Cybersecurity Readiness Checklist

Prepared by the APCO Cybersecurity Committee

Please Note: the checklist order will vary for each ECC and each agency will prioritize the list differently.

Back-up and restore capability (Data, HW and O/S) (cloud and disconnected, off-prem) – The number one thing ECC's need in order to protect themselves from a cyberattack, such as ransomware. Paying ransom does not guarantee you'll get the key to unlock the encryption, and worse, even if you do get the key, you will still need to restore your environment because its infected. The ability to quickly get back up and running is key to managing cybersecurity.

US Cert Reference

A well-defined COOP – A COOP plan should include aspects related to cybersecurity (when to call, who to call, how to react, how to initiate restore processes, etc.).

- COOP must include response planning as well as DDOS/TDOS mitigation and preparation.
- Prevent the Cyber Insurance from driving the response.

US CERT Cyber Incident Response Plan

NIST Reference

Patch management capability – These are tools that allow admins to follow a patch management process are crucial to any IT environment. IT in the ECC has special concerns regarding patch management, and patches cannot be deployed without testing and affirmation from vendors that the patch will not affect operations. Therefore, this item should also include the concept of a "sandbox" environment that can be used to test patches prior to deployment.

NIST Reference

Microsoft Windows Update Services

Two-factor authentication. – The ECC environment is "vendor-rich", and there are folks in and out of the client systems all the time. At a minimum, there should be a third-party, multi-factor authentication in place to control and track who has access, when they were in, and what they did.

NIST Reference

Password management tools - These are designed to do everything from create strong passwords, to store passwords in a repository or identify if someone has created a weak password, based on defined rules. Stronger passwords in the ECC environment would raise most PSAP cyber profile by 40%. There are many tools available with a simple online search. Whatever tool you select, look for the following.

- Ease of Use
- Knowing the Security method of the tool (how does it secure your data)
- Is it offline or online

Firewall – Purchase the best firewall that your agency can afford. The firewall should include Nextgen services such as intrusion protection services, application filtering and SSL decryption. The firewall should be correctly configured and well maintained.

NIST Reference

Cybersecurity monitoring capability (ideally as part of a wholistic IT monitoring capability) – The TFOPA and NIST guidelines both make monitoring of an assessed network a priority and one of the six pillars of a strong cybersecurity strategy. One must monitor the remediations put in place and ensure that no new vulnerabilities appear.

TFOPA Report

NIST Reference

Regular Cybersecurity Assessments – Initial assessment creates the baseline understanding of network vulnerabilities; follow-on assessments track improvement and catch new vulnerabilities.

NIST Reference

Cyber Insurance - Make sure you're educated and informed on the options you have to provide for any expenses related to third party liability, or direct expenses related to recovery from an attack that are incurred operationally or directly related to resolving the incident itself (such as legal, forensic or credit monitoring services).

CISA Reference

IT Management and Cybersecurity Oversight committee – The formation of a state-level body as part of the legislature (top down 911 oversight) that defines and helps ECC's maintain minimum IT and cybersecurity standards

Harvard Law School Article

- Placeholder for APCO document labelled "Who Should own and drive Cybersecurity in the ECC"

Cybersecurity Training – A complete training plan for end users, technical and executive staff that will teach about cybersecurity risks and threats, as well as how to manage those threats. This can often include phishing simulation and testing.

NIST Resources

CISO or equivalent - Every agency should have a person or vendor who is responsible for cybersecurity at the center. This can be someone in an existing dedicated position such as a director or in a larger environment a Chief Information Security Officer.

CISO Handbook