ITEM NO.
11.1

DIRECTOR AB 1234 REPORT

Director Name: Kathye Armitage

Meeting Attended: Webinar: Is Your Water Supply Safe from Cyberattacks?

Date of Meeting: April 28, 2021

Location: Virtual

Board Meeting to Be Presented At: May 4, 2021

Points of Interest:

- Host: Association of Water Agencies of Ventura County (AWA)

- Guest speakers:
  - Drew Batten
    - Department of Homeland Security ~ Cybersecurity & Infrastructure Security Agency
  - Marylu Smith
    - Federal Bureau of Investigation (FBI)

- Key points from Drew Batten's segment:
  - The Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) monitors and assesses threats to sixteen different sectors
    - Water infrastructure is one of those sectors
  - They assess where the risks are and how adversaries are likely to attack them
  - Four areas they focus their work around
    - Federal network protection
    - Comprehensive cyber-protection
      - They have a team ready to deploy to help with networks that have been attacked
    - Infrastructure resilience and field operations
      - They provide best practices, white papers, research, alerts about bad domains/IPs
      - They provide free tools for agencies to use
        - **Is our agency aware of these tools and are we using them?**
    - Partnership development
      - Developing relationships with community partners is vital
        - It's important to them to have the perspective from those who operate utilities and understand the on-the-ground issues
      - They provide free technical assistance, tools, and exercises/training to agencies/utilities

        - **They have a team that will come to your agency for a couple of days and run exercises with them to help identify weaknesses**
            - **Can we request this?**
        - They also have a 3-4 day class to learn about defensive tools for high-level industrial control systems
    - They have a National Cyberincident Response Plan
        - There is a "watchboard" with representatives from various agencies that consult with each other and help distribute information about potential attacks and actual attacks
            - **Is our agency connected to this information?**
    - Operational Technology vs Information Technology
        - There can be competing department priorities
        - Cybersecurity often isn't given attention and resources until there is a problem
        - Fancy tools don't necessarily mean better protection
            - You need three things
                - People who know what they're doing
                - Tools to help do the work
                - Access to the data and understanding about how to use it
    - Remote access to control systems
        - Understand and implement best practices
    - Be aware of publicly accessible information
        - Photos shared online and on social media can reveal information that should be protected
        - Job postings should not include information specific to IT systems software packages

- Key points from Marylu Smith's segment:
    - The FBI has a unit that covers critical infrastructure and looks at what happens during attacks from the victim's point of view
        - They assess how it was attacked, how to recover, and who the attacker was
        - Water and Wastewater is one of the sectors they assess
            - Vital because everyone needs clean water to live, but also because of the intersection between water and energy sectors
    - Effects of cyberattacks
        - Possible water contamination or impact to flow of water to community
        - Attack on business operations
    - How this is done
        - Malware that compromises systems
        - Ransomware
        - Insider threats from people familiar with systems manipulating them
    - Examples of attacks
        - Unauthorized remote access to SCADA system in Florida due to outdated software
        - Unauthorized remote access to chemical levels in a California system by former employee whose credential were not removed in a timely fashion

        - **Human Resources departments needs to prioritize disabling credentials for employees who don't leave amicably**
    - SCADA systems in Nevada and North Carolina were hacked and held ransom
- Mitigation
    - Multi-factor authentication
    - Strong passwords to protect RDP
    - Up-to-date anti-virus, spam filter and firewalls
    - Identify and suspend access of users exhibiting unusual activity
    - Audit
        - Network configurations and isolate computer systems that can't be updated
        - Networks for systems using RDP, closing unused ports, applying two-factor authentication when possible, and logging RDP login attempts
    - Train users to identify and report attempts at social engineering
    - Keep software updated
        - **Are we implementing all these mitigation strategies?**
- FBI involvement
    - If you think you're experiencing an attack, contact:
        - Los Angeles Field Office
            - Ventura Resident Agency
            - InfraGard
                - Partnership between FBI and agencies
        - Internet Crime Complaint Center
            - IC3.gov
        - Water-ISAC
            - waterisac.org
                - 60% of utilities belong to this group
                    - **Are we part of this?**
                - They give information to support and protect utilities