



Prioritizing Security Investment April, 2024



Adam Kehler

CISSP, HITRUST CCSFP

Introduction online

HEALTH CYBERSECURITY

Objectives

❖ What is a Security Program?

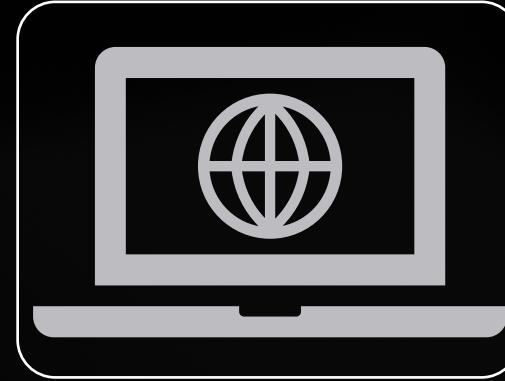
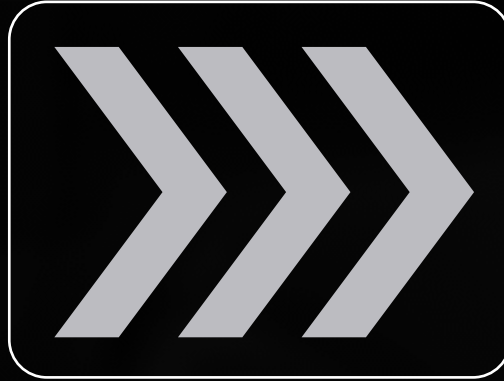
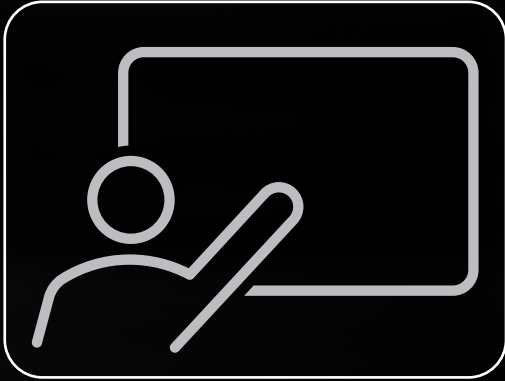
❖ Risk-based approach

❖ A case study

❖ Questions!!!

What is a Security Program?

Information Security Program



People

Leadership

IT

Users

Process

Policies

Procedures

Activities

Training

BCP/IRP

Technology

Authentication

Access Controls

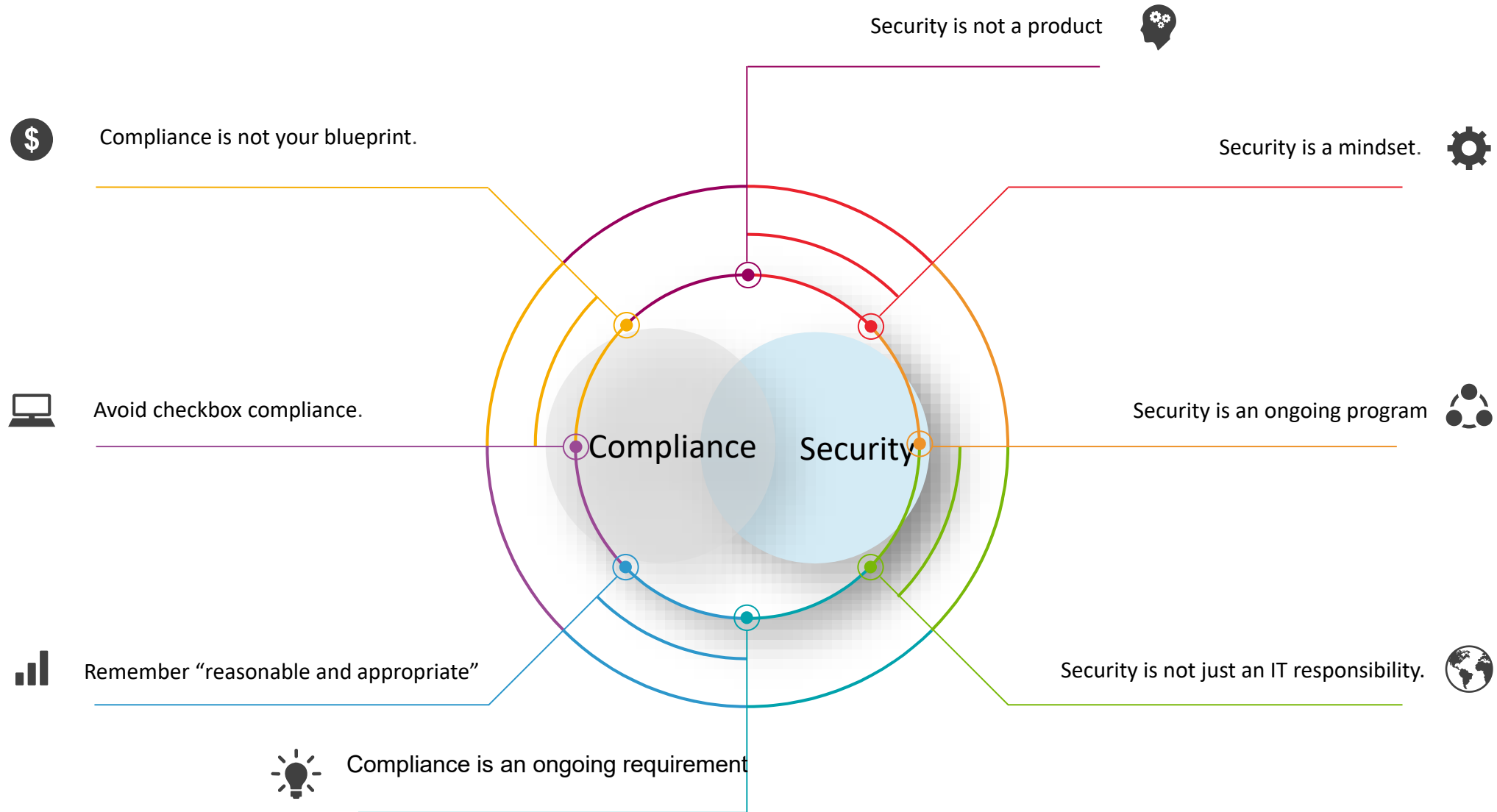
Encryption

Endpoint Protection

Email Protection

Security Risk Management

Compliance vs. Security



HIPAA and Risk Management

Standard 164.308(a)(1)(i), *Security Management Process*, requires regulated entities to:

Implement policies and procedures to prevent, detect, contain, and correct security violations.

The Security Management Process standard includes four required implementation specifications. Two of these specifications deal directly with risk analysis and risk management:

1. **Risk Analysis (R¹⁴)** – 164.308(a)(1)(ii)(A): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
2. **Risk Management (R)** – 163.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).

[NIST SP 800-66 r2 \(Draft\)](#) Implementing the Health Insurance 4 Portability and Accountability Act 5 (HIPAA) Security Rule

Security Risk Analysis

Does your SRA provide a list of gaps or a list of risks?

Gap

The organization does not have Multi-Factor Authentication in place.

The organization does not have network segmentation.

Risk

There is a high likelihood that a phishing attack would succeed due to the absence of MFA and network segmentation. This could result in attackers gaining access to the local network and pivoting to critical systems such as the EMR resulting in loss of data, a large breach, or loss of services.

Assessment/Analysis Approach



The Security Risk Assessment approach is designed to allow organizations to implement “reasonable and appropriate” security controls as opposed to being prescriptive



For example, what is a reasonable disaster recovery plan for a large health system would be excessive for a small doctor’s office; this allows flexibility while still being enforceable



If other organizations of the same size are encrypting their laptops, it would seem reasonable to expect your organization to do the same



But how can you determine what is “reasonable and appropriate” for your organization?

Take a Security Risk Management approach and look to industry standards and guidance





Prioritizing Security Enhancements

Prioritizing Security Enhancements

		Impact →				
Likelihood ↑		Negligible	Minor	Moderate	Significant	Severe
	Very Likely	Low	Moderate	High	High	High
	Likely	Low	Moderate	Moderate	High	High
	Possible	Low	Low	Moderate	Moderate	High
	Unlikely	Low	Low	Moderate	Moderate	Moderate
	Very Unlikely	Low	Low	Low	Moderate	Moderate

		Impact →				
		Negligible	Minor	Moderate	Significant	Severe
Likelihood ↑	Very Likely	Low	Moderate	High	High	High
	Likely	Low	Moderate	Moderate	High	High
	Possible	Low	Low	Moderate	Moderate	High
	Unlikely	Low	Low	Moderate	Moderate	Moderate
	Very Unlikely	Low	Low	Low	Moderate	Moderate

Prioritizing Security Enhancements

- Examples
 - You have a static website hosted on a website hosting service. It has vulnerabilities, isn't monitored, and doesn't require MFA on the admin portal.
 - Likelihood? Impact? Overall Risk? Priority?
 - Your EMR system is in a dedicated network segment, requires VPN to access, has intrusion detection systems and strong physical safeguards. Your CEO is worried about it getting breached and wants to hire an MSP to manage it.
 - Likelihood? Impact? Over Risk? Priority?
 - Your patient portal has a critical vulnerability that is being actively exploited by attackers.
 - Likelihood? Impact? Over Risk? Priority?

Prioritizing Security Enhancements




Risk	Recommendations	Risk	Cost
Ransomware affecting EMR System	Engage Managed Service Provider (MSP)	Moderate	\$20,000
Attackers breaching website	Work with developer to fix holes, Multi-Factor Authentication (MFA) on portal, possibly move to another platform.	Low	\$8,000
Patient Portal vulnerabilities	Work with vendor to patch	High	\$4,000



Putting Security Into Action

- With risks in hand, translate to organizational risk
- Executives are good at making risk-based decisions
- Which makes it easier for a CFO or CEO to make a risk-based decision:
 - “We need \$20,000 to implement Multi-Factor Authentication (MFA) and network segmentation. MFA will make people take extra steps to login to our systems and network segmentation will increase the amount of time we’ll need from our network management contractor.”
 - “There is an extremely high likelihood that Phishing/Ransomware will affect our EMR server. If this happens, we may have to pay a hefty ransom, go through an OCR audit, pay fines, or lose all of our patient data. We can greatly reduce this risk by implementing MFA and network segmentation which will cost \$20,000.”

Prioritizing Security Enhancements

1. Does this approach comply with HIPAA? 
2. Does this approach increase security? 
3. Does this approach optimize use of security dollars? 
4. If you DON'T implement security controls, who owns the risk?

Case Study

Security Breach Preparation, Response, and Avoiding Fines

Case Study: Consider an FQHC

- Rural Arkansas
- Internal Information Technology (IT) team of two people – IT Director and System Administrator/Technician
- Recently converted from on-premises electronic medical record (EMR) to cloud-based EMR
- Have done their own Risk Assessment using publicly available tools
- No formal security budget



Case Study: Far, Far, Away Health Center

Annual Risk Assessment findings reviewed by IT Director.

Risk Assessment sent to leadership team as an FYI. They may or may not read it.

IT Director makes patches and configuration changes to address technical risks.

Compliance person gets a policy template, fills out to address policy gaps, and sends to Human Resources to have everyone sign.

Everyone trusts the IT Director because he “knows security.”



Case Study: Apex Health Center

- Risk Management Plan (RMP) was developed based on the findings of the Risk Assessment.
- RMP was discussed at executive team meetings and decisions made regarding risks as they relate to their potential impacts on the operations, finances, and goals of the organization.
- Decision was made to address High and Critical risks immediately.



This Photo by Unknown Author is licensed under CC BY

Case Study: Apex Health Center

- Risk Assessment updated when migrating to new EMR
- Risk Team reviews plan periodically and makes updates as necessary
- Security Controls follow a well-established framework



This Photo by Unknown Author is licensed under CC BY

Apex Health Center	Far, Far Away Health Center
Sees Information Security as an organizational responsibility	Sees Information Security as an IT task
Compliance - an outcome of good security	Compliance - a checkbox exercise
Risk-based decisions - based on organizational impact and goals	Security controls - implemented in response to “requirements” and based on experience
Follow a well-established framework	Ad-hoc security controls
Conduct exercises to test incident response plan and Business Continuity Plan	Had a security incident and downtime last year, so feel like they are well-practiced

Apex Health Center	Far, Far Away Health Center
Leadership Team approves budget for Critical and High Risks but encourages use of existing solutions and some manual processes.	Budget was approved based on what the IT Director says is needed.
Example: They approve multi-factor authentication (MFA) using built-in capabilities of their email/collaboration federated solution. IT Director pushed for enhanced 3rd party solution but will consider in the budget for next year.	Example: They signed up for a new antivirus program because the clinic down the street said this new one was better. They are using both just to “cover our bases.”
Example: Security risk assessment (SRA) recommended a full Managed Security Services Provider (MSSP) for monitoring, but compromise was that a local security and event management (SIEM) would be implemented, and the System Administrator would start building the most necessary reports.	Example: They implemented site-to-site real-time replication system so that a hot standby is immediately available in case the main site goes down.
Example: Purchased a platform for conducting phishing campaigns because phishing has been an issue.	There was no money left for training.

It's Tuesday morning, and the IT Director is just getting his coffee. The phone rings. It's the FBI.



Apex Health Center	Far, Far Away Health Center
Follows procedures in tested Incident Response Plan	Scramble to figure out what to do
Notify legal and cyber insurance as practiced	Where is that phone number?
Identify critical systems, disable accounts, and patch holes	Identify critical systems, disable accounts, and patch holes
Document incident using approved templates and rehearsed process	?
Update procedures and retrain users	?
Notify Office of Civil Rights (OCR), affected patients, the State Attorney General, etc.	Notify OCR, affected patients, the State Attorney General, etc.

Case Study: Office for Civil Rights (OCR) Investigation

- Review Health Insurance Portability and Accountability act (HIPAA) Safeguards
 - Could the health center have prevented the breach?
 - Should the health center have detected the breach?
 - Request among other things: Risk Assessment, Risk Management Plan, and Policies and Procedures
 - Request evidence of what was done in response to the breach

Apex Health Center	Far, Far Away Health Center
Provides Security Risk Assessment (SRA), Risk Management Process (RMP), Policies and Procedures (P&Ps), Incident Response Plan (IRP), Business Continuity Plan (BCP), and evidence of tabletop exercises	Provides SRA, P&P, quickly documents an RMP
Provides evidence of technical remediation	Provides evidence of technical remediation
Provides documentation of incident response activities including updated P&Ps and evidence of retraining	Writes an after-the-fact narrative of what occurred
Provides evidence of notifications including affected patients, OCR, State AG, and the media	Provides evidence of notifications including affected patients, OCR, State AG, and the media

Apex Health Center

OCR closes the case indicating that the Health Center was found in compliance with HIPAA and responded appropriately. Some suggestions made for System Activity Review and implementing MFA (which was already planned).

Far, Far Away Health Center

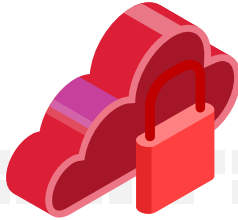
OCR finds that the organization has not complied with HIPAA and enters into a Settlement Agreement that includes fines and a Corrective Action Plan (CAP) that includes:

- Document a Risk Management Plan
- Fully implement P&Ps
- Implement System Activity Review
- Enhance Access Controls
- Document and Test Incident Response Plan
- Provide quarterly updates of compliance activities to OCR for 10 years

405(d) HHS Managing Threats (HICP)

Social Engineering

E-mail phishing is an attempt to trick you, a colleague, or someone else in the workplace into giving out information using e-mail. An inbound phishing e-mail includes an active link or file (often a picture or graphic)..



Theft of Equipment

Every day, mobile devices such as laptops, tablets, smartphones, and USB/thumb drives are lost or stolen, and they end up in the hands of hackers. Theft of equipment and data is an ever-present and ongoing threat for all organizations.



Ransomware

“Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user’s data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid.



Insider, Accidental or Intentional Data Loss

Insider threats exist within every organization where employees, contractors, or other users access the organization’s technology infrastructure, network, or databases



Questions?

