Empowering Election Judges to Secure Our Elections

Lorraine Black and Saraubi Harrison • Advisors: Dr. Natalie M. Scala and Dr. Josh Dehlinger

In collaboration with the Harford County Board of Elections

Abstract

This research develops and creates educational modules that will increase back-end security of the State of Maryland’s election process. An increase in security will be achieved by educating Election Judges on cyber, insider, and physical threats that pertain to their specific role within the election process as well as informing them of actions to control, mitigate, and/or eliminate these threats.

The security of elections in the United States has been particularly scrutinized within the past few years. While most media attention has been paid to foreign actors potentially tampering or meddling with voter databases and votes, attention must also be paid to back-end activities occurring inside polling places. Training modules for Check-In, Provisional, and Scanning Unit Judges are developed in partnership with Harford County. The efficacy and effectiveness of the educational modules are tested via a pre-post test and usability study.

The goal of the research is to empower Election Judges to take an active role in back-end security and encourage adoption of the training across the entire state. The more aware Election Judges are to threats that pertain to their specific role and the more knowledgeable they are to properly handle these threats, the more secure our elections can be.

Example Threats and Mitigations

Check-In / Electronic Pollbook Judge

Physical

An individual steals the passwords for voting equipment & resets the settings to the machines prior to election

Watch/assist other Election Judges, when able, to ensure all steps are being done correctly

Provisional Voting Judge

Insider

Election Judges may compromise ballots by error, carelessness, distraction, or deliberate means

Each voter must present their Voter Authority Card with ballot reason and proper signatures

Scanning Unit Judge

Cyber

A malicious cyber actor overwrites unprotected memory on flash drives used by optical scanners

Have more than one person assist in set up of the Scanning Unit & always stand within two feet of unit when in use

Notes:

Training Modules

Next Steps and Acknowledgements

• Pilot each Election Module
• Conduct a pre-post test and a usability study

This project is partially supported by Towson University’s School of Emerging Technologies and the BTU Initiative.