Who Owns Cybersecurity in the ECC?

Introduction

Due to the 24/7/365 mission-critical nature of their operations, and the life-safety mission they are designed to deliver, ECC networks have become juicy targets for cyber-thugs looking for profit. The past five years have seen a relentless, rapid increase in the number of cyber attacks against ECCs, especially ransomware attacks. The Great Pandemic of 2020 has added fuel to the fire with the rise of COVID-19-related phishing attacks and an unfortunate decline in the resources required to fend them off. In this environment, it becomes harder and harder to define and execute on a cybersecurity strategy and more and more important that everyone recognize the role they play in protecting the networks, data and systems required to deliver the mission. Now, more than ever, it is crucial that roles are clearly defined, protocols are put in place and enforced, and a culture of cybersecurity be instilled.

But who should be the “owner” of a cybersecurity strategy? Who needs to nurture, cultivate and drive the cybersecurity culture that is required to create an environment that makes it difficult for cyber-thugs to crack? While everyone has a role to play in a successful cybersecurity strategy there needs to be someone ultimately responsible for driving it and has their finger on the pulse of how well the strategy is being executed, providing guidance where required, changing course when new threats arise, planning for breaches and executing on those plans when necessary.

Cybersecurity is not a “stand-alone” concept. That is, it is not something that can be managed in isolation from operational, financial, or political considerations. All aspects of ECC operations are affected by, and have an impact on, cybersecurity strategy. It is a grave mistake to assume that “cybersecurity belongs to IT”. While it is certainly true that there is a large technical aspect to cybersecurity that must be managed by IT teams, it is not true that managing only the technical aspects of cybersecurity will address all cybersecurity risks.

Additionally, even the technical aspects of cybersecurity are not isolated, but must be considered in relation to the entire technical environment, including available resources, capabilities and operational considerations and incorporated into the larger IT strategy of the organization.

Is it possible for a non-technical leader to successfully develop a strategy that enables the successful integration of IT, operations, politics, resource management and still deliver on the life-safety mission with which they have been charged? Where does one begin? How should ECC operations and IT work together to ensure there is a good cybersecurity strategy in place? In the event of a breach, who will be ultimately responsible for managing the result and keeping the chaos to a minimum?

Guideposts

Luckily, there are a number of standards and best practices that can serve as guideposts that can provide the answer to these questions and provide insight to who should own and drive cybersecurity strategy in the ECC.

The **Information Technology Infrastructure Library** (**ITIL**) is an internationally recognized set of best practices for delivering IT services. The latest version (version 4) has as one of its core principles the idea that IT services must be focused on supporting the client's mission. Ideally, IT delivers services that enable the process and goals of the ECC, whether this is an ECC-controlled IT team or an external IT team, such as a county IT, a third-party IT provider or a systems provider such as a telephony, CAD, or Radio system vendor. The ECC's life-safety mission is the priority, and IT and vendor management must work with ECC management to achieve these goals. This can be challenging, as by its very nature ECC operations breaks some of the core tenets of good cyber hygiene, such as not interacting with unknown data sources or unknown people. It is the responsibility of ECC leadership to help IT teams and vendors understand these requirements, and work to define the cost-benefit relationship between operational parameters and cybersecurity protocols.

As mentioned previously, cybersecurity in the ECC must be managed as part of a wholistic approach to management, understanding and defining roles and responsibilities required to execute on the overall strategy, and ITIL v4 provides guidance on how to streamline the integration of operational and technical requirements.

Another source of information useful to helping ECC Leadership understand the various aspects of cybersecurity is the **National Institute of Standards and Testing (NIST).** While there are many standards and best practices provided by this organization that are designed to provide guidance to governmental organizations on cybersecurity protocols, there are two key publications provided by NIST that can be very useful to ECC Leadership and ECC IT teams regarding cybersecurity that should be part of an overall IT strategy:

- NIST 800-53 – This publication focuses on the access controls that must be in place to help ensure a safe operating environment. ECC Leadership should understand these well enough to be able to communicate to IT teams and third-party vendors the importance of implementing these controls and be able to craft operational protocols that incorporate these access controls that balance the need for security with the need for streamlined operations.
- NIST 800-61 – This publication provides information on how to manage security incidents (breaches). It is the responsibility of ECC management to incorporate security incident response protocols relating to breaches into all aspects of ECC operations, especially Continuity of Operations Plans (COOP). This includes determining roles and responsibilities for the appropriate response to each incident including how to identify a breach, who to call, and what specific steps to take.

While not specifically directed at the ECC environment, NIST publications are a great source of information for IT best practices, and while they are somewhat technical in nature, are written in plain language and can be understood by anyone in a position of leadership within the ECC environment. They will provide the technical education required to be able to speak intelligently with IT teams and systems vendors regarding what needs to be implemented to ensure as safe an operating environment as possible.

Perhaps the best source of information for ECC leadership, IT Teams and systems vendors interested in crafting and executing on a useful IT and cybersecurity strategy is the **Task Force on Optimal PSAP Architecture (TFOPA) guide**, which was chartered by the Federal Communications Commission (FCC) to

"… make recommendations on structure and architecture…" that enable continuous, robust, cost-effective and secure operations of the nation's emergency communications networks between citizens, ECC's and local first responders.

The main document, released on January 29th, 2016 provides a vision and strategy for successful management of ECC networks generally, and quite a bit of good information for securing those networks, with appendixes (appendix 1 and 2, specifically) that provide good summaries and checklists for ECC leadership to help them ensure they can build a strategy for managing cybersecurity in their own environment.

The TFOPA Team consisted of several working groups, one of which (Working Group One) provided a supplement to the TFOPA Guide focused specifically on cybersecurity. This document provides a wealth of information, checklists and recommendations specific to how to manage cybersecurity in the NextGen911 operating environment and provides links to many other sources of valuable information relating to this topic. It should be considered mandatory reading for anyone involved in crafting IT and cybersecurity strategies at local, regional, state or national levels.

Putting it all together

It should be clear by now that the ownership and responsibility of securing the ECC networks, data and applications belong squarely with ECC Management, not IT. Based on ITIL best practices, ECC management is responsible for initiating and enforcing the policies and procedures for IT, including Cyber Defense strategies.

It is important that roles and responsibilities be defined for all stakeholders, including operations, IT, 3rd party vendors and really anyone that uses the networks, data and systems used in the ECC. Once roles and responsibilities have been clearly defined, a communications plan must be put in place that communicates the plan on a regular cadence. This ensures that any time new applications, hardware or SOP's are put in place, everyone understands the impact on cybersecurity and what their individual responsibility is to execute on it.

Ensuring that adequate network support is in place is crucial. This will mean different things depending on available resources, but the concept is that an unsupported network is an insecure network. At a minimum, a well-supported network includes the following items:

- A functional, real-time view of performance and device health
- 24/7/365 Incident response with appropriate SLA's
- All devices remotely monitored for device or circuit failure
- A clearly defined incident response process
- Incident data should be captured using a ticketing system and should be available for reporting and analysis

NIST and TFOPA both recommend a complete inventory of network devices because monitoring requires that the network be defined. Additionally, dynamic inventories can alert when rogue devices or network connections are added to the environment.

A baseline assessment of the network health and cybersecurity profile is necessary in order to identify vulnerabilities and remediate them

Creating a remediation plan following the assessment enables measurement of the level of improvement over time. Assessments are recommended on a 6- to 12-month cadence to ensure vulnerabilities are identified and remediated as quickly as possible.

ECC Management should continuously monitor the on-going cybersecurity strengthening project and initiate a cybersecurity training plan to ensure that a culture of cybersecurity awareness and responsibility permeates the environment. Training should be appropriate for the role, and should include:

- IT Teams
- Telecommunicators
- Supervisors
- Administration
- ECC Management
- Board members

Finally, and most importantly, ECC management needs to create a restoration plan. In today's environment a cybersecurity breach is an almost certain event, and being able to recover your data, networks and systems quickly following a breach is one of the most important elements of a cyber defense strategy.

Conclusion

Ultimately, it is the director of the ECC that is responsible for the successful delivery of the life-safety mission of the ECC. This requires the continuous, secure, robust operation of the networks, data and systems on which that mission depends. Due to the fact that cyber attacks on those networks are an ever-increasing threat to the continuous operations of the ECC, every director must educate themselves regarding how to implement a good cyber defense strategy, and work with their boards, their IT teams, their operators and their 3rd-party vendors to ensure that a culture of cybersecurity exists, and that for every new SOP, for every new system, for every new application that is put in place, the question "How does this affect our cybersecurity strategy?" needs to be asked.