An accessible best practices guide to implementing effective cybersecurity policies and procedures within your PSAP.

An Introduction to Cybersecurity

A Guide for PSAPs

Version 1.0 July 2016

APCO Cybersecurity Committee

Contents

Introduction

The primary goal of this document is inform PSAP supervisors (and above) how to identify, prevent and minimize exposure to cybersecurity risks and vulnerabilities. It can be used to help PSAPs develop policies and procedures and raise awareness of areas that require further consideration. Case studies have also been provided in order to demonstrate how theoretical vulnerabilities have manifested into operationally impactful events.

"Our 9-1-1 is down." There is nothing more sobering to hear for a 9-1-1 call center. Of course, most PSAPs have procedures in place to deal with this scenario. But once the system is back up and running, there will be questions, the most difficult of which is likely to be, "Could this have been prevented?"

Every center should also consider the possibility of a cyber-attack. Many attacks, such as *ransomware attacks*[1] have made the news of late. PSAPs need to consider these types of attacks, along with many others, and whether or not they have a solid business continuity plan. In the event of an attack, can your center continue to provide service to the community and your employees? Has your center considered all of the systems that are vulnerable to cyber-attack and both the short and long term impact of such an event?

While these scenarios may invoke fear for anyone working at a 9-1-1 center, considering them and examining how to prevent and prepare for them is a critical step in the risk assessment process. Utilizing this document as a tool to focus your assessment on vulnerable systems will help your center establish a proactive and preventative program designed to minimize the risk of a cyber-attack. Being unprepared for attacks can be catastrophic resulting in the loss of response capabilities, image, personal information, and possibly even death.

Physical Security

Physical security is a major component of your agency's overall security policy. Physical security incorporates building security, proxy access, vendor access and security measures.

Building Security

Physical security is a critical component of overall network security. Physical security prevents unauthorized access to the Intelligent Building Management System's (iBMS) devices, networks, and information. Without it, intruders have the means to circumvent all other methods of protection. It is very important that all employees are aware and adhere to physical security policies. Multiple aspects need to be considered when developing policies. A full assessment of security and infrastructure is required before writing a policy.

Consider the following when making design decisions:

- Combine multiple barriers to restrict access; such as building, room, and cabinet access control.
- Locate mission critical devices in access controlled areas or in locked cabinets. Preventing unauthorized physical access to network devices such as routers, firewalls, and switches is a must.
- Protect communication cable runs with conduit or ruggedized cable chases.

Proxy Access

Security is comprised of several subcomponents to include key and proxy card access and control. To maintain control of keys, an inventory and receipt form process has to be in place. Just like passwords, keys and proxy cards have levels of access and should be issued on an as needed basis. Additionally, regularly scheduled audits (quarterly at a minimum) should be conducted to prevent unauthorized access.

Visitor Access

A visitor badge process is required to screen and log visitor activities in your facility. Official identification should be required prior to granting access and visitors should be escorted at all times.

Security Measures

Security cameras with a recording device provide an external layer of security to your facility. Proper lighting is fundamental for security and safety. Walls, gates and bollards reduce the risk of an unauthorized vehicle entering or damaging your building. A reoccurring comprehensive employee security training class is key to your agency's success. Well trained employees know how to identify and report security violations and suspicious activity.

Employee Integrity

The people who interact daily with an agency's network and iBMS play a critical role in maintaining overall system security. Security policies and procedures can easily be undermined, either knowingly or unknowingly, by a single individual. Policies and procedures must clearly outline what is considered acceptable use of the agency's networks, proper email usage, and approved use of removable media.

Acceptable Use

Restrictions on internet use must be clearly defined and monitored. Some PSAPs limit access to only pre-approved websites while others have established criteria for blocking sites which are not work related or which pose a potential security threat. Due to the risk rootkits and viruses represent, any system which reaches beyond the PSAPs internal network must be closely monitored and restricted as much as possible without adversely effecting operations.

Policies detailing restrictions on the use of email must also be enacted and enforced. Phishing emails are a serious threat to internal networks and continue to be commonplace. Employees should only be looking at emails from known sources and must be educated on how to identify suspect emails. For example, phishing emails often come for emails outside of the U.S. so an address ending in ".uk" or something other than ".com" could be an indication of a phishing attempt. Some organizations create their own phishing emails as a security test in an effort to assess employee awareness, vigilance and agency susceptibility.

Removable media, including individual USB drives, hard drives, SD cards, etc. should only be used with specific authorization from the agency. Employees should not be allowed to use personal removable media in the workplace. Employees must also be prohibited from plugging their phones, tablets, laptops, or other electronic devices into the agency's equipment. Additionally, access to the agency's wireless systems must also be restricted and not available to employees' personal devices.

Awareness Training

Personnel training is key to building awareness about the role each person plays in maintaining security within an organization.

Training should include:

- The dangers of plugging phones, tablets and other personal equipment into the agency's systems
- Proper handling of account credentials
- Roles and responsibilities of each person in maintaining security
    - Wearing credentials at all times
    - Using key card access to track user entry
    - Employee awareness of the work environment including anybody entering behind others without using proxy cards
- Reasons behind various security policies and procedures
- Ways to recognize and respond to attempts by others to garner private information for the purpose of compromising a system (social engineering)
- Ongoing refresher training, reminders, and overall awareness building

Security training works best if participation is mandated and the training itself is monitored for effectiveness. Quality Assurance/Quality Improvement programs should include required monitoring of security procedures.

FBI Advises Ransomware Delivered via Email

"In a ransomware attack, victims—upon seeing an e-mail addressed to them—will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax, but which actually contains the malicious ransomware code. Or the e-mail might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software."[1]

Perform Security Audits

Periodic security audits provide the means to ensure that systems, policies, and procedures devoted to security are effective and that no gaps exist. Security audits may include:

- Attempts to gain network or server access (penetration testing)
- Evaluation of past breaches to determine if potential for exploitation has been eliminated
- Attempts to acquire passwords from users
- Checks to verify that security procedures are being followed and security systems are not being bypassed
- Assessment of protection against new types of threats. An effective audit provides a comprehensive assessment of an organization's security and informs an ongoing process of improvement
- At a minimum, quarterly audits of key card access

Vendor Access

In today's environment, virtually all organizations have networks, systems and facilities that rely on outside vendors for service. Vendors might require physical access, dedicated remote network access, network cloud access, or any combination of the three. When using a vendor, a level of risk is inherent in the relationship.

Vendors can be a service division of the product manufacturing company (e.g. Cisco Corporate Support Team supporting Cisco Networks and Hardware). Vendors can also be Third Party equipment agnostic, supporting multiple platforms. Prior to granting system access to a vendor, a thorough screening and contract process should be completed. Policies are normally contained within vendor contracts.

Risk Management should be employed to negate as much risk as possible. A fine line exists between risk to the agency and the level of access required for the vendor to complete their assigned tasks. Remote access to the network can be accomplished through either a Secure Shell (SSH) Tunnel, a Virtual Private Network (VPN) or dedicated point to point line. This access can increase risk to the network if security patches are not kept up to date.

The vendor staff should also be taken into consideration. Vendor staff should meet your agency security and background check requirements. Employee continuity is very important and several questions

Target Hack via Subcontractor's Credentials

"Last week, Krebs said the hackers snatched the data using credentials stolen from Fazio Mechanical Services Inc., a refrigeration, heating and air conditioning subcontractor that has worked at a number of Target stores…

According to multiple sources close to the investigation, "those credentials were stolen in an email malware attack at Fazio that began at least two months before thieves started stealing card data from thousands of Target cash registers," Krebs said…

Krebs also points out that Fazio did not completely have their guard up against an attack.

The company said last week that its security measures are in full compliance with industry practices. But Krebs says Fazio was using a free version of an anti-malware software, which is not intended for corporate use and does not offer real-time protection against threats"[2,11]

should be asked when negotiating with a vendor. Should a vendor's employee leave their employ, does the vendor have the ability to continue support? Is the support documentation available to more than a single employee? Is the vendor company stable and financially sound? If the vendor were to go out of business, how would this affect your agency?

When a vendor accesses your agency network regardless of the method (tunnel, VPN, point to point, cloud) a strong password policy is required (see Password Policy section). All passwords should have an expiration timeframe; the more sensitive the password, the shorter the expiration timeframe. Single use passwords for vendors are also an effective means of minimizing the risk of vendor access.

A procedure should be in place to create, assign, track and audit passwords. A mechanism is required to deliver passwords to the vendor. Various security methods can be implemented. Passwords should not be written on paper and handed to a vendor. Passwords can be provided over the phone. You place the call to pre-determined vendor phone number contacts. Third party software allows encrypted passwords to be sent through email. Your password administrator should conduct regularly scheduled audits to remove old passwords and users.

Your agency's data should be protected as part of your security policy. Data can be lost, stolen, leaked or altered. Steps should be taken to limit access to data to an "as needed" condition. Administrators can create levels of passwords used to limit access to the agency's data. Physical means add additional layers of data protection. Data storage devices, both local and hosted, should be encrypted. Access to data storage facilities should be limited and defined in your physical security policy. Vendors should be escorted at all time when working in sensitive area of your facilities. Regularly scheduled data backups, preferably off-site backups, provide another level of security.

If possible, vendors should have a requirement to use on-site dedicated computers/terminals to access the network. Access to unused serial, USB and Ethernet data ports should be shut down electronically and physically secured.

Off-site vendor computers should not be connected to additional networks or the internet when accessing your network. A virus protection policy for vendors and their computers, terminals, servers, etc., are a necessity. Insure the vendor is only running or installing manufacturer approved software. A good vendor policy requirement is a statement necessitating logging off the network when not in close proximity to computers/terminals used for network access.

Best Practices

- Thorough vendor screening and contract process
- Background checks on vendor staff
- Include policies in contracts
- Security patches must be kept up to date
- Establish password guidelines with limited durations and specific password delivery methods
- Regularly scheduled audits of vendor access
- Limit access to networks and unused ports

Policy and System Integrity

Password Policy

Password security and maintenance within all public safety systems is often the first, and last, step in preventing outside attackers access to the PSAP. The well documented corporate hacks of large retailers like Target[2, 11], Home Depot[3] and eBay[4], which are believed to have been possible due to the use of stolen login credentials to the corporate network, prove just how important it is for proper password creation and protection.

User passwords on public safety networks must be able to meet stringent security requirements, without being a burden to remember for the user. Forcing unrealistic password policies on users actually leads to less secure networks than properly managed password policies that allow for comfortable password management to coexist with secure password policies. According to the 2016 Verizon Data Breach Investigation Report[5], "63% of confirmed data breaches involved weak, default or stolen passwords."

In addition to creating strong passwords, it is important to protect those passwords as well. Password protection policies include routine changing of passwords, storage of passwords, repetitive use of similar passwords, separate passwords for separate systems, and review of the password policy with employees. Additionally, some employers will intentionally try to "crack" their employees' passwords through brute force attacks in order to assess password effectiveness. All of these measures are employed for the purpose of ensuring the public safety network remains secure and that passwords are adhering to the password policy set in place.

It is recommended that all Public Safety Answering Points adhere to the Framework for Improving Critical Infrastructure Cybersecurity (Framework) published by the National Institute of Standards and Technology (NIST)[6]. The purpose of the Framework is to provide guidance "(t)o strengthen the resilience of critical infrastructure", providing "a 'prioritized, flexible, repeatable, performance-based, and cost-effective approach' to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services." With that guidance in mind, it is the recommendation of the Cyber Security Committee of the Association of Public Safety Communications Officials, that PSAPs use the following guidelines and practices with regards to password creation and protection.

Password Guidelines

This guideline applies to employees, contractors, consultants, temporary and other workers within the PSAP, including all personnel affiliated with third parties. This guideline applies to all individual user passwords including but not limited to user-level accounts, system-level accounts, network equipment logins, web accounts, e-mail accounts and public safety application accounts.

Password Creation Guidelines

- All passwords should meet or exceed the following guidelines
    - Strong passwords have the following characteristics:
        - Contain at least 8 alphanumeric characters.
        - Contain both upper and lower case letters.
        - Contain at least one number (for example, 0-9).
        - Contain at least one special character (for example, !$%^&*()_+|~-=\`{}[]:";'<>?,/).
    - Poor, or weak, passwords have the following characteristics:
        - Contain less than eight characters.
        - Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
        - Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
        - Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
        - Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
        - Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
        - Are some version of “Welcome123” “Password123” “Changeme123”
    - You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.
        - (NOTE: Do not use any of these examples as passwords!)

Password Protection Guidelines

- Password Creation
    - Users must not use the same password for business accounts as for personal access (for example, personal ISP account, option trading, benefits, and so on).
    - Where possible, users must not use the same password for various business access needs.
    - User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user to access system-level privileges.
- Password Change
    - All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.
    - All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.

  - Password cracking or guessing may be performed on a periodic or random basis by the IT Security Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Creation Guidelines.
- Password Protection
  - Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
  - Passwords must not be inserted into email messages, or any other form of electronic communication.
  - Passwords must not be revealed over the phone to anyone.
  - Do not reveal a password on questionnaires or security forms.
  - Do not hint at the format of a password (for example, "my family name").
  - Do not share business passwords with anyone, including administrative assistants, secretaries, managers, co-workers, and family members.
  - Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
  - Do not use the "Remember Password" feature of applications (for example, web browsers).
  - Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

Removable Media and Access Ports Policy

As important as password protection is, it is just as important to protect removable media, and network access ports to PSAP computers and networks. Removable media has long been a source of spreading malware and viruses. Since the rise of personal computing in the 1980's and the invention of the floppy drive, computer viruses were first created to cause chaos and cheap thrills for early hackers. Nowadays, it means big money and that big money is usually paid from the pockets of the infected agency. Viruses can allow hackers various opportunities of malicious intent, from using PCs to send out SPAM email in the hopes of advertising nefarious websites to collect personal passwords, to full control of remote computers to steal sensitive data and access secure networks.

The threat of viruses and malware is real and worldwide. According to the 2015 Ponemon[7] Institute Cost of Cyber Crime Study, cyber-crime, on average, cost business and organizations $7.7 million annually. These dollars are realized through software subscriptions, loss of productivity due to network and equipment failures, and even ransoms paid to malware authors. Nearly every company surveyed for the Ponemon report, 99%, experienced cyber-attacks in the form of Malware and Viruses, Worms and Trojans.

While the cost associated with fighting cyber-attacks is great, there is also the real threat of damage to equipment as more and more control devices are networked together. The Stuxnet[8] virus was

introduced through USB storage devices onto control computers that monitored nuclear centrifuges for the Iranian government. Hackers were able, in this case, to cause physical damage to the equipment while other hackers used similar methods to hack ATM[9, 10] machines and empty the cash within them.

As stated above, removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations. Open and unsecured network access ports pose a similar threat as individuals are able to connect devices to network ports to gain physical presence on the agency network. A well-documented, and closely followed, removable media and network port policy will help ensure the integrity of the network, data, and computer systems of the agency. The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by public safety organizations and to reduce the risk of acquiring malware infections on computers operated by those organizations.

This policy should be adhered to at all times, but specifically whenever any user intends to store any information used by the agency to conduct official business on removable media devices.

Removable media devices include, but are not restricted to the following [amend list as appropriate]:

- CDs.
- DVDs.
- Optical Disks.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- MP3 Players.
- Digital Cameras.
- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines).

Policy Guidelines

Restricting Access to Removable Media

- It is standard policy to prohibit the use of all removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed. There are large risks associated with the use of removable media. Therefore, clear business benefits that outweigh the risks must be demonstrated before approval is given.
- Requests for access to, and use of, removable media devices must be made to the department supervisor. Approval for their use may only be given by a department manager

Procurement of Removable Media

- All removable media devices and any associated equipment and software must only be purchased and installed by IT Services. Non-agency owned removable media devices must not be used to store any information used to conduct official agency business and must not be used with any agency owned or leased IT equipment.
- The only equipment and media that should be used to connect to any agency equipment or network is equipment and media that has been purchased by the agency and approved by IT Services or has been sanctioned for use by IT Services.

Security of Data

- Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment than data which is frequently backed up. Therefore, removable media should not be the only place where data obtained for agency purposes is held. Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system.
- In order to minimize physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.
- Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way while in their care or under their control.
- All data stored on removable media devices must, where possible, be encrypted. If this is not possible, then all PROTECTED, RESTRICTED or CONTROLELD data held must be encrypted.
- Virus and malware checking software approved by the agency must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned before the media is loaded on to the receiving machine.

Network Port Access

- All open network ports on switches, routers, firewalls, etc., pose a threat to network and system security. These ports are potential access points for cyber criminals to gain physical access to agency network and computer systems.
- All open, and unused, network ports must be turned off through the management console of the respective switch, router or firewall.
    - The network device shall be secured itself adhering to the Password Creation and Protection Policies.
- Any ports which will not be used for an extended period of time, for example when an employee goes on extended leave or retires, should be turned off and not accessible until it is needed again.

User Responsibility

- All considerations of this policy must be adhered to at all times when using all types of removable media devices. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), recordable CDs, DVDs and diskettes:
    - Any removable media device used in connection with agency equipment or the network or to hold information used to conduct official agency business must only be purchased and installed by IT Services. Any removable media device that has not been supplied by IT must not be used.
    - All data stored on removable media devices must be encrypted where possible.
    - Virus and malware checking software must be used when the removable media device is connected to a machine.
    - Only data that is authorized and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved.
    - Removable media devices must not to be used for archiving or storing records as an alternative to other storage equipment.
    - Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

System Security

Radio

When addressing security surrounding communications systems and infrastructure, it's easy to forget about the actual radio system itself. Many have a perception that a radio system is basically a mobile radio in a building using an outside antenna on a tower without much of the "cyber" portion that actually exists. However, the fact is today's radio system infrastructure has a closer resemblance to a traditional data center than that of an old "radio room."

As it relates to cyber-security in a radio system, all of the best practices outlined in this document apply. There are servers, routers, and firewalls as well as other IP connected devices which need to be secured. These devices might have "radio centric" names such as a Prime Site Controller, M-Core or L-Core, or other vendor specific names. However, they are still IP connected devices. Passwords must be used on all devices in addition to prohibiting the connection of any unapproved device.

It's important to note that remote radio sites must be considered just as important as a primary site with regard to security. It must be understood that there are many points of entry for a cyber-attack to occur within a radio system, many of which exist at remote sites. It's a good practice for all individuals that are going to work in and around a radio system to have passed a background check or be constantly

escorted by those who have. The level of background check required will depend on individual agencies and their specific policies.

It's also important to be aware of the fact the radio systems can be jeopardized by harmful radio frequency (RF) interference, creating a situation that makes communications difficult or sometimes impossible. The symptoms which can accompany this kind of event are usually recognized by users as scratchy or indecipherable audio or unidentified users coming up on the "air" or "channel." As a user, this can be a difficult thing to combat. However, there are many resources available which include the FCC as well as the APCO International Automated Frequency Coordination (AFC) Group.

CAD and Phones

PSAPs vary widely in their construction and make up. They do business with a wide range of vendors and employ numerous hardware and software combinations. While brand names may differ from center to center, there should be a consistent application of security guidelines that adhere to all who enter your center, be they vendor, visitor, employee or manager.

These processes must be clear and consistent. The processes themselves must be subject to routine compliancy checks. This consistent review of your security processes will allow you to address the ever evolving landscape of what constitutes a cybersecurity threat.

Whether you have a hosted, shared or dedicated CAD and phone system, there are some basic security concerns of which every PSAP supervisor should be aware.

Access Security

User accounts and password management

The following guidelines were extracted from NENA's PSAP Security document[12]. They were published in 2005 and still hold true today.

- Maintain a simple, useable structure, which can be administered by the fewest number of personnel possible.
- Grant rights only to those who need them.
- Adhere to the policy of least privileged use, meaning if a basic user can perform all of the tasks necessary, don't grant administrator access to them.
- Limit the number of administrator accounts and only use them for administrative work, use a regular log on for day-to-day work.

UH Gets $2.6M to Protect Next-gen 911 Centers[3]

University of Houston has been awarded $2.6 million to develop technology to help protect emergency response systems, such as current and next-generation 911 systems, against Distributed Denial of Service (DDoS) attacks. UH's award is part of a larger Distributed Denial of Service Defenses (DDoSD) program announced by DHS recently.

Shi and his co-PIs professor Stephen Huang and assistant professor Omprakash Gnawali, also in the Department of Computer Science at UH, will be working to develop low-cost mitigation strategies to significantly strengthen the resilience of emergency response systems against DDoS attacks.[13]

- Disable or rename built in Administrator accounts.
- Deny Anonymous or Guest accounts as these typically can be exploited.
- Periodically run audits against the users to determine what is actually their effective rights and permission. If a user is a member of several security groups, it is possible for that user to have elevated privileges that were not intentional.

Physical

Perform a review of the physical structure of your PSAP. While doing so, look at it from the various perspectives of those who enter your center: vendors, administrators, dispatchers, call takers, sit-alongs, commissioned personnel and the occasional reporter.

What level of access do they have to the various physical components of your center's infrastructure? Does the route provided on a tour of your PSAP expose a CAD monitor with sensitive CJIS information? Could anyone quickly plug a flash drive into an exposed USB port? Or can they access your Wi-Fi or Bluetooth enabled devices with their smart phone?

While you can minimize many of these concerns simply by employing good personnel access measures, it is much harder to manage risk and exposure by trusted personnel.

Carelessness or unawareness of procedure can pose a substantial threat to your center. For example, a well-meaning employee may simply be looking to charge their smart phone by plugging into any visible USB port. Or they could be doing it defiantly. Another common scenario is where an employee brings in a work-related PowerPoint they made on their personal computers or devices. However, it's stored on a family shared personal flash drive that unknowingly contains *malware, ransomware* or other malicious software.

Avoid not considering malicious intent as a security threat. A disgruntled employee can be a serious cause of concern. But this too can be mitigated with good security practices.

While you cannot eliminate these risks entirely, the security policies you implement today can institute an organizational-wide awareness of these issues. When new policies are put in place, be mindful of how security policies are discussed and the subsequent perception by employees. They may view it as a sign of distrust and it can have a negative impact on morale. Security awareness needs to be a group effort with everyone made to feel they are part of the solution. This is key to having effective policies and procedures. Allow employees to engage in dialogue where they can raise their own concerns.

Best Practices

- Keep network connected equipment in a secure location
- Maintain controlled access to physical keys
- Institute dissuasive measures such as: line-of-sight security cameras, USB dummy plugs, password protected Basic Input/Output Systems (BIOS)
- Employ a system where employees can easily report technical issues to be logged and tracked

- If email is accessible via CAD workstations, never open attachments or open links from unsolicited sources
- Minimize the number of users with administrative privileges
- Implement a strong password policy; use unique passwords for each account
- Implement weekly vulnerability network scans
- Routinely audit user access lists; remove previous employees, confirm new users
- Routinely train employees in current cybersecurity practices

Geographic Information System (GIS)

For many PSAPs, managing their GIS is not a dedicated component in their daily activities. Often times, updating their CAD maps and Master Street Address Guide (MSAG) maintenance is just one of many duties left to the supervisors or delegated to their service provider. But it is important to keep in mind that GIS systems are a method of accessing your PSAP. It is not unusual for GIS systems or resources to be shared amongst several PSAPs which brings a greater vulnerability and level of exposure to those connected PSAPs.

The good news is GIS components, typically speaking, are isolated and not directly exposed to open networks such as the internet. But it does not mean that systems configured to access your GIS are not exposed.

- Limit access to systems that access your GIS
- Limit software applications on systems that access your GIS
- Ensure strong password policies are in place
- Use unique passwords for each account

Other IP-Based Systems

Many systems within PSAPs are IP based. It is imperative that centers consider all of the various systems which could be threatened by a cyber-attack. Some of these systems are:

- Power
- Uninterrupted Power Systems (UPS)
- Climate controls
- Building monitoring systems
- Battery chargers
- Remote monitoring systems
- Security cameras
- Fuel pump systems
- Any device with an assigned IP-address

9-1-1 System Done in by a Malfunctioning Air Conditioner

Erie County's 9-1-1 system shut down for nearly four hours on a Wednesday morning – done in by a malfunctioning air conditioner.

An overnight county building engineer was notified that the air conditioning unit in the circuit room had shut down, but by the time he arrived, the room was already so hot that circuit breakers automatically tripped as a defense mechanism to protect the expensive equipment against damage.

"It was easily in excess of 120 degrees."[14]

The following guidelines provide important information on how to tighten security for IP based systems.

Network Infrastructure

The network is the conduit that allows information to flow between the Intelligent Building Management Systems (iBMS), the enterprise system, and the outside world. Intruders able to tap into the network can disrupt the flow of information.

Limit Network Access Points:

- Isolate the iBMS as much as possible. Locating it on a virtual local area network (VLAN), for example, ensures that building traffic, including broadcasts to all nodes, remains within the logical boundary you establish.
- Think carefully before granting outside access. Each network entry and exit point must be secured. By granting access only when a valid reason exists, you can minimize risk and keep security costs down.

Use Firewalls to Control Access

Firewalls contribute to security by controlling the flow of information into and out of network entry points. Using a set of user defined configuration rules a firewall determines which traffic will be allowed to pass through and onto the network. Traffic that doesn't satisfy the configured rules is rejected. A single best practice applies to adding firewalls to your network design:

- Place a firewall at every transition point into or out of the iBMS network.
- Providing recommendations for the proper selection and placement of firewalls is a detailed endeavor and is beyond the scope of this document.

Firewall Basics: A firewall…

- Is either a stand-alone device or a software application running on a host.
- Supports at least one internal and one external connection
- Filters information in the following ways:
  - Service control
  - Direction control
  - Behavior and content control (email, web)
- Functionality ranges from basic to complex:
  - Packet filtering
  - Application level – proxy server
  - Deep packet inspection
- Requires special expertise for proper selection and configuration

Manage User Access

Secure user access is achieved through the use of authentication and authorization. Authentication is the means by which a user's identity is confirmed. Once authenticated, a user is authorized to perform certain functions as defined by their role within the organization.

- Restrict user access by capitalizing on solutions commonly deployed by IT departments, such as Central Authorization, Password Control, User Management, and Network Monitoring. Examples include Active Directory®, Kerberos, and Radius.
- Further restrict user access by establishing authorization requirements for individual devices such as routers, servers, embedded controllers, and workstations. The type of device will dictate the best approach.
- Consider stronger authentication methods for critical host devices such as:
    - Smart Cards or USB tokens
    - Biometric Authentication limits access based on a physical or behavioral characteristic such as a fingerprint.
    - Two-Factor Authentication limits access to users with both a password and a physical token.

Restrict Remote Access

Providing iBMS access to remote users presents a unique set of security challenges. Addressing these challenges requires building additional protections into the network infrastructure. Even then, remote access should only be considered for systems that already have sufficient protection against external threats. Best practices for providing remote access include:

- Use a secure connection, such as a VPN, which provides encryption and authentication of remote sessions.
- Use secure protocols and applications such as HTTPS, SSH, and SCP/SFTP whenever possible and avoid Telnet and FTP.
- Evaluate the risks associated with SNMP (Simple Network Management Protocol) before incorporating it into your design. When using SNMP, limit access to authorized system administrators with known IP addresses.
- Restrict remote access by using Two-factor Authentication and by limiting access to required users only, such as system operators.
- To provide public access to information, create a demilitarized zone (DMZ), place a server within the zone, and mirror the required information onto the server.

Selecting Components - Security Features that Matter

Consider the following best practices when selecting system components:

- Choose devices and protocols that support encryption, integrity, and nonrepudiation whenever possible. Encryption protects the information traversing a network by making it unreadable to

unauthorized users. Integrity checks determine if any changes have been made to a network message. Nonrepudiation verifies the identity of an information source.

- Give preference to devices with logging capability, such as Syslog support. Event logging is available in a wide range of devices including routers, firewalls, backup systems, and access control systems. Logs can aid in early threat detection by recording significant network events, changes to firewall configuration, or user access to an area or device. Syslog is a logging standard that can be used to consolidate log information from multiple devices on a network.
- Look for tamper proofing, built-in locks, and other access control features when selecting mission critical components.
- Consider adding an Intrusion Detection System (IDS). An IDS is a stand-alone device or host based application that monitors system events in an effort to identify threats early. Events such as failed login attempts, traffic patterns, and changes to port configurations are evaluated.
    - Choose an IDS that allows you to customize the rules used to define acceptable network behavior.

Wireless Technology

Wireless networking technology offers several advantages over wired technology including lower installation costs and greater design flexibility. These advantages must be weighed against the increased security risk associated with its use. Best practices for the use of wireless technology are as follows:

- Choose wireless devices with built-in firewalls and support for the highest level of encryption available.
- Harden wireless access devices by following these steps:
    - Replace the default administrator name and password with strong alternatives.
    - Follow the device's "Before You Begin" protocols.

System Installation

In preparation for system installation, consider the following:

- Throughout the installation process, the iBMS may be particularly vulnerable to attack. Consider temporarily isolating the system from the outside world until all the components of your security plan are in place.
- Update new and legacy equipment with the latest security patches.
- Security measures, particularly those designed for enterprise networks, can sometimes interfere with proper iBMS function. Anti-virus software, for example, has been known to disrupt workstation performance by consuming large amounts of processor time. While this occurs infrequently, it is important to have a method in place for evaluating system performance as security features are brought online.

Configuring Security Features

The goal in this phase of the process is to properly configure the security features of each system component. Configuring firewalls, hardening system devices, configuring user accounts, and enabling threat detection are all tasks that contribute to secure system installation.

Configure Firewall Rules

Firewalls use a set of rules, established by the user, as the basis for determining which traffic is allowed to pass in or out of the network. For example, a rule might block all access to a specific IP address or port. Proper configuration of firewalls is essential to securing the network and should only be performed by experienced personnel. Best practices for configuring firewalls include:

- Use a combination of rules to both permit authorized traffic and deny unauthorized traffic. A typical approach is:
  - Create rules that explicitly deny access
  - Add rules to permit only the required access
  - Add a broad-based rule to deny access to all remaining traffic
- Confirm that the firewall can detect TCP "SYN-flood" attacks by tracking the state of a TCP handshake (stateful firewall).
- Include rules to restrict outbound network traffic in order to minimize the spread of damage in the event of a breach.

Harden System Devices

By taking steps to harden system devices, you can close potential points of access into the iBMS and reduce the risk of an internal attack. The hardening process varies depending on whether the target is an embedded device or an off-the-shelf Windows or UNIX®/Linux® based computer running host software.

All Devices

- Evaluate each device to determine what ports and services are available. And, whenever possible, disable any that do not have a planned use. Port scanning applications can help expedite the identification process. Be sure to disable ports and services that were used temporarily for device commissioning but won't be needed during operation.
- Removable media, such as USB memory sticks and compact discs, are often the source of malicious software. The safest solution is to prevent the use of all removable media, by mechanically blocking ports, for example. For those applications where removable media is necessary, take measures to restrict port access and enforce media checking procedures (i.e. anti-virus scans).
- Enable the security features built into each device including encryption, firewall capability, access control, intrusion detection and prevention, and user authorization.

Host Devices

- Install anti-virus software from a reputable vendor (i.e. Symantec, McAfee) and enable its automatic update features.
- Install and configure firewall software.
- Enable automatic operating system updates. Centrally managed updates are preferable.

Configure User Accounts

User accounts establish access levels to the domains within a system. Best practices for configuring user accounts include:

- Replace all default vendor passwords with strong alternatives (twelve characters minimum with a mix of letters, numbers, and symbols). Likewise, remove all default logins (i.e. administrator) and system IDs.
- Disable every user's access to the system by default and add permissions only as required.
- Restrict each group of users to the lowest level of privileges necessary to perform their role.
- Prevent duplication of passwords across multiple sites.
- Use expiration dates to require users to periodically change passwords.

Enable Threat Detection and Mitigation

Measures to detect and limit the impact of security breaches are an important component of any security plan. Consider the following best practices for detecting and mitigating threats:

- Create logs to monitor all aspects of the system including physical access, network activity, device activity, and firewall configuration. Consider system performance when setting logging parameters and collect log files in a central location to prevent unauthorized modification.
- If you are using an intrusion detection system, take the time to thoroughly understand the capabilities and limitations of the system you selected before configuring the alerts and active response rules governing its operation. Configuration rules should reflect the operating behavior of your network which may differ significantly from those of a typical enterprise network.

Operate Securely

The need to address security does not end once a system has been installed. System monitoring, account management, patch management, and firewall maintenance are all important to operating a system securely.

Monitor the System

Through vigilant monitoring of system parameters, you can detect security breaches earlier and take steps to limit the spread of damage. Monitoring guidelines include:

- Treat alerts from intrusion detection systems with the highest priority.
- Proactively scan the network for new hosts and out-of-date systems.

- Routinely review system logs for irregular activities. Indicators such as numerous failed login attempts, unusual credential card use, and increases in network load can provide early signs of a breach.
- Create an incidence response plan which describes the actions to be taken when system irregularities are detected.

Maintain User Accounts and Access Lists

When a user changes roles within an organization or leaves altogether, it is important to have a documented procedure in place to remove or alter the level of access they have to the overall system. The procedure should address all types of access including physical, remote, network, and device level access.

Manage Security Patches

Security patches provide protection against the never-ending flow of new threats. A good patch management plan combines policies, procedures, and qualified personnel in an effort to close security gaps without major disruption to the system.

Best practices for patch management include:

Take Inventory: Make a list of the devices that will require periodic security updates. The list should include network devices such as routers, firewalls, and VPN concentrators, as well as application and operating system software. An annual report on data breaches, a subset of the overall security landscape, highlights the importance of system monitoring.

Out of 141 confirmed data breaches in 2009:

- 86% of the victims had log files containing evidence of a breach
- 61% were discovered by someone other than the victim[15]

Use Trusted Sources

- Use vendor issued firmware updates, service packs, and hot fixes.
- Whenever possible, use patches with digital signatures. A digital signature validates a patch's source and integrity.
- Stay up-to-date on newly released patches and vulnerability reports. Develop a plan for installation. A patch installation plan should include the following:
    - Use a method of prioritizing patches. Most patches are routine updates that can be implemented according to a schedule. Others require immediate action to close a critical gap in security.
    - Pre-approved patch installation tools that provide change management and security audit features.

- Procedures for vendor certification of patches, testing of patches prior to installation, and a staged installation process to minimize the risk of disruption from the change.
- The verification of digital signatures. Signed security patches should be verified just prior to installation to ensure that they have not been tampered with internally.

Develop a Backup and Recovery Plan

A backup and recovery plan should identify responsible parties, list the items to be backed up, and provide specifics such as backup intervals, locations, and number of versions to retain. Verify that recovery procedures work as expected.

Firewalls Require Special Attention

Firewalls must be properly managed by trained personnel to ensure continued system security. A firewall management plan should be developed to address the following requirements:

- Regular review of firewall configuration
- Strict change control measures
- Continuous monitoring of logs and relevant statistics

Conclusion

There are numerous resources available, in addition to this introductory guide, to assist PSAPs, 9-1-1 Authorities, and agencies involved with Emergency Communications in preparing for, mitigating, responding to, and recovering from cyber-attacks. Those resources include the NIST Cybersecurity Framework[6], The FCC Task Force on Optimal PSAP Architecture Cybersecurity report[16] and reporting and sharing mechanisms such as the Department of Justice IC3 portal.[17]

This document is intended to provide high level guidance and as such, it is the first in what will be a series of documents and works from APCO designed to prepare the Emergency Communications community for the coming transition to IP networks and systems. Whether Next Generation 9-1-1 (NG9-1-1), FirstNet, or legacy systems that already interact with networks and systems in a variety of forms, cybersecurity is critical to all aspects of our profession. The safety and well-being of the citizens we serve, and the responders we work to protect, will be impacted by the decisions we make, and the practices we implement with regard to cybersecurity. APCO encourages agencies of all sizes, and personnel at all levels, to get engaged in the cybersecurity conversation, get educated about the threat, and become proactive in the defense of the public safety communications ecosystem.

References

1. *Incidents of Ransomware on the Rise - Protect Yourself and Your Organization* https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise
2. *Target "Target Hackers Broke in Via HVAC Company". www.KrebsonSecurity.com.*
3. *Home Depot "Home Depot: Hackers Stole 53M Email Addresses". www.KrebsonSecurity.com.*
4. *Ebay "eBay Inc. To Ask eBay Users To Change Passwords". www.ebayinc.com.*
5. *Verizon "2016 Data Breach Investigation Report". www.verizonenterprise.com.*
6. *National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity".* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
7. *Ponemon "Cyber Crime Report". www8.hp.com/.*
8. *Falliere, Nicolas. "Exploring Stuxnet's PLC Infection Process". www.symantec.com.*
9. *ATM: http://www.securityweek.com/skillful-hackers-drained-atms-using-malware-laden-usb-drives*
10. *Prince, Brian. "New Malware Found Infecting ATMs in Mexico". www.securityweek.com.*
11. *O'Connell, Liz. "Report: Email phishing scam led to Target breach". BringMeTheNews.com. Retrieved September 15, 2014.*
12. *National Emergency Number Association – "PSAP Security".* https://www.nena.org/?page=PSAP_Security
13. *University of Houston – "Hackers Gonna Hack: UH Gets $2.6M to Protect Next-gen 911 Centers"* http://www.uh.edu/news-events/stories/2015/November/111215DHS911grant.php
14. *Tan, Sandra. "911 System Done in by a Malfunctioning Air Conditioner".* http://www.emergencymgmt.com/disaster/Erie-County-officials-seek-answers-after-911-failure.html. *The Boston News, NY March 31, 2016*
15. *Verizon "2010 Data Breach Investigation Report". www.verizonenterprise.com.*
16. *Federal Communications Commission "Task Force on Optimal PSAP Architecture". https://apps.fcc.gov/edocs_public/attachmatch/DA-16-179A2.pdf*
17. *Federal Bureau of Investigation Internet Crime Compliant Center (IC3) https://www.ic3.gov/complaint/default.aspx*