CYBER SAFETY FOR EMERGENCY SERVICE ORGANIZATIONS

The importance of cyber safety, best practices and free resources to help ensure you're not a cybercriminal's next victim.

The Department of Homeland Security (DHS) and the Multi-State Information Sharing and Analysis Center warn that cyberattacks against the Emergency Services Sector (ESS) have become commonplace and are likely to increase in frequency (Green, 2016). Emergency Service Organizations (ESOs) deliver essential and urgent services to our most vulnerable citizens. Add to that the interconnected nature of emergency response networks and ESOs are an attractive target for hackers. As advanced communication technologies become more prevalent in the ESS – including 5G, AI and IoT solutions – ESOs must address the vulnerabilities new technology presents.

THINK IT CAN'T HAPPEN TO YOU? THINK AGAIN

Emergency-response networks, including call-center communications-management software, closed-circuit TV camera systems, interactive voice response systems, and emergency alert systems — particularly wireless emergency alert systems – may be dangerously vulnerable to cybercriminals who won't think twice about holding a town's services at ransom for a big payoff.

Here are a few alarming statistics:

- A new cyberattack occurs somewhere on the web every 39 seconds.
- 64% of companies worldwide have experienced at least one cyberattack.
- 77 local governments and agencies, and 1,043 schools were impacted by ransomware in 2021.
- Since 2016, public reports show more than 400 ransomware attacks have hit city and county governments in the United States.

Know Your Terminology

With cyberattacks on the rise, staying up-to-date on key terminology can be an important first step to becoming cyber-aware and secured. The International City/County Management Association (ICMA) and the Cybersecurity & Infrastructure Security Agency (CISA) highlight the following definitions:

- **Malware:** Malicious software that's installed and can encrypt data and files, block user access, exfiltrate data, etc.
- **Ransomware:** A type of malware that encrypts sensitive data and files, followed by demanding a ransom to unlock the encrypted info.

- **Phishing:** A form of social engineering in which cybercriminals fish for victims by sending emails with promises, opportunities or threats to deceive victims.
- **Spear phishing:** A more sophisticated, targeted form of phishing which has cybercriminals using just enough information to make the victim believe the email came from someone known to the victim or another trusted source.
- **Brute force:** When an attacker uses software to continuously "bang away" in an attempt to gain access to a victim's computer, network or IT system.
- **Zero-day:** An attacker's identification of a weakness in a network or IT system. One example includes using defects in outdated software versions.
- **Denial of Service (DoS):** An attack that sends massive volumes of traffic to overwhelm an organization's website or server.
- **Distributed Denial of Service (DDoS):** A type of DoS attack that uses multiple computers simultaneously to shut down a website or server to all users.
- **Advanced Persistent Threats (APTs):** Attacks in which an unauthorized user gains access to a system or network and remains there for some time without being detected.
- **Telephony Denial of Service (TDoS):** An attack that overloads communications network elements with telephone calls—disrupting a jurisdiction's ability to provide emergency response services.

As this invisible threat continues to sweep the nation, let's take a look at two cyberattacks in the Emergency Services Sector.

Baltimore, Maryland

The city of Baltimore was unfortunate enough to find themselves dealing with not only one, but two cyberattacks within two years.

In March 2018, a ransomware attack targeted and took down the city's computer assisted dispatch (CAD) system that supports their 911 emergency dispatch and 311 non-emergency phone systems. Thankfully, city IT and cybersecurity staff quickly identified the problem and the system was restored in less than 24 hours. What caused the breach? It was later revealed that staff were working on part of the IT system and accidentally disabled a firewall—leaving them exposed for 24 hours.

A little over a year later, the city found that it had been hacked once again—but this attack was far more devastating. Through a phishing attack, almost all of Baltimore's IT infrastructure was taken over, and a ransom was demanded to release the city's systems and data. After refusing to pay the ransom of 13 bitcoin (which was worth around $76,000 at the time), it took months to get things back up and running.

Over this period, impacted services included water billing, property taxes, parking tickets, email and voicemail. Because the city's system that handled property transfers was also offline, property sales were interrupted as well. In this case, if Baltimore had installed a Microsoft patch that was made available in 2017, this cyber breach could have potentially been prevented.

TDoS Attacks

In October 2016, a digital "prank" targeted multiple 911 departments in Arizona, California, and Texas. The hacker tweeted a link to a webpage that, when visited on a mobile phone, would cause the phone to place repeated 911 calls. The bug overwhelmed 911 centers and the resulting volume of calls to 911 operators threatened availability of services.

According to the CISA, this strategy is not overly complicated to enact, yet it is difficult to foresee and prevent. As people place more emergency calls from cell phones, the potential for TDoS attacks to resemble DDoS attacks rises.

The Road to Recover

The recovery process can vary—in some cases dragging on for months and even more than a year—and in instances where you pay a hackers' ransom demands (which is never encouraged), the time it takes to restore and upgrade equipment can still be significant. In addition to the disruption to day-to-day operations, the cost of a breach can rack up millions.

In fact, according to IBM's annual Cost of a Data Breach Report—which studied over 500 data breaches worldwide—the average cost of a breach rose from 3.86 million in 2020 to 4.24 in 2021 (with the average cost in the U.S alone being 9.05 million). This ranks as the highest average total cost in the history of the report. To calculate this number, four elements were taken into consideration: detection and escalation, notification activities, post breach response and lost business.

While these numbers are alarming enough, in some high-profile and extreme cases, they can be even higher. For example, following a ransomware attack on the city of Atlanta in 2018, the city spent more than $17 million to recover. The 2019 ransomware attack on Baltimore that we just reviewed cost the city a whopping $18 million. While there is no one-size-fits-all solution to preventing a cyberattack, there are plenty of additional strategies that you can put into place to help you minimize your cybersecurity risks. Consider the following tips to help keep your community safe and your sensitive data secured.

1. Put Policies In Place

It is strongly recommended that businesses and organizations implement a variety of cybersecurity policies to help boost security and keep team members educated. According to ICMA, important policies to adopt include:

- Formal cybersecurity policy
- Password management policy
- Policy regarding applying software patches
- Cyber risk management plan
- Incident response/disaster recovery/business continuity plan
- Policy on the use of external devices, such as cell phones, flash drives, etc.
- Policy for vendors, contractors and cloud services

Establishing policies will be critical to protecting your operations and community, and all policies should be reviewed periodically to ensure they are up-to-date.

2. Minimize Vulnerabilities and The Risk of Operational Disruptions

Following the ransomware attack on the Colonial Pipeline in May 2021 – which halted services from the 5,500-mile natural gas pipeline for five days – the CISA and the Federal Bureau of Investigation (FBI) released an announcement with recommendations to help prevent business disruptions from an attack and mitigate vulnerability.

While these recommended strategies are aimed toward the critical infrastructure industry, this information is relevant to almost all businesses and public entities.

- **Reduce your risk of compromise:**
  - Require multi-factor authentication for remote access to OT and IT networks
  - Enable strong spam filters to help prevent phishing emails
  - Implement a user training program and simulated attacks for spear phishing
  - Filter network traffic to help prevent access to malicious websites
  - Update software such as operating systems, application and firmware on IT network assets regularly
  - Limit access to resources over networks, especially by restricting Remote Desktop Protocol (RDP)
  - Set antivirus/antimalware programs to conduct regular scans
  - Implement unauthorized execution prevention

- **To minimize severe business disruption in the event of a future attack:**
  - Implement and ensure network segmentation between IT and OT networks
  - Organize OT assets into logical zones
  - Identify OT and IT network inter-dependencies and develop workarounds or manual controls
  - Regularly test manual controls
  - Implement regular data backup procedures on both the IT and OT networks
  - Ensure user and process accounts are limited through account use policies, user account control and privileged account management.

- **If impacted by a ransomware incident:**
  - Isolate the infected system.
  - Turn off other computers and devices that share a network with the infected computer(s) that have not been fully encrypted by ransomware.
  - Ensure your backup data is offline and secure.

The FBI suggests to never pay a ransom. Denying criminals payment prevents future attacks. You can recover from ransomware, so long as you plan ahead.

3. Learn to spot phishing emails

Considering the fact that more than 90% of all cyberattacks begin with phishing, being able to identify these types of emails will be critical. Here are 4 red flags to look out for:

1. Unknown email sender
2. Email requests personal or financial information
3. Email wants the recipient to respond immediately or makes an urgent request for information (be on the lookout for upsetting or exciting statements asking you to act fast)
4. Email wants the recipient to open an attachment or click a link unexpectedly (hover your mouse over the link to see what website URL appears)

4. Find additional cyber resources

Visit our cybersecurity site for even more free, valuable tools and best practices to help keep you and your ESO safer online.

Additionally, the CISA's Emergency Services Sector Cybersecurity Initiative is an ongoing effort to enable the Emergency Services Sector (ESS) to better understand and manage cyber risks and to coordinate the sharing of cyber information and tools between subject matter experts (both inside and outside the federal government) and the ESS disciplines.

Just one cyber breach can have you forking over millions, impact the operations that your community members rely on and damage your reputation. Don't wait. Now is the time to make sure you're taking steps in the right direction to better protect yourself from cybercriminals.

REFERENCES

- Bulao, J. (2023). How many cyber attacks happen per day in 2023. [blog]. Retrieved from https://techjury.net/blog/how-many-cyber-attacks-per-day/?_sm_au_=iVV6kWQ5JLtHS7p2k4ctvKsHftFMW#gref
- CISA (2019, August). Emergency services sector landscape. Retrieved from https://www.cisa.gov/sites/default/files/publications/Emergency%20Services%20Sector%20Landscape.pdf
- CISA (2021). Alert (AA21-131A) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks. Retrieved from https://www.cisa.gov/uscert/ncas/alerts/aa21-131a
- EMSI Soft (2022, January 18). The state of ransomware in the US: Report and statistics 2021. [blog]. Retrieved from https://www.emsisoft.com/en/blog/40813/the-state-of-ransomware-in-the-us-report-and-statistics-2021/
- Green, J.J. (2016). DHS: Hackers increasingly targeting emergency systems. WTOP News. Retrieved from https://wtop.com/j-j-green-national/2016/02/dhs-hackers-increasingly-targeting-emergency-systems/?_sm_au_=iVV6kWQ5JLtHS7p2k4ctvKsHftFMW
- Marks, J. (2021, September 3). Amid a surge in ransomware attacks, cities are taking some of the biggest hits. Retrieved from https://www.washingtonpost.com/politics/amid-a-surge-in-ransomware-attacks-cities-are-takingsome-ofthe-biggest-hits/2021/09/02/9bd5d654-0a84-11ec-aea1-42a8138f132a_story.html
- McElroy, T. (2021, August 10). Tech safety in the emergency services sector: Overcoming obstacles in the adoption new mission-critical technology. Forbes. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2021/08/10/tech-safety-in-the-emergency-services-sector-overcoming-obstacles-in-the-adoption-of-new-mission-critical-technology/?sh=38afeb0f6c3a
- Norris, D.F. (2021, July 14). A look at local government cybersecurity in 2020. PM Magazine. Retrieved from https://icma.org/articles/pm-magazine/look-local-government-cybersecurity-2020?_sm_au_=iVV6kWQ5JLtHS7p2k4ctvKsHftFMW#:~:text=Table%201%3A%20Key%20Cyberattack%20Definitions