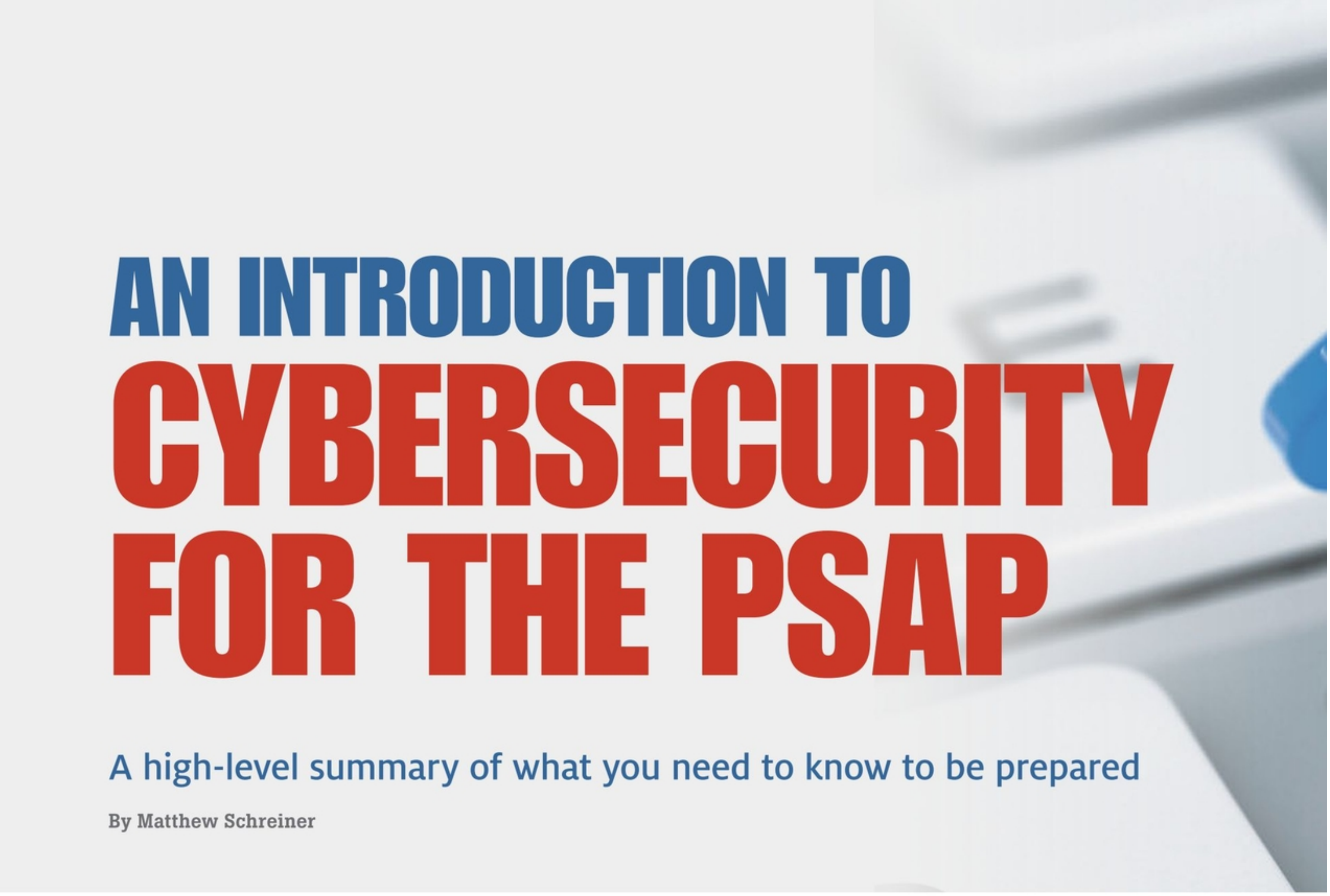


AN INTRODUCTION TO CYBERSECURITY FOR THE PSAP

A high-level summary of what you need to know to be prepared

By Matthew Schreiner

A NIGHTMARE SCENARIO

It was 0300 hours on a cold winter morning. John Smith (name changed), the director of a mid-sized PSAP in the Midwest, was sound asleep, buried in the warmth of his dreams. Suddenly, he was shaken by the ring of his bedside phone. As the director of a PSAP, he was used to early-morning phone calls, but he could usually count on sleeping through most January nights. He grabbed for the phone: "This is John. What is it?"

"John, it's Pete." John recognized the voice of his IT manager, but he wasn't his usual calm, cool, collected self. "We've been hit with something. It looks like it could be a denial of service attack, like they had in Ferguson and Madison earlier from Anonymous. We're not completely sure what it is yet. First, a few CAD workstations locked up. Then it quickly spread to more and more workstations, and now we're getting reports of mobile data lockups, too. We're on cards now. We think we may have it isolated, and no RMS or radio systems are affected. But we don't really know exactly what it is yet, much less how it got in or how to stop it except to shut everything down!"

"I'm on my way in. And, Pete, settle down—we'll figure it out." He hung up the phone. As he was getting ready to leave, John thought to himself, *We just invested in a bunch of anti-virus software and bought new, state-of-the-art firewall and hardware solutions. I thought we were covered! How did this happen?*

"How did this happen?" is a question many PSAP directors have to ask themselves following such a nightmare scenario. The answer lies in the fact that many focus solely on software and hardware solutions, failing to consider that a total cybersecurity strategy includes technology, but also well-defined processes and fully-trained people. Equally important is a thorough understanding and implementation of cybersecurity best practices and recommendations from standards bodies such as APCO, NENA, CJIS, NIST and a host of others. Finally, thorough training of non-technical personnel is required to ensure the strategy actually operates as designed.

This article provides a high-level overview of the elements that are needed to develop a total cybersecurity strategy for PSAPs and reduce the likelihood of such nightmare scenarios.

TECHNOLOGY

One of the first things a PSAP needs to consider is the scope of its cybersecurity strategy, defining which systems and data need to be protected. It is important to consider all of the systems that are potentially vulnerable to attack and to look beyond the "obvious" systems such as CAD, reporting and telephony solutions and the devices on which they run. Most PSAPs do a reasonably good job of protecting those systems.

©ISTOCK.COM/BLACKJACK3D

However, radio systems, mobile data applications and devices, smart phones, access control systems (door keys, ID cards, etc.) and many other systems that were previously completely isolated are now managed in the cloud or over the internet and, as such, need security-related consideration. As the internet of things continues to expand, there will be more devices, applications and data, with more vulnerability to be potentially exploited by enterprising cybercriminals.

Don't forget to ensure personal information of employees is protected against hacks. Information contained in HR systems is often used to define users in other systems in the PSAP and includes email addresses, phone numbers and Social Security numbers, which are all data that can be used not only to harm individual PSAP employees, but also to launch attacks against systems within the PSAP.

Other technical aspects to consider include:

- the level of encryption to be deployed for different data types (often mandated by local, state or federal regulations)
- asset management (do you know where all your data is, who owns it and on what devices it is created, stored and shared?)
- version control (keeping track of all application and device versions)
- understanding dataflow; that is, the path data takes from where it is created (or enters your system), where it is stored and with which systems it is shared, creating potential vulnerabilities anywhere along the path

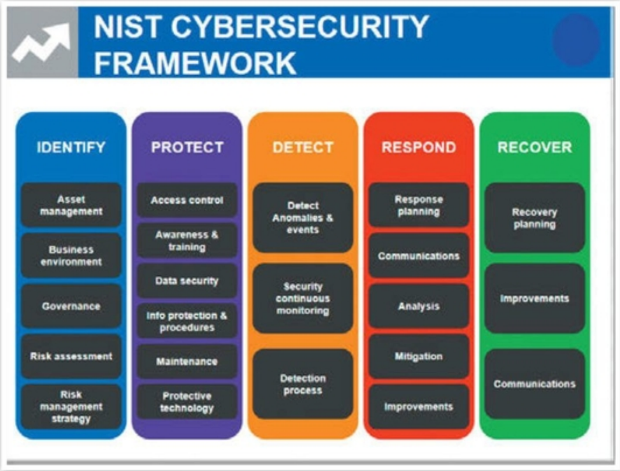
Lastly, make sure to fully research and understand the best practices and regulations defined by all the government agencies and standards bodies. Some are recommendations; some are regulations. Some can affect your ability to get local, state and federal funding. All will provide something useful to be included in your cybersecurity strategy.

Once the risks and threats to systems, networks and associated data are fully understood, processes can be developed to ensure the technology operates securely.

> "As the internet of things continues to expand, there will be more devices, applications and data, with more vulnerability to be potentially exploited by enterprising cybercriminals.

PROCESSES (SOPS)

Almost everything that happens within the four walls of a well-run PSAP is described and managed by a set of standard operating procedures (SOPs) that determines how and when to do things, so defining a set of SOPs to ensure cybersecurity protocols are followed should be second nature and fit easily into the existing SOPs. The purpose of most SOPs is to ensure things run smoothly during times of duress, but they also exist to address risk and manage liability.



The NIST Cybersecurity Framework. COURTESY OF MOTOROLA SOLUTIONS, INC.

Cybersecurity-related SOPs will answer questions such as:

- Who is responsible and accountable for managing the various aspects of the cybersecurity strategy
- Which government and industry standards are required? Which best practices will you adopt?
- What will the Incident Response Plan be, and what are the steps for implementing it?
- What is the contingency plan? What is the recovery plan if systems or data are compromised?
- How are the various elements of the cybersecurity solution to be funded? Is the funding model CAPEX or OPEX?

SOPs will also form the basis for a cybersecurity training plan and be used to ensure everyone understands their role, responsibility and accountability for the success of the overall cybersecurity strategy.

PEOPLE (ROLES)

Perhaps the most important element in a strong cybersecurity strategy is the people in the PSAP. A cybersecurity strategy is only as strong as the weakest link, so everyone needs to understand and execute their defined role and responsibilities. Success depends on the understanding that everyone, not just IT, plays a role in cybersecurity.

The following questions should be considered when defining the part each person in the PSAP plays in the overall cybersecurity strategy:

- Who is responsible for the overall cybersecurity strategy? Who sets, and enforces the SOPs?
- Who will design the cybersecurity plan and end-to-end solution?
- Is cybersecurity to be managed internally or contracted with an outside firm?
- Who are the cybersecurity stakeholders? How do roles outside the IT organization, such as telecommunicators, supervisors, clerks, admin management and others, fit into the cybersecurity strategy?
- Who is responsible for managing the individual elements of the cybersecurity strategy?
- How are people to be held accountable in the event things don't go quite as planned?

Every person in the PSAP needs to fully understand the risks and threats cybercrime poses to the infrastructure and data they use every day and how to mitigate those risks through the way they perform their day-to-day mission. Regular training, risk assessments and testing of all personnel regarding the cybersecurity SOPs is required.

NIST SECURITY FRAMEWORK

In 2013, President Obama signed an executive order that established the National Institute of Standards and Technology (NIST) Cybersecurity Framework, designed to help federal agencies assess their risks and devise a strategy to mitigate them. In May 2017, President Trump signed into law an additional executive order designed to hold specific federal agencies that are responsible for the safety of the nation's technical infrastructure, including public safety networks such as NG9-1-1 and i3 networks, accountable for implementing the NIST Cybersecurity recommendations.

A couple of key quotes from the May 2017 executive order:

- "...the President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises…"
- "...Effective immediately, each agency head shall use the (NIST) Framework for improving Critical Infrastructure cybersecurity…"

The NIST Cybersecurity Framework defines the technology, processes and people that are required for a strong defense against cyberattacks and provides guidance on the following five areas:

- **Identify:** Identifying physical and logical assets (systems and data) and what needs to be protected
- **Protect:** How to protect identified data and systems
- **Detect:** Define, identify and detect anomalies and security breaches
- **Respond:** How to respond to contain and/or mitigate breaches and improve (lessons learned)
- **Recover:** How to recover and regain normal operations

Compliance with the NIST Cybersecurity Framework may be required to obtain federal grants that are available for implementing cybersecurity solutions within a PSAP. It is crucial that PSAP directors and PSAP IT management have a thorough understanding of the NIST Framework and make every effort to be compliant with it, as it is likely to affect the ability to obtain federal grants related to cybersecurity in the near future.

CONCLUSION

In the nightmare scenario presented earlier, John Smith, PSAP director, wondered how that cyberattack happened. While we don't know for sure, it most likely happened because of a failure to design a complete end-to-end cybersecurity solution based on the NIST Cybersecurity Framework, which integrates technology with processes and the people who use them. It could have been a failure to train all PSAP employees on the role they play in ensuring a safe operating environment, or maybe there was some other weakness in the cybersecurity armor.

Whatever the cause, there are effective strategies that can be employed to thwart the efforts of cybercriminals and their attacks on PSAP systems and data, but it requires proactive vigilance to achieve. This edition of *PSC* contains many useful articles to educate you about and help you deploy solutions that will ultimately stop cybercriminals in their tracks. ●

***Matt Schreiner's** public safety experience began 25 years ago with multiple roles in a multi-agency PSAP near Chicago. Matt is currently a user experience manager for Motorola Solutions, Inc.*