Technology Safeguards and Best Practices

JAMESON MORGAN

JAMESON MORGAN ENTERPRISES

WEDNESDAY, MARCH 20, 2019

Disclaimer

- THIS PRESENTATION IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THIS PRESENTATION. THE VIEWS EXPRESSED WITHIN THIS PRESENTATION ARE FOR GUIDANCE ONLY AND DO NOT IMPLY COMPLIANCE.

Basic Safeguards

EASY TO IMPLEMENT TECHNOLOGY SAFEGUARDS

Passwords

THE TRIED AND TRUE METHOD FOR AUTHENTICATION

Passwords

- Certainly the “tried and true” method for authenticating users
- Passwords must be unique for each account for maximum security benefit
  - Leaked usernames and passwords can be used on other websites with the same (or very similar) credentials
- Think of a password as a passphrase rather than just a few words strung together
  - Why? This causes the password to have higher *entropy* and therefore is much more difficult to crack
  - And, for what’s it worth, a passphrase is much easier to remember
- Always utilize two-factor authentication if available
  - It does slow down productivity, but the productivity reduction is worth it in the long-run
- Consider using a password manager which allows for longer passwords since they need not be remembered
  - Lastpass is a personal product that is available
- Keep passwords (or passphrases) between 16 – 64 characters and include a mix of alpha-numeric characters as well as special characters

https://blog.lastpass.com/2016/06/password-smarts-how-to-improve-your-first-line-of-defense.html/
https://www.us-cert.gov/ncas/tips/ST04-002
https://resources.infosecinstitute.com/password-security-complexity-vs-length/#gref
https://www.schneier.com/blog/archives/2017/10/changes_in_pass.html

Passwords

- Length is more important than complexity, all though both are required for a strong password
- Password change reminders are not deemed helpful according to a recent NIST (National Institute of Standards and Technology) report on digital identities
  - I would personally recommend a modest password change cycle with an emphasis on lengthy and complex characters

https://blog.lastpass.com/2016/06/password-smarts-how-to-improve-your-first-line-of-defense.html/
https://www.us-cert.gov/ncas/tips/ST04-002
https://resources.infosecinstitute.com/password-security-complexity-vs-length/#gref
https://www.schneier.com/blog/archives/2017/10/changes_in_pass.html

Some Examples

- The Good:
  - britishKitesflyhigh18!
    - 3597 centuries when brute forced on a typical home computer
  - d0gsaremybestfr13nds
    - 3119 centuries when brute forced on a typical home computer
  - F orgottenD3ams!
    - 120 centuries when brute forced on a typical home computer
  - to!nfinityAndb3yond
    - 4 centuries when brute forced on a typical home computer

https://www.lifewire.com/strong-password-examples-2483118
https://password.kaspersky.com/

Some Examples

- The Bad:
  - decemberWinter19!
    - 4 months when brute forced on a typical home computer
  - ForgottenD3ams!
    - 2 years when brute forced on a typical home computer
- The Ugly:
  - Password
    - 1 second when brute forced on a typical home computer
  - 7ate9
    - 3 minutes when brute forced on a typical home computer

https://www.lifewire.com/strong-password-examples-2483118
https://password.kaspersky.com/

Encryption and Decryption

PLAINTEXT TO CIPHERTEXT…IT'S MAGIC

Current Encryption Standards (NIST)

- AES
  - Advanced Encryption Standard
  - Approved November 2001
  - AES has not been broken
- Triple DES (3DES)
  - Triple Data Encryption Standard
  - Uses the DES cipher three times
  - Approved November 2017
  - Broken cipher if certain adjustments are not met
  - Used by payment processors
- Currently withdrawn:
  - DES
  - Skipjack

https://csrc.nist.gov/News/2017/Update-to-Current-Use-and-Deprecation-of-TDEA

Bit Length

- AES
  - 128, 192 or 256 bit key length
- Triple DES (3DES)
  - 128 or 192 bit key length
- A key is used to translate the plaintext into ciphertext and is required to translate the ciphertext back into plaintext
- The longer the key the better for security
  - This is because all encryption algorithms can be broken by brute force (running through all possible combinations) but if the key is substantially large such that brute force is infeasible, we say that computational security has been achieved

https://en.wikipedia.org/wiki/Key_size

Other Encryption Types

- Hash
  - Takes data of any size and produces a fixed length collection of characters known as a digest
  - Commonly used to store passwords with an additional piece of information called a “salt”
  - Useful for integrity checking
- Public/Private Key Encryption
  - A pair of keys (one kept private, the other made public) that are mathematically related in such a way that the pair of keys enables encryption and decryption of data
  - SSL Certificates
  - Useful for authentication and privacy
- Digital Signatures
  - Takes a hash and combines it with public/private key encryption
  - Useful when authentication is required not privacy
  - Useful for authentication

Where is Encryption Used

- Encryption should be enabled whenever possible as it is always better to have data encrypted so that it is rendered useless if intercepted
- Typical applications of encryption include:
  - SSL to transmit data across the Internet
  - Database backups
  - Record encryption
  - Email transmissions

Mobile Devices

Danger Will Robinson!

- Mobile devices bring major concerns regarding the privacy and protection of protected health information
- Mobile devices are not prohibited by HIPAA (which is a good thing) but the risks of utilizing mobile devices to access protected health information need to be considered and incorporated into a practice's risk analysis and it's risk management
- Risks Include (but not limited to):
  - Loss or theft
  - Improper security controls
  - Malware
  - Lack of sophisticated security features
  - Ease of access

Implementation Suggestions

- We live in a digital age and telling people they cannot text your office to make an appointment goes against the very core of HIPAA
- Do not allow a bring your own device (BYOD) strategy in your office
- Below, are some helpful suggestions if you decide to utilize mobile devices in your practice:
  - Maintain a separate device that is only used for patient communication (in other words, no BYOD) and is always left at the practice in accordance with security procedures and policies
    - Patient communication includes text, phone calls and email (in certain instances)
  - Only allow certain features to be enabled as is necessary to complete one's job
    - Restrictions are an excellent way of "locking down" a mobile device so that only certain functions may be performed
  - Always include a password or passcode (longest length allowed)
  - Install or enable encryption
  - Do not "jailbreak" the device; this introduces the potential for serious problems
  - Always install updates as they become available
  - Do not install apps unless necessary, thoroughly researched and designed by reputable companies
  - Implement a mobile device policy for your practice
  - Enable remote wiping of data

What Not To Do!

- Patients may initiate (or reply to) a communication and provide protected health information to you through an electronic means and you, as the provider, are not liable so long as you do not reply to such a message
  - Once you reply however, you are now responsible for safeguarding that information
- Do not utilize a mobile device that has come into contact with patient data on an unsecured network
- Do not connect a mobile device to an unsecured computer or desktop
- Never leave your mobile device unattended

SecurityMetrics Guide

Workstation Use

HOW TO PROPERLY UTILIZE A COMPUTER

Proper Use

- Any company should have a workstation use policy and implement technical safeguards to enforce such a policy
- Work computers should not be allowed to visit social media sites due to security and productivity issues
- Work computers should have automatic logoff timers and screen savers in order to prevent unintentional information leak
  - This is actually a HIPAA requirement
- Public workstations should be monitored either via auditing, cameras or both
- Credit card terminals should be completely visible to the customer and if an employee needs to handle the credit card, such a transaction should take place entirely in front of the customer while also avoiding disclosure to other nearby individuals

Proper Use (cont.)

- Privacy screens should be implemented on computer screens to limit the viewing angle
- Passwords or protected health information placed on “Sticky Notes” must never be allowed and should be addressed within sanction provisions
- Employees should not be allowed to conduct personal transactions (banking, shopping, research, etc.) while on a company device or network
  - Providing a segmented network for such activities while at work is certainly a viable work-around if proper risk analysis and risk management procedures are taken into consideration
- Protected health information must not remain on an individual’s desk for longer than is necessary to complete the job
- Store all protected health information in locked drawers or cabinets
- Place paper shredder next to every waste basket and label the waste baskets so that it is obvious that protected health information must be shredded

Proper Use (cont.)

- Investigate procedures (discussed later) for properly discarding protected health information
  - Secure shredding companies
  - Electronic waste disposal companies
    - Such companies must provide you with serial numbers and certificates of safe disposal
- Discuss training regularly and provide open discussions at regular intervals
- Ensure blinds and office fixtures are in place and configured so that protected health information is not viewable from extraneous or inadvertent angles
- Do not discuss details regarding customers in front of them
- Scheduling should not take place within the lobby or waiting room
- The personal devices of employees must be considered in risk analysis and policies and procedures put in place to address privacy concerns
- Auditing and session recording features should be considered (discussed later) and implemented as necessary in accordance with HIPAA

Social Media

"LOOK, THAT DOG JUST WALKED OFF THE DECK AND FELL INTO THE SNOW"

The Danger of Social Media

- As everyone knows, social networks have their own “bag of worms” but in a medical environment social networks are the equivalent of opening Pandora’s box
- Inadvertent Disclosure of Information
  - Social media is all about sharing and protecting someone’s privacy is absolutely juxtaposed to this
- Spam
  - Spam is easy to create and share because of the very friendly nature of social media sites
- Phishing
  - May contain links to malicious websites or provide a download that contains a Trojan
- Social Engineering
  - Social engineering is about using pieces of known information in order to have a better chance at getting access to the desired information
  - For example, a fraudulent text message saying that your card could not be processed for your auto-payed telephone bill and would you mind re-entering it

https://www.trendmicro.com/vinfo/dk/security/news/cybercrime-and-digital-threats/linking-the-enterprise-to-social-media-security
https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering

But What About Marketing My Business?

- Social media can permit excellent marketing for your business
- Social media is simply another tool in our technology toolbox that has a lot of potential but must be carefully utilized to make sure privacy is still being upheld
- Suggestions:
  - Utilize an independent, non-healthcare related device to perform all social media operations
  - Create a separate, social media only email
  - Train employees on how to spot various types of scams that exist (phishing, spam, Trojans, malware, etc.)
  - Ensure that policies and procedures are in place to prevent disclosure of protected information+
  - Monitor your social media feed (or the equivalent) to ensure decency and appropriateness
  - Never utilize a device which has access to protected health information to perform social media operations

Email

THE TREE SAVER

A Word of Caution

- HIPAA does not specifically restrict the use of email in a covered entity
- The problem with email is not so much that it is used as much as it is extremely difficult to confirm that the email arrives without interception along the way
- Email disclaimers are not a solution
  - Protection and valid security practices must exist; a disclaimer just alerts an individual to the risks associated with using a particular form of communication
- Encryption must exist throughout the entire communication chain; from inception to destruction and while at rest
- Always assume that a consumer does not realize the dangers of sending health information through email
- Responding to an email sent (or any other form of communication) requires that you now protect such data from disclosure
  - Be careful what messages you respond to and be sure to comply with the guidelines of HIPAA and your company's own policies and procedures

SecurityMetrics Guide

Updates

"HELLO. WHEN WOULD YOU LIKE TO INSTALL YOUR UPDATE?"

Updates

- Updates are absolutely necessary for a properly functioning HIPAA compliance program
- Updates contain security patches in addition to feature updates and usability improvements
- A cycle should be established for updating devices on regular intervals in order to take advantage of the latest security improvements
- Depending upon the technology environment, Windows may automatically download and install updates
  - Windows can even be configured to do this for software and hardware that is not, strictly speaking, Windows
  - Macs can also be configured to update themselves automatically
  - Mobile device updates very but can generally be done from the device

Updates

Critical Update – is an update which fixes specific, non-security related, critical bug. That bug can cause for example serious performance degradation, interoperability malfunction or disturb application compatibility.

Security Updates – is an update which fixes security vulnerability. Security updates have their own severity defined by Microsoft Security Response Center. There are 5 levels of the security update severity defined by MSRC:

Critical - The update fixes a vulnerability whose exploitation could allow for the propagation of an Internet worm without user action.

Important - The update fixes a vulnerability whose exploitation could result in the compromise of the confidentiality, integrity, or availability of users' data, or of the integrity or availability of processing resources.

Low - The update fixes a vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

Moderate - The update fixes a vulnerability whose exploitation is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.

Unspecified - The update does not have a severity rating.

https://blogs.technet.microsoft.com/dubaisec/2016/01/28/windows-update-categories/

What Should Be Updated

- ❑ The Operating System of Computers
- ❑ Server Software
  - As applicable and after researching
- ❑ Internet Browsers and Plug-Ins
- ❑ Credit Card Processing Software
  - Do not forget about the terminal itself
    - This may require contacting your credit card provider
- ❑ Electronic Medical Record Software
- ❑ Routers and Access Points Firmware
- ❑ Mobile Devices
- ❑ Java Runtime Libraries

Security Reminders

"DISTRUST AND CAUTION ARE THE PARENTS OF SECURITY"

-BENJAMIN FRANKLIN

Remind, Remind, Remind

- All the best security in the world means nothing if the individuals using it are careless with information
- Setup routine security checks
- Perform random security checks on employees to confirm security standards, policies and procedures are being adhered to
- Organize routine meetings to discuss security with employees and listen to any concerns they may have
- Make training a priority and the rest will be natural

Some Unique Approaches

- During a routine security meeting setup some scenarios and discuss what is the proper way to handle the situation
  - People enjoy thinking through scenarios much more than listening to a list of “No, don’t to that”
- Place sticky notes with security principles in conspicuous areas around the facility
- Educate patients with one or two employees present
  - This way individuals think they are helping to educate rather than being the ones who need educated
- Reward safety and security through a prize system or similar approach
- Make safety and security part of your conversation
- Hire individuals who exhibit a strong conviction regarding privacy and security

Typical Safeguards

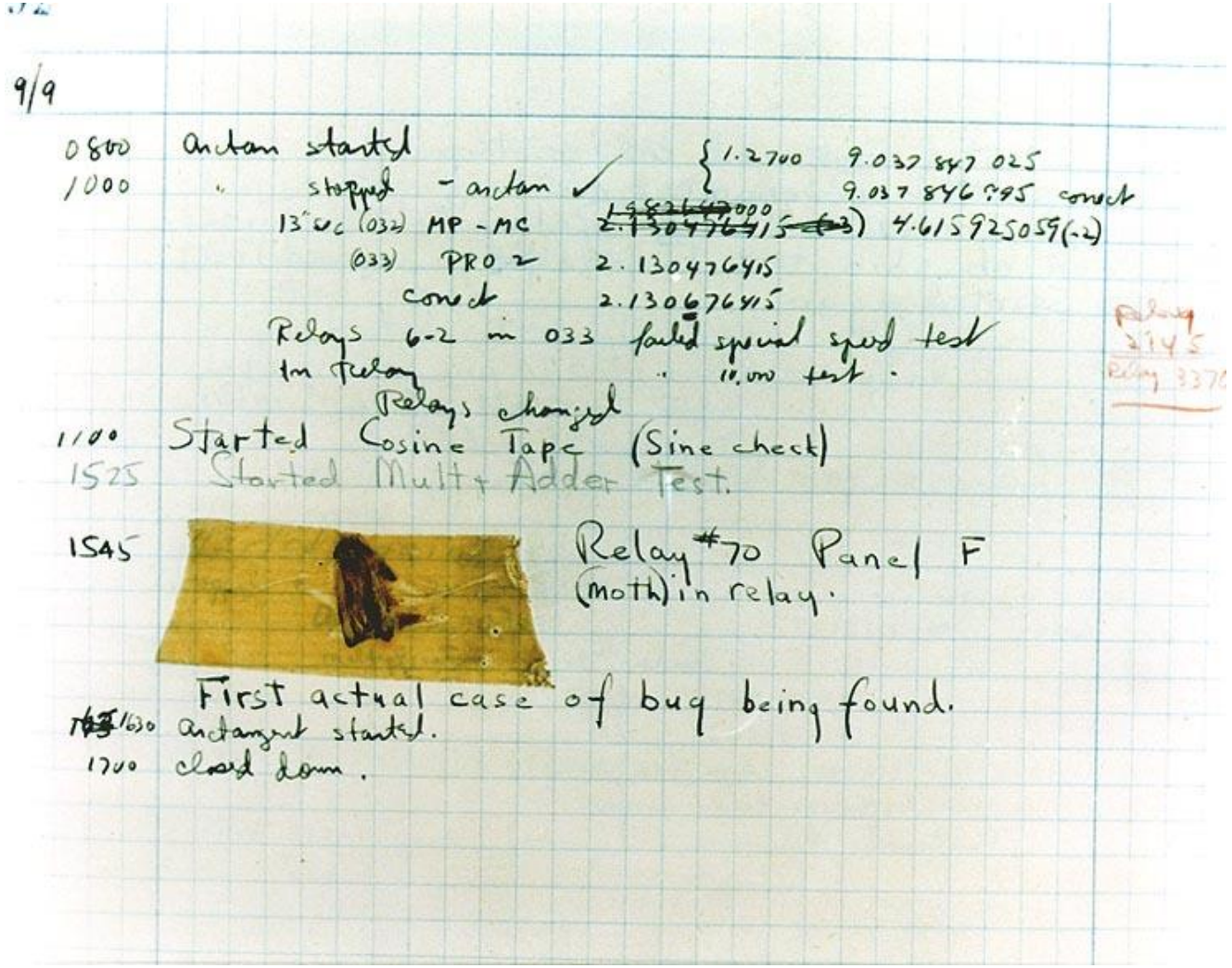
THE STANDARD TECHNOLOGY USED TO PROTECT DATA

Backup Systems

THE RECOVERY PART OF A RECOVERY PLAN

What is a backup?

- A backup is an easily retrievable copy of data that can be used to restore data to a known, former state should a data failure occur
- Data failure is a state where data is considered not useful because it has been deemed, in whole or in part, unusable
- Causes of Data Failure:
  - Power outages
  - Malicious Software
  - Corrupt Data
  - Erroneous Entries
  - Improper data handling
  - Software bugs
  - Hardware bugs



9/9

0800 Arctan started
1000 " stopped - arctan ✓ { 1.2700 9.037 847 025
9.037 846 995 correct
13 sc (032) MP - MC ~~1.9821642000~~ ~~2.13047641515 (-3)~~ 4.615925059(-2)
(033) PRO 2 2.13047641515
correct 2.13067641515
Relays 6-2 in 033 failed special speed test
In relay " 11.00 test.
Relays changed
1100 Started Cosine Tape (Sine check)
1525 Started Mult + Adder Test.
1545 Relay #70 Panel F
(moth) in relay.
First actual case of bug being found.
~~1700~~ 1630 Arctangent started.
1700 closed down.

Relay 2145
Relay 3370

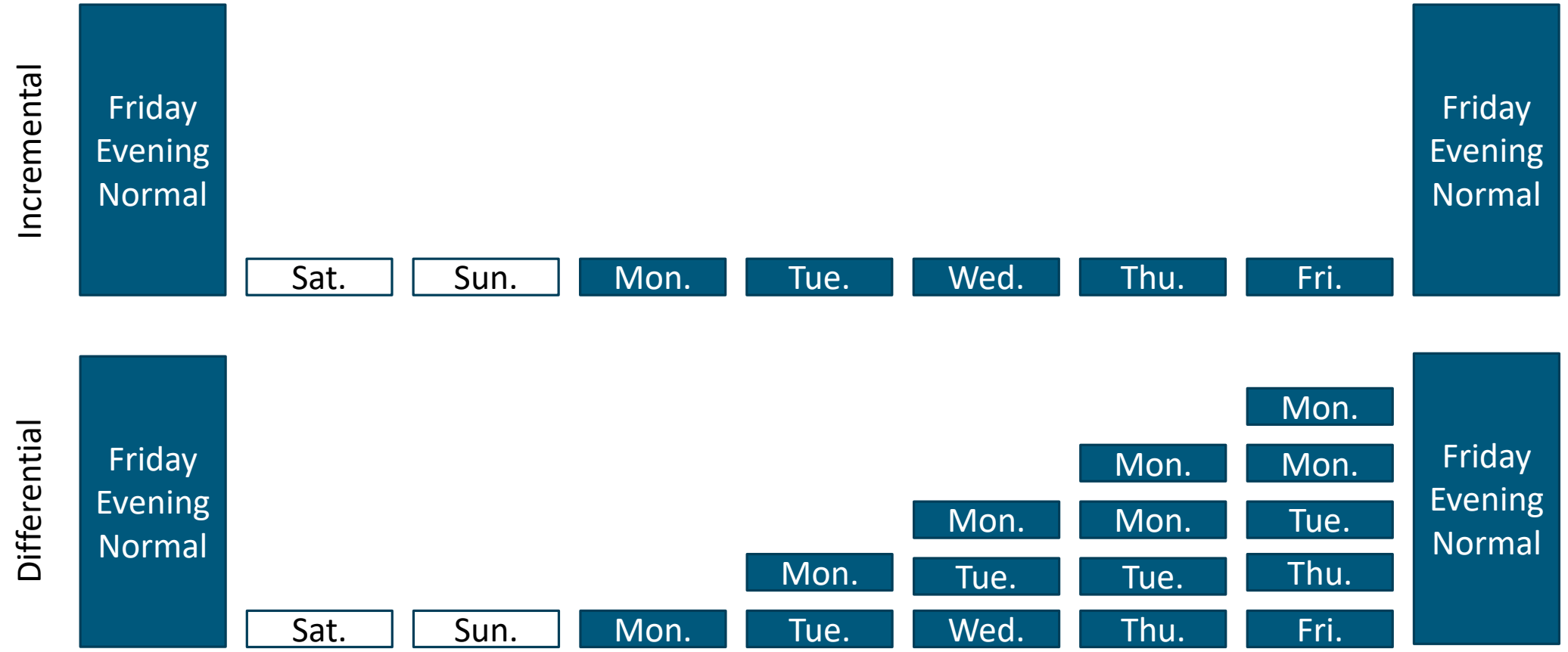
The “First” Computer Bug

Ways to Backup Data

- There are many ways to backup files
- Archival Bit: A bit in the file that indicates whether or not a good copy of the file exists on a backup
- The following are the three common ways of backing up files:
  - Full
    - Backs up everything in the backup set every time regardless of whether or not the file has changed
    - Wastes a ton of resources because typically not every file in the backup set changes
  - Incremental
    - Backups only those files that have changed and turns off the archive bit
    - Faster and uses less resources because only files that have been modified are changed
  - Differential
    - Backups only those files that have changed but it does not turn off the archival bit
    - Again, faster and uses less resources but also allows for full backups later on because the archival bit is not turned off
- It is health to have a combination of all three backups to decrease recovery time and increase data protection

CompTIA A+ Book

Differential versus Incremental



CompTIA A+ Book

Ways to Backup Data

- Continuous Backups
  - Also known as real-time backups
  - Continuously monitors files for changes and backs them up as changes occur
  - Now much more feasible due to higher Internet bandwidth; although throttling is still necessary for large files
- Exact Copy
  - Takes an exact copy of the data and stores it on the desired medium
  - Can be stored on flash drives, CDs, hard drives and more
- RAID
  - Stands for Redundant Array of Independent (or Inexpensive) Disks
  - Provides redundancy and performance improvements
  - Several varieties exist depending upon the desired characteristics

https://en.wikipedia.org/wiki/Continuous_data_protection
https://en.wikipedia.org/wiki/RAID

RAID

- RAID 0
  - Also known as Disk Striping because data is spread amongst several drives
  - Performance only, no redundancy
  - Requires two (2) drives
- RAID 1
  - Also known as Disk Mirroring or Duplexing
  - Redundancy
  - Requires at least two (2) drives
- RAID 2, 3 and 4
  - Unimportant RAID levels rarely used today
- RAID 5
  - Also known as Disk Striping with Distributed Parity
  - Requires at least three (3) drives
- RAID 6
  - Also known as Disk Striping with Extra Parity
  - Safer alternative to RAID 5 but requires more drives

CompTIA A+ Book

Backup Companies

- The following are HIPAA compliant (assuming one follows the appropriate business agreement requirements):
  - iDrive
  - Carbonite
    - https://www.carbonite.com/globalassets/files/datasheets/cep-hipaa-fs.pdf
  - Mozy (now owned by Carbonite)
    - https://mozy.com/hipaa
- Disclaimer: The companies listed above support HIPAA compliance at the time of writing. Certain HIPAA requirements may not be met out-of-the-box and one should always consult with an information technology specialist for additional details.

Backup Considerations

- Encryption, if available, should always be utilized
  - If it is not available, find a new backup software or program
  - Be sure to create a strong encryption key by following the password policies discussed earlier
- Backup pass-phrases that encrypt entire backup directories should be utilized
  - Again, be sure to create a strong encryption key by following the password policies discussed earlier
- Compressed backups are possible, however, due to the relatively cheap cost of disks, are not as necessary as before and increase restore time (leading to longer downtime)
- Backups can occur either in software or hardware depending upon the environment

https://www.veritas.com/support/en_US/article.TECH34346

Recommended Backup Strategies

- Backups should be performed locally and remotely to ensure proper recovery in case of data failure
- Backups should be kept onsite for easy restoration in case of data failure
  - Critical systems should be backed up in such a way that restoration is quick after a data failure
- Critical systems should be backed up continuously, if possible
  - Additionally, RAID 1 (at the minimum) should be utilized for critical systems so that a redundant, exact copy version exists of critical data and can be restored should a drive failure occur
- In other words, a combination of backups and RAID should be used
- Backups should also take place remotely so that if something happens locally data can still be restored
- "As a general rule, the amount of time in between backups should be no more than the amount of time you are willing to spend re-doing any lost work. For example, if spending a week re-writing lost documents is too long for you, you should back up at least once per week.[1]"

[1] https://help.gnome.org/users/gnome-help/stable/backup-frequency.html.en

Anti-Virus Software

PROTECTING AGAINST VIRUSES

Defending Your Computer

- Antivirus is a computer program that actively protects a computer from malicious computer viruses
- Antivirus achieves this by scanning the system contents (files) against a set of known virus signatures in it's database
  - This threat database is updated continually as new threats emerge
- Antivirus also scans files in the background as they are used by a user or as they are downloaded from the Internet
  - This provides real-time protection
- Typical antivirus programs use rules and heuristics to detect threats
- A common trend nowadays is to use the power of Machine Learning to detect threats and create the threat signatures

https://en.wikipedia.org/wiki/Antivirus_software

What You Need?

- Any computer, including Macs, need to have antivirus software in order to protect them from the latest threats
  - Any computer means a computer that runs Windows, Macs and Linux/Unix
- Typically, you can find antivirus software that has antivirus and a software firewall (discussed later) together
- A web shield – a service which scans websites and reports their reputation – is also critical to identifying malicious websites (which could also produce malicious software)
  - A web shield is somewhat like a first line of defense
- No software is 100% successful at detecting viruses because viruses can morph and change their signatures, nevertheless, antivirus based on heuristics and machine learning go a long way towards building a strong defense
- Central management for a large number of computers is critical for effective management

What You Need? (cont.)

- Website Antivirus
  - Protects a website from malware attacks
    - Software firewalls may also exist
  - Not an end-all solution since good software is also a necessity to prevent attacks
  - Examples include Google (accessible to website owners through Google Webmasters), ClamAV and SiteGuarding.com
- Desktop/Computer Antivirus
  - Protects a computer from a variety of threats including spyware, malware, Trojans, worms, etc.
  - Usually include software firewalls as well
  - Typically include a suite of features to help protect devices in unique situations
  - Examples include Norton, McAfee, Webroot, Avast and Kaspersky
- Mobile Antivirus
  - Mobile devices are inherently different than traditional computers and therefore present a unique security challenge
  - Mobile applications are typically run in what is called a *sandbox* and therefore have restricted access to system resources
  - Security provided is somewhat different than that of desktop antivirus because of the nature of mobile devices
  - Examples include McAfee, Avira Mobile Security, and Avast

Firewall

ONE OF THE MOST CRITICAL PIECES IN CYBERSECURITY

Firewalls

- A firewall is an application or an entire computer (e.g., an Internet gateway server) that controls access to the network and monitors the flow of network traffic. A firewall can screen and keep out unwanted network traffic and ward off outside intrusion into a private network. This is particularly important when a local network connects to the Internet. Firewalls have become critical applications as use of the Internet has increased.[1]
- Named after the walls and design principles used to protect buildings from having fire spread
  - In this case, a technology firewall limits the spread of malicious attacks to a private network
- There are two general types of firewalls:
  - Software
    - Typically integrated with antivirus software
    - Examples include Norton, Kaspersky, Windows Defender and Webroot
    - The most prevalent variety because of the low entry cost
  - Hardware
    - A physical device that protects
    - May be implemented and integrated on a router
    - Examples include Cisco, Netgear and Fortinet
    - Higher investment cost and much more complicated to configure

[1] https://www.gartner.com/it-glossary/firewall

But Both Varieties are Important!

- All firewalls attempt to prevent unwanted traffic from entering a private network
- It is true that hardware firewalls are more difficult to configure, but they are nonetheless critical to a proper cybersecurity policy
- Software firewalls run locally on a particular computer or device and monitor the traffic coming into and out of that particular device
- A hardware firewall performs a similar function but does so externally from any one device
- Hardware firewalls are incredibly powerful because they are not running on top of other software but instead are built to provide a particular service
- Software and hardware firewalls can be incredibly difficult to setup properly but are absolutely vital to a proper security policy
  - Seek professional help where necessary…a non-working firewall is just as bad as no firewall

Uninterrupted Power Supply (UPS)

A CRITICAL COMPONENT TO DEFENDING AGAINST POWER FAILURES

Uninterrupted Power Supply (UPS)

- An Uninterrupted Power Supply (UPS) is critical in protecting against power failures
- An UPS works just like a power surge protector except that when a power failure occurs (because of brownout, power grid failure or natural disaster) a battery backup kicks in and becomes the source of power
- The time an UPS can maintain uninterrupted power varies based upon the model and load
- Best practice is to use an UPS at each workstation in order to maintain system performance throughout a power failure
  - Only connect the critical pieces of hardware to the UPS; a welcome sign is not as vital as the credit card reader in the case of a power failure
- A larger UPS should also be present in the technology closet and have only the core technology components connected
- Even if the UPS does not last throughout the entirety of the downtime, it will at least provide an individual with the ability to properly shutdown equipment

Wireless Networks

PROVIDING FREEDOM TO CONNECT WITHOUT ETHERNET

Wireless Access

- Wireless access is incredibly powerful and provides access to network resources without having to be physically tethered to the network
- Wireless access includes (but is not limited to) wireless internet (WiFi), Bluetooth communication, ZigBee and cellular communications
- We will focus our attention on wireless network access but, generally speaking, the same procedures and precautions apply to any wireless network

KRACK

- KRACK is a **K**ey **R**einstallation **A**tt**ack** whereby the attacker causes the victim to re-use a key and therefore the attacker is able to decrypt the communication
- When a computer attempts to connect to a wireless network, a 4-way handshake is used to establish the key that should be used to protect the privacy of the communication
- It is during message 3 of the 4-way handshake that an attacker can cause key reuse and thereby cause the client to reuse the same key
- This reuse of key would not have been detrimental except that it also causes the nonce to be reset
  - A nonce is a number that may only be used once
- Resetting the nonce is where the trouble comes because once the nonce is reset the encryption method used to encrypt the data becomes susceptible to attack (WiFi uses a stream cipher which is susceptible to attack with nonce reuse)
- WPA2 is provably secure (through mathematics) but such a proof did not consider key reuse
- Android 6.0 (and higher) and Linux are particularly vulnerable because they can be more easily manipulated to provide an all-zero encryption key
- An attacker must be within range of the network and thus this attack cannot take place across geographical boundaries

https://blog.cryptographyengineering.com/2017/10/16/falling-through-the-kracks/
https://www.krackattacks.com/

KRACK Takeaways

- Select vendors notified on July 14, 2017
- Major notification on August 28, 2017
- Changing a router's WiFi password does not prevent or discourage the attack because KRACK does not attempt to use or collect the WiFi password
- The attack, contrary to popular media hype, requires certain networking features not typically found in home networks
  - Nevertheless, certain companies, after researching have discovered other vulnerabilities
- Update your router with the latest firmware
- Update any client devices as well
  - KRACK affects both the access point and the client devices

https://www.krackattacks.com/

Properly Securing your Wireless Network

- Change all default administration login credentials as these are readily known
- Change the default SSID to something else
- Only utilize the WPA2 (Wi-Fi Protected Access 2) security protocol when setting up your wireless networks
  - WPA2 is now the only recognized standard
- AES (Advanced Encryption Standard) should be used for encryption; TKIP is outdated
- Never use WEP (Wired Equivalent Privacy)
- Use strong router passwords (as detailed previously)
- Broadcasting or not broadcasting the network name (SSID) is irrelevant; anyone who wants to access your network maliciously already knows how to find it
- Limit access to the network for only office devices
  - Never allow guests on the same business network
  - It is recommended to have an entirely separate network for employee devices as well

Properly Securing your Wireless Network (cont.)

- Be sure to update router and network firmware routinely
- Be sure all Internet of Things (IoT) devices are capable of handling information securely and in accordance with best policies
- Wireless routers should not be placed near windows or areas within easy reach
- Consider turning off wireless network capabilities when you are not present
  - Physical security is always the best
- Changing the default IP address also increases security because you are using one that is less common
- Always disable remote access
- Turning off DHCP may also be beneficial depending upon the network setup as this requires manually entering all devices that connect to your network

https://heimdalsecurity.com/blog/home-wireless-network-security/

Remote Access

HOW TO PROPERLY ACCESS YOUR NETWORK WHILE AWAY

Virtual Private Network (VPN)

- A Virtual Private Network (VPN) allows remote users to login to a network as if they were physically present
- A fundamental quality of a VPN is that allows secure communication over non-secure channels
- This allows for secure access to network resources while remote and potentially unsecure
- A VPN does this by encrypting communications at the packet level
  - This poses troublesome for firewalls because now a firewall cannot tell if the packet is malicious
- VPNs usually need to be coordinated with firewalls in order to work properly
- Examples include logging into your office in order to access the x-ray server, using a VPN to connect to a University's network or using VPNs to allow mobile scheduling
- It is important to remember that proper security must be present on both the host and the client since VPNs are not an end-all solution

https://technet.microsoft.com/pt-pt/library/cc779919(v=ws.10).aspx

Remote Desktop Access

- Remote desktop access provides you with access to a desktop as if you were physically there
- Thus, with a remote desktop application you can use another PC and its applications as if you were physical present
  - This is beneficial because it allows you to use the software and hardware already present without having to install it on your local machine
- It is important to remember that HIPAA still applies and proper standards and regulations must be followed if one decides to use remote desktop access
- Anyone deciding to use a remote desktop application should always enable additional authentication measures to ensure proper authorization prior to giving access
- Examples include LogMeIn, Splashtop and RemotePC

Software

THE PROGRAMS AND OTHER OPERATING INFORMATION USED BY A COMPUTER

– GOOGLE DICTIONARY

Best Practices

- Always use reputable companies and research software prior to installation and use
  - You may have to hire a professional if you are unable to determine all the details
- Be very careful when downloading software to:
  - Ensure that you are downloading from a reputable company
  - SSL is used for payment and information transfers
  - Read reviews about the software
- Be very careful with free or open-source software
  - Free and open-source software are tremendously powerful but need to checked and vetted before being installed
- Consider using checksums to confirm file integrity
- Software should be routinely updated
  - Major security holes are fixed in software updates

Advanced Safeguards

STILL NECESSARY, BUT MORE ADVANCED

Emergency/Disaster Plans and Recovery

PLANNING FOR THE INEVITABLE

Why You Should Have Disaster Plan

- Businesses large and small create and manage large volumes of electronic information or data. Much of that data is important. Some data is vital to the survival and continued operation of the business. The impact of data loss or corruption from hardware failure, human error, hacking or malware could be significant. A plan for data backup and restoration of electronic information is essential.[1]
- Disasters can come at any time and with very little warning
- Consider, for example the damage caused by hurricane Harvey in 2017 or the more recent lava flows in Hawaii
  - In all of these events, any business (or even person) that was affected may have suffered data loss if proper precautions were put in place
  - Even if proper precautions were in place, a plan is necessary to restore a business to functioning order after such an event
- Enter, the emergency/disaster plan

[1] https://www.ready.gov/business/implementation/IT

Managing Disasters

- It is important to have emergency/disaster plans in place so that when a disaster strikes you will not be trying to *figure out what to do*, but instead can focus on *implementing your plan*
- Not only is having an emergency/disaster plan a good idea, it is also required by HIPAA
- An emergency/disaster plan must prioritize the order of recovery in order to align with the business' continuity plan
  - Top priorities should be chosen such that the effects to consumers are as limited as possible
  - Top priorities would always be (in no particular order) ensuring safety and health, securing the premises, gaining access to utilities, re-installation of technology equipment and/or testing procedures, access to critical software and temporary access solutions
- Additionally, an emergency/disaster plan should specify what is currently being done to limit or mitigate the effects of a disaster
  - Examples include uninterrupted power supplies, secondary Internet providers, duplicate telephone lines, etc.

https://www.ready.gov/business/implementation/IT

Designing a Basic Recovery Plan

- A basic emergency/disaster plan can be developed as follows:
- Identify all hardware and software
  - This includes desktops, laptops, servers, access points, modems, security cameras, hard drive storage bays, firewalls, telephones, backup locations, software programs, etc.
- Organize the hardware and software from most relevant and critical to daily operation to unimportant and rarely used
- Note which of the hardware and software is standardized (i.e. can be repurchased or redownloaded easily)
  - For the hardware and software which is not standardized, elaborate on how recovery should proceed
- Finally, note which pieces of hardware and software should be backed up
  - Yes, hardware can be backed up by keeping an extra (or two) around in case of failure
- Congratulations, this listing is the prioritization of tasks in a disaster recovery scenario and can serve as a basic recovery plan

https://www.ready.gov/business/implementation/IT

Audit Controls

AUDITS AREN'T JUST FOR CPAS

What is An Audit Control?

- Audit Entry
  - The fundamental unit of a record that details the who, what, where, when and how of all monitored activities
- Audit Record
  - A collection of audit entries, ordered by time, which provide a historical accounting of the monitored activities
- Audit Trail
  - Audit trails are the manual or electronic records that chronologically catalog events or procedures to provide support documentation and history that is used to authenticate security and operational actions, or mitigate challenges. Numerous industries use versions of an audit trail to provide a historical record of progression based on a sequence of events. These records provide proof of compliance and operational integrity. Audit trails can also identify areas of non-compliance by providing information for audit investigations. Whether it is logging the design changes of a product build, keeping the record of financial transactions for an e-commerce site, communication transactions, healthcare activity, or legitimizing the outcome of an election, an audit trail validates actions and outcomes. Audit trail records will contain details that include date, time, and user information associated with the transaction.[1]
- Audit Control
  - A mechanism that is used to produce audit entries for all monitored activities

[1] https://www.smartsheet.com/audit-trails-and-logs

What Is Necessary?

- Auditing
  - an official inspection of an individual's or organization's accounts, typically by an independent body[1]
- Thus, when deciding what is necessary we must ensure that we are maintaining enough documentation to prove the details
- An entry should be basic but provide the who, what, where, when and how
  - Keep the message as small as meaningful to ensure storage does not become an issue early on
- Implement an audit control for all systems which have access to electronic protected health information
- System logs should be backed up routinely, just as one would critical data

[1] Google Dictionary
https://www.smartsheet.com/audit-trails-and-logs

Implementation Details

- So, if you are like most people the previous slide sounds really good but extremely vague
- Let's discuss implementation details
- Maintain a list of all hardware and software which has access to electronic protected health information
  - You already should have this from your risk analysis
- Determine how many of these products already have logging and audit controls built in
  - You will be surprised by the number of products that already include audit/logging capabilities; it is very common in software
  - For those that do not have logging capabilities built-in, one must immediately stop using them if they are used with electronic protected health information
  - Ensure logs are detailed enough to provide back-tracking capabilities
  - Also, be sure to document which ones have logging capabilities
- Ensure that all logs are backed up
- Define a log retention time
  - Forever is the best but may be unpractical depending upon situation
- Establish procedures for regular review of logs

File Integrity Monitoring

INTEGRITY IS THE ESSENCE OF EVERYTHING SUCCESSFUL

-R. BUCKMINSTER FULLER

Monitoring Files for Discrepancies

- File integrity monitoring (FIM) is an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and a known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.[1]
- Integrity of data is very important because decisions may be made based upon that data
- Services can be purchased which will allow for file integrity monitoring

https://en.wikipedia.org/wiki/File_integrity_monitoring

Network Intrusion Detection Systems (NIDS)

Network Intrusion Detection Systems

- A network intrusion detection system (NIDS) listens to network and logs and alerts analyst of threats to a target application[1] or computer[1]
  - A passive component
- A NIDS is a passive device and cannot be used for prevention but instead is used for monitoring the state of a network in such
  - Still useful as sometimes the best we can do is simply monitor when an intrusion occurs
- In intrusion prevention system (IPS) is similar to a NIDS but can actively defend a network as it can block[2] or prevent threats[2]

[1] https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids
[2] *Computer Security, Principles and Practice, 3rd Edition* by W. Stallings and L. Brown, 2015, Pearson

Vulnerability Scanning and Penetration Testing

Vulnerability and Penetration Testing

- Vulnerability Testing
  - Scan a system (either automated or manually) for vulnerabilities
  - Technical resources may be consulted to identify issues
  - Mitigations may be presented as part of the analysis
  - Mitigations and vulnerability testing re-ran to confirm successfully mitigation of the threat

- Penetration Testing
  - Similar to vulnerability testing as it searches for weaknesses but in penetration testing the vulnerability is actively exploited
  - Essentially, it is attempting to break into your own system to discover exploitable weaknesses
  - Also known as ethical hacking
  - The information discovered from the penetration test is provided to the information technology staff in order to build mitigations to such weaknesses

https://www.indusface.com/blog/what-is-vulnerability-testing/
https://www.secureworks.com/blog/vulnerability-scanning-vs-penetration-testing

https://searchsecurity.techtarget.com/definition/penetration-testing
https://www.secureworks.com/blog/vulnerability-scanning-vs-penetration-testing

Media Destruction

HOW TO PROPERLY DESTROY DATA

Media Destruction

- "the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored…"[1]
- Protected Health Information cannot be disposed off as tradition trash
- Electronic media on which sensitive data was stored may not be transferred for non-HIPAA purposes without properly destroying the data on the media
- HHS.gov recommends the following:
  - Traditional Paper Records: shredding, burning, pulverizing or pulping records such that they are rendered unreadable/unusable
  - Electronic Media: use software to overwrite hardware where sensitive data was stored, using magnetic fields to destroy media, or physically destroying the hardware

[1] https://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html

Media Destruction (cont.)

- SSDs cannot be properly destroyed using strong magnetic fields
  - You should overwrite the SSDs (typically a zero or one fill) and then have the SSD physically shredded with a certificate of destruction
- Cell phones and similar hand-held devices have memory that is similar to SSDs and therefore caution should be taken before re-using such devices for non-HIPAA purposes
- Procedures should also be implemented for the storage of media when not required anymore but not yet destroyed
- Online, it is much harder to ensure that all data has been deleted due to the nature of the Internet
  - Where possible, when closing a no longer needed account associated with electronic protected health information follow the company's procedures for removing and deleting your account

Goal

- It is my goal that this lecture provides:
  - An understanding of the various types of technology safeguards
  - The purpose of each technology safeguard
  - How such a safeguard protects the privacy of information
  - The best practices associated with the various safeguards
  - And finally, practical and implementable tips to get started
- I understand that each person's propensity towards technology is different and therefore provided the basic details necessary to understand the technology
- It was my desire to provide "just the right amount" of detail; enough to provide you a working knowledge as you consult with a technology professional or the details necessary to start you on your own research

Main Takeaways

- Technical safeguards are a must for assuring the privacy of data
  - Similar to how you would not go on vacation and leave your door unlocked, you should not take sensitive data and assume no one will want it
- Sorting through the myriad of technical safeguards can be daunting, but it is my hope that this lecture provides some basic details in order to help you know what you need and what you should consider
- It is important to remember that security is foundational; start small and work on improving
- Technical safeguards are not an end-all solution; it is important to have proper physical security as well as administrative safeguards