Election Security Workshop
December 12th, 2017

	Dan Wallach's "HOWTO"	Belfer Center's "Playbook"
Problem Statement *and* Adversarial Model	Problem: - espionage (leaked secrets) - sabotage (data corruption or destruction) Adversaries: - criminal hackers - foreign nation-state governments Types of attack: 1. Untargeted, remote (phishing, ransomware) 2. Targeted, remote (spear phishing) 3. Targeted, in person (snooping, police)	Problem: - increased digitization + human error - campaigns are vulnerable Adversaries: - nation states - hacktivists Types of attack: 1. Breach + release of secrets to public 2. Overloading of websites 3. Theft of donor data 4. Destruction of digital infrastructure
Proposed Solutions	Know Your Tech: - update all equipment and software - best of breed cloud services (Google) - beware of apps and antivirus software - 2FA, but not verified through SMS - never directly handle credit card data - DNS security How to Communicate: - secure cloud office suite (Google, Slack) - interview 3rd party providers about security - discourage comms with personal devices - look for https connections - assume all social network behavior is public Threat-Specific Considerations: - for legally compelled attacks, use encrypted communication (Signal) and anonymous browsing (Tor) - for extra sensitive matters, use air-gapped computer + CDs or physical dead drops Basic Operational Security: - don't put foreign USBs into your computer - charge phone with charger, not computer - assume mic and camera are always on - pay attention to surroundings - backup all devices	The Human Element: - provide basic and ongoing security training - additional training for VIPs - thorough vetting of all staff - system of classification for campaign data Communication: - secure cloud office suite (Google, Microsoft) - encrypted messaging (Signal, Wickr) - switch off archiving; turn on auto-delete - no campaign business on personal accounts Account Access and Management: - 2FA, but not verified through SMS - require strong passwords - separate accounts for admins and users Incident Response Planning: - legal counsel and technical experts - incident response team with chain of command Devices: - new equipment if possible, else strong policies - updated operating systems - cloud backups and remote wiping - change defaults, auto-lock, require encryption - install vetted endpoint security apps Networks: - segmented cloud-based storage - access to content invitation only - separate guest WiFi, encrypted connections - VPNs (wary of free ones) and secure browsers - don't connect to unknown ports or devices

Discussion Questions:

1. What are some similarities and differences between the two sets of recommendations?
2. Which of the recommendations do you feel is most relevant or important in our current climate? Why?
3. What changes might you make to the content or format of either document before presenting it to a campaign?