

# Elections Security in Wisconsin



# Agenda

1. Elections Security in Wisconsin 2019
2. Plans for 2020
3. Discussion
4. Conclusions



# Election Security in Wisconsin

## Where are we now?



# A Reminder: Wisconsin is Unique

## Wisconsin

## Other States

# of Jurisdictions	Many	Few
Command & Control	Decentralized	Centralized
Computer Networks	Decentralized	Centralized
Voting Equipment	Many Types	Few (or one) type
Paper Ballots	100% Paper Trail	Paper and Digital
Voter Registration	Same Day	Advance only
Voter Identification	Photo ID Required	No Photo Required



# 2016-2019: What Changed?

## Federal:

- Designation of elections as critical infrastructure.
- Creation of the Cybersecurity and Infrastructure Security Agency (CISA)

## State:

- Multifactor Authentication, Tabletop Exercises, Securing WisVote Training
- Expanded the audit process to include all counties
- Election security staff

## Local:


- What changes have you seen? Is there increased awareness?

# Plans for 2020

## Where are we going?




Election Security Tabletop Exercise  
Pyle Center, Madison  
May 31, 2018



“They’re going to keep going  
after the basics until we take  
the basics away.”

Christopher Krebs

Director of the Department of Homeland  
Security’s Cybersecurity and Infrastructure  
Security Agency (CISA)



“They’re going to keep going  
after **the basics** until we take  
the basics away.”

Christopher Krebs

Director of the Department of Homeland  
Security’s Cybersecurity and Infrastructure  
Security Agency (CISA)





# Who Remembers?

I LOVE YOU 

Damaged 50 million computers and 10% of the internet in ten days.

\$15 billion of damage

Where did it go?



# Plans for 2020

1. Expanding the TTX program
2. Hardware loaner program
3. Endpoint testing
4. Public information campaign
5. Secure Communications
6. Pending proposals

# Discussion





# TRUE or FALSE?

You'll know if your computer is infected or hacked.

**FALSE.** Modern malware is stealthy and hard to detect. Phishing campaigns often gather information for months before taking any action.



# Discussion

Who would you call if you suspected malware?



# TRUE or FALSE?

Hackers usually target large jurisdictions and businesses.

**FALSE.** Over half of all cyber-attacks target small organizations. In fact, you don't have to be targeted at all. The 2017 NotPetya attack did \$10 billion of 'collateral damage.'



# Discussion

How would you respond if a computer in your office had ransomware two weeks before an election?



# TRUE or FALSE?

Going to paper (or disconnecting) minimizes risk.

**SORTA.** But . . . disconnected systems are harder to monitor and receive security patches less often.





# Discussion

How would you replace your computer systems if they were unavailable?



# TRUE or FALSE?

I comply with password requirements so I'm safe.

**FALSE.** We mostly use passwords that are hard for people to remember but easy for computers to guess.



# Discussion

How long is your password?



# Passwords: Good News & Bad News

Old Guidance	New Guidance*
Complexity over length	Length over complexity
Hard to remember is good	Complexity is the enemy of security
Change passwords frequently	Change passwords for a reason
A good password is enough	Multifactor is the future

\* National Institute of Standards and Technology (NIST) Digital Identify Guidelines 800-63B (5)



# TRUE or FALSE?

The most common cybersecurity risks are inside the office.

**TRUE.** Up to 75 percent of data breaches are caused by an insider action - either accidental or deliberate.



# Discussion

Do you trust all your office staff not to click that suspicious link?

What training does office staff receive?



# TRUE or FALSE?

The IT department will take care of it.

**FALSE.** If employees aren't properly trained they will end up downloading malware through emails or unsafe websites. We are all responsible for cybersecurity.



# Discussion

Who ensures that computers receive regular patches?

What about in your municipalities?



# Conclusions





# What We Can (All) Do

We need your help.

- **Communicate:** *Elections in Wisconsin are locally run and backed by paper ballots.*
- **Educate:** Teach others about the risks of phishing, malware, and exploits.
- **Safeguard:**
  - Endpoint Protection
  - Firewalls
  - Update Software
  - Strong Passwords
  - Multi-Factor Authentication
  - Back Up Regularly



# Thank You

Robert Kehoe

Wisconsin Elections Commission

Robert.Kehoe@wi.gov

SecureElections@wi.gov

608-261-2019

