Election Systems and Their Network Connections

Any given piece of election technology fits into one of three classes of “connectedness” based on how they interact with networks, other systems, and the internet. This connectedness is extremely influential in the overall risk profile–the types of attacks the technology might face–and thus is a good starting point for threat modeling.

While there are many components to a complete election system, many of the cybersecurity risks associated with them can be grouped to simplify the steps to manage risk. One approach to this is by analyzing the manner in which they connect to networks and other devices.

The three connectedness classes are:

1. **Network connected systems and components**. Network connected components are interconnected with other devices to achieve their objectives, whether through the internet or internal networks, hardwired or WiFI or Bluetooth. The level of interconnection, while providing various benefits, also introduces additional risks that must be taken into consideration when managing the lifecycle of the device. Most network connected devices will provide a remote means for accessing and managing the devices, which means organizations must make extra efforts to protect access to those capabilities. Network connected devices do not necessarily have to be connected to the internet, nor does their connection have to be persistent. Examples include:
    - Digital voter registration systems.
    - Election results transmission via cellular modems or the plain old telephone system.
    - An Election Management System (EMS) connected to a private county network.
2. **Indirectly connected systems**. Indirectly connected components are not connected to a network at any time and are not persistently connected to other devices. They do, however, have to exchange information with other elections system components including network connected systems in order to complete their objectives in the election process. These information exchanges are done using removable media such as USB drives. While the risks associated with being connected to a network or the internet are no longer relevant, threats are introduced by exchanging information with other devices, either through the use of removable media or a direct connection to another device such as a printer or an external disk drive. Examples include:
    - Using a USB stick to transfer ballot definitions and other election information to a vote capture device such as a ballot marking device.
    - Using write-once removable media to transfer precinct definitions from a networked machine to an election management system.
3. **Non-digital elections components**. These are aspects of the elections process that have no digital component but still may face relevant risks through business processes. An example would be the mailing, completing, and returning of a paper mail-in ballot. While aspects of the overall process—-such as an online request for a ballot–may leverage digital infrastructure, the aspect of this process that is purely paper-based does not face the same cybersecurity risks.

Transmission between components creates vulnerabilities

While securing elections systems components is important, one of the largest sources of vulnerabilities, and thus most common methods of attack, lies not in the systems but in the transmission of data between systems. Weaknesses in communications protocols, or in their implementation, risk exposure or corruption of data, even for systems that are otherwise not network connected.

For instance, while paper pollbooks wouldn’t typically have cybersecurity risks, if the data for the pollbooks is sent electronically to a printing service, this transmission introduces risks that must be addressed. Similar vulnerabilities exist in transmission of ballot layout information to printers or in loading ballot information into ballot scanning (i.e., vote capture) devices. These transmission risks must also be managed.