it does not measure or predict actual behavior
- Solicited 230 valid responses from previous/current poll workers for analysis

Systemic Threats

- First academic team to define threats systemically in elections
- Framing extends beyond elections
- Cyber
  - Digital machines and media
  - Regardless of Internet connection
- Physical
  - Tampering with or disrupting equipment
- Insider
  - Adversaries and insiders
  - Simple, honest mistakes
  - Deliberate actions with ill-harm effects

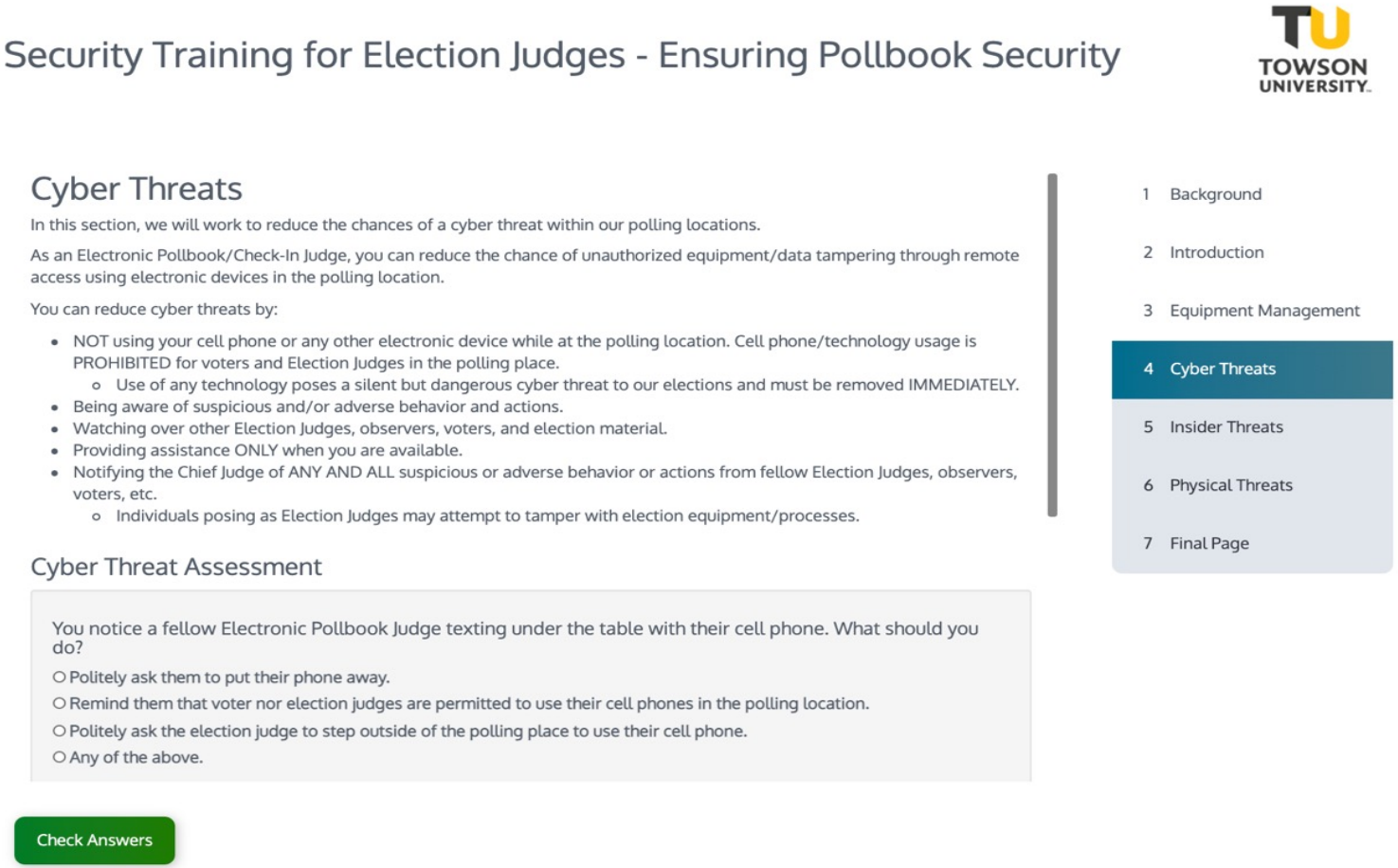


Sources of Threat



Training Modules

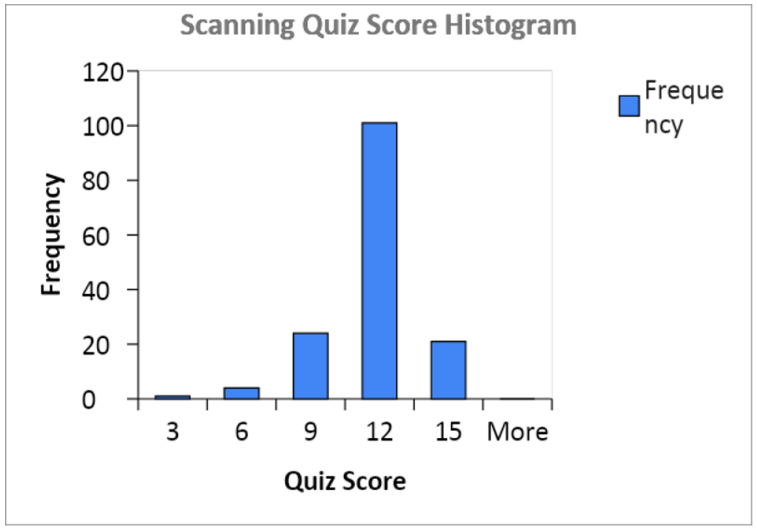
- Sections
  - Equipment use
  - Cyber threats
  - Insider threats
  - Physical threats
  - Self assessments
- Pedagogy
  - Segmentation
  - Interactivity

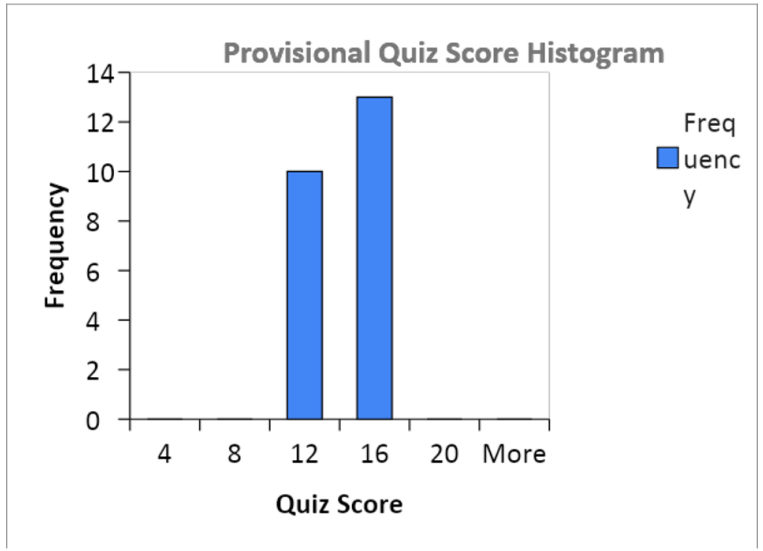


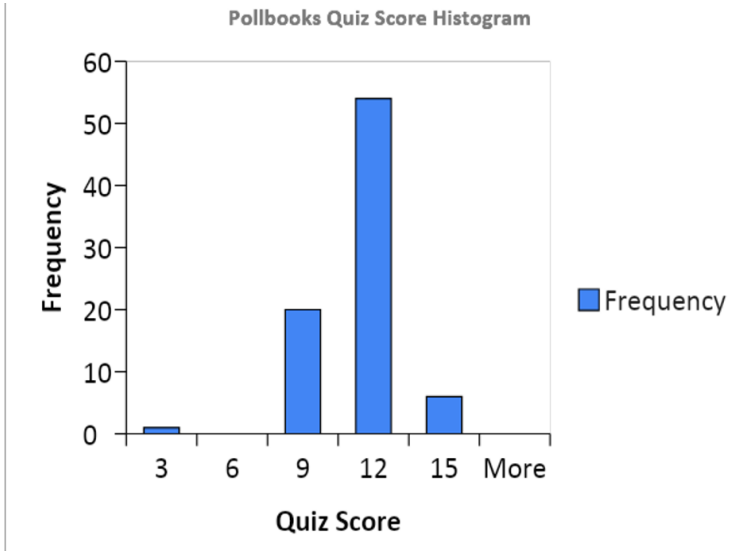
Example Test Question

- What should you do when you leave your pollbook station?
  - Sign out and lay the pollbook screen down
  - Unplug the pollbook from the hub temporarily
  - Turn the pollbook off
  - All of the above
- Physical threat
- Maps to equipment use

Poll Worker Training Results







Data Analysis

- 230 valid SEBIS responses
  - 20 completed SEBIS inventory and Scanning Unit, Provisional Voting, and Pollbook training
  - 124 completed SEBIS inventory and Scanning Unit training
  - 82 completed SEBIS inventory and Pollbooks training
  - 24 completed SEBIS inventory and Provisional Voting training
- Regression analysis was performed to understand relationship between SEBIS scores and training module performance
- For statistically significant results, k-mean analysis was used to find relationships among groups of poll workers
- With k-means results, pivot tables were developed to identify patterns within poll worker security behaviors based upon their demographics and training scores

Data Analysis

SUMMARY OUTPUT

Regression Statistics	
Multiple R	0.40698096
R Square	0.1656335
Adjusted R Square	0.11582058
Standard Error	1.63248017
Observations	72

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	4	35.4455692	8.8613923	3.3251109	0.01519187
Residual	67	178.5544308	2.6649915		
Total	71	214			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	12.8123015	1.738414764	7.37010624	3.283E-10	9.3424111	16.2821919	9.3424111	16.2821919
Average of Device Securement Score	0.65429852	0.313211014	2.08900226	0.04050915	0.02912671	1.27947032	0.02912671	1.27947032
Average of Password Generation Score	-0.94283127	0.404163357	-2.33279749	0.02267053	-1.7495447	-0.13611783	-1.7495447	-0.13611783
Average of Proactive Awareness Score	-0.82793508	0.369433208	-2.24109545	0.02833814	-1.56532685	-0.09054331	-1.56532685	-0.09054331
Average of Updating Score	-0.03565879	0.258561308	-0.13791231	0.89072336	-0.55174932	0.48043174	-0.55174932	0.48043174

Data Analysis Results

How does personal cybersecurity behavior (i.e., cyber hygiene) of a poll worker predict training outcomes?

- Within the clusters of the pollbooks training scores, the most driving construct was the average score on the device securement section of the SEBIS survey
- The Scanning Unit training scores had the largest range of scores; the driving construct were updating, device securement, and password generation SEBIS scores

Data Analysis Results

Are the predictions and corresponding strength moderated by demographics?

- Poll workers who identify as female generally score higher on the SEBIS survey, Pollbooks, Scanning Unit, and Provisional Voting training modules
- The more education a poll worker has, the more likely they are to score higher on the training modules
- Younger poll workers scored better on the SEBIS inventory but retired poll workers tended to score the highest on the training module quizzes

Data Analysis Results

What are the election security policy implications of these results?

- The strongest relationship was found between security behaviors and the Pollbooks training. Thus, SEBIS could be used to aid in the prediction of the ability of poll workers to mitigate threats related to this voting process/equipment.
- Retired poll workers could be used to manage the Scanning Unit process/equipment and others may need to be trained more extensively.
- Understanding security behaviors followed by training was shown to be an efficient model of predicting employee security behaviors and showed a positive relationship

Key Takeaways

- The nearly 1 million poll workers are the first line of defense for election security, yet they oftentimes receive little to no security threat training
- Poll workers are highly seasonal, trusted insiders to a national critical infrastructure process and need to be able to identify and mitigate any potential threat that arises
- Understanding a poll workers' specific security behaviors through simple inventory questions may help effective allocation of duties on Election Day

IISE ANNUAL CONFERENCE & EXPO 2024

Dr. Josh Dehlinger
jdehlinger@towson.edu

Remember to complete your evaluation for this session within the app!

iise.org/annual #IISEANNUAL2024