Proceedings of the 2021 IISE Annual Conference
A. Ghate, K. Krishnaiyer, K. Paynabar, eds.

Poll Worker Security: Assessment and Design of Usability and Performance

Josh Dehlinger, Saraubi Harrison
Department of Computer and Information Sciences
Towson University, Towson, MD 21252

Natalie M. Scala
Department of Business Analytics and Technology Management
Towson University, Towson, MD 21252

Abstract

Election infrastructure includes socio-technical systems that are designated as United States critical infrastructure within the Government Facilities sector. Following the 2016 United States' General Election and during the 2020 Presidential Election cycle, election security and the integrity of election processes became a prevalent, national conversation. From the 2019 U.S. Senate Intelligence Committee report indicating that election systems in all 50 states had been targeted by foreign adversaries to the more recent broadened use of, and concern about, mail-based voting during the COVID-19 pandemic, election integrity is increasingly important. Furthermore, poll workers play a crucial role in elections and election equipment, as they are one of the first lines of defense in systems security. This paper contributes to improving the security of election infrastructure through intentional, targeted, cyber, physical, and insider threat training for poll workers. Specifically, this paper details the engineering design, including pedagogical approach, and deployment of online, election-specific, threat training modules. Results of a System Usability Scale assessment from 44 poll workers indicate the content and online platform are easy to interact with and use. Further, the developed modules were piloted and then deployed in a mid-Atlantic state; participating counties include over 1,900 poll workers who serve nearly 750,000 voters.

Keywords
Election security, poll worker training, usability study, systems security

1. Introduction
In 2017, the U.S. Department of Homeland Security (DHS) first recognized elections equipment and voting processes (i.e., "elections infrastructure") as critical infrastructure within the Government Facilities sector, indicating that "a secure and resilient electoral process is a vital national interest" [1]. U.S. elections infrastructure constitutes distributed, state and locally managed, socio-technical systems, including systems used to manage elections, voting systems and associated infrastructure, polling places, etc. Following the 2016 U.S. General Election, the 2019 U.S. Senate Intelligence Committee report indicating that election systems in all 50 states were targeted by foreign adversaries [2] and the 2020 U.S. General Election's broadened use of, and concern about, mail-based voting, election integrity and security are increasingly important. The nearly 1,000,000 predominantly voluntary and temporary poll workers [3] managing and administering elections infrastructure during elections are the first line of defense and a key, overlooked component to ensuring the integrity of and securing election infrastructure at the state and local level on a day-to-day basis. It is critical that effective, validated, usable training methods to empower poll workers to identify and mitigate election security threats would strengthen the resiliency of U.S. elections infrastructure.

The predominant use of electronic voting equipment in the U.S. followed the 2000 U.S. General Election's punch-card controversy that led to the subsequent *Bush v. Gore* court proceedings and the resulting Help America Vote Act of 2002 [4]. Cybersecurity issues related to electronic voting equipment emerged publicly as a widespread concern following the U.S. Senate Intelligence Committee's conclusion that election systems in all 50 states were systematically targeted by the Russian Federation leading up to the 2016 General Election [5]. Despite this, poll worker training specific to cybersecurity threats is lacking [6].

Our prior work partnered with the Boards of Elections (BoE) of two counties from a mid-Atlantic state to develop and pilot election threat training modules for poll workers [6], [7]. Using a pre-post-test experimental setup with current poll workers, the developed training content was validated; evidence from statistical analysis suggests that the training was effective in increasing poll worker threat knowledge. Yet, to broadly disseminate the threat training modules for poll workers, the training modules need to be designed such that they are (1) accessible; (2) pedagogically informed; and (3) usable. Thus, this work extends our prior efforts and details the engineering design, pedagogical approach, usability assessment, and online deployment of the election-specific threat training modules.

Specifically, the contribution of this paper is the engineering design, including pedagogical approach, assessment, and deployment, of online election threat training modules. The work presented here is part of a larger effort to develop and disseminate readily available, effective, and useable training modules to empower local polling places to improve the security of election infrastructure through intentional, targeted, cyber, physical, and insider threat training for poll workers. The long-term goal is to develop a comprehensive cybersecurity risk model and informed mitigation policies to enable robust and secure election processes.

2. Related Work

Existing research on election security mostly examines technical cybersecurity threats to statewide voting systems [7-8] and very little work has focused on election security efforts at polling places. For example, Lazarus et al. [8] describe county-level threats but do not include an actual model; Cahn [9] documents existing election equipment vulnerabilities without providing specific mitigations; and, Price et al. [10] identifies election equipment and process vulnerabilities specific to local polling places in Maryland along with a preliminary risk model. However, none of these approaches suggest training of polling places' poll workers as an asset to mitigate potential vulnerabilities.

The work presented here is novel from existing literature, which focuses mainly on cyber threats and does not consider threat systemically. We contribute to the election security literature by applying the systems approach in [10-11] to develop training modules for poll workers that consider the varied sources of threats that may emerge at local polling places. That is, our overall work offers a solution for identifying and mitigating cyber, physical, and insider threats that may emerge during the election process. Cyber threats include digital attacks on the computing equipment (e.g., ballot scanning machines) used to facilitate an election; physical threats involve physically tampering with elections equipment (e.g., breaking sealed, collected ballot envelopes); and insider threats include human interactions with the elections process (e.g., a poll worker accidentally or maliciously leaving an election check-in computer unlocked) [10]. We recognized the need to develop poll workers as the first line of defense in elections security and developed, piloted, and assessed training modules to enable poll workers to identify and mitigate security threats [6] , [7]. The content of the developed training modules was shown to be effective in increasing poll worker threat knowledge. This paper addresses the engineering design and usability assessment of these modules.

3. Training Module Design

To illustrate the engineering design and deployment of the elections security training modules, we focus on three education modules. These modules were chosen for the initial study by our partnering BoE and are, briefly:

- Scanning Unit Module: The scanning unit is a type of elections equipment that receives a voter's marked paper ballot, optically reads, and electronically records a vote.
- Electronic Pollbooks Module: The electronic pollbook is the elections equipment that a poll worker uses to check-in, validate, and provide a voter with the correct paper ballot based on their designated precinct.
- Provisional Voting Module: Provisional voting is the Election Day voting mechanism used to allow citizens to mark a ballot before verifying their eligibility.

As shown in Figure 1, each module consists of text and image content and was developed with four main sections: elections equipment use, cyber threats, insider threats, and physical threats. The equipment use section reviews material covered in traditional in-person poll worker training, while the threat sections are intended to be comprehensive, as election threats training is not currently covered in our partnering BoE counties current poll worker training materials [11]. As partially shown in Figure 1, all modules are designed to: (1) review and assess the operating procedures/protocols of a specific Election Day process (e.g., electronic pollbooks); (2) cover and assess the particular cyber, physical, and insider threats for the specific Election Day process; and (3) provide a certificate indicating that

Figure 1: Ensuring Pollbook Security Module Screenshot [6]

a poll worker has successfully completed the education module. Participants cannot move between content sections without correctly answering a set of self-check assessment questions at the end of each section. The self-check questions ensure the participant poll worker is actually reading and interacting with the content and not just scrolling through. The participant poll worker selects answers for the multiple-choice questions, and the option to move to the next section is displayed once all answers to all questions are correct. The process is iterative; the self-check question highlights in green when correct and red when incorrect. The participant can then select new answers until all questions are correct and highlight green. Within each of the threat subsections, scenarios are presented along with recommendations on how to reduce and mitigate the corresponding threats in each scenario. Figure 1, for example, illustrates the cyber threat section in the Electronic Pollbooks module. The content of the threat scenarios is built from the cyber, physical, and insider threats identified in [10], the state's poll worker training manual [12], interviews with partnering BoE's personnel, and literature attack tree data [13]. During development, the content was reviewed and modified for validation by an expert panel of poll worker trainers who are employed by the partnering BoEs in the mid-Atlantic state. The design is rooted in established pedagogical literature and practice.

All developed poll worker training modules are independent of each other, modular, and designed to target one specific voting process (e.g., scanning a ballot, checking in a voter) for which a poll worker could be responsible during an election. The modules are also designed to be injected into existing poll worker training processes to provide short, approximately 20 minutes, supplemental content (e.g., cyber, physical, and insider threats are not currently covered in many election training procedures) and review content (e.g., setup and teardown procedures/protocols). A module-based approach has been shown to be a successful pedagogical approach in education and was selected for the proposed voting processes training because: (1) the module-based approach is an easy and effective way to integrate new knowledge into existing courses/training [14]; (2) course/training content modules are appropriate learning vehicles for diverse learners [15]; and (3) a library of poll worker focused training modules is a reusable and extensible resource that can be readily adapted for other precincts/states.

Following pedagogical research, all poll worker training modules were designed to reduce cognitive overload and focus the poll worker's efforts on attaining the content. Specifically, this was done through:

- Segmentation: Presenting a large amount of information all at once can increase extrinsic cognitive load, and pedagogical research suggests that breaking large amounts of information into logical, smaller chunks (i.e., segmentation) can reduce a user's cognitive load and better facilitate learning [16]. In all developed education modules, content was segmented into tabs (i.e., Introduction, Background, Equipment/Process Management, Cyber Threats, Insider Threats, Physical Threats) to reduce cognitive load, and a user cannot proceed to the next tab until successfully completing the assessment questions.
- Interactivity: Interactivity/dialoguing provides a user with immediate feedback to questions related to the current content. Immediate feedback through dialoguing enables users to relate the provided feedback to the current content [17-18]. In all developed poll worker training modules, interactivity/dialoguing was utilized in each tab's assessment questions that, once answered, provide immediate feedback to the user (through green/red coloring to indicate the correct/incorrect assessment question answers).

To deploy the developed poll worker training modules for broad dissemination and use, the established Security Injections@Towson e-learning system was used [17]. The Security Injections@Towson project is increasingly recognized as a model for introducing secure coding in lower-level programming classes. To date, over 360 faculty across 221 institutions have completed more than 3,100 cybersecurity modules. The efficacy of this platform has been established in the literature, and a natural extension of its design is to this training context. Further information about the application of this platform for elections security can be found in [6].

4. Usability Study

Scala et al. [7] establishes that poll workers learn about cyber, physical, and insider threats by interacting with these modules. In that study, poll workers and potential poll workers took a pre-test quiz, completed a training module, and then took the same quiz again as a post-test. Results show that the post-test scores statistically significantly increased across each of the three modules and categories of threat (cyber, physical, and insider). However, in addition to an increase in poll worker cyber, physical and insider threats awareness, the design of the training modules and online platform must be usable and accessible to poll workers in order to be widely disseminated and adopted for future elections. Measuring the usability of a developed system before extensive deployment is critical to ensure that it is easy for the intended users to interact with. For example, Meiselwitz and Sadera studied the relationship of usability and learning outcomes in a web-based asynchronous learning environment in a college setting and statistically showed that when overall system usability increases, overall student learning experience also increases [18]. Usability is assessed along three dimensions: effectiveness, efficiency, and satisfaction [19]. Usability assessments can employ quantitative (e.g., time to complete a task) and/or qualitative metrics. The use of subjective metrics in usability studies allow for comparisons across several systems because they are less task specific [20]. For this research, the use of subjective metrics in the usability study provides stronger user interface (UI) validation and enables intended user feedback to become UI enhancements prior to deployment.

To ensure that the developed online education modules were easy to use and accessible for a diverse population of poll workers, a System Usability Scale (SUS) survey [21] was conducted. A SUS survey allows for an "extremely simple and reliable tool" for assessing the perceived usability of a system [22]. While there are a number of usability study surveys that employ subjective metrics, the SUS survey was selected for this study because it is freely available for public use, easy to administer to intended users, has strong reliability and validity measures, and has been frequently used to assess mobile and web applications, providing strong benchmark comparisons [20]. For quantitative usability studies such as SUS, Nielsen suggests using at least twenty users to get statistically relevant results [23].

As shown in Figure 2, the SUS survey consists of 10 questions to be answered by the system's intended users with a rating from Strongly Disagree to Strongly Agree. A participant's individual usability scores are calculated and validated by [24]:

> *For odd numbered questions, subtract 1 from the initial rank value to get a new value. For even numbered questions, subtract the initial rank value from 5 to get the new value. After computing the new values for each question, adding them together to get their sum and then multiple that sum by 2.5. The resulting value will be the usability score and can range from 0 to 100.*

The individual usability scores for each participant are then averaged to determine the overall system usability and assessed using the Acceptability Ranges, Grade Scale, and/or Adjective Ratings shown in Figure 3.

		Strongly Disagree				Strongly Agree
1.	I think that I would like to use this website frequently.	☐	☐	☐	☐	☐
2.	I found this website unnecessarily complex.	☐	☐	☐	☐	☐
3.	I thought this website was easy to use.	☐	☐	☐	☐	☐
4.	I think that I would need assistance to be able to use this website.	☐	☐	☐	☐	☐
5.	I found the various functions in this website were well integrated.	☐	☐	☐	☐	☐
6.	I thought there was too much inconsistency in this website.	☐	☐	☐	☐	☐
7.	I would imagine that most people would learn to use this website very quickly.	☐	☐	☐	☐	☐
8.	I found this website very cumbersome/awkward to use.	☐	☐	☐	☐	☐
9.	I felt very confident using this website.	☐	☐	☐	☐	☐
10.	I needed to learn a lot of things before I could get going with this website.	☐	☐	☐	☐	☐

Figure 2: System Usability Scale [21]

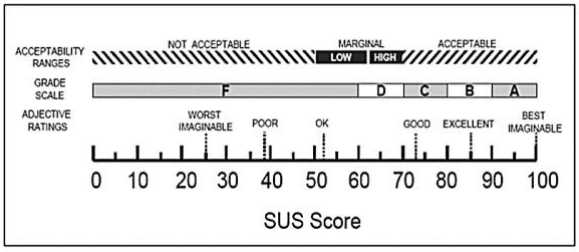

Figure 3: System Usability Scale Grading Scale [21]

For this study, the SUS survey was administered to 48 experienced poll workers during an in-person data collection in summer 2019. These poll workers are a subset of the respondents in [7] and participated in the SUS survey after interacting with at least one of the three modules. In this population, 65.9% identified as female and 34.1% as male. Regarding age, 4.8% were over 75, 61% were 56-74, 24.4% were 40-55, and 9.8% were 24-40 years old. Almost half (48.8%) indicated extreme comfort with computers, while 34.1% indicated very comfortable, 12% were comfortable, and 2.4% said somewhat comfortable. No personally identifying information was collected for any participant, and the Institutional Review Board at the authors' academic institution reviewed this study. The goal is to assess the perceived usability of the education modules by its intended users (i.e., poll workers). Of the 48 completed surveys, two surveys were removed due to straight lining, and an additional two surveys were removed due to being incomplete, yielding 44 usable individual usability scores. After removing invalid surveys, the overall usability score was calculated as 84.15. Based on the Acceptability Ranges, Grade Scale, and/or Adjective Ratings shown in Figure 3, this falls in the Acceptable range/B grade/Good-Excellent ranking. Thus, this work considers the developed training modules to be usable and ready for deployed use. As such, these modules were then deployed to over 1,900 poll workers in a partnering county during the 2020 General Election.

5. Concluding Remarks

Poll workers are the first line of defense to protect the U.S. election infrastructure at local polling places where votes are cast and tabulated. As such, poll workers need to be equipped to be able to identify and mitigate cyber, physical and insider election threats that may arise during the election process. This work partnered with BoEs of two counties from a mid-Atlantic state to develop, validate, and pilot election-specific threat training modules for poll workers that were designed specifically with effective pedagogical strategies and shown, through a usability assessment, to be usable and accessible for the intended poll workers. The combination of effective training modules deployed on a widely used, pedagogically informed, and usable online platform can empower local polling places to improve the security of election infrastructure through intentional cyber, physical, and insider threat training for poll workers.

Acknowledgements

This research is partially supported by Towson University's School of Emerging Technologies.

References

[1] Department of Homeland Security, "Election Security," 2017. https://www.dhs.gov/topic/election-security (accessed Dec. 30, 2020).

[2] U.S. Senate Intelligence Committee, "Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election," 2019. [Online]. Available: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

[3] U.S. Election Assistance Commission, "EAVS Deep Dive: Pollworkers and Polling Places," 2017. [Online]. Available: https://www.eac.gov/documents/2017/11/15/eavs-deep-dive-poll-workers-and-polling-places.

[4] United States Election Assistance Commission Advisory Board, "Help America Vote Act," 2018.

[5] D. Sanger and C. Edmonson, "Russia targeted election systems in all 50 states, report finds," *The New York Times*, Jul. 25, 2019.

[6] N. M. Scala, J. Dehlinger, L. Black, S. Harrison, K. Licona Delgado, and A. Ieromonahos, "Empowering Election Judges to Secure Our Elections," *Baltimore Business Review: A Maryland Journal*, 2020.

[7] N. M. Scala, J. Dehlinger, and L. Black, "Preparing Pollworkers to Secure U.S. Elections," 2021.

[8] E. Lazarus, D. L. Dill, J. Epstein, and J. L. Hall, "Applying a Reusable Election Threat Model at the County Level," in *Proceedings of the 2011 Conference on Electronic Voting Technology/Workshop on Trustworthy Elections*, 2011, pp. 1–14.

[9] D. Cahn, "Risk assessment: How secure are voting machines," University of Pennsylvania, 2017.

[10] M. Price, N. M. Scala, and P. L. Goethals, "Protecting Maryland's Voting Processes," *Baltimore Business Review: A Maryland Journal*, pp. 36–39, 2019.

[11] H. Locraft, P. Gajendiran, M. Price, N. M. Scala, and P. L. Goethals, "Sources of Risk in Elections Security," In *Proceedings of the 2019 IISE Annual Conference*, 2019.

[12] K. K. Keene and D. E. Livingston, "Election Judge Manual 2016," 2016.

[13] United States Election Assistance Commission Advisory Board, "Election operations assessment: Threat trees and matrices and threat instance risk analyzer (TIRA)," 2009. [Online]. Available: https://www.eac.gov/assets/1/28/Election_Operations_Assessment_Threat_Trees_and_Matrices_and_Threat_Instance_Risk_Analyzer_(TIRA).pdf.

[14] B. Goldschmid and M. L. Goldschmid, "Modular instruction in higher education: A review," *High. Educ.*, vol. 2, no. 1, pp. 15–32, Feb. 1973, doi: 10.1007/BF00162534.

[15] "Computer Science Curricula 2013 - Curriculum Guidelines for Undergraduate Degree Programs in Computer Science," 2013. [Online]. Available: http://www.acm.org/education/CS2013-final-report.pdf.

[16] M.-C. Tseng, "The Difficulties that EFL Learners have with Reading Text on the Web," *Internet TESL Journal*, vol. 14, no. 2, 2008.

[17] S. Kaza, B. Taylor, H. Hochheiser, S. Azadegan, M. O'Leary, and C. F. Turner, "Injecting Security in the Curriculum – Experiences in Effective Dissemination and Assessment Design," In *The Colloquium for Information Systems Security Education*, vol. 8, 2010.

[18] G. Meiselwitz and W. A. Sadera, "Investigating the Connection between Usability and Learning Outcomes in Online Learning Environments," *Journal Online Learning Teaching*, vol. 4, no. 2, pp. 234–242, 2008, Accessed: Mar. 18, 2021. [Online]. Available: https://www.researchgate.net/publication/273993682.

[19] I. 159/SC 4 E. of H.-S. I. Subcommittee, "Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs).: Guidance on Usability. International Organization for Standardization," 1998.

[20] P. T. Kortum and A. Bangor, "Usability Ratings for Everyday Products Measured With the System Usability Scale," *International Journal on Human Computer Interactions*, vol. 29, no. 2, pp. 67–76, Jan. 2013, doi: 10.1080/10447318.2012.681221.

[21] J. Brooke, "SUS: A 'Quick and Dirty' Usability Scale," in *Usability Evaluation In Industry*, CRC Press, 1996, pp. 207–212.

[22] J. Brooke, "SUS: A Retrospective," *Journal of Usability Studies*, vol. 8, no. 2, pp. 29–40, 2013, doi: 10.5555/2817912.2817913.

[23] J. Nielsen, "How Many Test Users in a Usability Study?," *Nielsen Norman Group*, 2012. http://www.nngroup.com/articles/how-many-test-users.

[24] N. Thomas, "How To Use The System Usability Scale (SUS) To Evaluate The Usability Of Your Website." https://usabilitygeek.com/how-to-use-the-system-usability-scale-sus-to-evaluate-the-usability-of-your-website/ (accessed Dec. 28, 2020).