**CYBERSECURITY CONVERSATION STARTER**

**IT: Intermediate**

# Learnings to share with your it colleague

I’ve been learning about how to p**rotect and prioritize sensitive data** that’s held in different sections of our election system.

I’ve seen how the National Institute of Standards and Technology’s **Identify--Protect--Detect--Respond--Recover framework** can be applied to different sections of our election system. For instance, with election-night reporting, I’m thinking about how it’s important to identify who has access to the system and how, if something bad did happen, we’d need to respond by publishing results over another channel.

I’ve gotten exposed to some great **partnerships** that provide free resources. For instance, I know that Department of Homeland Security offers free vulnerability scanning.

# Questions to ask your IT colleague

Do you maintain an **inventory to track IT assets**? I know it’s important to have one, so we should make an effort to create and maintain our inventory.

I know that in the event of an attack on our VR database or EMS, we should **disconnect from the network**. Can you talk about how you would do that?

Let’s talk about the [**FINRA cybersecurity checklist**](https://www.finra.org/compliance-tools/cybersecurity-checklist) and how it might apply to our local election system

I’d like to integrate more cybersecurity ideas into our **training for seasonal staff**. For instance, I want to stress the one-way/one-time rule with media storage devices. Are you willing and able to review a draft of my training materials and/or visit the training classes to speak about cybersecurity?

The **Cybersecurity and Infrastructure Security Agency (CISA)** [offers election departments free services](https://www.cisa.gov/election-security) like phishing campaign assessments and vulnerability scanning. Have we done things like this in the past? Could we benefit from these services in the future?

Are we members of **MS-ISAC or EI-ISAC**? I know these partnerships provide lots of good resources and cyber threat updates.

Do we have **denial-of-service protection** in place? Protection services are available for free from [Cloudflare’s Athenian Project](https://www.cloudflare.com/athenian/) and [Google’s Project Shield](https://projectshield.withgoogle.com/landing).

I’ve heard that sometimes **other local government offices** like the Sheriff and Tax Assessor have cybersecurity training or systems that could also benefit the election office. Are you aware of any local government offices that have cybersecurity resources that might benefit elections?

I understand that cybersecurity requires resources. In closing, do you have any **resource needs** that you’d like to talk about? Can I be an advocate to help you get the resources you need?