CENTER FOR DEMOCRACY & TECHNOLOGY

ELECTIONS
Short, simple, usable guides to help election administrators and staff better understand key concepts in cybersecurity.

PHYS SEC

Election Cybersecurity 101 Field Guide: Physical Security Field Guide

Physical safeguards are an essential part of securing elections infrastructure. If left unsecured, elections infrastructure components (e.g., machines, memory cards, and ballot drop boxes) can be stolen, damaged, tampered with, or corrupted.

Although most cyber attacks are conducted remotely, cyber attacks may be initiated by someone gaining physical access to a voting machine. An attacker with physical access to a machine could insert a memory card or plug in a USB drive, installing malware and potentially altering vote counts on the machine. That malware could even infect other voting machines, including the final vote tabulator. Unique security challenges are posed by the public nature of polling places and the requirement that voters be able to use machines to cast a secret ballot.

The coronavirus pandemic may have introduced additional concerns about the functionality and availability of physical facilities. Some polling places may be locations that have been largely unused or uninhabited since the start of the pandemic, such as school buildings. Accordingly, systemic problems (like animals chewing through electrical systems) may have gone undetected, only to present themselves as the polling place is set up. These physical concerns may be just as disruptive to elections as remote attacks, so it is important that election officials have plans in place to mitigate them.

[Mitigating Physical Attacks]

Different types of physical attacks or concerns will require different approaches, several of which are discussed below.

Ballot drop box security: This year, many municipalities have begun to offer ballot drop boxes for voters who choose to vote absentee and prefer to drop their vote off rather than send it through the mail. These boxes may be indoor drop-off points or heavy-duty outdoor steel boxes. All drop boxes should be locked, tamper-proof, and monitored either by in-person surveillance or 24-hour video surveillance in well-lit locations.

Tamper-evident devices: Voting machines should be equipped with tamper-evident devices. Tamper-evident devices may be seals, stickers, or locks that, if tampered with, become visibly different in a way that is irreversible. They may deter attackers and should indicate to election officials that something has gone awry, allowing them to take necessary mitigation steps.

USB port locking devices: Port locking devices can offer some protection from hackers who would otherwise use an open USB port to upload malware onto a machine. These devices are designed to either lock an input into place in a port, or lock the port closed so that no input can be inserted. Some USB port locking devices are tamper-evident (see above).

Physical access controls: Access to voting machines must be managed both before and during elections. Before elections, machines should be stored in locked facilities with 24-hour video surveillance and

controlled access. Facility managers should maintain logs of everyone who accesses the facility and their reason for doing so. Additionally, inventory and maintenance logs should be maintained for all stored equipment to ensure that it is accounted for and in good working order.

Building preparation: For polling sites that have been unused or minimally used for several months due to the pandemic, it may be necessary to do more set up than is typical. Officials should run tests to ensure that the infrastructure of the building, such as the electricity and internet are in good working order. If any voting machines will be stored at the polling place prior to the election, ensure that they can be secured by testing the locks on doors and windows into the storage location.

Voter access: Election officials must allow voter privacy while still ensuring that an attacker masquerading as a voter does not tamper with equipment. Election officials should make vulnerable elements of a voting machine, such as its power supply and ports, visible to poll workers but inaccessible to voters while they are inside the privacy screen of the voting booth.

[Conclusion]

Physical security, like cybersecurity, is a key component of maintaining safe and trustworthy elections. We hope that this guide and the resources listed here help you in your important work.

[Additional Resources]

- https://www.lawfareblog.com/rise-ballot-drop-boxes-due-coronavirus *(drop boxes)*
- https://www.eac.gov/sites/default/files/eac_assets/1/6/260.pdf *(mention of tamper-proof port locks)*
- https://www.electioncenter.org/national-association-of-election-officials/election-security-infrastructure/Election-Center-Checklist-Elections-Security-Checklist-Released-2017-05-22.pdf *(checklist includes a physical security section, but it is a bit basic in some ways and maybe overkill/achievable in other ways)*
- https://www.sos.state.tx.us/elections/forms/election-security-best-practices.pdf *(checklist for physical security of machines including tamper proof seals (TX))*
- https://www.eac.gov/documents/2017/10/14/ten-things-to-know-about-managing-aging-voting-systems-voting-technology-voting-systems-cybersecurity *(physical security on aging systems, includes basics lille tightening screws)*
- https://www.cs.princeton.edu/~appel/voting/SealsOnVotingMachines.pdf *(failures of tamper evident seals. Includes references to vendor pages.)*
- https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120 *(physical security more generally)*
- https://www.securitymagazine.com/articles/92518-the-need-for-cybersecurity-and-physical-security-convergence *(convergence of physical and cybersec)*
- http://aceproject.org/ace-en/topics/vo/vof/vof04/vof04b *(some discussion of physical security including concerns like crowd control and site selection. Search for "Voting Site Security".)*
- https://fedtechmagazine.com/article/2009/02/dont-put-walls-between-your-security-people *(joining physical and cyber sec.)*
- https://padlocks4less.com/usb-port-locks/ *(example of keyed USB port locks.)*

For more info, contact Mallory Knodel (mknodel@cdt.org) or Will Adler (wadler@cdt.org). Other election security resources: bit.ly/CDTelectsec.