CDE #51399

WHY CYBERSECURITY MATTERS

To be effective, defenses must be integrated.

By Megan Bixler

MTV launched a TV show called "Catfish" in 2012. The show got its name from a type of internet fraud in which a person creates fake personal profiles on social media sites, using someone else's pictures and false biographical information to pretend to be someone other than themselves.

Each episode of the hour-long show aims to ascertain if a person — over the course of one week — is being "catfished" or not. The show highlights people's emotional investment into hackers that they have never met over the course of years.

VECTORFUSIONART/SHUTTERSTOCK.COM

If an individual thinks they don't have enough information to damage their employer and chooses to not adhere to basic cyber hygiene practices — including creating strong passwords — then they are leaving their accounts vulnerable to hackers.

This "catfish" type fraud usually aims to trick an unsuspecting person (or persons) into falling in love with the hacker. Typically, a person is being deceived for a myriad of reasons – financial gain, emotional manipulation or notoriety.

WHO IS VULNERABLE?

Today, the reality is that every individual, business and government is connected to the internet. As such, everybody is vulnerable to cyberattacks. The types and sophistication of attacks continue to grow.

The scenario described earlier is a type of phishing attack called catfishing. The trick to this type of cyberattack is gaining the trust of strangers. This can be accomplished through a variety of tactics. The hacker performs enough research before engaging their victim so that, to the victim, the hacker will seem trustworthy and barriers will break down. On an individual level, outcomes of a phishing attack may be identity theft, being "tricked" out of money, or divulging confidential personal or professional information.

Phishing attacks and social engineering aren't new. In fact, one could argue that intelligence operatives have been using these proven tactics for centuries. During the Cold War, it is known that Russian operatives lived in the United States and often exploited individual's emotions in order to gain classified information.

Some individuals might think that they have nothing of value that a hacker would be interested in. They think that they are so low on the "food chain" that the information they have will not be of value. Every individual carries a piece of the puzzle. It is important to remember that every piece of the information puzzle is important.

For example, if an individual thinks they don't have enough information to damage their employer and chooses to not adhere to basic cyber hygiene practices — including creating strong passwords — then they are leaving their accounts vulnerable to hackers. Now this employee is susceptible to a hacker gaining access to their computer to be used as a botnet. Botnets gain access to an individual's machine through some piece of malicious coding. In some cases, the machine is directly hacked, while other times what is known as a "spider" (a program that crawls the internet looking for holes in security to exploit) does the hacking automatically.[1]

More often than not, botnets aim to add the target computer to their web. That usually happens through a drive-by download or by fooling the victim into installing a seemingly harmless "Trojan horse" on their computer. A drive-by download happens through something as simple as opening a compromised web page. Once a compromised webpage has been visited (the drive-by), without stopping to click or accept any software, the malicious code can download in the background to your device. A drive-by download refers to the unintentional download of a virus or malicious software (malware) onto your computer or mobile device. Once the software is downloaded, the botnet contacts its master computer and lets it know that everything is ready to go. At that point the target computer, phone or tablet is entirely under the control of the person who created the botnet.

PHYSICAL ACCESS IS IMPORTANT TOO

In emergency communications centers (ECCs) across the United States, there are many people in various roles that have access to the building. These people can range from vendors to employees to administrators and even the general public. Physical security is just as essential as cybersecurity. Physical security helps companies protect assets, including information technology (IT) infrastructures and servers that make their businesses run and that store sensitive and critical data. Physical security encompasses measures and tools such as gates, alarms and video surveillance cameras. But physical security also includes another central element: an organization's personnel. Here are some precautions to consider regarding personnel:[2]

- Foster a culture of security: Personnel are an ECC's first line of defense, so it is important to train employees in security awareness and build an enjoyable workplace to equip and motivate employees to protect the ECC.
- Secure entry points: ECCs can improve cybersecurity by investing in security gates and doors. Requiring access cards helps restrict access and deploying "smart locks" allow ECCs to add additional barriers with wireless unlocking mechanisms.
- Use surveillance cameras: Inexpensive yet invaluable, surveillance cameras can detect potential threats as well as provide solid evidence for forensic review after incidents.
- Install alarms: They are crucial security elements for warding off intruders.
- Guard the server room: Small businesses often maintain their data center in a small room, in which case monitoring and even securing access with security gates is especially important.

CREATING OR IMPROVING A CYBER PROGRAM

According to APCO's "Broadband Implications for the PSAP" report,[3] "It is essential that cybersecurity is considered at the onset and not treated as an afterthought, when adopting new technologies. In other words, cybersecurity must be baked in, not bolted on." In order to ensure that an ECC properly plans for a cyber related incident, a cybersecurity program must be thoughtfully made. According to the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity,[4] the following steps illustrate how this framework can be used to create a new cybersecurity program or improve an existing program:

- **Step 1: Prioritize and Scope**. The organization identifies its mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.
- **Step 2: Orient.** Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements and overall risk approach. The organization then consults with sources to identify threats and vulnerabilities applicable to those systems and assets.
- **Step 3: Create a Current Profile**. The organization develops a current profile by indicating which category and subcategory outcomes from the framework core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.
- **Step 4: Conduct a Risk Assessment**. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact it could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.
- **Step 5: Create a Target Profile**. The organization creates a target profile that focuses on the assessment of the framework categories and subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional categories and subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers and business partners when creating a target profile. The target profile should appropriately reflect criteria within the target implementation tier.

- **Step 6: Determine, Analyze and Prioritize Gaps**. The organization compares the current profile and the target profile to determine gaps. Next, it creates a prioritized action plan to address gaps — reflecting mission drivers, costs and benefits, and risks — to achieve the outcomes in the target profile. The organization then determines resources, including funding and workforce necessary to address the gaps. Using profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management and enables the organization to perform cost-effective, targeted improvements.
- **Step 7: Implement an Action Plan**. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the target profile. For further guidance, the framework identifies example informative references regarding the categories and subcategories, but organizations should determine which standards, guidelines and practices, including those that are sector specific, work best for their needs.

Cybersecurity is becoming more and more essential to the overall security posture of all organizations, governments and individuals. Again, with this in mind, cybersecurity should be "baked in, not bolted on".[5] When implementing new systems and networks, ECCs should always consider cybersecurity measures in the initial plans in order to ensure that sensitive data is secured. By following the steps outlined above, any ECC will be well on its way to establishing a cybersecurity program that will assist in the mitigation of attacks. ●

Megan Bixler *is APCO International's Technical Program Manager for the Communications Center and 9-1-1 Services Department.*

REFERENCES

1 us.norton.com/internetsecurity-malware-what-is-a-botnet.html
2 Goldstein, P. (2016, Oct 11). "Why physical security should be as important as cybersecurity." BizTech. https://biztechmagazine.com/article/2016/10/why-physical-security-should-be-important-cybersecurity
3 apcointl.org/ext/pages/p43/p43book.html
4 NIST Framework for Improving Critical Infrastructure Cybersecurity, nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
5 apcointl.org/ext/pages/p43/p43book.html

CDE EXAM #51399

1. Some individuals are so low on the professional "food chain" that they don't need to think about cybersecurity or cybersecurity needs.
   a. True
   b. False

2. Phishing and other social engineering tactics have been around for centuries.
   a. True
   b. False

3. The NIST Framework for Improving Critical Infrastructure Cybersecurity outlines seven steps to create or improve on a cyber program. Which of the following is NOT one of those steps?
   a. Determine, analyze and prioritize gaps
   b. Create a current profile
   c. Ignore all current cyber related issues until after the cyber program is complete.
   d. Conduct a risk assessment

4. What does physical security encompass?
   a. Measures and tools like gates, alarms and video surveillance cameras, but also another central element: an organization's personnel.
   b. All computer networks and systems
   c. Alarms
   d. ECC's training program

5. Who is vulnerable to cyber attacks?
   a. Only the important people in an organization — ECC directors and managers.
   b. Everybody
   c. It isn't really that important

6. What is catfishing?
   a. Fishing for catfish
   b. A "catfish" is a person who creates fake personal profiles on social media sites using someone else's pictures and false biographical information to pretend to be someone other than themselves.
   c. A new type of dog
   d. Internet slang

7. Cybersecurity should be "baked in, not bolted on."
   a. True
   b. False

8. What are some of the outcomes of an individual being catfished?
   a. Loss of money
   b. Loss of sensitive information
   c. Identity theft
   d. All of the above

9. Server rooms don't need to be guarded.
   a. True
   b. False

10. When making or modifying a cyber program, ECCs should first identify its mission objectives and high-level organizational priorities.
    a. True
    b. False

FOR CREDIT TOWARD APCO RECERTIFICATION(S)

Each CDE article is equal to one credit hour of continuing education

1. Study the CDE article in this issue.
2. Answer the test questions online (see below for online exam instructions) or on the exam page from the magazine article (photocopies are not required).
3. Add/upload your CDE article information and certificate of achievement in the "My Classes Taken" section of APCO's Training Central at www.apcointl.org/trainingcentral.

Questions? Call us at (386) 322-2500.

You can access the CDE exam online!
To receive a complimentary certificate of completion, you may take the CDE exam online. Go to http://apco.remote-learner.net/login/index.php to create your username and password. Enter the "CDE article" in the search box, and click on the "2019 Public Safety Communications Magazine Article Exams," then click on "enroll me" and choose "Why Cybersecurity Matters **(51399)**" to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.