Three High-Value, Low-Cost Strategies to Strengthen ECC Cyber Defense

Prepared by the APCO Cybersecurity Committee

The Situation

From small, two-seat centers scattered throughout the country in rural areas, to large, multi-jurisdictional regional dispatch centers in heavily populated metropolitan areas, our nation's ECCs are under a relentless, ever-increasing onslaught of cyber-attacks. The 24/7 nature of ECC operations makes them an ideal target for cyber thugs looking to steal their computing power for crypto-mining and other nefarious bot-style attacks, while the life-safety mission of the ECC makes them a perfect target for Ransomware attacks.

Protecting the ECC against these relentless attacks is a never-ending responsibility, and it falls to ECC leadership to ensure that a cyber defense strategy is in place to protect the continuous, robust operation of the networks, data and systems required to fulfill their life-safety mission.

Yet, many ECC directors and boards are ill-equipped to fully comprehend the nature of the situation described above. Too often it is assumed that there is no threat to their tiny little center, out in the middle of nowhere, or that it is the responsibility of IT to "figure it out." However, these assumptions fail to address that cybersecurity is much larger than a set of IT-based and managed solutions and can only be successfully managed as part of a wholistic approach which identifies and incorporates security best practices into all operational, technical and infrastructure management.

A strong cyber defense strategy is owned, managed and monitored by ECC management. That takes into account that virtually every area for which ECC management is responsible has a cybersecurity element. For every SOP, every application, every system, and every time any of those items is upgraded or changed, the questions must be asked: "What is the impact on our cybersecurity management plan?" and "What is the risk to our continued operations?"

Given this complex environment it is easy to see why many directors and boards fail to take action. It's hard to even know where to begin to uncover, much less remediate, vulnerabilities. The National Institute of Standards and Testing (NIST) and the Task Force for Optimal PSAP Architecture (TFOPA) both recommend cybersecurity assessments be conducted at regular intervals to ensure a baseline understanding of vulnerabilities is understood and a plan is in place to remediate them. However, most ECCs have little to no funding and few resources for even the minimum level of recommended assessments. They know they must do something but don't have the knowledge to understand where to begin. It's a frustrating situation.

The good news is that there are some common things that almost all ECCs have both the funding and skills required to remediate, that should be a basic part of any healthy IT service delivery plan. These are strategies that will cost nothing but "keyboard time" or at worst the time and effort required to define and implement new policies and procedures. The following three items are things that should be in place at all ECCs and will yield positive results in terms of securing the ECC networks, data and systems, at little to no cost to deliver.

Planning

The first thing that needs to be in place is to define an over-arching strategy for managing cybersecurity at your ECC. Creating a "culture of cybersecurity" is a crucial step to increasing your ability to fend off cybersecurity attacks. Studies by the FBI and others show that just keeping all stakeholders more aware of cybersecurity policies and procedures decreases the likelihood of a cybersecurity breach occurring at an ECC.

Every person in your ECC, from managers to maintenance should understand their responsibilities in executing the cybersecurity strategy. It needs to become second nature as part of everything they do, and they should know the answer to the question, "What am I going to do to prevent a cybersecurity breach today at my ECC?"

In order to accomplish the goals of your cybersecurity strategy, a regularly scheduled communication plan should be put into place to keep everyone abreast of progress on the plan and anything each individual needs to know about their role in the process.

Be sure to provide information and checklists about what to do in the event of a cybersecurity breach in your plan and make sure everyone understands the process for where to find the checklist, who to call, what to do, and when to do it.

This is a low-cost, high-value activity that is a vital part of improving your ECC's cybersecurity profile, and costs little or nothing to implement.

Password Management

Most cybersecurity breaches involve cyber thugs gaining administrative access to networks, devices or applications through password guessing or password cracking of end user accounts, especially administrative accounts. Therefore, strong policies should be in place to reduce the risk that passwords can be compromised.

Yet, it is the rare ECC that has a strong password management policy in place. Balancing the need for quick access to applications at the beginning of each shift and following breaks with the need for longer, more complex passwords can create an operational nightmare. Add into this mix the needs and "requirements" of vendors, who often want to keep usernames and passwords the same across all their customers to make remote support easier and it creates a situation in which cyber thugs rejoice.

While it may cause some "angst" among end-users and vendors, a strong password policy needs to be in place that defines password requirements for every user (including the Director!!), role and device. It is the ECC Director that needs to work with vendors to ensure and enforce that the ECC password policy is being used on new and legacy systems.

A strong password management policy, which can be implemented for no cost, should adhere to the following standards and will significantly reduce the risk of a cybersecurity breach:

- Complexity – This means a mix of upper- and lower-case letters, numbers and special characters. Turn on Password Complexity in Active Directory (AD) if AD is in use
- Force Logoff – This means logging off end users after a specific time has elapsed, typically recommended to be a couple hours longer than the duration of a normal shift.

- Maximum Password Age – This is the timeframe for requiring users to change their password. CJIS requirement is 90 days (Note that there is some flexibility here when pass-phrases are implemented. See below).
- Minimum Password Length – Should be a minimum of 12, 15 for administrative accounts
- Password History Length – This defines the number of times a new password must be created before re-using a previous password. This should, ideally, be at least 11
- Lockout Attempts – The number of times an incorrect password can be entered before the system locks out that user. This should be 5 or less attempts
- Lockout Duration – This defines how long the user is locked out following too many attempts entering the incorrect password. This should be 30 minutes.

Increasingly, cybersecurity experts are recommending the use of passphrases, rather than passwords, as they usually meet and exceed password length rules and are easier to remember, which in itself makes them more secure. For example: **IL0v3F00tb@ll!** Is a passphrase that would be easily remembered by most end-users but would take even the most powerful password-cracking tools millennia to crack. (some would argue that particular example could be more easily guessed than cracked, but it would not be a simple thing to guess without a serious phishing campaign!!). Another benefit of introducing 15-character passphrases is that the maximum password age can be extended to 6 to 12 months.

Lastly, there are many free, enterprise-level password management tools that are in the market. There are many that include online (cloud) and offline (local) versions, making management much easier and more secure, and would meet the operational needs of most ECCs.

Patch Management and Windows Hardening

Another strategy that requires proactive management, but costs little to implement is in the area of patch management. Hackers know that one of the easiest ways to gain access to systems remotely is through the exploitation of inadequate or outdated patches in software, hardware or network devices.

In the public safety environment, implementing patches can be a tricky thing. Patches must be completely tested both by the vendor prior to release, and by local IT teams prior to installing in an operational environment to avoid the risk of causing operational hiccups or full-fledged outages. If at all possible, they should be deployed in a test bed or sandbox before installing in the operational environment.

When purchasing new applications and systems, it is crucial that the patch management process be clearly spelled out in the contract, including release cadence, back policies, and other considerations to avoid confusion and conflicts following go-live. While the IT manager may own defining and executing on this process, it is up to the ECC Director to enforce the policy in this area, especially with vendors.

It will take time and patience to define the right balance of risk with reward, but it is important that operating system, database, hardware, and applications be patched at the vendor recommended levels to ensure smooth, secure operations and reduce the risk of a cybersecurity breach.

One other area in which it is possible to gain some quick wins without expending a lot of extra money is in the area of Windows™ hardening.

In the interest of expediting upgrades and backwards compatibility, there are many legacy protocols that are enabled by default during installation of Windows™ operating systems, such as SMBv1, NetBIOS, LLMNR, and WPAD. These protocols originally were designed to enable plug and play and make it easy for peripherals and remote users to gather information on the network, other devices connected to the network segment and resolve host names. While this does make it easier for administers to install, upgrade and manage their networks, these are also the very things cyber thugs are looking to do on a network. Today, there are other ways to accomplish these tasks and most of these legacy protocols can, and should, be disabled. It will take some time and effort to do this, especially if one is relying heavily on these protocols; but it is possible, it just takes keyboard time and a strategy.

Conclusion

Successfully managing today's ECC is a complex mix of interconnected operational, technical, financial and political strategies, all of which require boards and directors to take strong leadership. It can be a daunting task and adding additional stress to this mix is the fact that there are nefarious people trying to bring it all down and stop it in its tracks.

Boards and ECC Directors should be doing all they can to develop funding and capabilities to do a full cybersecurity assessment and identify all the vulnerabilities in the ECC network. However, this may not be readily forthcoming.

In the meantime, the areas discussed in this article will bring ECCs a long way towards building up cyber defense, without expending much more than doing a little research, a little sweat equity and re-defined policies and procedures.