Emergency Services Sector Cybersecurity Best Practices

Cybersecurity is one of the most important security considerations for Emergency Services Sector (ESS) organizations. From targeted incidents, such as ransomware attacks, to unintentional acts, such as failure to properly install security updates, poor cybersecurity practices can cause severe operational problems and the needless expenditure of funds. Many cybersecurity incidents can be prevented with a few simple, low cost protective measures.

General Practices

ESS organizations frequently use networked computers and smartphones for a variety of operational functions, such as computer-aided dispatch systems, communications backup to radio systems, and storage of and connectivity to databases. Below are general practices that can be implemented and included in plans and policies:

- Create strong passwords using a combination of upper and lowercase letters, numbers, and special characters. Avoid words and basic patterns (i.e., “12345” or “qwerty”). Use a different password for each account.
- Ensure devices require the user’s password to be entered each time it is turned on, restarted, or woken up.
- Change the default password (set by the manufacturer) on all devices that have one.
- Ensure autorun is turned off for USB drives, CD/DVD drives, etc., to prevent programs from being run just by inserting the drive into a device or by turning the device on.
- Ensure devices automatically sleep or shut down when unattended for a period of time.
- Ensure antivirus software is turned on and kept up to date on all devices.
- Ensure firewalls are turned on and kept up to date on all devices.
- Ensure application updates are downloaded and installed as they become available.
- Ensure the operating system is updated to the newest version on all devices.
- Do not use an administrator account as your primary user account.
- When not specifically being used, ensure Wi-Fi, Bluetooth, and personal hotspots are turned off.
- When disposing of a computer or smartphone, do not donate or throw away after deleting information. Data recovery software exists that may be able to retrieve information even after deletion. Information is still on the device until removed by specialized software designed to wipe the hard drive or complete physical destruction of the hard drive.
- For agencies with a bring your own device (BYOD) program, ensure implementation of security policies and practices to limit risk.
- Restrict personal use of agency devices. Specific vulnerabilities include browsing websites, accessing personal email, and downloading apps without encryption.
- Use multi-factor authentication to access computer systems with at least two of the following:
  - Knowledge factor (i.e., something you know, such as a password).
  - Possession factor (i.e., something you have, such as an identification card that a computer can read).
  - Inherence factor (i.e., something you are, such as fingerprint identification). A common possession factor tool is the use of a mobile phone to receive a single-use PIN.

Social Networking Practices

ESS organizations and personnel are increasingly using social media not only for personal use, but also as a means to inform the public about day-to-day activities and emergencies and to receive feedback and information from the public. Social media practices that ESS organizations and personnel can implement include:

- Avoid posting work-related information, such as employer name, job location, and security clearance.
- Avoid posting personal information, such as home address, phone number, email address, and social security number.
- Avoid posting current or future travel plans that broadcast when your home will be unoccupied.
- Avoid posting personal information about family members/friends/co-workers, and ask them to avoid posting personal information about you.
- Use caution when posting pictures. Pay specific attention to close-up facial pictures, locations, backgrounds, and picture metadata.
- Be aware of your privacy and security settings to limit your visibility as desired.
- Verify through other means that a contact request actually came from the person that it appears to have come from.
- Occasionally search for yourself in various social media sites (even if you do not have an account) to see if any data appears, such as personal info or a fraudulent account with your name.
- Use caution when you "like" pages or accept contacts. The page owner or contact will now have your contact information and access to your profile.
- Do not post pictures or other information unless you are comfortable with everyone having access to it.
- Once you post information to the internet, it is there forever—even if you delete it from your account and your computer. Some sites and applications track what you type, even if you delete it before actually posting.
- Be cautious with add-ons (i.e., plug-ins, games, and applications) because they are frequently written by other users, not the host site. Once installed, the author (and others) may be able to access your data.
- Information posted on social networking sites has led to retractions of job offers and employment terminations, and has been used in civil and criminal proceedings.

Email Practices

Emails are an easy and reliable mechanism to transmit a variety of data. Desktop and laptop computers, tablets, and smartphones can all access emails, but they also provide a variety of vulnerabilities. Some easy measures to protect your devices that access email include:

- Pay attention when using Reply vs. Reply All vs. Forward. They are all different and can be the difference between a single infected computer and multiple infected computers.
- Be cautious of unsolicited emails as they are a common method of virus transmission.
- Be cautious of suspicious emails, even if they appear to come from people or organizations you know. Someone may have spoofed the email address so it appears to come from a known source.
- If you receive an unsolicited or suspicious email, and you cannot verify through other means that it is legitimate, delete it without opening it.
- Do not reply to spam or harassing emails.
- Turn off the option to automatically download attachments.
- Create a user account on your computer for day-to-day use that is separate from the administrator account. The day-to-day account should have limited or restricted privileges in order to limit the ability of malware to function.
- Turn on automatic disabling of hyperlinks to prevent hyperlinks within suspicious emails from being enabled.
- Do not open attachments until you have scanned them with anti-virus software.

Wi-Fi Practices

Wi-Fi is any wireless local area network (WLAN) and is commonly used as a way to wirelessly connect mobile devices to a network, such as the internet, using radio waves. Public Wi-Fi hotspots (i.e., coffee shops, libraries, airports, etc.) are convenient, but they are often not secure. If you connect to a Wi-Fi network and send information through websites or mobile apps, it might be accessed by someone else. Below are some helpful tips on protecting yourself while using Wi-Fi networks:

- Encryption scrambles the information you send over the internet into a code so it is not accessible to others. When you are using wireless networks, it is best to send personal information only if it is encrypted—either by an encrypted website or a secure Wi-Fi network. An encrypted website protects only the information you send to and from that site. A secure wireless network encrypts all the information you send using that network.
- To determine if a website is encrypted, look for "https" (as opposed to "http") at the start of the web address. (The "s" stands for "secure.") Some websites use encryption only on the sign-in page, but if any part of your session is not encrypted, your entire account could be vulnerable. Look for "https" on every page you visit, not just when you sign in.
- Unlike websites, mobile apps do not have a visible indicator like "https." Researchers have found that many mobile apps do not encrypt information properly, so it is a bad idea to use certain types of mobile apps on unsecured Wi-Fi. If you plan to use a mobile app to conduct sensitive transactions—like filing your taxes, shopping with a credit card, or accessing your bank account—use a secure wireless network or your phone's data network (often referred to as 3G or 4G).
- If you must use an unsecured wireless network for transactions, use the company's mobile website (where you can check for the "https" at the start of the web address) instead of the company's mobile app.
- To protect your information when using Wi-Fi hotspots, send information only to sites that are fully encrypted and avoid using mobile apps that require personal or financial information.

Bluetooth Practices

Complementing Wi-Fi, Bluetooth is a wireless technology used for transmitting and receiving data over short distances using very little power. Bluetooth simplifies discovery and connection between a variety of devices that are commonly used by the ESS, such as smartphones, tablets, laptops, headsets, and vehicles. Bluetooth specifications establish a minimum range of 10m/33ft, but, depending on conditions, can operate at a range of 100m/330ft or more.

- Bluetooth can be set up on devices to establish trusted users with known connections; any other connection will require the user to allow the connection. Also, Bluetooth can be placed in a non-discoverable mode, which limits the ability of other Bluetooth devices to detect it, or it can be turned off completely, when not needed.

Contact Information

For more information, visit the DHS Emergency Services Sector Cybersecurity Initiative website at www.dhs.gov/emergency-services-sector-cybersecurity-initiative or email essteam@hq.dhs.gov.

OMB Control Number: 1601-0014
Expiration Date: 4/30/2018

Homeland Security

Emergency Services Sector Critical Infrastructure Stakeholder Feedback Survey

Emergency Services Sector Cybersecurity Best Practices

3/1/2017

General Information

Please select the category that best describes your organization: Select One

Overall Assessment

1. Please evaluate the following statement: *The information received through this activity or product was current and relevant.*

◯ Strongly Agree ◯ Agree ◯ Neutral ◯ Disagree ◯ Strongly Disagree

2. Please provide any recommendations that you may have on how future activities or products of this type could be improved to enhance their relevance.

3. Please evaluate the following statement: *The information received through this activity or product will effectively inform my decision making regarding safety and security risk mitigation and resilience enhancements.*

◯ Strongly Agree ◯ Agree ◯ Neutral ◯ Disagree ◯ Strongly Disagree

4. Please provide any recommendations that you may have on how future activities or products of this type could be improved to increase their value in support of your mission.

5. Please evaluate the following statement: *I will encourage my agency/organization to incorporate information I learned through this activity or product into our safety, security, or resilience practices.*

◯ Strongly Agree ◯ Agree ◯ Neutral ◯ Disagree ◯ Strongly Disagree

6. Please provide any recommendations that you may have on how future activities or products of this type could be improved so they can be better incorporated into safety, security, or resilience practices across the critical infrastructure community.

Privacy Notice

Paperwork Reduction Act Burden Notice

Submit