A Simple Cybersecurity Strategy and How to Implement it at Your ECC

Prepared by the APCO Cybersecurity Committee

Introduction

The rise of the Big Three Nets (FirstNet, ESINet and the Internet of Things) has provided public safety emergency communications with ever-increasing opportunities for improved interoperability and data sharing with modern solutions that had not been possible previously, reducing response times, and increasing operational efficiencies resulting in more saved lives. However, with this increased opportunity comes increased risks. Incidents of cybersecurity attacks against ECC networks are rapidly and relentlessly increasing. Ransomware, once a fairly obscure form of attack, has become the primary type of attack against ECC's because cyber thugs assume their life-safety mission will require them to pay. Many do, and cyber thugs are laughing all the way to the bank.

Most ECC boards and directors realize there is a crisis but do not know where to begin. They ask themselves "what do I know about cybersecurity?" They are experts in public safety response, not cybersecurity, and don't know where to begin to create a strong cyber defense strategy.

Luckily, there have been several efforts designed to provide guidance on managing cybersecurity in the ECC, most notably the FCC's Task Force on Optimal PSAP Architecture (TFOPA). The TFOPA Charter lists the duties of the Task Force as:

> 1. Optimal PSAP system and network configuration in terms of emergency communications efficiency, performance, and operations functionality;
>
> 2. Cost projections for conversion to and annual operation of PSAPs that incorporate such optimal system design;
>
> 3. Comparative cost projections for annual maintenance of all existing PSAPs annually and upgrading them to NG911;
>
> 4. Recommendations on ways to ensure states use E911 funding for their intended purpose; and
>
> 5. Whether states that divert E911 funds should be ineligible to participate on various FCC councils, committees, and working groups.

In order to deliver on the various duties included in the charter, sub-committees, or working groups were formed. Working Group One was focused on addressing cybersecurity issues and built upon the National Institute of Standards and Testing (NIST) cybersecurity framework and other sources to devise a simple, easy-to-implement strategy for strengthening cyber defense in the ECC environment.

Six Steps to a Stronger Cyber Defense Strategy

The TFOPA recommendations for Optimal Cybersecurity for PSAPs provide a wide-ranging set of recommendations and best practices which incorporates the NIST Cybersecurity Framework (NCF), the National Initiative for Cybersecurity Education (NICE) Workforce Framework, the Department of Homeland Security (DHS) and Communications Security, Reliability, and Interoperability Council (CSRIC) to develop an overall architecture for PSAPs as they moved from traditional 911 networks to NG911 and ESINets.

From an operational perspective, all of these best practices and recommendations can be boiled down to the following six steps. While it may be an oversimplification of all the information included in Section Four of the TFOPA report, these six items can be used by ECC boards and directors as a pathway to a stronger cybersecurity strategy:

- **Step One: Identify / Discover** – During this phase of the process, the goal is to understand the environment, including the network, the devices, the applications, the roles and responsibilities and policies and procedures. A good inventory of all network elements is identified and documented (you can't protect what you don't know you have). Identify and document all SOPs related to security, the support model and any key regulatory, operational and industry standards.
- **Step Two: Assess / Prioritize –** During this phase it is important to identify and understand all vulnerabilities and areas of risk in your baseline developed from Step One. (you can't fix what you don't know is broke). Conduct an objective third-party, cybersecurity assessment (for the same reason that a bank does a financial audit, namely that if your house is in perfect order, you simply saying so doesn't ***prove*** it ***is*** in perfect order). Once the vulnerabilities have been assessed, prioritize a set of tasks designed to remediate them. Go for the most "bang for the buck", that is the least effort and cost for the greatest value, such as instituting a new, stronger password management protocol. Build a project plan to address the prioritized list of remediations and aggressively manage them, beginning with the highest risk items.
- **Step Three: Implement / Operate –** The goal of this step is to begin to implement the remediation plan into the operational environment and understand the changing and ongoing operational requirements related to the remediations. For example, inserting a new set of backup-and-restore protocols into the normal operation of your networks. During this phase it is time to include regular cybersecurity awareness training into end user training regimens. Lastly, it will be important to more fully understand and manage access controls like:
    - Access to networks, data, applications, infrastructure
    - Authorization – who has access to what
    - Disaster Recovery Planning / COOP plans
    - Physical Security
    - Please refer to the NIST 800-53 standard for the full set of relevant Access Controls
- **Step Four: Monitor / Evaluate –** The goal here is to continually monitor your environment for anomalies and your monitoring tools for effectiveness on an ongoing basis. Define metrics to determine that monitoring capabilities are doing their job, and institute event logging to document network activities.
- **Step Five: Test / Evaluate –** It is important to ensure compliance with the policies, procedures and protocols put in place to increase cybersecurity on an ongoing basis. Test end users to ensure best practices are being followed, and document compliance, not to punish but to establish progress toward more cyber awareness. Regularly review and test disaster and recovery plans, which should be incorporated into larger organizational Continuity of Operations (COOP) Plans, and test systems settings to ensure they are working the way you expect them to work.

- **Step Six: Improve and Evolve –** The idea here is to ensure continuous improvement. This is achieved through the implementation of yearly, objective third-party assessments, measuring progress of remediation plans, and identifying new threats, regular reviews of the remediation plan, and re-assessment of cybersecurity policies and procedures including training needs and plans, and making changes where required.

Following this plan, or some version of it, will increase an ECC's cybersecurity awareness and significantly reduce the risk of a successful cyberattack. No plan is failsafe, but instituting policies relating to backup and recovery, and knowing who to call in the event of a breach will go a long way toward reducing risk and costs associated with a cybersecurity attack at your ECC, at least in the current IT environment.