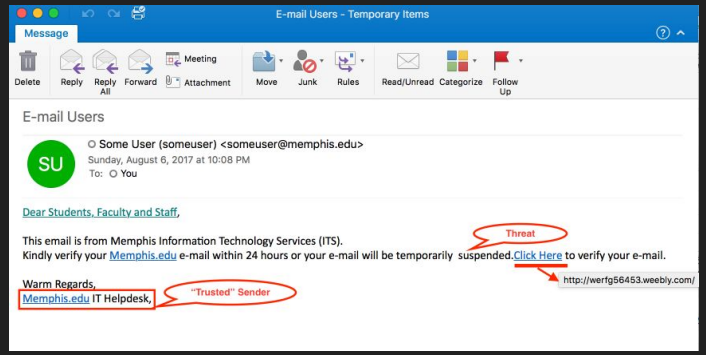
Cybersecurity Threat Analysis and Recommendations in the Healthcare System

By:
Thamarat Singcharoenchai, Jeremy Convocar, and Aileen Ni

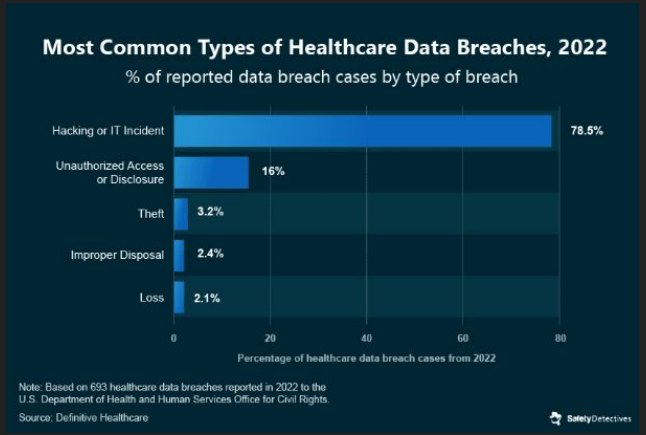
Current State of Cyber Threats

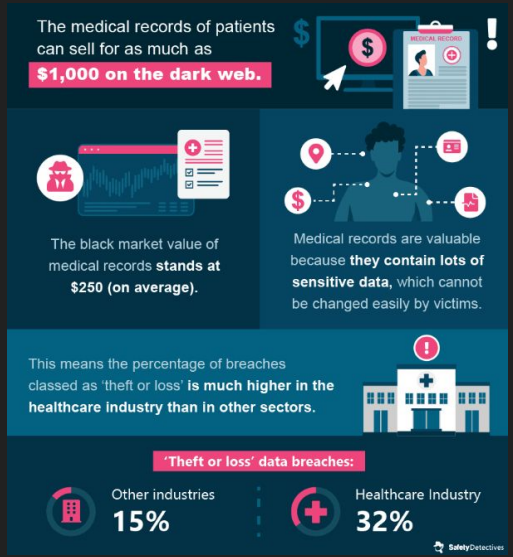
- **Phishing** - Contacting by someone posing a legitimate institution as an attempt to lure the target into clicking a malicious link or providing sensitive information
- **Ransomware** - Malicious software injected into the target's electronic device, and blocks access until a ransom is paid.
- **Insider Threats** - Individual who has access to authorized company data and uses them in malicious ways
- **Distributed Denial-of-Service (DDoS) Attacks** - Large internet traffic,to a site, by fake connections, forcing the availability of the service to shut down and denying access to legitimate users
- **Advanced Persistent Threats (APTs)** - Undetected cyber attacks designed to steal sensitive data
- **Man in the Middle attack** - Person between two communicating parties and intercepting with traffic



Cyber attacks in the HealthCare System

- Healthcare has been one of the primary focus of cyber threats
  - Sensitive information
    - Identity theft
    - Information can be used to target individuals with scams or frauds
  - Security vulnerabilities
    - Financial cost to investing in security
    - Inadequate Employee training
- 45% of healthcare organizations experienced a data breach
- Anthem Data Breach: [Case Study]
  - Affected around 78.8 million people
  - Phishing attack targeted an employee with malicious content and installed malicious software





Impacts

→ Financial

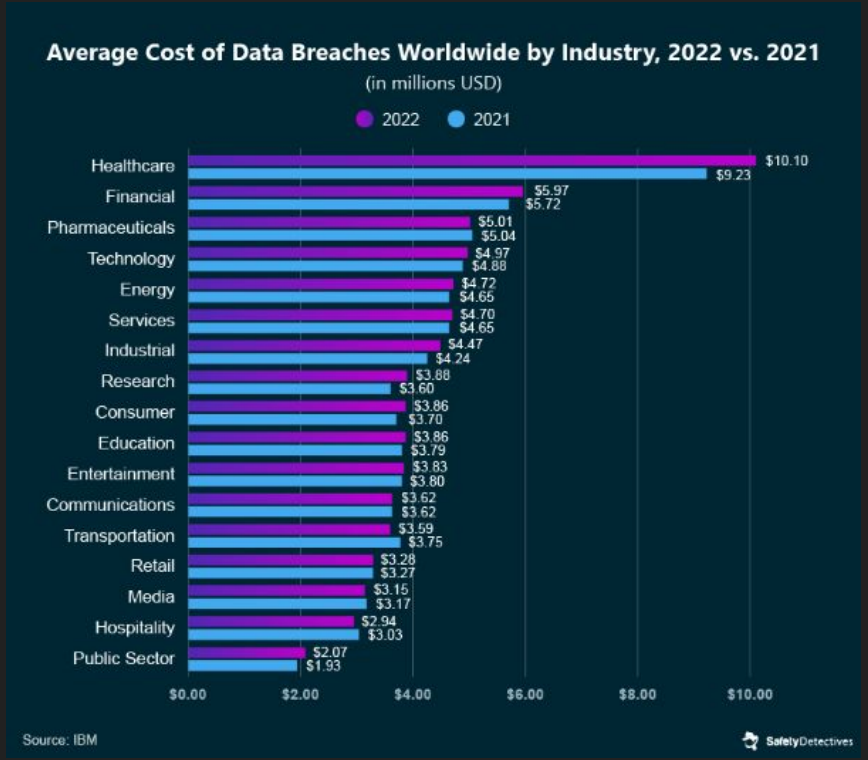
- Cost companies a large sum to fix the issue, pay damage to affected individuals
  - Anthem: Incident cost up to $260 million
    - Notifying public, offer condolence to affected individuals, enhance cyber security measures

→ Organizational

- Impacts on reputation and customer trust, affecting company business
  - Anthem: Received criticisms on not properly imposing security measures, such as failing to keep it's record held in its data warehouse
  - Faced numerous lawsuits regarding the incident

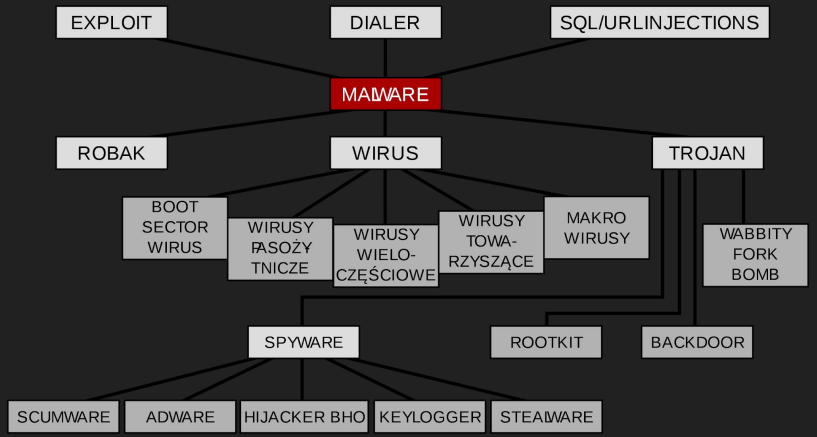
→ Personal

- Impact on individuals whose data is leaked. May cause damage to mental health and finances



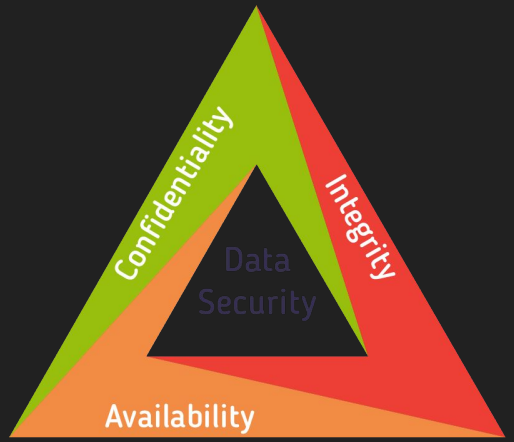
Modes of Attack

- Malware and Exploits
  - Malicious software like viruses, worms, and trojans infect systems, while exploits take advantage of software vulnerabilities to gain unauthorized access or escalate privileges.
- Web Application Attacks
  - Attackers target web-based applications used in healthcare, such as patient portals and EHRs, through techniques like SQL injection and cross-site scripting.
- Cloud and Remote Access Vulnerabilities
  - As healthcare adopts cloud services and remote access solutions, insecure configurations, protocols, or vulnerabilities in these technologies can be exploited.
- Internet of Things (IoT) and Medical Device Attacks
  - IoT devices and medical equipment with limited security controls are increasingly targeted by cyber attackers.



Security Measures

- Firewalls
- Data Protection and Encryption
- IDS and IPS
- Employee Awareness and Training
- The Health Sector Cybersecurity Framework Implementation Process
- HIPAA
- Key Ideas of Security

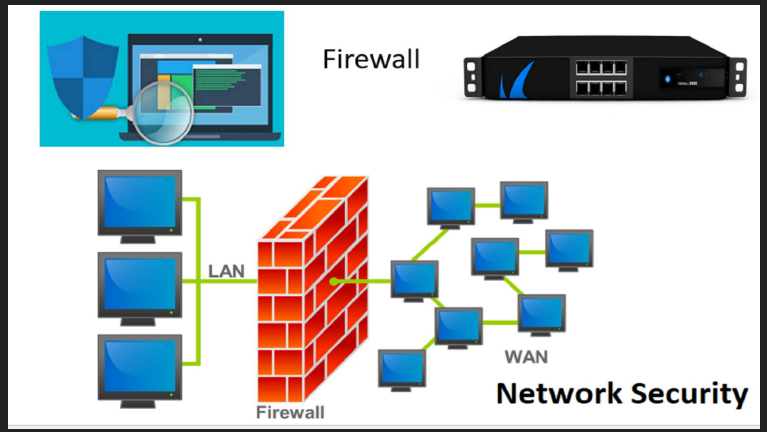


Firewalls

Security barrier between the internal network (LAN- Local Area Network) and the internet (WAN- Wide Area Network).

Blocks incoming and outgoing traffic based on predefined rules

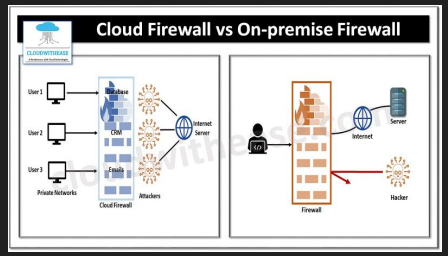
Convenient platform for non-security related platforms like NAT [Network address translation]

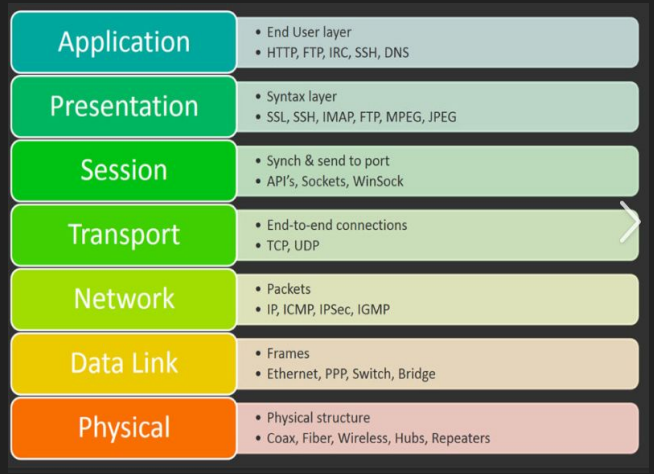


Limitations

- Vulnerable to internal threats
- Cannot prevent attacks bypassing firewall [IP spoofing]

Implementing a Firewall

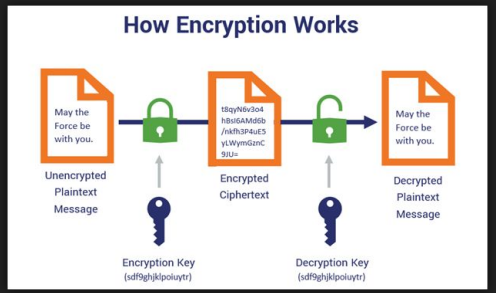


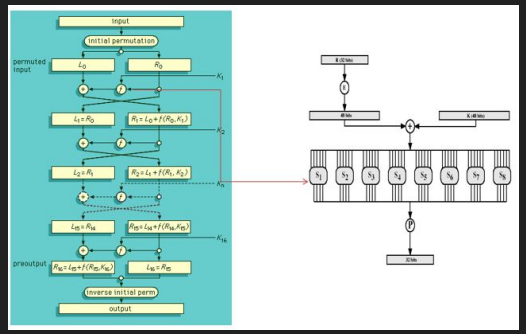


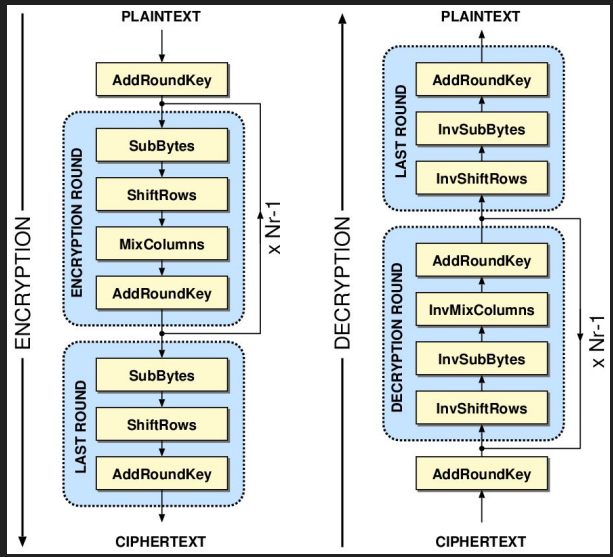
Generation	Firewall	OSI Layer	Pros	Cons
Cloud Firewall	Virtual Firewall	Layer 2	Applicable transversally on cloud platforms. Provides protection on a broader range of machines.	Implementation constraints in WAN networks using Wi-Fi devices/software-based technology Extra design charges required to avoid network exposure.
	Next-Gen. Firewall	Layer 2-7	Wider protection at OSI layer, compatibility with Intrusion Detection System (IDS)/Intrusion Prevention System (IPS), Access Control List capabilities, advanced threat intelligence.	Too much complexity and high investments required. Some functionalities are not intended to standard network environments (cloud and not cloud).
	Web Application Firewall	Layer 2, 7	Very specific solution against major malicious attacks at application level with adaptation capabilities for the target layer. Encryption and SSL force mode to establish secure connections.	Advanced troubleshooting skills required to avoid false positive patterns.
Traditional Firewall	Packet Filtering	Layer 3	Easy to configure. Good packet processing efficiency.	Impossible to protect the entire network. Risk of attacks for misleading firewall configuration. Not able to filter at application layer.
	Stateful Inspection	Layer 5	Able to manage multi packets and fewer open ports. Efficient management of threats and ability in blocking attacks, especially DDoS attacks, data packets memory.	High degree of skills to configure it Risk of network issue if not periodically maintained. Not effective in stateless protocols.
	Application proxy	Layer 7	Able to "proxy" the network with a man-in-the-middle behavior. Deep packet inspection. Able to translate addresses, a comprehensive firewall system in tandem with Network Address Translation (NAT) and IDS/IPS.	Risk of network bottlenecks if not periodically maintained

Data Protection and Encryption

- ➔ Using a known algorithm and a key to scramble the plaintext to a ciphertext.
  - Symmetric Encryption
    - Advanced Encryption Standard (AES) [2000]
      - Faster and more powerful than DES, Data Encryption Standard
        - 128/192/256 bit key
  - Asymmetric Encryption
    - Secure online communication, digital certificates
    - Exchange protocol for AES
  - Hashing
  - **Confidentiality, Integrity, Non-repudiation**







IDS [Intrusion Detection System]

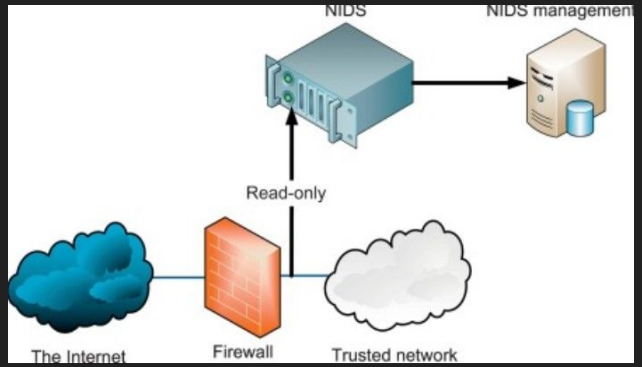
Detects malicious activity and generates an alert to the administrator.

Network Based IDS

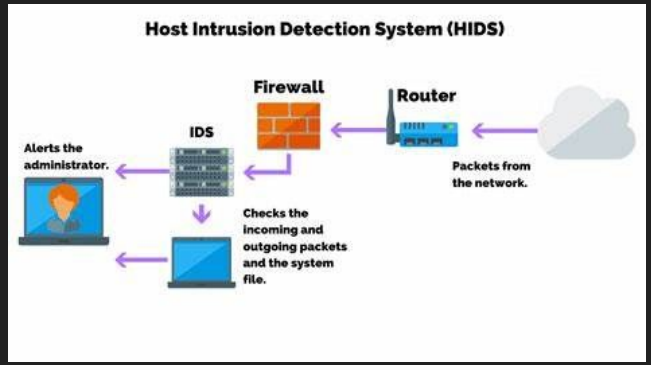
- Monitors Network traffic
  - Data packets, ISP

Host Based IDS

- Monitors activities on individual hosts
  - Data centers, endpoints



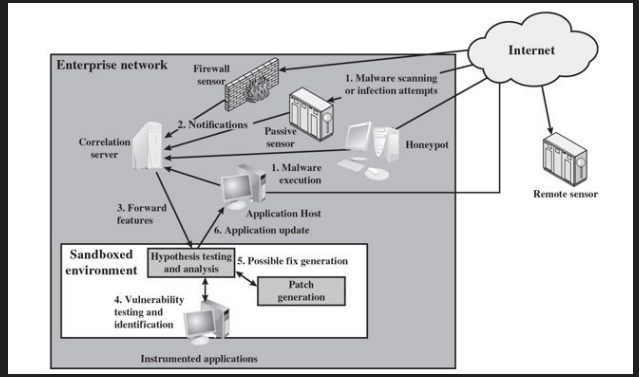
Monitoring network traffic	Protecting individual hosts
Deployed at a strategic point in the network	Gathering data directly from the host's OS
Centralises monitoring	Resource intensive
Effective against attacks that target multiple hosts	Detailed visibility into host specific activity
Overwhelmed by high network traffic	Cannot detect network wide threats



IPS [Intrusion Prevention System]

Intrusion Detection and Prevention System

- Capability to attempt to block or prevent malicious activity
  - Signature: patterns that have been identified as malicious
  - Anomaly: behavior patterns that indicates malware



Network Based IPS

Modify, discard packets, teardown TCP connections

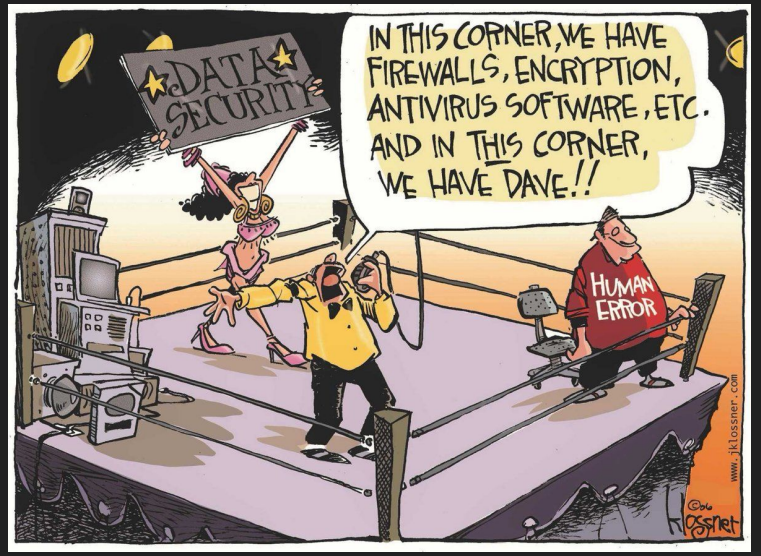
Host Based IPS

System calls, File system access, Host input/output

Employee Awareness and Training

Awareness Training [IMPORTANT]

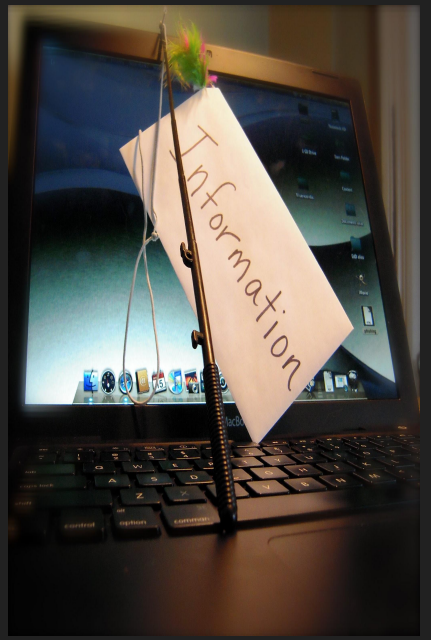
➔ Cybersecurity safeguards, firewalls and tech can only go so far if the people running it and within your organization aren't also properly trained!



Spotting a Phishing Scam

Ask Yourself any of the following when sent any sort of email, text message or online message, be it within your job or life:

1. Is this message asking me to input or give sensitive information or credentials?
2. Is this the first message you have received from this specific sender?
3. Does their number, email address, or username match with an official organization? (or have a mismatched email domain)
4. Does the sender use unfamiliar language or greetings than they would normally use?
5. Is there generally bad grammar or spelling within the message?



If you answer yes to any of these, hesitate and think twice before giving the sender any confidential information or access.

Good Password Habits and Myths

Myth: You should change your passwords every year or two.

Fact: The frequency in which you change your password is dependent on how strong it is, how often your account is used, etc.

- Nowadays, numbers such as every 30, 60 or 90 days are being thrown around by experts.
- Best practices are to change your password after any of the following:
  - After a Security Breach that affects one or more services you use/work for.
  - Email alert of an unauthorized access you do not remember
  - If it does not meet the password requirements of certain sites
  - If you have given password access to somebody else temporarily.

Good Password Habits and Myths (Continued)

Myth: Password complexity is more important than password length.

Fact: password length makes password harder to crack as opposed to diversity of characters, as each additional character adds exponentially more possibilities.

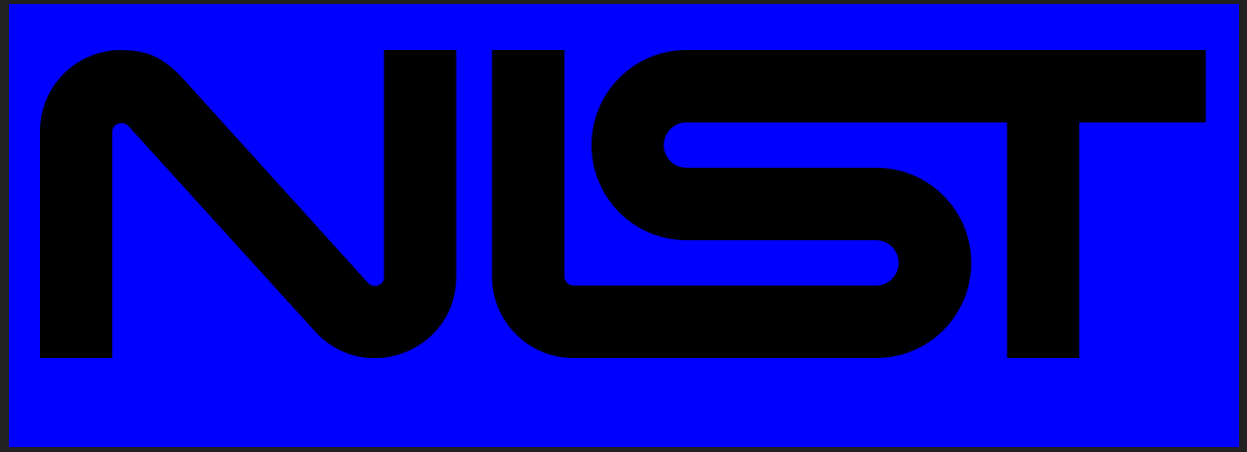
- A 12 character password takes 62 trillion times longer to crack than a 6 character password.
- Ideally, you would have both complexity and length.

Weak Password	OK Password	Strong Password
rose	rosemary1033	Rosemary1033@-@
isum	isumsoft$$	iSumsoft100$$*-*
jellyfish	jelly22fish	Jelly22fi$h
blackberry	blackberry:D	bLackberry:D
alibaba	alibaba666	Alibaba&mayu666+
eby123	eby7slow	Eby7slow:p

NIST Password Recommendations

The National Institute of Standards and Technology (NIST) actually has a guideline released every few years on good password habits.

- Always have Single Sign-On (SSO) and Multi-Factor Authentication (MFA) enabled.
- MFA options include:
  - SMS verification
  - Authentication app
  - biometrics

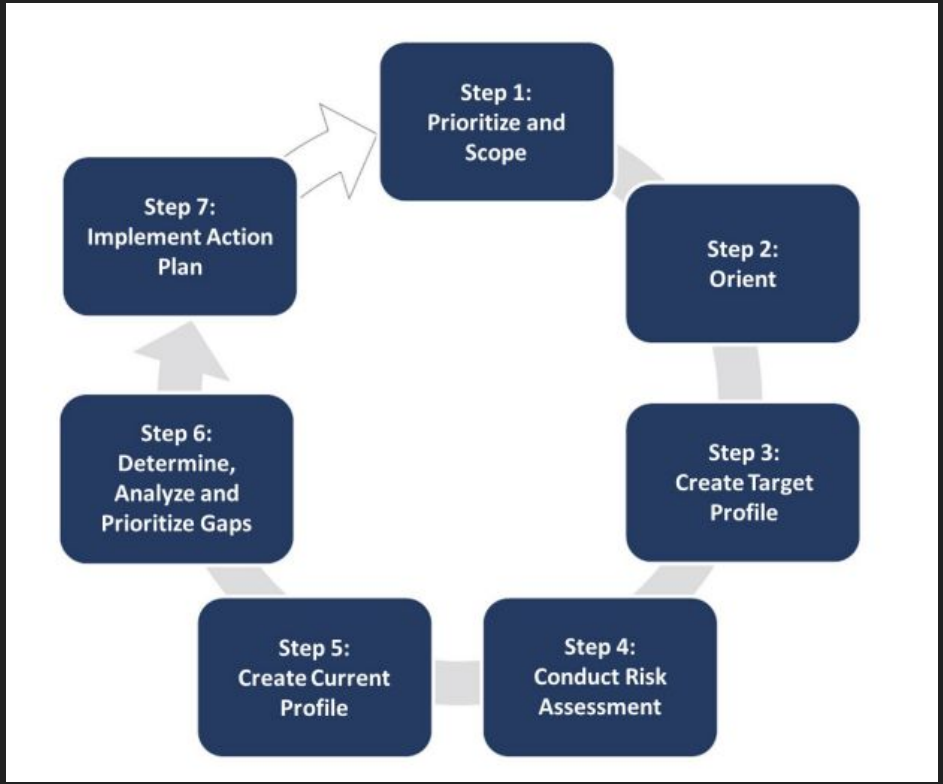


The Health Sector Cybersecurity Framework Implementation Process

The U.S. HHS and ASPR

The U.S. HHS - United States Department of Health and Human Services

The ASPR - Administration for Strategic Preparedness & Response.



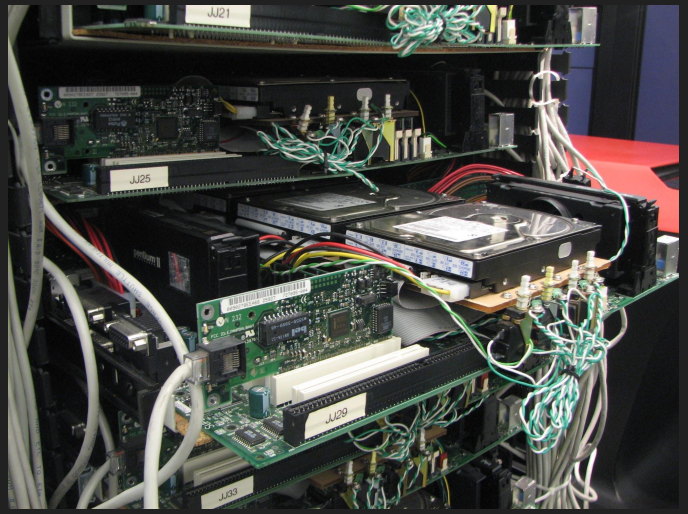
Step 1: Prioritizing and Scoping

This first step is all about taking inventory and assessing threats.

- Strategizing how to frame, assess and respond to risks
- Categorize your systems based on sensitivity & criticality

Step 2: Orientation

In the orientation step, the organization wants to identify the systems and assets they have at their disposal, and connect them with the appropriate regulatory and authority to supervise and manage them.



Step 3: Creating a Target Profile

Create a Target/Goal/Plan for the organization.

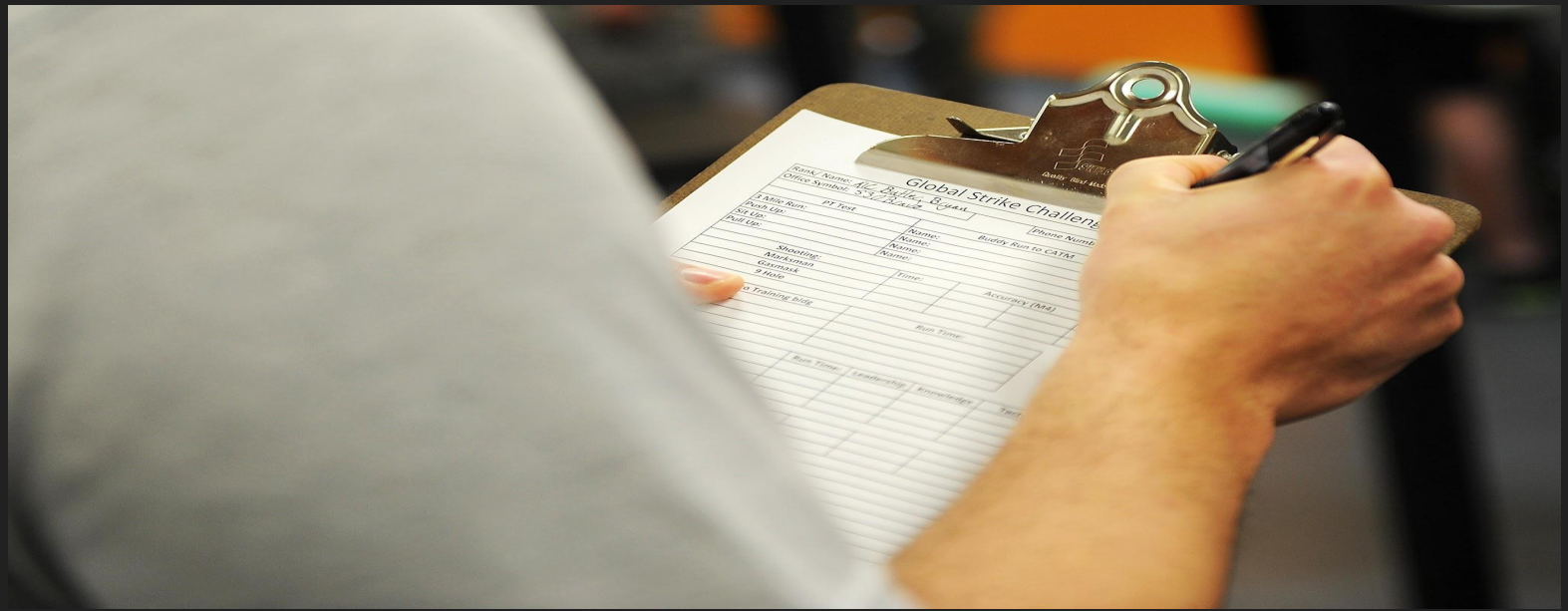
Step 4: Conducting a Risk Assessment

Identify and evaluate threats, weaknesses and targets within your organization.

Probability of Mishap Occurring	Mishap Severity: Catastrophic	Critical	Marginal	Negligible
Frequent				
Probable	HIGH RISK			
Occasional		MEDIUM RISK		
Remote			LOW RISK	
Improbable				NEGLIGIBLE RISK

Step 5: Create a Current Profile of your Organization

What is the current state of your organization’s cybersecurity system as it stands?

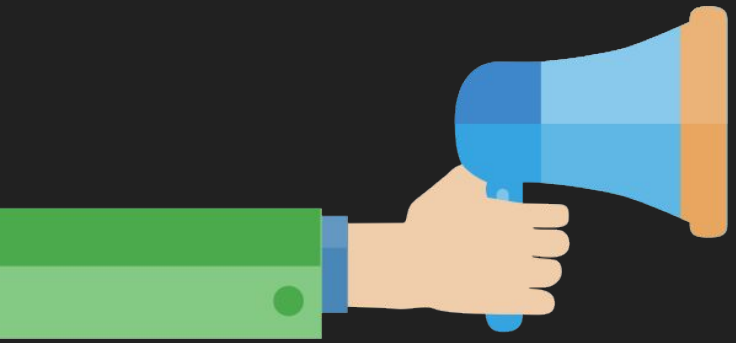


Step 6: Gap Analysis

Compare the Target Profile with the organization’s Current Profile and assess deficiencies.

Step 7: Taking Action

Compare the Target Profile with the organization’s Current Profile and assess deficiencies.



HIPAA

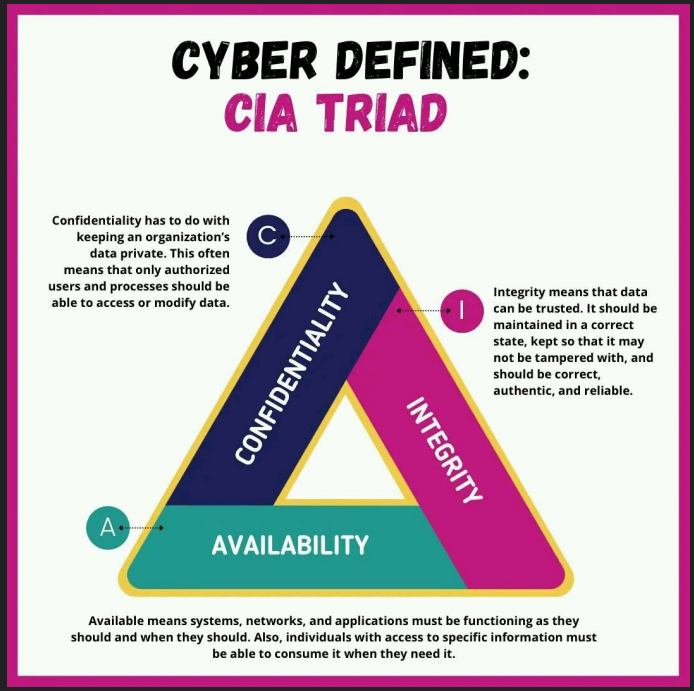
- Health Insurance Portability and Accountability Act of 1996
- Issued by the US Department of Health and Human Services
  - Protect sensitive patient health information from being disclosed without the patient's consent or knowledge

HIPAA Security Rule

- Applies to electronic protected health information, e-PHI
  - Ensure confidentiality, integrity, and availability of all e-PHI
  - Detect and safeguard against anticipated threats

Key Ideas of Security

- Confidentiality
- Integrity
- Availability



Challenges

- ➔ Complicated
- ➔ Placement (Layered model)
- ➔ Attackers only need to find a single weakness
- ➔ Constant monitoring

Conclusion

- Key Takeaways:
  - Cybersecurity threats to healthcare organizations are rapidly evolving and increasingly sophisticated.
  - A multi-layered security approach is essential to protect patient data, ensure operational continuity, and maintain public trust.
  - Proactive measures, including firewalls, employee training, continuous monitoring, security configurations, and data encryption..
  - Ongoing vigilance, regular reviews, and continuous improvement according to standards described are necessary to stay ahead of the ever-changing threat landscape.
- Call to Action:
  - Prioritize cybersecurity as a strategic imperative for Hospital Systems.
  - Allocate necessary resources and obtain executive support for implementing the recommended security measures.
  - Foster a culture of cybersecurity awareness and accountability across all levels of the organization.

Works Cited

- 2022. *A Guide to Firewall Security: Concerns, Capabilities, an Limitations.* Network Security What is Firewall Security? Types, Capabilities, Limitations|EC-Council (eccouncil.org)
- 2023. *HPH Sector Cybersecurity Framework Implementation Guide*. Administration for Strategic Preparedness and Response. HPH Cybersecurity Framework Implementation Guide (hhs.gov)
- 2024. *Healthcare Cybersecurity: The Biggest Stats and Trends in 2024*. Safety Detectives. Healthcare Cybersecurity: The Biggest Stats and Trends in 2024 (safetydetectives.com)
- 2024. *Physician cybersecurity*. AMA Physician cybersecurity | American Medical Association (ama-assn.org)
- Anwar, R.W.; Abdullah, T.; Pastore, F. Firewall Best Practices for Securing Smart Healthcare Environment: A Review. Appl. Sci. 2021, 11, 9183. https://doi.org/10.3390/app11199183
- Brook, Chris. 2023. *A Guide to Data Encryption Algorithm Methods & Techniques.* DataInsider A Guide to Data Encryption Algorithm Methods & Techniques | Digital Guardian
- Butaka, Gopikrishna. 2021. *Is CyberSpace Secure From Humans?* ISACA. Is Cyberspace Secure From Humans? (isaca.org)
- D. B, P. J, S. C. M, S. Rajagopal and B. Jegajothi, "Secure Cloud-based E-Health System using Advanced Encryption Standard," 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2022, pp. 642-646, doi: 10.1109/ICESC54411.2022.9885501.
- *Health Insurance Portability and Accountability Act of 1996.* Centers for Disease and Control Prevention Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC
- *HIDS vs NIDS: Unravelling the Differences in Intrusion Detection Systems.* Neumetric HIDS vs NIDS: Unravelling the Differences in Intrusion Detection Systems (neumetric.com)
- Insider Threats: Verizon. (2022). 2022 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/
- Kost, Edward. 2024. *What are the Biggest Cyber Threats in Healthcare?* UpGuard. What are the Biggest Cyber Threats in Healthcare? | UpGuard
- Modes of Attack: MITRE ATT&CK. (n.d.). ATT&CK for Enterprise. https://attack.mitre.org/matrices/enterprise/
- Riggi, John. *A high-level guide for hospital and health system senior leaders*. AHA Center For Health Innovation. The importance of cybersecurity in protecting patient safety | Cybersecurity | Center | AHA
- Young, Kelli. 2021. *Cyber Case Study: Anthem Data Breach*. Coverlink Insurance. Cyber Case Study: Anthem Data Breach - CoverLink Insurance - Ohio Insurance Agency