ACHC U®
EDUCATIONAL RESOURCES

ACUTE CARE HOSPITAL CRITICAL ACCESS HOSPITAL

UNDERSTANDING HEALTHCARE CYBERSECURITY & RISK

Susan Snedaker, MBA, CHCIO, CHISL

Welcome

- Discuss the current cybersecurity environment.
- Learn about cybersecurity program elements.
- Compare risk management frameworks.
- Learn about Key Performance Indicators (KPIs) for cybersecurity.

Introduction

- CIO at El Rio Health, a large FQHC in S. Arizona
- Formerly CISO at TMC Health, a large community health system in S. Arizona.
- Author of numerous IT and healthcare IT books, including Renovating Healthcare IT – Building the Foundation for Digital Transformation
- https://www.susansnedaker.com
- https://www.linkedin.com/in/snedaker

2023 Healthcare Breach Statistics

Figure 1.
Number of Breaches Reported

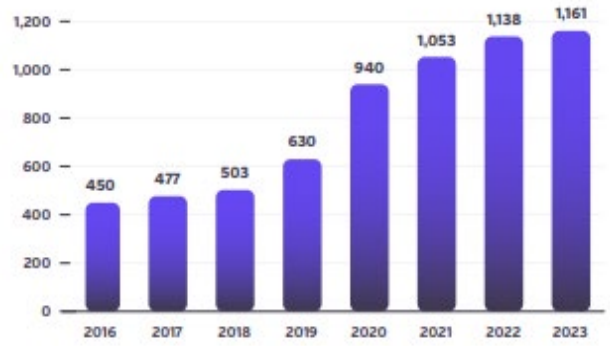
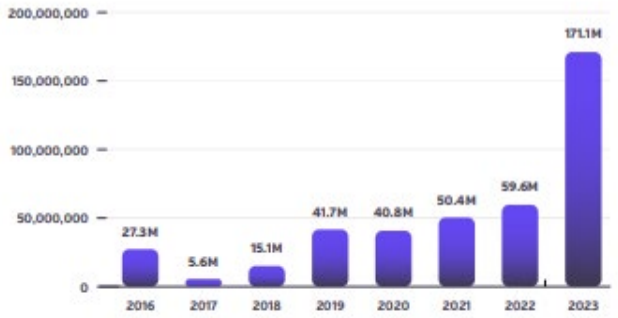
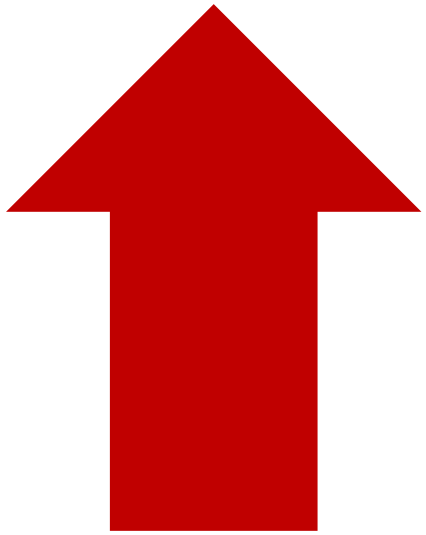


Figure 2.
Number of Records Breached



- **1,161** breaches reported
- **171M** patient records breached
- **97%** of records breached were due to hacking
- **187%** increase in the number of patient records (2023 vs. 2022)
- **$10.9M** average cost of breach

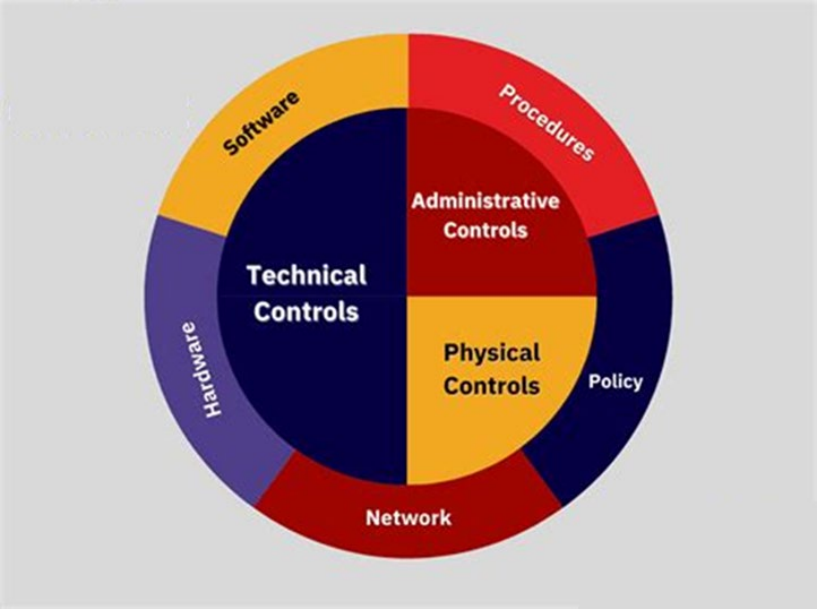
Cybersecurity Environment



1. Ransomware-as-a-service.
2. Nation-state sponsored activities.
3. The use of AI in cyberattacks.
4. The complexity and interconnectivity of systems.

Defense-in-Depth

1. **Defense in depth** (DiD) is the strategy of layering different physical and digital resources.
2. A *preventative* approach aiming to decrease the likelihood of a breach.
3. Defense in depth uses a wide variety of tools.
4. Some small organizations may only have a few tools, but they should be carefully selected.



Cybersecurity Program Overview

A cybersecurity program should contain:

1. An assigned person accountable for cybersecurity in the organization.
2. A defined framework for managing risk.
3. Policies and procedures to define organizational requirements and to meet regulatory requirements.
4. Threat and vulnerability monitoring.
5. Risk assessment and remediation efforts.
6. Periodic testing and auditing.
7. Management of program.

1. Assigned Responsibility

Every organization should have an assigned person accountable for cybersecurity.

This is required by HIPAA and is critical for managing cyber risk.

2. Defined Framework

Every organization should select a cybersecurity risk framework to help facilitate the development and management of the cybersecurity program.

NIST CSF and **HITRUST** are two commonly used frameworks in healthcare.

Many HC organizations use NIST CSF.

You can find info here:

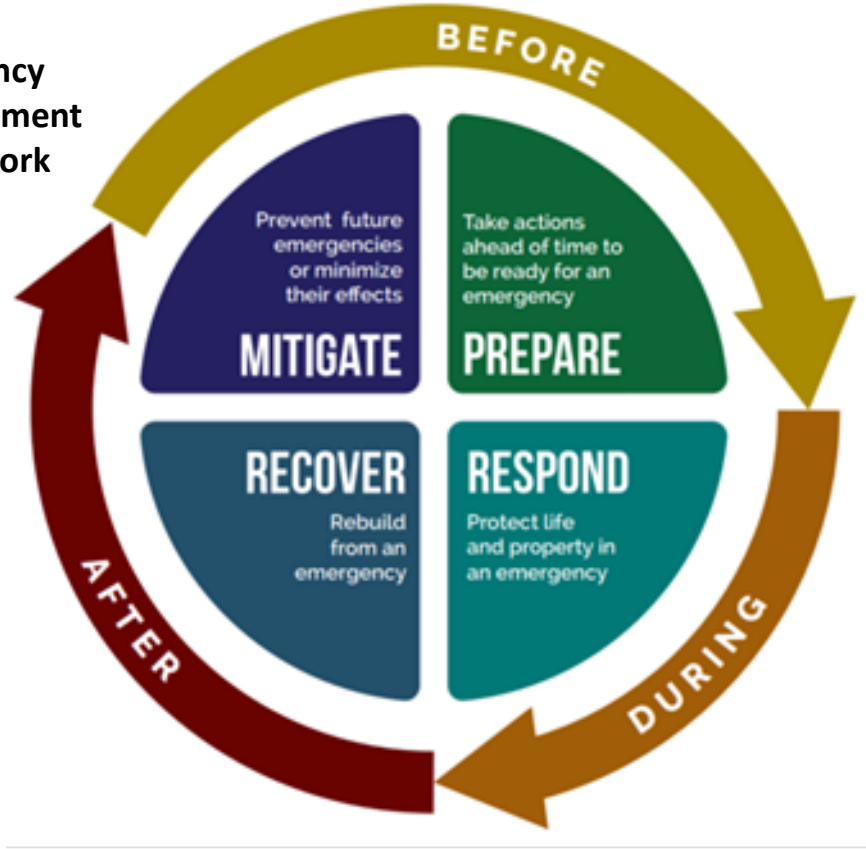
HPH Sector Cybersecurity Framework Implementation Guide: Introduction (hhs.gov) and Cybersecurity Framework | NIST

Risk Management Frameworks

Compare NIST CSF and Emergency Management Framework

NIST Cybersecurity Framework

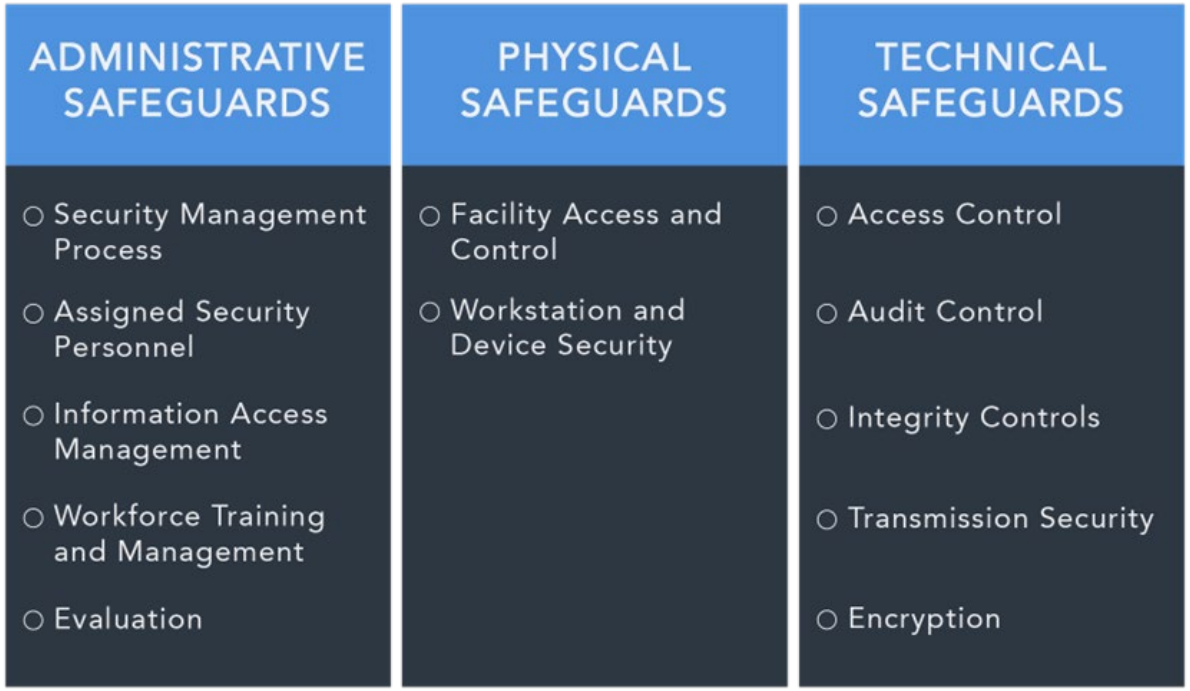
Emergency Management Framework



3. Policies and Procedures

HIPAA Security Rule has three elements:

- *Administrative*
- *Physical*
- *Technical*



[Security Rule Guidance Material | HHS.gov]

[Security Administrative Safeguards (hhs.gov)]
Small Provider Guidelines

Monitoring, Assessment, Auditing

4. Threat and vulnerability monitoring ensure the cybersecurity team is aware of threats that could impact the organization.

5. Risk assessment and remediation involve actively addressing issues to reduce risk.

6. Periodic testing and auditing includes testing technical controls and auditing user permissions/system access.

7. Management of the program requires periodic review, updates, and evaluation of the effectiveness of the program.

Key Performance Indicators

Develop meaningful metrics

What metrics best reflect the risk and risk reduction of the organization?

1. Phishing education – total count vs. total failures.
2. Patching (desktop & server) percent complete.
3. Devices encrypted (desktop & server) percent complete.
4. Vulnerabilities identified vs. remediated.
5. Mean Time to Resolution for identified vulnerabilities.

Next Steps

1. **Assess** and **document** your risk environment.

2. Create a **project plan** to remediate top risks. Track progress.
   [SimpleRisk.com is a free risk management tool for IT.]

3. Focus on **fundamentals** first – patching, encryption, email & web filtering, end user device protection, and 2-factor authentication.

4. Focus on **perimeter** second – firewalls and routers should be patched/updated and hardened; servers should be hardened* by default.

* *Hardening means disabling and removing all unused services, ports, and features of a system. If it's not needed, remove it. This reduces risk by eliminating the risk of unused features being exploited.*

Questions?

For more information on HIPAA requirements for small entities,
visit For Small Providers, Small Health Plans, & other Small Businesses | HHS.gov

ACHC U®
EDUCATIONAL RESOURCES

ACUTE CARE HOSPITAL CRITICAL ACCESS HOSPITAL

Thank you

Susan Snedaker,
susants@elrio.org