DRAFT -- AGA Q&A

Cyber Attacks and Incidents

Question 1:

I heard that the number of ransomware attacks is increasing and has victimized numerous government entities. What is ransomware and what can I do to protect my data and networks?

Answer:

According to the Cybersecurity and Infrastructure Security Agency (CISA), ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. After the initial infection, ransomware will attempt to spread to connected systems, including shared storage drives and other accessible computers. It will attempt to encrypt the files on each drive, rendering the files inaccessible to the victim. Once encryption is complete, ransomware will create and display a file containing instructions on how the victim can pay the ransom.

CISA recommends the following precautions to protect users against the threat of ransomware:

- **Update software and operating systems** with the latest patches. Outdated applications and operating systems are the target of many attacks.
- **Never click on links** or open attachments in unsolicited emails.
- **Backup data on a regular basis**. Keep it on a separate device and store it offline. Scan backup data with anti-virus software to check that it is free of malware. Regularly test your backup data to ensure the information is sufficient to restore your operations.
- Follow safe practices when browsing the Internet.

CISA also recommends that organizations employ the following best practices:

- **Restrict users' permissions** to install and run applications, and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread throughout a network.
- **Use software whitelisting** to allow only approved programs to run on a network.
- **Enable strong spam filters** to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
- **Scan all incoming and outgoing emails** to detect threats and filter executable files from reaching end users.
- Configure firewalls to **block access to known malicious IP addresses**.

If infected with ransomware, CISA recommends that organizations:

Cyber Attacks and Incidents

- **Isolate the infected system**. Remove the infected system from all networks, and disable the computer's wireless, Bluetooth, and any other networking capability, and consider the option of power-off. Ensure all shared and network drives are disconnected. Remember that if you should you power down the system you may inadvertently destroy system log files that could be used to prosecute an attacker. Consider contacting a computer forensic expert if you suspect illegal activity. Ensure all malware has been remediated prior to restoring the infected system.

- **Report infection immediately** to internal IT department and to CISA at www.us-cert.gov/report, a local FBI field office, or Secret Service office. Report suspected data breaches to internal privacy and disclosure offices.

For additional information, see https://www.us-cert.gov/ncas/tips/ST19-001

Cyber Attacks and Incidents

Question 2. How can I protect my systems and networks from malicious code? How do I recover if malicious code infects my systems?

Answer: According to the Cybersecurity and Infrastructure Security Agency (CISA), malicious code is unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Malicious code includes viruses, worms, and Trojan horses. *Viruses* have the ability to damage or destroy files on a computer. Users can spread viruses by sharing an already infected removable media, opening malicious email attachments, and visiting malicious web pages. *Worms* are a type of virus that requires no user interface to spread; they self-propagate from computer to computer. *Trojan horses* are computer programs that are hiding a virus or a potentially damaging program that performs malicious actions on the host computer. Free software is a common vehicle for spreading Trojan horses.

CISA recommends these security practices to reduce the risks associated with malicious code:

- **Install and maintain antivirus (AV) software**. Obtain AV software from a reputable vendor and keep it up-to-date. Use automatic scanning feature of AV software, if available. If not, manually scan files and media from outside sources before opening them. Enable the anti-spyware feature that is available in most AV software.

- **Use caution with links and attachments**. Be wary of unsolicited email attachments and always visit vendor sites directly rather than clicking on advertisements or email links.

- **Block pop-up advertisements**. Enable blocking feature, which is available on most browsers, to disable ads that may contain malicious code.

- **Disable external media AutoRun and AutoPlay features** to prevent external media infected with malicious code from automatically running on your computer.

- **Install software and operating system patches on your computer** so attackers do not exploit known vulnerabilities. Consider enabling automatic updates.

- **Backup data** to the cloud or external hard drive so information will not be lost in the event of an infection. Regularly test backups to ensure they are sufficient to recover your operations.

- **Install or implement a firewall** to prevent some types of infection by blocking malicious traffic before it enters your computer.

If infected with malicious code, CISA recommends the following actions:

- **Minimize the damage** by contacting your IT department immediately. If you are on home computer or laptop, disconnect your computer from the Internet. Try to avoid powering down the infected system, as you may inadvertently destroy system log files

that could be used to prosecute an attacker. Consider contacting a computer forensic experts if you suspect illegal activity.

- **Remove the malicious code**. Update AV software on your computer and perform a manual scan of your entire system. If AV software cannot locate and remove malicious code, you may need to reinstall the operating system. Relying solely on AV may not be appropriate if we are talking about a critical system

For additional information, see https://www.us-cert.gov/ncas/tips/ST18-271.

DRAFT -- AGA Q&A

Cyber Attacks and Incidents

Question 3. My state maintains a voter registration database. What types of threats place that data at risk? What preventive measures should I employ and what should I do if a malicious actor gains unauthorized access to voter registration data?

Answer: According to the Cybersecurity and Infrastructure Security Agency (CISA), voter registration databases present attractive targets for cyber threat actors to steal voter information or disrupt voting operations. Malicious actors may use a variety of methods to interfere with voter registration websites and databases including:

- **Phishing attempts** are forged emails, texts, and other messages used to manipulate users into clicking on malicious links or downloading malicious file attachments.
- **Denial-of-service attacks** can prevent legitimate users from accessing a voter registration website or voter registration data.
- **Ransomware** is a type of malicious software that restricts users' access to system resources or data until a ransom is paid.

CISA advises election officials to employ the following prevention measures to protect against these threats:

- **Patch applications and operating systems**. Patching these with the latest updates greatly reduces the number of exploitable entry points available to attackers.
- **Implement software whitelisting**. This allows only specified programs to run while blocking all others, including malicious software.
- **Restrict administrative privileges**. This may prevent malicious software from running or limit its capability to spread through the network.
- **Implement input validation**. This is a method of sanitizing untrusted user input by users of a web application and may prevent many types of web-based security flaws.
- **Implement firewalls**. These can control or block data from certain locations or applications while allowing relevant and necessary data through.
- **Backup and store data offline**. This can greatly assist the restoration of services after a breach. Regularly test data to ensure it is sufficient to restore operations.

If a malicious actor gains unauthorized access to voter registration data, CISA recommends:

- **Implement your security incident response and business continuity plan** to maintain your organization's essential functions and operations.
- **Contact CISA or law enforcement immediately** to report an intrusion or to request incident response resources or technical assistance.

DRAFT -- AGA Q&A

Cyber Attacks and Incidents

For additional information, see https://www.us-cert.gov/ncas/tips/ST16-001.

Question 4. What can my organization do to limit its exposure to denial-of-service attacks? What should I do if we are experiencing such an attack?

Answer: A denial-of-service attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access to legitimate users.

According to the Cybersecurity and Infrastructure Security Agency (CISA), there is no way to avoid becoming a target of a denial-of-service (DoS) attack. However, CISA recommends the following steps to reduce the effects of an attack:

- **Enroll in a DoS protection service** that detects abnormal traffic flows and redirects traffic away from your network. The service filters out DoS traffic and passes clean traffic on to your network.
- **Create a disaster recovery plan** to ensure successful and efficient communication, mitigation, and recovery in the event of an attack. Regularly test your disaster recovery plan to identify bottlenecks and failure points.
- **Strengthen security of all internet-connected devices** in order to prevent malicious individuals from compromising them. Specifically,
    - **Install and maintain antivirus software**
    - **Install and maintain a firewall to restrict traffic** coming into and leaving your computer
    - **Limit access to your information- develop, install and maintain a strong policy concerning all access to information**
- **Monitor and analyze network traffic** via a firewall or intrusion detection system to quickly detect and identify a DoS attack.
- **Implement an intrusion prevention system** to automatically attempt to block suspicious activity on your network.

If you think you are experiencing a DoS attack, CISA recommends:

- **Contacting your network administrator** to confirm whether the service outage is due to in-house maintenance or due to an attack. The administrator can apply firewall rules and reroute traffic through a protection service to ameliorate the effects of an attack.

- **Contacting your internet service provider** to ask if their network is the target of the attack and you are an indirect victim. Seek advice from the ISP on appropriate course of action.

- **Monitor other hosts, assets, and services** residing on your network. Many attackers conduct DoS attacks to deflect attention away from their intended target and use the opportunity to conduct secondary attacks on other services within your network.

For additional information, see https://www.us-cert.gov/ncas/tips/ST04-015

Question 5. How can I avoid social engineering and phishing attacks?

Answer: Social engineering and phishing attacks are among the most frequent and effective means attackers use to compromise information systems and information. In these attacks, an attacker—often posing as an individual from a legitimate organization—uses human interaction or social skills to deceive victims into providing sensitive information or performing other detrimental activities. Phishing is a form of social engineering that uses email or malicious websites to solicit information or download malicious software to the victim's computer. Other attacks use voice communications or text messages to interact with the targeted victim. Social engineering and phishing attacks are often used during peak periods, such as the end of a quarter, or deployed when organizations are facing other emergencies.

According to the Cybersecurity and Infrastructure Security Agency (CISA), the following are common indicators of phishing attempts:

- **Suspicious sender's email address** that may imitate a legitimate business by altering or omitting a few characters.

- **Generic greetings and lack of contact information**. A trusted organization will normally address you by name and provide their contact information.

- **Spoofed hyperlinks**. If you hover your cursor over any links in the body of an email, and the links do not match the text that appears when hovering over them, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

- **Suspicious attachments**. An unsolicited email requesting a user to download and open an attachment is a common delivery mechanism for malicious software.

To avoid being a victim of social engineering and phishing attacks, CISA recommends that you:

- **Be suspicious of unsolicited phone calls**, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his/her identity directly with the company.

- **Do not reveal personal, financial, or sensitive information in email** or respond to email solicitations for this information. **Never** provide multifactor authentication codes to anyone.

- **Install and maintain anti-virus software, firewalls, and email filters** to reduce some of this traffic.

If you believe you are a victim of a social engineering or phishing attack:

- **Report it to the the IT/Security team** within your organization and consider reporting the attack to law enforcement and the Federal Trade Commission.

- If your financial accounts are compromised, **contact** your financial institution, **close** compromised accounts, **watch** for unexplainable charges to your account.

For additional information, see https://www.us-cert.gov/ncas/tips/ST04-014.

Question 6. How can I prevent being a victim of identity theft and what should I do if I am?

Answer: According to the Cybersecurity and Infrastructure Security Agency (CISA), identity theft is usually a crime of opportunity, so you may become a victim simply because your information is available. The internet has made it easier for thieves to obtain personal and financial data (such as credit card numbers, phone numbers, account numbers, and addresses). Companies and other institutions often store information about their clients in databases. If a thief can access that database, he/she can obtain information about many people at once and use that information to impersonate the victims to purchase items, open new accounts, and apply for loans.

According to CISA, there is no way to guarantee that you will not be a victim of identity theft. However, there are ways to minimize your risk:

- **Do business with reputable companies**. Before providing any personal or financial information, make sure you are interacting with a reputable, established company.

- **Take advantage of security features**. Passwords and other security features add layers of protection.

- **Check privacy policies** to see how a company will use or distribute your information.

- **Be careful what information you publicize.** Attackers may be able to piece together information from various sources.

- **Be aware of your account activity.** Review statements and credit reports. Be aware of unusual or unexplainable charges on your bills; phone calls or bills for accounts, products, or services that you do not have; failure to receive regular bills or mail; new,

strange accounts appearing on your credit report; and unexpected denial of your credit card.

If you suspect or know that someone has stolen your identity, CISA recommends that you:

- Visit IdentityTheft.gov – a trusted, one-stop resource to help you report and recover from identity theft.
- Contact credit reporting agencies and companies where you have accounts.
- Consider other websites for information and guidance for recovering from identity theft:
    - Federal Trade Commission: https://www.consumer.ftc.gov
    - Dept. of Justice: https://www.usdoj.gov/criminal/fraud/websites/idtheft.html
    - Social Security Administration: https://www.ssa.gov/pubs/EN-05-10064.pdf

For additional information, see https://www.us-cert.gov/ncas/tips/ST05-019