Cybersecurity Best Practices

Gerry Cochran, IT Specialist III
Agenda

• Cybersecurity Threats
• Recent Cyberattacks
• Cybersecurity best practices
Cybersecurity Threats (Network)

- Malware
- Social Engineering
- Ransomware
- Denial-of-Service (DoS) Attacks
- Man-in-the-Middle (MITM) Attacks
- Password Attacks
- Wireless Attacks
- Insider Threats
Recent Cyberattacks
The 2018 Verizon Breach Report

What tactics are being utilized?

• 48% of breaches featured hacking.
  – 56% of hacking-related breaches leveraged stolen and/or weak passwords.
• 30% included malware.
  – 49% of malware was installed via malicious email.
• 17% were social engineering attacks.
  – 76% of social engineering attacks involved phishing.
• 12% involved privilege misuse.
The 2018 Verizon Breach Report

Other noteworthy items:
• 14% of breaches involved public sector entities.
• 58% of all victims are categorized as small business.
• 76% of breaches were financially motivated.
• 68% of breaches took months or longer to discover.
• Organized crime accounts for 62% of external breaches.
• 69% of all compromised data consisted of personal and/or payment data.
Atlanta Ransomware Incident

• Impacted five of the city’s 13 local government departments.
• Spent $2.6M to recover from a $52,000 ransom.
• Also delayed the budget proposal as the cyber incident compromised the budget planning system.
• This ransomware variant infiltrates by exploiting vulnerabilities or guessing weak passwords in a target’s public-facing systems.
• Atlanta is still recovering from the ransomware attack.
Ygnacio Valley High School Phishing Attack

• A student used a phishing scam to access the school district’s computer system and change a number of students’ grades.

• The student created a fake website that looked identical to the school’s and then sent emails to teachers in an attempt to get them to sign into his fake site.

• Police tracked his IP address back to his home where electronics-sniffing dogs found a flash drive hidden in a tissue box.

• The student has been arrested and charged with 14 felony counts.
Hyatt Point-Of-Sale Breach

- Impacted 41 of the company’s properties worldwide.
- In several public cases, adversaries called the front desk complaining of an issue and then sent an email with supporting information.
- The email contained VBScript or Macros that downloaded malware on the computer and then stole passwords and enabled Remote Desktop.
Uber

- Exposed 57 million client records (names, email addresses, phone numbers) and 600,000 driver records (names and driver’s license numbers).
- Two hackers accessed Uber’s Amazon cloud account (where stored data was unencrypted).
- Uber paid $100,000 to delete the data and keep the breach quiet.
Equifax

- Exposed **145.5 million** Americans’ names, Social Security numbers, dates of birth and addresses. Also exposed **209,000** credit card numbers.
- Attackers exploited a vulnerability in an Equifax web application.
- Evidence of a second breach was discovered just one month later - Equifax took down a consumer webpage to investigate the possible breach.
Cybersecurity Best Practices
Hardware, Software and Data Inventories

**Best Practice:** Maintain detailed, up-to-date inventory records for all computer hardware, software and electronic data.

Without the proper identification of all devices on a network, unauthorized devices and software can be easily introduced, putting the network and data at risk. A single compromised device can become a launching point for further network attacks, quickly turning one compromised device into many.

Inadequate inventory records makes it unlikely that software patches necessary to address known security vulnerabilities can be applied on a timely basis, if at all.
Hardware, Software and Data Inventories (Continued)

Inadequate records increases the likelihood that you may inadvertently violate copyright laws by having more software users than licenses for a particular application and incur penalties as a result.

IT security alerts and bulletins issued by software vendors, municipal associations, and federal and state agencies reference specific types and versions of devices and software. These alerts are intended to raise awareness about threats, sometimes imminent threats, to computer systems. Accurate inventory records can help you determine if these advisories are relevant to your unique computing environment.

It is very challenging to protect computer resources, including data, if you do not know exactly what resources you have and where those resources reside.
Data Classification

Data classification is the process of assigning data to a category (e.g., public, internal use, confidential) that will determine the level of internal controls over that data.

An inventory of information assets (i.e., data) that classifies data according to its sensitivity and identifies where the data resides (e.g., servers, workstations, and laptops) is important because different kinds of information require different levels of protection.
Policies and Training

**Best Practice:** Adopt IT policies that define appropriate user behavior, describe the tools and procedures needed to protect data and information systems, and explain the consequences of policy violations. Provide entity-wide, cybersecurity training that is closely tied to the IT policies.

- Acceptable Use
- Breach Notification (New York State Technology Law Section 208 (8))
- Password
- Online Banking

While your IT policies tell users what to do, training provides them with the skills to do it.
Access Controls

**Best Practice:** Know all points of entry to your computing environment and data, and ensure that all access is authorized and secure. Use available electronic means to enforce and monitor compliance with access controls. Place particular emphasis on limiting access to and protecting personal, private, and sensitive information.

- Have written procedures in place for granting, changing, and terminating access rights.
- Allow users to access only what is necessary to complete their job duties (principle of least privilege).
- Periodically review all accounts and disable any account that cannot be associated with an authorized user.
User Accounts and Passwords

• To ensure individual accountability within the network, each user should have his or her own network account (username and password). Likewise, to ensure individual accountability within software applications, each user should have his or her own user account (username and password).
• Users should be able to set their own passwords.
• Criteria you should consider with regard to passwords:
  – Complexity requirements
  – Length
  – Aging
  – Reuse of old passwords
  – Failed log-on attempts.
Strictly Control the Use of Administrative Privileges

Administrative privileges are highly privileged accounts that generally allow users to: view all data on the system or network; make changes to the settings configured on the system or network; and create new user accounts, or change the levels of privileges granted to existing user accounts, on the system or network.

Administrative privileges are necessary for only a small number of users with particular job duties.

There are countless ways that attackers who gain administrative privileges can leverage their positions to increase the level of damage caused when a system or network is breached.
Antivirus Protection

**Best Practice:** Install antivirus software and configure it to update automatically. Force scans of all newly discovered devices, such as flash drives and digital cameras, and disable the auto-play feature for USB devices.

Antivirus software scans your computer or device and looks for certain characteristics of known malware (signatures) or other suspicious activity. If something of concern is identified, the software attempts to prevent the agent from causing harm by, for example, removing malware from within a file or quarantining files.

Since malware is constantly taking new forms, an antivirus program cannot be expected to identify and neutralize all types of malware. This is one of the reasons why multiple layers of IT security (defense in depth) are required to keep computer systems and data safe.
Patch Management

**Best Practice:** Adopt patch-management policies and procedures that ensure that all patches and updates are applied on a regular basis.

A “patch” is software that is used to correct a problem, such as a security vulnerability, that exists within an application or an operating system.

When security vulnerabilities in software are discovered, the software vendor typically issues a free patch (fix) to correct the problem. The patch should be applied as soon as possible to reduce the likelihood that someone with malicious intent could successfully exploit the vulnerability.

At some point, vendors discontinue issuing patches (e.g., Microsoft Windows XP).
Online Banking

**Best Practice:** Entities should adopt a suite of technology-based and nontechnical controls to ensure online banking is conducted as safely as possible.

- Adopt an online banking policy and enter into bank agreements.
- Segregate duties.
- Enable alerts and other security measures available from the bank.
- Set up accounts that do not have access to and/or cannot be accessed through the Internet, and use those accounts for long-term savings.
- Provide cybersecurity training to officers and employees responsible for online banking.
- Consider using a separate (dedicated) computer for online banking transactions, one that is not used for email or Internet browsing.
Online Banking (continued)

- Type the bank’s website address into the Internet browser’s address bar every time.
- Do not allow the computer or web browser to save online banking login names or passwords.
- Use a wired rather than wireless network for financial transactions.
- Monitor accounts on a timely basis, at least every two or three days, for unauthorized or suspicious activity.
  - Any suspicious activity should be reported immediately. There is a limited recovery window, and a rapid response may prevent additional losses.
  - To be effective, monitoring must occur frequently even during times when many personnel may be on leave (e.g., 4th of July week; the weeks before, during and immediately after Christmas).
Wireless Networks

**Best Practice:** Configure your wireless network to broadcast only as far as necessary, enable the best available encryption, and require strong passwords.

- Wireless access point coverage should radiate out to the windows, but not beyond.
- Enable the most-secure encryption available (currently WPA2).
- Require a strong password for connecting to the wireless network.
Public Website Information Disclosure

**Best Practice:** Establish a framework for classifying data based on its level of sensitivity, review *all* materials *before* they are posted to your public website, and then periodically review the content of your public website to ensure that your internal controls over sensitive information are operating as intended.

Google search operators:
- Limit search results to those that match criteria beyond simple keywords.
- Maintain a list of websites, file types, and keywords to search on a regular basis.
- Google allows users to create searches and periodically receive email alerts of new content that matches those searches.

http://www.googleguide.com/advanced_operators_reference.htm
http://www.google.com/alerts
Physical and Environmental Security

**Best Practices:** Periodically assess physical and environmental security measures to ensure they adequately protect computer resources and the facilities or infrastructure that house or support those resources from intentional or unintentional harm, loss or impairment.

- Physical access controls restrict the entry and exit of personnel and/or equipment and media from an area.
- Locks, gates and security personnel.
- Smoke detectors, fire alarms and extinguishers, protection from water damage due to plumbing leaks or other flooding, and uninterruptible power supplies.
Physical and Environmental Security (Continued)

An organization’s personnel can play an important part in physical security by being trained and encouraged to question people whom they do not recognize in restricted areas.

It is important to consider and evaluate physical security measures both during normal business hours and at other times for example, when an area or building may be unoccupied.

We have found servers:

- On a basement floor in a municipality that experienced flooding in the past.
- Next to the refrigerator in a break room.
- In an open area in a recreation center.
- In a closet used daily by staff and visitors to the facility.
Firewalls

**Best Practice:** Install one or more securely configured firewalls, and monitor the logs and alerts the firewall(s) generate. Update the firewall rules as necessary using a formal change management control process.

Firewalls consist of hardware and/or software that control the flow of network traffic between networks or hosts (e.g., computers) that employ differing security postures or goals.

There are several types of firewalls, each with varying capabilities, to analyze network traffic and allow or block specific instances by comparing traffic characteristics to existing policies.
IT Disaster Recovery Planning

**Best Practice:** Develop a formal IT disaster recovery plan that addresses the range of threats to your IT system(s), distribute the plan to all responsible parties, and ensure that it is periodically tested and updated as needed.

- The plan should focus on sustaining critical business functions during and after a disruption.
- Technology recovery strategies should consider the possible restoration of hardware, applications, data and connectivity.
- The plan should include policies and procedures to ensure that all critical information is routinely backed up so that it would be available in the event of an emergency.
Backups

**Best Practice:** Back up data at regular intervals; verify the data has been backed up; store the backup media in a secure, off-site location; and verify the ability to restore the data backup.

While many entities perform some type of backup procedures, far fewer periodically attempt to restore a backup to ensure the process is functioning as intended and that data would be available in the event of an emergency.

As noted in the discussion of ransomware, it is important to maintain offline copies of backups in case an attack renders online files unusable.
Information Disposal and Media Sanitization

**Best Practice:** Adopt written policies and procedures that outline the proper process to use in verifying that personal, private and sensitive data is entirely destroyed or removed from electronic media prior to the equipment’s disposal or reuse.

Local governments can contract with third parties who specialize in information disposal and media sanitization. Prior to doing so, the entity can, among other things, review and evaluate the disposal company’s information security polices, require that the company be certified by a recognized trade association or similar third party, and/or require the company to provide written certification that information was disposed of in the agreed-upon manner.

Contracts for IT Support Services

**Best Practice:** Contracts (service level agreements or SLAs) for IT support services should be in writing, clearly state the local government’s security needs and expectations, and specify the level of service to be provided by the independent contractor or vendor.

The components of an SLA vary but can include: identification of the parties to the contract; definitions of terminology; term/duration of agreement; scope/subject; limitations (what, if anything, is excluded); service level objectives and performance indicators; roles and responsibilities; nonperformance impact; pricing, billing and terms of payment; security procedures; audit procedures; reporting; reviews/updates; and approvals.
Cybersecurity Experts and Resources

Center for Internet Security’s Multi-State Information Sharing & Analysis Center
https://www.cisecurity.org/ms-isac

New York State Office of Information Technology Services
http://www.its.ny.gov/incident-reporting

United States Cyber Emergency Response Team
https://www.us-cert.gov
Questions?

Gerry Cochran, gcochran@osc.ny.gov