PSTA Cybersecurity Technical Subcommittee Report

Background

The number of mobile phone users around the world is projected to exceed the five billion mark by 2020. This rapid increase, unfortunately, sees cybercriminals adapting and changing their methods to profit from this growing number of potential victims. Public Safety users are no less vulnerable than consumers using similar technology. Our goal with this report is to provide guidance to public safety agencies that they can leverage to be cyber secure while implementing technology to support their first responders. We are also providing checklists for agencies to leverage that can assist with each agency's own cyber policies and implementation of best practices. We truly believe technology can empower public safety, but that agencies need practical advice and resources to implement appropriate cyber processes that allow them to take advantage of technology while being smart about cyber security policies and procedures.

Cybercriminals continue to look for ways to exploit vulnerabilities in applications, operating systems, and software, trying to capitalize on security flaws before manufacturers can find and patch them. All operating systems such as Linux, Windows, iOS, and Android can be vulnerable.

User data is a major target of cybercriminals—from credit card credentials to email passwords and contact lists. Victims have also been baited into downloading adware or subscribing to paid services. Opening the wrong attachment through email can unleash Trojan viruses that attack then steal information then propagate this form of attack to others gained from stealing your contacts. This happened recently to the town of Allentown, PA that shut down the town's computer system for over two weeks with a cost of over one million dollars to update and secure the system. Public safety must look at protecting key information and cybersecurity must be a top priority for any agency.

Since cybercriminals usually cast wide nets to reach more potential victims, public safety users should protect their devices early on to defend against threats. The PSTA Cybersecurity Technical Sub-committee will recommend best practices and steps that can be taken to protect the mobile device.

Key Areas of Concern Considered and Discussed

The Cybersecurity sub-committee identified three areas to focus initial work efforts.

1. Define areas of Cybersecurity threats in a mobile/server environment related specifically to public safety users.
2. Identify and agree on a set of Cybersecurity best practices for the mobile/server environment
3. Identify and agree on a method to inform and educate public safety users on the critical nature of cybersecurity threats on an ongoing basis

The sub-committee considered several key areas of focus for cybersecurity threat and mitigation:

1. Email/Attachments
2. Messaging
3. Password strength and rotation
4. Secure browsing
5. File sharing
6. Updating your OS, Apps, and most recent security patches on mobile device
7. Up to date anti-virus and malware definitions

8. Regular OS, application, and security scanning intervals
9. Managing access through secure VPNs

Quick Overview of Identified Best Practices

Below are just a few examples of best practices that can be applied to secure your mobile device:

- Avoid connecting to unsecured Wi-Fi networks. Turn off the automatic Wi-Fi connection feature on your smartphones, laptop, or tablets. Users should refrain from connecting to public hotspots as they are not secure and connecting to them can expose the device to a multitude of risks. If connecting is necessary, avoid logging into key accounts or financial services. Setting up a VPN is also a good way to secure data sent and received online. Most public safety agencies today offer users a VPN client to use for connecting to agency content.
- Download apps from trusted sources. According to a recent Android Security Review by Google, Potentially Harmful Apps (PHA) are still the biggest threat to Android users. Certain third-party app stores have proven to be more likely carriers of malicious apps, so always download from trusted sources. Users should also do their due diligence and check reviews or comments on the app page to make sure it is legitimate. Users who use mobile payment and popular gaming apps should also be cautious as they have become hot cybercriminal targets in the past.
- Know the risks of jailbreaking/rooting. Manufacturers place security restrictions and safeguards on their devices to protect users' devices and data. Jailbreaking or rooting removes these limitations, leaving the system more vulnerable to malware and other threats.
- Be wary of unsolicited calls or messages. Attackers use a variety of methods to get users to download malware or reveal personal information. Scan or verify any messages, calls, or emails from unknown senders before opening.
- Set automatic locks on mobile devices. Ensure that the mobile device locks automatically and has a strong passcode—a simple pattern or swipe password isn't much of a deterrent. If a device is lost or stolen, a strong password prevents anyone from quickly peeking at personal information. The use of biometric authentication features such as fingerprint scanner and facial recognition makes unlocking the device much more convenient and the security harder to crack.
- Limit the personal information given to apps and websites. Signing up for a new service or downloading a new app sometimes requires personal information. Be wary of revealing too much, and research on how secure the application or site is before logging on.
- Manage what is shared online. Make sure to use privacy settings on social media apps and sites. Some sites can broadcast location, email, phone numbers, or more to the public by default.
- Users could also take advantage of multilayered mobile security solutions that can protect devices against online threats, malicious applications, and even data loss.

Appendices

PSTA Cybersecurity Checklist
Organizations with less than 500 personnel

The PSTA recommends that all public safety agencies have a cybersecurity policy in place. Additionally, employees should read and sign their agreement to this policy every year.

Below are the minimum elements that should be considered for inclusion in the development or enhancement of a public safety agency's cybersecurity policy, based on individual needs.

Device management

- ☐ Maintain detailed asset inventory
- ☐ Maintain asset inventory information
- ☐ Utilize client certificates to authenticate hardware assets

Software management

- ☐ Maintain inventory of authorized software
- ☐ Ensure software is supported by vendor
- ☐ Utilize software inventory tools
- ☐ Track software inventory information
- ☐ Integrate software and hardware asset inventories

Controlled use of administrative privileges

- ☐ Maintain inventory of administrative accounts
- ☐ Change default passwords
- ☐ Ensure the use of dedicated administrative accounts
- ☐ Use unique passwords
- ☐ Use multi-factor authentication for all administrative access

Email and web browser protections

- [ ] Ensure use of only fully supported browsers and email clients
- [ ] Disable unnecessary or unauthorized browser or email client plugins
- [ ] Block unnecessary file types

Malware defenses

- [ ] Utilize centrally managed anti-malware software
- [ ] Ensure anti-malware software and signatures are updated
- [ ] Configure devices to not auto-run content

Data recovery

- [ ] Ensure regular automated backups
- [ ] Perform complete system backups
- [ ] Protect backups
- [ ] Ensure all backups have at least one offline backup destination

Secure configuration for network devices, such as firewalls, routers, and switches

- [ ] Maintain standard security configurations for network devices
- [ ] Install latest stable version of any security- related updates on all network devices
- [ ] Manage network devices using multi- factor authentication and encrypted sessions
- [ ] Use dedicated workstations for all network administrative tasks
- [ ] Manage network infrastructure through a dedicated network

Data management

- [ ] Maintain an inventory of sensitive information
- [ ] Remove sensitive data or systems not regularly accessed by organization
- [ ] Monitor and block unauthorized network traffic
- [ ] Only allow access to authorized cloud storage or email providers
- [ ] Monitor and detect any unauthorized use of encryption
- [ ] Encrypt mobile device data

- [ ] Manage USB devices
- [ ] Encrypt data on USB storage devices

Application software security

- [ ] Establish secure coding practices
- [ ] Ensure that explicit error checking is performed for all in-house developed software
- [ ] Verify that acquired software can still be supported
- [ ] Only use up-to-date and trusted third-party components
- [ ] Use only standardized and extensively reviewed encryption algorithms
- [ ] Ensure software development personnel are trained in secure coding

Cloud security

- [ ] Have in place clear contracting SLAs
- [ ] Clear responsibilities for cloud provider versus agency. Each area of responsibility should have one clear owner of accountability
- [ ] Agency owns responsibility for security of the data
- [ ] Use multifactor authentication for cloud credentials
- [ ] Assign user access rights
- [ ] Create and enforce resource access polices
- [ ] Ensure continued access to critical data in the event of failures and errors
- [ ] Review procedures to ensure there are steps take to prevent accidental disclosure of data
- [ ] Monitor cloud deployed data

Mobile Device Management (MDM)

- [ ] All agencies should have an MDM solution in place.
- [ ] Ability to remotely wipe or lock devices
- [ ] Whitelist application policy
- [ ] Blacklist application policy

Security Awareness Training

- ☐ Minimum yearly training
- ☐ Human factors in cybersecurity, phishing, USBs, etc.

Additional Resources

DHS Cybersecurity and Infrastructure Security Agency (CISA) resources: https://www.us-cert.gov/resources

DHS Vulnerability Assessments: https://www.dhs.gov/cisa/critical-infrastructure-vulnerability-assessments

PSTA Cybersecurity Checklist

Organizations with 500+ personnel

The PSTA recommends that all public safety agencies have a cybersecurity policy in place. Additionally, employees should read and sign their agreement to this policy every year.

Below are elements that should be considered for inclusion in the development or enhancement of a public safety agency's cybersecurity policy, based on individual needs.

Device management

- ☐ Utilize an active discovery tool
- ☐ Use a passive asset discovery tool
- ☐ Use DHCP logging to update asset inventory
- ☐ Maintain detailed asset inventory
- ☐ Deploy port level access control
- ☐ Utilize client certificates to authenticate hardware assets

Software management

- ☐ Maintain inventory of authorized software
- ☐ Ensure software is supported by vendor
- ☐ Utilize software inventory tools
- ☐ Track software inventory information
- ☐ Integrate software and hardware asset inventories
- ☐ Utilize application whitelisting
- ☐ Implement application whitelisting of libraries, scripts, etc.
- ☐ Physically or logically segregate high-risk application

Continuous vulnerability management

- ☐ Run automated vulnerability scanning tools
- ☐ Perform authenticated vulnerability scanning
- ☐ Protect dedicated assessment accounts
- ☐ Deploy automated operating system patch management tools
- ☐ Deploy automated software patch management tools

Controlled use of administrative privileges

- ☐ Maintain inventory of administrative accounts
- ☐ Change default passwords
- ☐ Ensure the use of dedicated administrative accounts
- ☐ Use unique passwords
- ☐ Use multi-factor authentication for all administrative access
- ☐ Use dedicated workstations for all administrative tasks
- ☐ Limit access to scripting tools
- ☐ Log and alert on changes to administrative group membership
- ☐ Log and alert on unsuccessful administrative account login

Email and web browser protections

- ☐ Ensure use of only fully supported browsers and email clients
- ☐ Disable unnecessary or unauthorized browser or email client plugins
- ☐ Limit use of scripting languages in web browsers and email clients
- ☐ Maintain and enforce network-based URL filters
- ☐ Subscribe to URL-categorization service
- ☐ Log all URL requests
- ☐ Use of DNS filtering services
- ☐ Implement DMARC and enable receiver-side verification

- [ ] Block unnecessary file types
- [ ] Sandbox all email attachments

Malware defenses

- [ ] Utilize centrally managed anti-malware software
- [ ] Ensure anti-malware software and signatures are updated
- [ ] Enable operating system anti-exploitation features/ deploy anti- exploit technologies
- [ ] Configure anti-malware scanning of removable media
- [ ] Configure devices to not auto-run content
- [ ] Centralize anti-malware logging
- [ ] Enable DNS query logging
- [ ] Enable command-line audit logging

Limitation and control of network ports, protocols, and services

- [ ] Associate active ports, services, and protocols to asset inventory
- [ ] Ensure only approved ports, protocols, and services are running
- [ ] Perform regular automated port scans
- [ ] Apply host-based firewalls or port-filtering
- [ ] Implement application firewalls

Data recovery

- [ ] Ensure regular automated backups
- [ ] Perform complete system backups
- [ ] Test data on backup media
- [ ] Protect backups
- [ ] Ensure all backups have at least one offline backup destination

Secure configuration for network devices, such as firewalls, routers, and switches

- [ ] Maintain standard security configurations for network devices

- [ ] Document traffic configuration rules
- [ ] Use automated tools to verify standard device configurations and detect changes
- [ ] Install latest stable version of any security- related updates on all network devices
- [ ] Manage network devices using multi- factor authentication and encrypted sessions
- [ ] Use dedicated workstations for all network administrative tasks
- [ ] Manage network infrastructure through a dedicated network

Data management

- [ ] Maintain an inventory of sensitive information
- [ ] Remove sensitive data or systems not regularly accessed by organization
- [ ] Monitor and block unauthorized network traffic
- [ ] Only allow access to authorized cloud storage or email providers
- [ ] Monitor and detect any unauthorized use of encryption
- [ ] Encrypt mobile device data
- [ ] Manage USB devices
- [ ] Manage system's external removable media's read/write configurations
- [ ] Encrypt data on USB storage devices

Application software security

- [ ] Establish secure coding practices
- [ ] Ensure that explicit error checking is performed for all in-house developed software
- [ ] Verify that acquired software will still be supported
- [ ] Only use up-to-date and trusted third-party components
- [ ] Use only standardized and extensively reviewed encryption algorithms
- [ ] Ensure software development personnel are trained in secure coding
- [ ] Apply static and dynamic code analysis tools
- [ ] Establish a process to accept and address reports of software vulnerabilities

- [ ] Separate production and non-production systems
- [ ] Deploy web application firewalls

Cloud security

- [ ] Have in place clear contracting SLAs
- [ ] Clear responsibilities for cloud provider versus agency. Each area of responsibility should have one clear owner of accountability
- [ ] Agency owns responsibility for security of the data
- [ ] Use multifactor authentication for cloud credentials
- [ ] Assign user access rights
- [ ] Create and enforce resource access polices
- [ ] Ensure continued access to critical data in the event of failures and errors
- [ ] Review procedures to ensure there are steps take to prevent accidental disclosure of data
- [ ] Monitor cloud deployed data

Mobile Device Management (MDM)

- [ ] All agencies should have an MDM solution in place
- [ ] Ability to remotely wipe or lock devices
- [ ] Whitelist application policy
- [ ] Blacklist application policy

Security Awareness Training

- [ ] Minimum yearly training
- [ ] Human factors in cybersecurity, phishing, USBs, etc.

Additional Resources

DHS Cybersecurity and Infrastructure Security Agency (CISA) resources: https://www.us-cert.gov/resources

DHS Vulnerability Assessments: https://www.dhs.gov/cisa/critical-infrastructure-vulnerability-assessments