Proceedings of the American Society for Engineering Management 2023 International Annual Conference
G. Natarajan, H. Zhang, and E.H. Ng eds

PREPARING POLL WORKERS TO SECURE U.S. ELECTIONS

Natalie M. Scala, Ph.D.
Josh Dehlinger, Ph.D.*
Lorraine Black, M.S.
Towson University

***jdehlinger@towson.edu**

Abstract
The security concerns surrounding the 2016 and 2020 United States Presidential Elections have underscored the critical importance of election security, prompting a renewed emphasis on preventing, detecting, and mitigating emerging threats associated with election infrastructure. With their pivotal role as the first line of defense on Election Day, poll workers bear the responsibility of identifying and thwarting any potential threats that may arise. Moreover, they possess unsupervised access to the U.S. critical infrastructure elections equipment at polling places and are entrusted with administering the election processes at their local precincts. However, despite their crucial role, poll workers receive minimal, if any, specific training on security threats prior to elections. To address this gap, this research investigates poll worker threat awareness through developing, piloting, and empirically evaluating online training modules aimed at teaching poll workers to identify and mitigate potential cyber, physical, and insider threats that may arise prior to, and on, Election Day. Through statistical analysis of a pre-post-test study involving eligible and current poll workers, this research demonstrates the effectiveness of these training modules to significantly enhance poll workers' understanding of cyber, physical, and insider threats associated with the processes of three critical areas in voting: electronic pollbooks, the scanning unit, and provisional voting. The implications of this work emphasize the need for resources for election officials and managers to provide effective and comprehensive poll worker training and, thus, ensure the security and integrity of U.S. election processes.

Keywords
Election security, Infrastructure vulnerability, Infrastructure risk management, Insider risk.

Introduction
The 2016 and 2020 U.S. Presidential Elections were unparalleled, as mainstream media, U.S. government and intelligence agencies, and subsequent judicial court proceedings established prevalent interference by foreign actors along with mis/disinformation narratives regarding the integrity of votes and voting processes. These events brought a renewed focus on election integrity to the extent that in 2017 the Department of Homeland Security designated Election Infrastructure as a subsector of national critical infrastructure under the Government Facilities sector.

Locraft, et al. (2019) and Price, et al. (2019) identified that threats to elections security can occur at both the state and local levels and were the first to recognize that a holistic cyber, physical, and insider approach should be taken to mitigate threat. Polling places serve as the crucial interface between the public and election processes, making them the starting point for ensuring security as they handle the majority of votes cast and recorded. The nearly one million poll workers needed to facilitate voting during a presidential election cycle are the first line of defense in elections security, but they need to be trained to be aware of real-time threats that may evolve on Election Day. As elections are primarily one-day events, they cannot be redone or postponed, so the security and integrity of the votes cast must be maintained throughout the entire process. Poll workers need knowledge of threats and to be empowered to mitigate or manage issues that may arise.

This research investigates poll worker threat awareness through the development of online training modules to educate poll workers about potential cyber, physical, and insider threats that may arise on Election Day and tests the efficacy of those modules via a pre-post-test. Evidence from the statistical analysis suggests that cyber, physical, and insider threat knowledge of current and potential poll workers *increases* after interacting with the training modules. We consider a mid-Atlantic state that uses precinct count optical scanners (PCOS) as our case study and developed training module(s) for every station that the public uses at a polling place. These stations include electronic pollbooks,

voting booths, scanning units, ballot marking devices, and provisional voting. This paper focuses specifically on three developed training modules: the scanning unit, electronic pollbooks, and provisional voting. The cyber, physical, and insider threat awareness training in these modules can be directly extended to other states that utilize PCOS as their election infrastructure equipment.

In summary, the specific contributions of this investigation of poll worker threat training includes:

- Development and validation of multiple online cybersecurity training modules for states and localities that adopt a systemic approach to educate poll workers to understand, identify, and mitigate cyber, physical, and insider security threats that can occur during an election.
- Statistical analysis evidence of study results with eligible and current poll workers suggesting the developed training modules targeting three specific Election Day processes were effective in increasing the poll workers' understanding of cyber, physical, and insider threats.

The work presented here is part of a larger effort to develop, assess, and disseminate readily available and effective security education modules to empower local poll workers to secure the election process.

Background and Related Work

Prior research on election security primarily focuses on the state level and considers security threats to statewide election infrastructure; very little work has examined elections security at the local or precinct/county level. Lazarus, et al. (2011) present an agenda for a risk model at local precincts which lacks details of the actual model. Price, et al. (2019) identifies vulnerabilities that may occur at a local polling place and presents a preliminary risk model with an application to identified vulnerabilities for Maryland. Cahn (2017) documents known vulnerabilities and issues that have occurred with various types of voting infrastructure. The DEFCON Voting Village reports summarized activities at the annual conference where hackers are given access to decommissioned voting infrastructure and tasked with exploiting vulnerabilities, which is achieved with shocking ease and speed, sometimes in as little as 30 seconds (Blaze, et al., 2017). Attacks can happen in physical proximity or through human action. For example, DEFCON hackers easily compromised an ACCUVote machine because it did not have strong passwords or encryption (Blaze, et al., 2017) and compromised the Sequoia AVC Edge voting equipment through an insider threat related to poll workers incorrectly pressing buttons which could prevent ballots from being cast (Cahn, 2017).

Various think tanks have also issued reports that provide prescriptive recommendations for states to improve their election infrastructure security, but they do not contain models or analyses to support the prescribed actions are indeed the best practices that a state can take. The Center for American Progress (CAP) (i.e., Root, et al., 2018) grades each state and the District of Columbia on the relative security of its elections' infrastructure and processes, but the approach used in the report does not include mathematical analysis or a systematic model. Many states do not have a standard voting process throughout the state, and each county chooses the type of equipment it wants to use. In 2020, 31 states had standardized equipment and processes across the state and 19 states used a mix of equipment and varied processes (Verified Voting, 2020). Locraft, et al. (2019) show that states with standardized equipment and the same process throughout the entire state were targeted more frequently by adversaries during the 2016 Presidential Election and that a standardized process and equipment may not necessarily be more secure, contradictory to what the CAP report suggests. Other reports on elections security, such as one from the Harvard Belfer Center (Mook, et al., 2018), make similar sweeping recommendations without analysis or evaluation by a model.

In summary, many types and vendors of voting equipment exist and threats to those types of equipment vary in severity, ease of attack/compromise, and method of attack (i.e., cyber, physical, insider). Price, et al. (2019) establish the need for a systems approach and that a pure cybersecurity focus, as in much of the current election security literature, does not address the full extent of various threats to elections infrastructure that may emerge. Threats can emerge at a polling place (e.g., in the case of button pushing with the Sequoia AVC Advantage voting machines), and poll workers must be aware of issues that may emerge and be empowered to act if a threat occurs. States and local precincts need actionable steps to implement and prevent threat, beyond the general recommendations made in the literature. The work presented here provides a solution through effective poll worker training to identify and mitigate potential cyber, physical, and insider threats that may emerge at a polling place and statistically demonstrates that poll worker knowledge about threats increases after interacting with the developed training.

Training Module Approach and Design

There are many types of voting infrastructure and processes in the United States. This work uses a mid-Atlantic state using PCOS voting equipment as a case study, and language in the training reflects the state's voting processes. However, the modules developed in this research can be adapted for other states and types of voting equipment. To ensure the training modules address holistic cyber, physical, and insider threats and do not focus on just one special

subset of threats, this work builds from the research approach taken in Price, et al. (2019) and Locraft, et al. (2019). Specifically, Price, et al. (2019) identified 25 potential threats to the voting processes in the State of Maryland and organized the threats into cyber, physical, and insider sources. Examples of threats include the Chief Judge tampering with the memory sticks or ballots, corrupting the entire election process (i.e., an insider threat) and accessing compartments on ballot scanning units not being secured (i.e., a physical threat). Locraft, et al. (2019) built on the analysis in Price, et al. (2019) and established influence diagrams to identify sources of cyber, physical, and insider threat and examples of how the vulnerabilities identified in Price, et al. (2019) can be executed real-time at a polling place. Despite these identified threats, Scala, et al. (2020) note that Maryland's poll worker training, as of 2018, did not include any cyber, physical, or insider threat training, even though poll workers could easily become insider threats themselves simply by being unaware of potential issues and subsequent needs to mitigate if such issues arose. The influence diagrams in Locraft, et al. (2019) illustrate the varied nature of threats that poll workers must be ready to respond to as a first line defense to elections integrity.

This research builds on the identification of threat and influence diagrams of Price, et al. (2019) and Locraft, et al. (2019) and incorporates the identified threat scenarios into training modules. This work specifically focuses on three training modules that were developed, piloted, assessed, and deployed for use in training poll workers on identifying and mitigating cyber, physical, and insider threats that may arise on Election Day. The three modules chosen for further study, by recommendation from a mid-sized county Board of Elections within in the case study state, are as follows:

- *Scanning unit* – The scanning unit is the equipment that receives a voter's marked paper ballot, optically reads, and electronically records a vote.
- *Electronic pollbooks* – The electronic pollbook is the equipment that a poll worker uses to check-in, validate, and provide a voter with the correct paper ballot.
- *Provisional voting* – Under federal law, every voter who claims they are eligible and registered must be given the opportunity to vote. Provisional voting allows citizens to vote before verifying their eligibility.

A full description of the modules' design, pedagogy, usability, and deployment can be found in Dehlinger, et al. (2021) and Scala, et al. (2020). Briefly, a training module consists of text and image content divided into four sections: equipment use, cyber threat, insider threat, and physical threat. Each section begins with an introduction, followed by content on the specific threat. Participants must correctly answer self-check assessment questions at the end of each section before progressing to the next. The process is iterative, with questions highlighting green when answered correctly. The content of the threat scenarios is built from the cyber, physical, and insider threats identified in Price, et al. (2019), interviews with board of elections personnel in the case study state, and literature attack tree data for the PCOS equipment (US EAC, 2009). Further, the design of the training modules follows pedagogical research reduce cognitive overload and focus the poll worker's efforts on attaining the content. All poll worker training modules were deployed using the established Security Injections@Towson e-learning platform (Taylor and Kaza, 2011).

Study Protocol

This section describes the hypotheses tested to measure the efficacy of the developed poll worker training modules.

Hypotheses and Research Question Design

For this study, we focus on three poll worker training modules: the scanning unit, electronic pollbooks, and provisional voting. The objective is to determine if poll workers and potential poll workers learn about security threats by interacting with the modules. Specifically, this work builds upon the systems approach to cybersecurity from Locraft, et al. (2019) and Price, et al. (2019) and explicitly assesses the developed cybersecurity training modules' descriptions on users' understanding of how to identify and mitigate cyber, physical, and insider cybersecurity threats that may arise during the voting process. Thus, three primary hypotheses are defined around prior experience of the participant as a poll worker, as follows:

- H1: Poll worker and potential poll worker awareness of security threats increases after interacting with the online training module.
- H2: For those who have not previously served as a poll worker, awareness of security threats increases after interacting with the online training module.
- H3: Even with previous poll worker experience, awareness of security threats increases after interacting with the online training module.

In addition, for each of the three primary hypotheses, three sub-hypotheses were developed to specifically assess the awareness of cyber (a), physical (b), and insider (c) threats, as shown in Exhibit 6.

To test these hypotheses, sets of multiple-choice questions (MCQs) were created for each module and a set of demographics questions were created to assess background, experience as a poll worker, comfort with technology, and gender/generational identification. The questions were directly based on the content in each module and were divided into three groups: cyber threat questions, physical threat questions, and insider threat questions. Fifteen pre- and post-test comprehension questions were created for each module, and the type of threat addressed by each question was not identified within the test. Grouping questions into cyber, physical, and insider threats was based on the influence diagrams in Locraft, et al. (2019). When creating their influence diagrams, Locraft, et al. (2019) generalized patterns of potential threats first identified in Price, et al. (2019). This work employs the same approach to categorize the content of our questions into cyber, physical, and insider threats. A full listing of all questions, along with their threat influence, can be found at https://tinyurl.com/pre-post-test-questions.

Validity

To address validity and ensure the questions address the intended threats and knowledge, an expert panel was employed to review the questions and corresponding answers and provide assessments on validity; three permanent Board of Elections employees in our case study mid-Atlantic state comprised the panel. Considine, et al. (2005) examine the use of MCQs to measure knowledge and define three types of validity – content, face, and construct – to establish overall validity of a MCQ assessment. *Content validity* addresses if the questions are relevant, appropriate, and representative of the content intended to test. The expert panel reviewed and approved the relevance and content of each set of MCQs and agreed that the questions addressed operations knowledge of the scanning unit, electronic pollbooks, and provisional voting processes as well as cyber, physical, and insider threats. *Face validity* addresses clarity, readability, and ease of administration and is established through editorial review and a pilot study. The expert panel was asked if the questions were readable, written clearly, and if the wording made sense or if some terms needed to be modified. The panel provided revisions to some questions as needed, and those updates were incorporated into the final sets of MCQs. Finally, *construct validity* assesses if the questions measure the domain of knowledge being tested. It is established through a key check, which determines if the correct answer is indeed correct and that only one correct answer exists amongst the multiple choices. The expert panel reviewed each question and provided feedback mostly to ensure only one clearly correct answer is listed for each question and verified the correct answers for each question.

Pre-Post Test Design and Pilot Study

To assess threat awareness, a pre-post-test design was used. MCQs are used to test end-point learning; the specific choice, instead of open-ended responses, assists in determining knowledge gained without interpretation or bias. For this study, a participant completes the fifteen-question MCQ quiz for a single module, interacts with the corresponding training module, and then immediately takes the same fifteen-question MCQ quiz. The assumptions to be tested in the hypotheses are that the test scores increase in the post-test as the participant would have gained security threats awareness and knowledge while interacting with the module. The purpose of the pre-test is to assess how much knowledge the participant had in cyber, physical, and insider threats related to elections security beforehand.

Before data was formally collected, a small pilot study was conducted, comprising of predominately graduate students in computer science at a large public mid-Atlantic institution. The pilot group was used to test that the data collection method and online modules were working with no broken links or errors and that the questions and materials were readable and comprehensible. Of those participants, 11 fully completed all steps for electronic pollbooks, 10 completed all steps for provisional voting, and 12 completed all steps for the scanning unit. The pilot participants did not report any issues with broken links, missing content, or difficulty following the directions. The pilot pre-test and post-test data were scored, but the small sample sizes of participants prevented drawing general conclusions regarding if the pilot results were statistically significant or were exhibiting any patterns.

However, when considering the entire data set of all participants, further examination of the patterns in the data uncovered three potential concerns with specific questions in the MCQ pre-post test. Specifically, Question (Q) 11 in the electronic pollbooks module was an insider threat question about suspicious behavior. The correct answer of "*the Chief Judge"* was coded correctly when scoring the pre-post tests, but the answer was misleading in the module content. A similarly worded question was included in the self-check section in the insider threat portion of the module. The answer coded as correct in the module referred to reporting suspicious behavior to other poll workers but not specifically to the Chief Judge. Participants seemed to have learned while interacting with the module, but they learned a misleading answer. They then chose the incorrect answer in the post-test, causing incorrect answers when the test was scored. As a result, we removed Q11 from the electronic pollbooks insider questions in the results analysis.

A similar concern was raised for Q8 and Q14 in the scanning unit module, which are both cyber questions. The answers to these two questions were never explicitly worded in the module, and participants continued to make

educated guesses when completing the post-test. To verify this assumption, we reexamined the pilot post-test data for these two questions. Specifically, we tested item difficulty, which is measure of the easiness of a question; item discrimination, to distinguish those who understand the material from those who do not; and the point biserial coefficient, which is a measure of an individual item reliability (Ding and Beichner, 2009). Exhibit 1 presents the pilot data results for these three questions, along with the acceptable ranges for each measure as reported by Ding and Beichner (2009). Note that item difficulty was sufficient for Q11 and Q8 and not acceptable for Q14. The item discrimination was not acceptable for any of the questions because the answers were either coded incorrectly or unclear in the learning modules. The point biserial coefficient was within the acceptable range for Q8 but not Q14. Furthermore, the point biserial coefficient for Q11 in the electronic pollbooks module was also not acceptable. Unacceptable ranges for point biserial coefficients could be a result of poorly worded questions and/or lack of participant attention when interacting with the modules. Unfortunately, removal of Q8 and Q14 in the results analysis left only two cyber questions for the scanning unit. The small sample size of the pilot data precluded identification of these patterns in participant responses, and we did not discover the concerns of the three questions until all data was collected. However, we removed these questions from the analysis and report our results for the study participants and remaining pre-post test questions.

Exhibit 1. Pilot Item Analysis for Cyber Threats Questions.

Item Difficulty			
Module	**Question Number**	**Pilot Post-test**	**Acceptable Range**
Electronic Pollbooks	11	0.615	0.3 to 0.9
Scanning Unit	8	0.615	
Scanning Unit	14	0.923	
Item Discrimination			
Module	**Question Number**	**Pilot Post-test**	**Acceptable Range**
Electronic Pollbooks	11	-0.615	0.3 or greater
Scanning Unit	8	0.286	
Scanning Unit	14	0.000	
Point Biserial Coefficient			
Module	**Question Number**	**Pilot Post-test**	**Acceptable Range**
Electronic Pollbooks	11	-0.21	0.2 or greater
Scanning Unit	8	0.471	
Scanning Unit	14	0.036	

Data Collection

Formal data collection was done in-person over 8 sessions. Participants were able to drop in during the sessions, which were each two to three hours long; most participants finished a complete study within 40 minutes. Upon entering the room, a participant was given a card and a unique participant number for one arbitrarily selected module. Participants comprised of eligible poll workers and previous/current poll workers. A total of 269 usable responses were collected across all samples and training modules tested. Of those total responses, 106 responses were usable for the provisional voting module, 79 responses were usable for the scanning unit module, and 84 responses were usable for the electronic pollbooks module. An additional 3 responses were thrown out, due to the pre-test or post-test taken in less than one minute, only one test completed in entirety, straightlining, and/or participants entering personally identifiable information instead of their participant number. The demographics of the final population are provided in Exhibit 2.

Data Analysis and Results

t-tests and Mann-Whitney tests were used to compare the mean pre- and post-test scores between samples. Specifically, the hypotheses propose that current and potential poll workers' security threats awareness increases by using the training modules. Thus, $\mu_1 - \mu_2 < 0$, where μ_1 is the mean score of the pre-test across the sample, and μ_2 is the mean score of the post-test across the sample. A higher post-test score would be reflected in a one-tailed less than zero test. For $n > 35$ samples, *t*-tests are used, otherwise Mann-Whitney tests are used, following the Central Limit Theorem.

Hypothesis 1: Poll Workers and Potential Poll Workers

Hypothesis 1 proposes that for poll workers and potential poll workers, awareness of security threats increases after interacting with the training modules. *t*-tests were used for analysis of the usable samples. Exhibit 3 presents the results for these tests. Hypothesis 1 addresses all questions across all individual modules. All modules, as well as all questions

considered in the aggregate across all modules, are significant, implying that post-test scores increase with statistical significance when interacting with the modules.

Exhibit 2. Partial Demographics of Study Population.

		Potential Poll Workers	Prior Poll Workers	Total
Gender Identification	Male	54.02%	31.58%	46.10%
	Female	42.94%	68.42%	52.42%
	Transgender	0.57%	0.00%	0.37%
	Choose not to disclose	1.72%	0.00%	1.12%
Age Group / Generation	Silent generation	2.87%	4.21%	3.35%
	Baby boomers	11.49%	62.11%	29.37%
	Generation X	5.75%	22.11%	11.52%
	Millennial	44.25%	9.47%	31.97%
	Generation Z	35.06%	2.11%	23.42%
	Did not answer	0.57%	0.00%	0.37%
Highest Level of Education	High school	20.69%	30.53%	24.16%
	Associates degree	30.46%	13.68%	24.54%
	Bachelors degree	34.48%	25.26%	31.23%
	Masters degree	11.49%	28.42%	17.47%
	Doctoral degree	2.30%	1.05%	1.86%
	Did not answer	0.57%	1.05%	0.74%
Comfort with Computers	Extremely comfortable	78.16%	52.63%	69.14%
	Very comfortable	15.52%	29.47%	20.45%
	Comfortable	5.75%	14.74%	8.92%
	Somewhat comfortable	0.00%	2.11%	0.74%
	Did not answer	0.57%	1.05%	0.74%
Heard of Potential Threat to Elections	Yes	90.23%	98.95%	93.31%
	No	9.20%	1.05%	6.32%

Hypothesis 1a proposes that awareness of cyber threats increases after interacting with the training modules. Exhibit 3 shows that the cyber threat awareness increase is significant for the data considered in its entirety and is also significant for the provisional and electronic pollbooks modules, implying that participants increased their awareness of cyber threats by interacting with the provisional and electronic pollbooks modules. For the scanning unit module, the cyber threat awareness increase is not significant; however, only two questions were tested in this sample, as two cyber questions (Q8 and Q14) had to be removed from the analysis. It is likely that two questions are not large enough to assess if knowledge significantly increases. The fact that the cyber questions considered in aggregate across all modules are significant suggests that interaction with the scanning unit module could increase cyber knowledge.

H1b proposes that awareness of physical threats increases after using the training modules. Exhibit 3 shows that awareness increase is significant for the data considered in its entirety and is also significant for all individual modules, implying increased awareness of physical threats by using all training modules.

H1c proposes that awareness of insider threats increases after using the training modules. Exhibit 3 shows that the insider threat awareness increase is significant for the data considered in its entirety across all modules and is also significant for the provisional voting and scanning unit modules, implying increased awareness of insider threats by interacting with these modules. However, for the electronic pollbooks module, the insider threat awareness increase is not significant, even with Q11 removed from the test. The remaining insider threat electronic pollbooks questions are Q8, Q10, Q12, and Q13. Specifically, for Q8, 72.62% of participants answered the question correctly in both the pre- and post-test. The same pattern of a correct answer in both tests held for Q10 (63.10%), Q12 (86.90%), and Q13 (88.10%), implying that participants already had some awareness of insider threat before interacting with the modules.

Hypothesis 2: No Previous Experience as a Poll Worker

Hypothesis 2 proposes that for those who have not previously served as a poll worker, awareness of security threats increases after interacting with the training modules. Exhibit 4 presents the results for the *t*-tests, to include H2, H2a (cyber), H2b (physical), and H2c (insider). Hypothesis 2 addresses all questions across all modules. Analysis found all modules, as well as all questions considered in the aggregate, are significant, implying that post-test scores increase with statistical significance when those inexperienced poll workers interact with the modules.

Hypothesis 2a proposes that awareness of cyber threats increases after interacting with the training modules. Exhibit 4 shows that increase in cyber threats awareness is significant for the data considered in its entirety. It is also significant for the provisional and electronic pollbooks modules, implying that potential poll workers increased their awareness of cyber threats by interacting with the provisional and electronic pollbooks modules. For the scanning unit module, cyber threat awareness increase is not significant. However, following the discussion for H1a, only two cyber questions were included in the analysis, and the results of only two questions may not provide enough insight to assess statistical significance. However, significance of cyber questions in the aggregate for all data suggests that cyber threat awareness related to the scanning unit might increase and could be reflected with more questions.

Exhibit 3. Statistical Analysis for Hypothesis 1.

		μ		σ					
Module	**Questions**	**Pre-test**	**Post-test**	**Pre-test**	**Post-test**	**μ Difference**	***t***	***df***	***p***
All Data *n* = 269	All	0.628	0.774	0.181	0.168	-0.1458	-9.69	536	0
	Cyber	0.534	0.756	0.416	0.375	-0.2214	-6.49	536	0
	Insider	0.612	0.782	0.235	0.206	-0.1701	-8.93	536	0
	Physical	0.619	0.779	0.211	0.190	-0.1599	-9.23	536	0
Provisional Voting *n* = 106	All	0.619	0.774	0.183	0.158	-0.1544	-6.57	210	0
	Cyber	0.406	0.792	0.493	0.407	-0.3868	-6.22	210	0
	Insider	0.587	0.696	0.233	0.230	-0.1094	-3.44	210	0
	Physical	0.661	0.816	0.213	0.153	-0.1545	-6.08	210	0
Scanning Unit *n* = 79	All	0.555	0.734	0.185	0.205	-0.1795	-5.79	156	0
	Cyber	0.506	0.544	0.380	0.377	-0.0380	-0.63	156	0.265
	Insider	0.585	0.747	0.236	0.225	-0.1614	-4.40	156	0
	Physical	0.552	0.781	0.229	0.245	-0.2297	-6.09	156	0
Electronic Pollbooks *n* = 84	All	0.709	0.812	0.138	0.130	-0.1031	-4.98	166	0
	Cyber	0.723	0.909	0.237	0.203	-0.1854	-5.45	166	0
	Insider	0.836	0.878	0.218	0.184	-0.0417	-1.34	166	0.091
	Physical	0.630	0.731	0.176	0.163	-0.1011	-3.86	166	0

H2b proposes that awareness of physical threats increases for those with no poll worker experience after using the training modules. Exhibit 4 shows that physical threat awareness increase is significant for the data considered in its entirety and is also significant for all individual modules, implying that participants with no previous poll worker experience increased their awareness of physical threats by interacting with the training modules.

H2c proposes that awareness of insider threats increases after interacting with the training modules. Exhibit 4 shows that insider threat awareness increase is significant at 0.001 for the data considered in its entirety. It is also significant for the provisional voting and scanning unit modules at 0.01, implying that participants increased their awareness of insider threats by interacting with the modules. However, for the electronic pollbooks module, the insider threat awareness increase is not significant, even with Q11 removed from the test. However, the pattern of answering insider questions correctly in both the pre-test and post-test continued with the potential poll workers in the sample; specifically, with Q8, 70.18% of participants answered the question correctly in both the pre- and post-test. The same pattern of a correct answer in both tests held for Q10 (56.14%%), Q12 (82.46%%), and Q13 (82.46%). This implies that participants already had some awareness of insider threats before interacting with the modules. This may appear counterintuitive, as this sample did not have previous experience as a poll worker. However, Q12 addressed when a poll worker should be alert to potential threat, and Q13 addressed examples of potential insiders. Both questions had a correct answer of "all of the above," and it is possible that potential poll workers already understood best practices of being alert should happen all the time, as well as those posing, distracting, and tampering all could be insider threats. Furthermore, examining the item difficultly in the pre-test pilot data, Q8 had a calculated difficulty of 0.615, Q10 calculated 0.846, Q12 calculated 1.000, and Q13 calculated 0.769. According to Ding and Beichner (2009), item difficulty scores between 0.3 and 0.9 are acceptable. Q8, Q10, and Q13 should have been significantly difficult in the tests to correctly assess knowledge. Overall, the fact that the insider questions considered in the aggregate across all modules are significant, along with significant tests for the provisional voting and scanning unit modules, suggests that the interaction with the modules increases insider threat knowledge, if it doesn't already exist.

Hypothesis 3: Previous Poll Worker Experience

Hypothesis 3 proposes that experienced poll workers' awareness of security threats increases after using the modules. Exhibit 5 presents the results for the *t*-tests and Mann-Whitney tests, to include H3, H3a (cyber), H3b (physical), and H3c (insider). For the Mann-Whitney tests, *p*-values unadjusted for ties are reported as they are more conservative than those adjusted for ties. Hypothesis 3 addresses all questions across all modules. All modules, as well as all questions considered in the aggregate, are significant, implying that post-test scores increase with statistical significance for experienced poll workers who use the modules. Specifically, all questions in aggregate and the scanning unit questions are significant at 0.001; provisional voting is significant at 0.01; and electronic pollbooks are significant at 0.05. This implies that experienced poll workers' awareness about threats increases after using modules.

Exhibit 4. Statistical Analysis for Hypothesis 2.

		μ		σ					
Module	**Questions**	**Pre-test**	**Post-test**	**Pre-test**	**Post-test**	**μ Difference**	***t***	***df***	***p***
All Data *n* = 174	All	0.577	0.746	0.175	0.178	-0.1684	-8.84	346	0
	Cyber	0.447	0.723	0.402	0.389	-0.2764	-6.51	346	0
	Insider	0.542	0.754	0.224	0.224	-0.2112	-8.79	346	0
	Physical	0.563	0.750	0.206	0.205	-0.1875	-8.51	346	0
Provisional Voting *n* = 71	All	0.564	0.759	0.182	0.176	-0.1915	-6.50	140	0
	Cyber	0.310	0.775	0.466	0.421	-0.4648	-6.24	140	0
	Insider	0.558	0.682	0.246	0.245	-0.1239	-3.01	140	0.002
	Physical	0.595	0.801	0.204	0.178	-0.2056	-6.41	140	0
Scanning Unit *n* = 46	All	0.488	0.667	0.159	0.196	-0.1789	-4.81	90	0
	Cyber	0.391	0.446	0.348	0.353	-0.0543	-0.74	90	0.230
	Insider	0.554	0.685	0.258	0.232	-0.1304	-2.55	90	0.006
	Physical	0.479	0.721	0.221	0.259	-0.2420	-4.82	90	0
Electronic Pollbooks *n* = 57	All	0.666	0.793	0.138	0.144	-0.1267	-4.81	112	0
	Cyber	0.662	0.883	0.241	0.232	-0.2211	-4.99	112	0
	Insider	0.803	0.864	0.235	0.195	-0.0614	-1.52	112	0.066
	Physical	0.591	0.711	0.179	0.174	-0.1209	-3.65	112	0

Hypothesis 3a proposes that awareness of cyber threats increases after interacting with the training modules. Exhibit 5 shows that increase in cyber threats awareness is significant at 0.05 for the data considered in its entirety. It is also significant at 0.05 for the provisional and electronic pollbooks modules, implying that poll workers increased their awareness of cyber threats by interacting with the provisional and electronic pollbooks modules. For the scanning unit module, cyber threat awareness increase is not significant. However, only two cyber questions were included in the analysis, and the results of only two questions may not be providing enough insight to properly assess statistical significance, especially with a sample size of only 33 poll workers. However, the fact that cyber questions are significant in the aggregate for all modules continues to suggest that cyber threats awareness related to the scanning unit could increase and, as with the other hypotheses, could be reflected if additional questions were tested.

H3b proposes that awareness of physical threats increases for experienced poll workers interacting with the training modules. Exhibit 5 shows that the physical threats awareness increase is significant at 0.001 for the data considered in its entirety. It is also significant at 0.001 for the scanning unit module and significant at 0.05 for the provisional voting and electronic pollbooks modules, implying that participants with previous poll worker experience increased their awareness of physical threats by interacting with the three training modules.

H3c proposes that awareness of insider threats increases after using the modules. Exhibit 5 shows the awareness increase is significant at 0.001 for the modules considered in aggregate and the scanning unit module. It is also significant at 0.05 for the provisional voting module, implying increased awareness of insider threats by using these modules. For the electronic pollbooks module, insider threat knowledge increase is not significant, even with Q11 removed from the test. The pattern of answering insider questions correctly in both the pre-test and post-test continued with the sample of potential poll workers, with Q8 (77.78%), Q10 (77.78%), Q12 (96.3%), and Q13 (100%). This implies that participants already had some awareness of insider threat, which is logical because this sample had prior poll worker experience. The insider questions address voter identity, use of cell phones, being alert, and potential insiders. Awareness related to voter identity and use of cell phones are generally covered in the case study state's poll worker training manual, although not as an insider threat. However, that prior awareness may cause a previous poll worker to answer correctly in both tests. Even though 100% of previous poll workers correctly identified potential insiders in both tests, the question has significant item difficulty. Because the insider questions considered in the

aggregate across all modules are significant, along with significant tests for the provisional voting and scanning unit modules, using the modules can increase insider threat awareness.

Data Analysis and Results Summary

Potential and current poll worker awareness of cyber, physical, and insider threats increases, with statistical significance, by interacting with the modules. Exhibit 6 summarizes the hypotheses and support at 0.05 significance.

Exhibit 5. Statistical Analysis for Hypothesis 3.

		μ		σ					
Module	**Questions**	**Pre-test**	**Post-test**	**Pre-test**	**Post-test**	**μ Difference**	***t***	***df***	***p***
All Data *n* = 95	All	0.722	0.826	0.151	0.133	-0.104	-5.05	188	0
	Cyber	0.695	0.816	0.392	0.340	-0.121	-2.27	188	0.012
	Insider	0.738	0.833	0.197	0.159	-0.095	-3.64	188	0
	Physical	0.722	0.832	0.180	0.147	-0.110	-4.59	188	0
Provisional Voting *n* = 35	All	0.731	0.803	0.129	0.109	-0.072	-2.53	68	0.007
	Cyber	0.600	0.829	0.497	0.382	-0.229	-2.16	68	0.017
	Insider	0.646	0.726	0.195	0.195	-0.080	-1.72	68	0.045
	Physical	0.795	0.846	0.162	0.076	-0.051	-1.68	68	0.049
Scanning Unit *n* = 33	All	0.69	0.92			-0.23			0
	Cyber	0.50	1			0			0.431
	Insider	0.75	0.75			-0.25			0
	Physical	0.71	1			-0.29			0
Electronic Pollbooks *n* = 27	All	0.79	0.86			-0.07			0.018
	Cyber	1	1			0			0.018
	Insider	1	1			0			0.503
	Physical	0.71	0.71			0			0.045

Exhibit 6. Summary of Support to Hypotheses at 0.05 Significance.

Hypotheses	**Support**
H1: Poll worker and potential poll worker awareness of security threats.	Supported
H1a: Poll worker and potential poll worker awareness of cyber threat.	Partially supported
H1b: Poll worker and potential poll worker awareness of physical threat.	Supported
H1c: Poll worker and potential poll worker awareness of insider threat.	Partially supported
H2: Awareness of security threats for those who have not previously served as a poll worker.	Supported
H2a: Awareness of cyber threat for those who have not previously served as a poll worker.	Partially supported
H2b: Awareness of physical threat for those who have not previously served as a poll worker.	Supported
H2c: Awareness of insider threat for those who have not previously served as a poll worker.	Partially supported
H3: Awareness of security threats for those with previous poll worker experience.	Supported
H3a: Awareness of cyber threat for those with previous poll worker experience.	Partially supported
H3b: Awareness of physical threat for those with previous poll worker experience.	Supported
H3c: Awareness of insider threat for those with previous poll worker experience.	Partially supported

Concluding Remarks

This research provides an investigation of poll worker threat awareness through the development of online modules to train poll workers about potential cyber, physical, and insider threats that may arise on Election Day and tests the efficacy of those modules via a pre-post-test. Evidence from the statistical analysis establishes that poll workers and potential poll workers learn about threats by interacting with the modules. By using the training modules, poll workers will be able to identify and mitigate threats that may emerge at a polling place, serving as a first line of defense in the integrity of elections in the United States of America. Future work expanding the reach of these educational modules, customizing content for different voting infrastructures, and extending the applicability of this approach to other critical systems in need of resilient and well-prepared workers.

Security threat training plays a crucial role in infrastructure vulnerability and risk management. By implementing appropriate training across the workforce, organizations can enhance their ability to identify, assess, and mitigate potential risks and vulnerabilities associated with their engineering infrastructure. Training can also improve

engineers' awareness of the threat landscape, enhance risk assessment practices, facilitate the implementation of security controls, support effective incident response, ensure compliance with regulations, and foster of a culture of security throughout the organization. Engineering managers should stay updated on emerging security threats so they can proactively identify vulnerabilities specific to their infrastructure and design appropriate mitigation strategies that can both minimize the impact of security incidents and prevent future occurrences. A well-trained workforce can also better defend against potential threats while striving for continuous improvement of infrastructure security.

Acknowledgements

This research was partially supported by the Towson University BTU Initiative. The authors would like to thank Katerine Delgado Licona, Saraubi Harrison, and Aikaterini Ieromonahos for their assistance at the eight data collection events.

References

Blaze, M., Braun, J., Hursti, H., Hall, J. L., MacAlpine, M., & Moss, J. (2017). DEFCON 25 voting machine hacking village. *Proceedings of DEFCON,* (pp. 1-18). Washington, D.C.

Cahn, D. (2017). *Risk assessment: How secure are voting machines?* [Capstone thesis]. University of Pennsylvania.

Considine, J., Botti, M., & Thomas, S. (2005). Design, format, validity and reliability of multiple choice questions for use in nursing research and education. *Collegian, 12*(1), 19-24.

Dehlinger, J., Harrison, S., & Scala, N. M. (2021). Poll worker security: Assessment and design of usability and performance. *Proceedings of the 2021 IISE Annual Conference*, (pp. 698-703). Virtual.

Ding, L. & Beichner, R. (2009). Approaches to data analysis of multiple-choice questions. *Physical review special topics: Physics education research, 5*, 020103-1 – 020103-17.

Lazarus, E. L., Dill, D. L., Epstein, J., & Hall, J. L. (2011). Applying a reusable election threat model at the county level. *Proceedings of the 2011 Conference on Electronic Voting Technology,* (pp. 1-14).

Locraft, H., Gajendiran, P., Price, M., Scala, N. M., & Goethals, P. L. (2019). Sources of risk in elections security. *Proceedings of the 2019 IISE Annual Conference*, (pp. 1190-1196). Orlando, FL.

Mook, R., Rhoades, M., & Rosenbach, E. (2018). *The state and local election cybersecurity playbook*. Belfer Center for Science and International Affairs. www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

Price, M., Scala, N. M., & Goethals, P. L. (2019). Protecting Maryland's voting processes. *Baltimore Business Review: A Maryland Journal,* 36-39.

Root, D., Kennedy, L., Sozon, M., & Parshall, J. (2018). Election security in all 50 states: Defending America's elections. Center for American Progress. www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/ election-security-50-states/

Scala, N. M., Dehlinger, J., Black, L., Harrison, S., Delgado Licona, K., & Ieromonahos, A. (2020). Empowering election judges to secure our elections. *Baltimore Business Review: A Maryland Journal*, 8-12.

Taylor, B., & Kaza, S. (2011). Security injections: modules to help students remember, understand, and apply secure coding techniques. Proceedings of the 16th Conference on Innovation and Technology in Computer Science Education, (pp. 3-7). Darmstadt, Germany.

United States Election Assistance Commission (2009). *Election operations assessment: Threat trees and matrices and threat instance risk analyzer (TIRA).* https://www.eac.gov/assets/1/28/Election_Operations_Assessment_Threat_Trees_and_Matrices_and_Threat_Instance_Risk_Analyzer_(TIRA).pdf

Verified Voting (n.d.). *The verifier – polling place equipment.* Retrived May 28, 2023, from www.verifiedvoting.org/verifier

About the Authors

Dr. Natalie M. Scala is an Associate Professor and Director of the graduate programs in Supply Chain Management in the College of Business and Economics at Towson University. She earned Ph.D. and M.S. degrees in Industrial Engineering from the University of Pittsburgh. Her work in elections security earned a University System of Maryland Board of Regents Award for Excellence in Public Service, the system's highest faculty honor. In conjunction with Anne Arundel County, Maryland, her work with Dr. Dehlinger in threat training for poll workers received a United States Elections Assistance Commission Clearinghouse Award for Outstanding Innovation in Election Cybersecurity and Technology.

Dr. Josh Dehlinger is a Professor in the Department of Computer and Information Sciences and the Director of the undergraduate Computer Science program at Towson University. He received his Ph.D. in Computer Science from Iowa State University in 2007 and served as a Research Scientist in the Charles L. Brown Department of Electrical and Computer Engineering at the University of Virginia in 2008. His research expertise lies, broadly, in software safety/reliability, election security, machine learning for software engineering, and computer science education.

Ms. Lorraine Black earned a B.A. in Business Administration and an M.S. in Supply Chain Management, both from Towson University. She currently is a Space Project and Supply Chain Administrator at Jacobs in Severn, Maryland.