SHCH Security Plan

#DontWannaCry

HIPAA Audit Results & Recommendations

Implementation of the Technical Safeguards standards represent good business practices for technology and associated technical policies and procedures within a covered entity.

Executive Summary

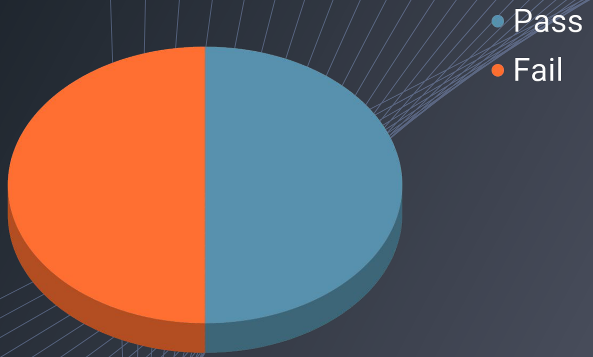
HIPAA Compliance Based on Existing Controls	Implemented	Partially Implemented	Not Implemented
Access Controls		🟧	
Audit Controls		🟧	
ePHI Integrity			🟧
Person or Entity Authentication		🟧	
Transmission Security		🟧	

Results

- Utilized the Security Risk Assessment Tool provided by ONC and evaluated **44 Technical Safeguards** to measure HIPAA Compliance.

- Found SHCH policies to be **50% Compliant** with 22 safeguards passing and 22 safeguards failing.

- Overall, the audit results indicate that SHCH's efforts minimally address audit requirements, they have made attempts to comply, but implementation is inadequate, or some efforts indicate misunderstanding of requirements.



Recommendations

- **Access Controls**
  - Enable Emergency Access Procedures
  - Enable Automatic Log-off Mechanisms
- **Audit Controls**
  - Setup Activity Monitoring
  - Conduct Internal Auditing
- **ePHI Integrity**
  - Deploy policies to prevent Unlocked or Unattended Workstations
  - Verify and Test all Backups and Recovery Steps
- **Person or Entity Authentication**
  - Deploy policies to prevent Unauthorized Access
- **Transmission Security**
  - Document Encryption Technology

Top 5 Threats and Recommendations

Top 5 Threats

Asset Name	Asset Type	Threat	Inherent Risk level			Current Risk Level		
Employee	Social Engineering	Phishing/Malware Tailgating/Shoulder Surfing	5	5	25	3	5	15
Application softwares	Software packages	RCE exploited through unpatched vulnerabilities such as Log4j	4	5	20	4	5	20
Firewall, Storage & File Servers	Network & Storage Layer Devices	Network Intrusion	4	5	20	3	5	15
Windows server	Storage server software	Unauthorized Access	4	5	20	4	5	20
Doctor's Patient Management Account	Employee Accounts	credential compromise	4	4	16	3	4	12

Social Engineering

Phishing, Malware, Tailgating, Shoulder Surfing

Inherent Risk			Current Risk					Residual Risk with Proposed Control			
Likelihood	Impact	Risk Value	Current Control(s)	Control Owner	Likelihood	Impact	Risk Value	Risk Strategy	Likelihood	Impact	Risk Value
5	5	25	MFA for remote connections	IT Security Lead	3	5	15	Mitigate	1	4	4

Social Engineering

Recommendations:

- Conduct regular CyberSecurity Awareness Training
- Antivirus/Antimalware software
- Principle of Least Privilege
- Password Policy
- Report Suspicious Activities

RCE exploited through unpatched vulnerabilities

Software packages

Inherent Risk			Current Risk					Residual Risk with Proposed Control			
Likelihood	Impact	Risk Value	Current Control(s)	Control Owner	Likelihood	Impact	Risk Value	Risk Strategy	Likelihood	Impact	Risk Value
4	5	20	Keep the records of software version	CISO	4	5	20	Mitigate	1	5	5

RCE exploited through unpatched vulnerabilities

Recommendations:

Create a patch management plan and update vendor patch within one week of release

Windows server Storage server software

Threat: Unauthorized Access

CVE-2016-2183: remote attackers obtain cleartext data via a birthday attack against a long-duration encrypted session

Risk Strategy	Likelihood	Impact	Risk Value
Migate	1	5	5

Recommendation: Conduct penetration testing and create documents for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated.

Firewall, Storage & File Servers

Network & Storage Layer Devices

Threat: Network Intrusion

Description: The attacker may gain access to the internal network through the public internet edge. This will allow the attacker to move horizontally across the internal network and carry out further attacks such as planting ransomware, stealing data, or shutting down critical services

Risk Strategy	Likelihood	Impact	Risk Value
Migate	2	3	6

Recommendation:

1) system wide NIDS to quickly identify potential intrusion and track down the malicious behavior.

2) automated tools for real time analysis.

Doctor's Patient Management Account

Employee Accounts

Threat: credential compromise

Description: the credentials of the doctor's account patient management is compromised due to weak password, visiting malicious sites, or social engineering

Risk Strategy	Likelihood	Impact	Risk Value
Migate	2	3	6

Recommendation:

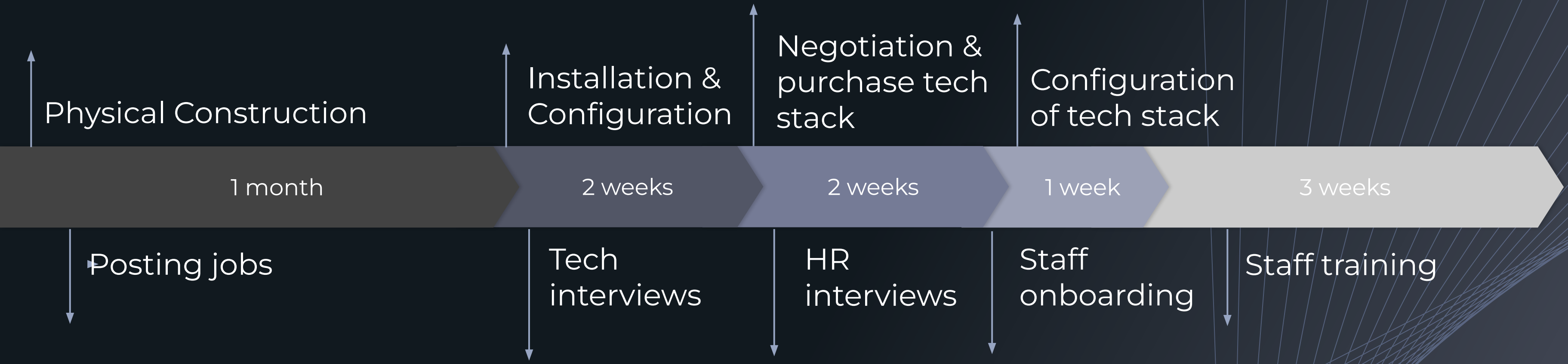
1) freeze/suspend the account immediately after detecting the compromise

2) require users to set a new password every quarter

3) enforce MFA for not just remote but all types of connections

SOC Plan

Timeline



Physical Construction

1 month

Posting jobs

Installation & Configuration

2 weeks

Tech interviews

Negotiation & purchase tech stack

2 weeks

HR interviews

Configuration of tech stack

1 week

Staff onboarding

3 weeks

Staff training

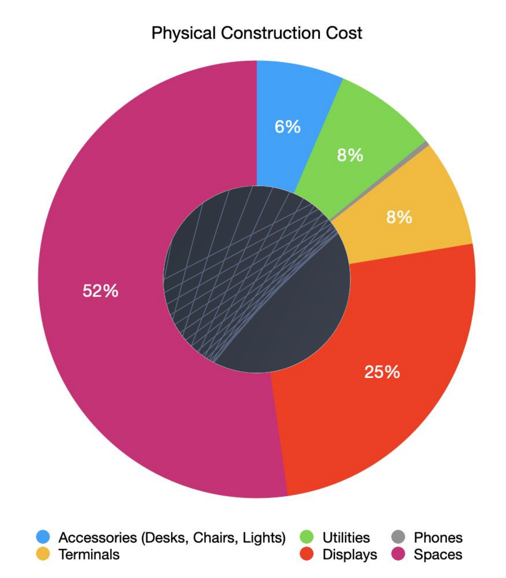
- Construction: six weeks
- Tech stack acquisition: one month
- Talent acquisition: two months
- Staff training: one month

Schedule

- Asset Monitoring
- Operation Monitoring
- Meeting
- On-call Duty

Physical Construction Cost

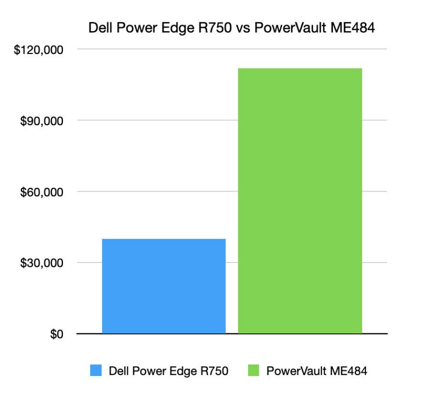
	Recommend Assets Name	Total Cost
Accessories	**Desk** **Chair** **Light**	**$2040**
Utilities	**House Utilities**	**$2400/month**
Phones	**Cisco Unified 7940G**	**$125**
Terminals	**Dell Inspiron**	**$2500**
Displays	**TV Displays**	**$8000**
Spaces	**Spaces**	**$16500**



Total one time cost: $29,165
Total yearly cost: $28,800

Monetary Cost (Endpoint Detection & Response)

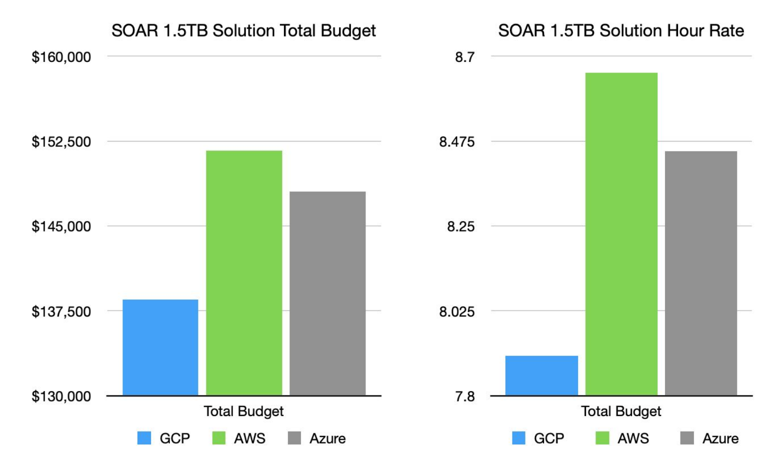
	Budget / Year (1400 devices)	Extra fee
Service	**$17,500**	**$8400**
Dell PowerEdge R750 Server (16 CPUs, 64GB RAM, 3.84TB)	**$40,000**	**$2000 /year maintenance**
PowerVault ME484 (16 CPUs, 64GB RAM, 3.84TB)	**$112,000**	**$22,400 / year maintenance**



Monetary Cost (SOAR 1.5TB storage)

	Hour Rate	Total Budget
GCP	**7.906**	**$138,513**
AWS	**8.656**	**$151,653**
Azure	**8.449**	**$148,026**

GCP is recommend to use. Since the size per zone is closed to the requirement (1.5TB) which do not have waste size. Also, the Kibana, Integrations Server and Enterprise Search has exactly 32GB RAM, 16CPUs. GCP is the cheapest among three solutions.



Job Descriptions & Salary

Responsibility & Requirement	SOC Junior Threat Analyst	SOC Senior Threat Analyst
conduct vulnerability scans & analysis	🟧	🟧
design and implement automated workflows	🟧	🟧
monitor hospital networks and security alerts for anomalies	🟧	
report significant findings to the SOC Lead		🟧
oversee the daily operations of threat intelligence and analysis		🟧
Degree requirement, certification, work experience	🟧	🟧
Salary	$90,000 - $110,000	$110,000 - $150,000

Incident Response Runbook

Why having a runbook?

- increased attack frequency on nationwide hospitals
- 42% of healthcare delivery organizations (HDOs) reported having encountered ransomware attacks across the past few years[1]
- Example: CommonSpirit Health ransomware attack[2]

[1] https://www.cybertalk.org/2021/08/10/best-practices-to-avoid-ransomware-attacks-on-hospitals-in-2022/
[2] https://www.healthcaredive.com/news/commonspirit-health-ransomware-cyberattack/634011/

Incident Response Team Structure

- Team lead - CISO
- Investigation lead - IT/Tech lead of the affected department
- Communication lead - SOC lead
- HR/Legal representation

Executive reporting frequency

Every 2 hours - attack discovery & forensic evidence gathering

Every 6 hours - recovery phase

Daily - RCA, mitigation implementation, operation restored

Once a week - mitigation effect follow up, previously affected systems monitored in the production environment again

Internal & External Resources

Internal

- IR team
- application/system logs
- operation history
- CCTVs & badge access record
- CFO(ransom negotiation)

External

- third party IR investigator
- FBI
- open source ransomware database

Response Procedures

- stop the attack
- preserve forensic evidence
- root cause analysis (RCA)
- attack recovery
- initial attack vector mitigation

Disclosure

- contact the FBI at the discovery phase of the incident
- host a public webpage for the official statements and updates regarding the incident - updates daily
- after restoring services, announce mitigation measures and enhanced security measures moving forward, as well as a summary of the impact of this incident

Mitigation Evidence

- data/service has been restored/recovered
- initial attack vector has been removed
- other discovered vulnerabilities has been patched systemwide
- attacker has been completely removed from the hospital network

Report Preparation

- event timeline, including person/department involved
- RCA result
- financial loss
- assessment of the response process
- security measures moving forward

Conclusion

- The organization is lacking in terms of the controls required for HIPAA compliance and needs to invest significant resources to be compliant

- As per the SOC plan, the organization will spend roughly:
  - 31K on one time costs for physical construction
  - 250K per year on personnel
  - 340K per year on maintenance and infrastructure

Thanks for watching!