SVMIC

Security Risk Analysis

Step 1 of an Effective Cybersecurity Program

Our Speaker

Loretta Verbeck, MS, FACMPE, CHC

Objectives

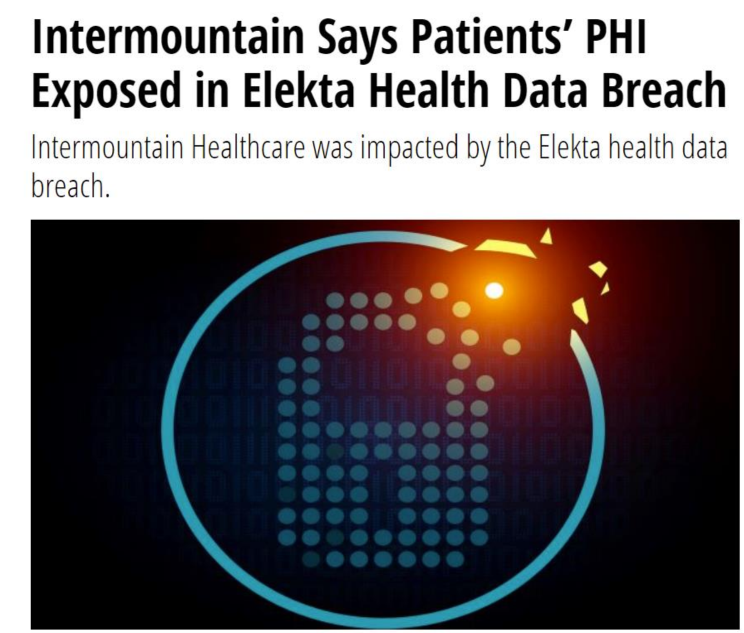
❑ Illustrate the importance of an accurate and thorough Security Risk Analysis and why it is essential to an Effective Cybersecurity Program

❑ Recognize systems and devices that create, receive, transmit or store ePHI

❑ Identify system vulnerabilities and the threats that could exploit them

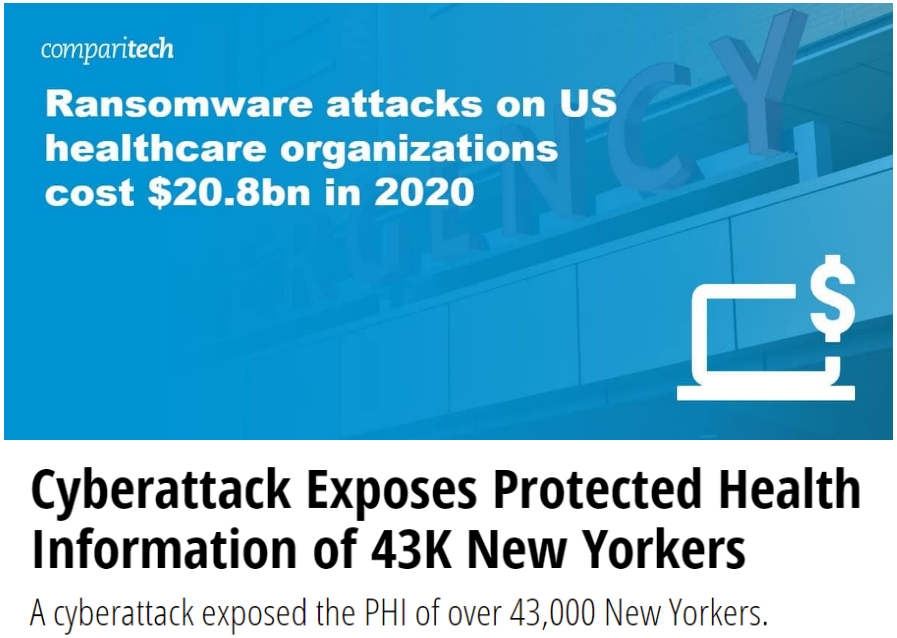
❑ Develop risk management strategies to protect ePHI from cyberattacks as well as other physical and environmental threats

Cyber Crime on the Rise



Intermountain Says Patients' PHI Exposed in Elekta Health Data Breach

Intermountain Healthcare was impacted by the Elekta health data breach.



comparitech

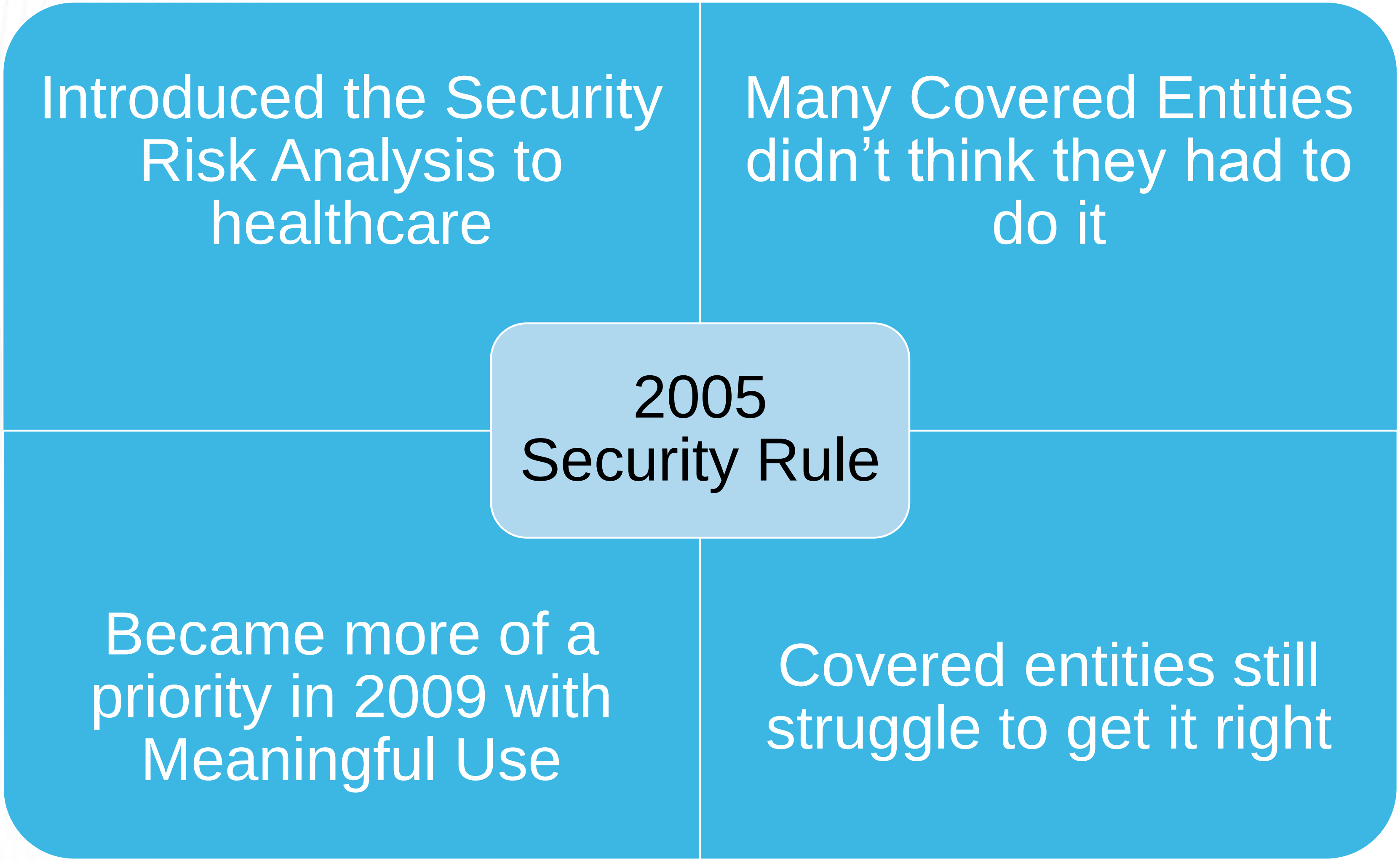
Ransomware attacks on US healthcare organizations cost $20.8bn in 2020

Cyberattack Exposes Protected Health Information of 43K New Yorkers

A cyberattack exposed the PHI of over 43,000 New Yorkers.

Cybersecurity Begins with an SRA

HIPAA Security Rule



Introduced the Security Risk Analysis to healthcare

Many Covered Entities didn't think they had to do it

2005 Security Rule

Became more of a priority in 2009 with Meaningful Use

Covered entities still struggle to get it right

Health Plan Breach Affecting Over 9.3 Million

"Hacking continues to be the greatest threat to the privacy and security of individuals' health information. In this case, a health plan did not stop hackers from roaming inside its health record system undetected for over a year which endangered the privacy of millions of its beneficiaries…Health care entities need to step up their game to protect the privacy of people's health information from this growing threat."

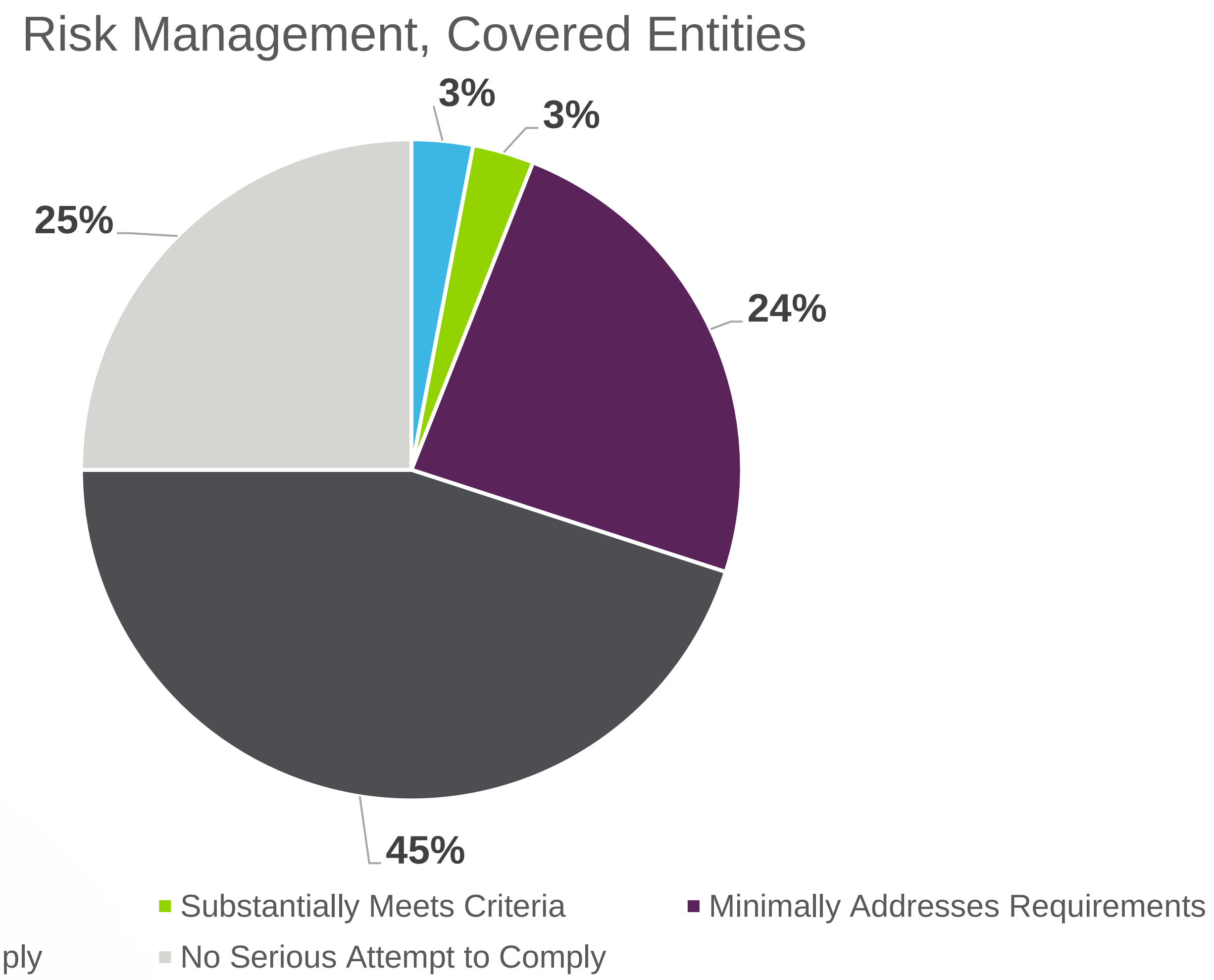
Roger Severino, Previous OCR Director
OCR News Release, January 15, 2021

Settlements & Civil Monetary Penalties (CMP)

$130,980,482

The lack of an accurate and thorough SRA has consistently been sighted in investigations conducted by the OCR and resulting in settlements or CMPs.

OCR Audit Results



OCR Audit Results

Minimally addressed

- Entity has made attempts to comply, but implementation is inadequate, or efforts indicate misunderstanding of requirements

Negligible efforts

- Policies and procedures are copied directly from an association template, evidence of training poorly documented and generic

No serious attempt to comply

- No evidence of a serious attempt to comply with the Rules

OCR Audit Results – Security Risk Analysis

Entities generally failed to:

Identify	Develop	Conduct	Consider	Review
Identify and assess the risks to all ePHI in their possession	Develop and implement policies and procedures for conducting a risk analysis	Conduct risk analyses consistent with policies and procedures	Identify threats and vulnerabilities, to consider their potential likelihoods and impacts, and to rate the risk to ePHI	Review and periodically update a risk analysis in response to changes in the environment and/or operations, security incidents, or occurrence of a significant event

SRA Misconceptions

- It’s a checklist.
- It’s a one and done.
- My EHR vendor does this for me.
- If I don’t participate in MIPS, I don’t have to do it.

An Accurate & Thorough Security Risk Analysis

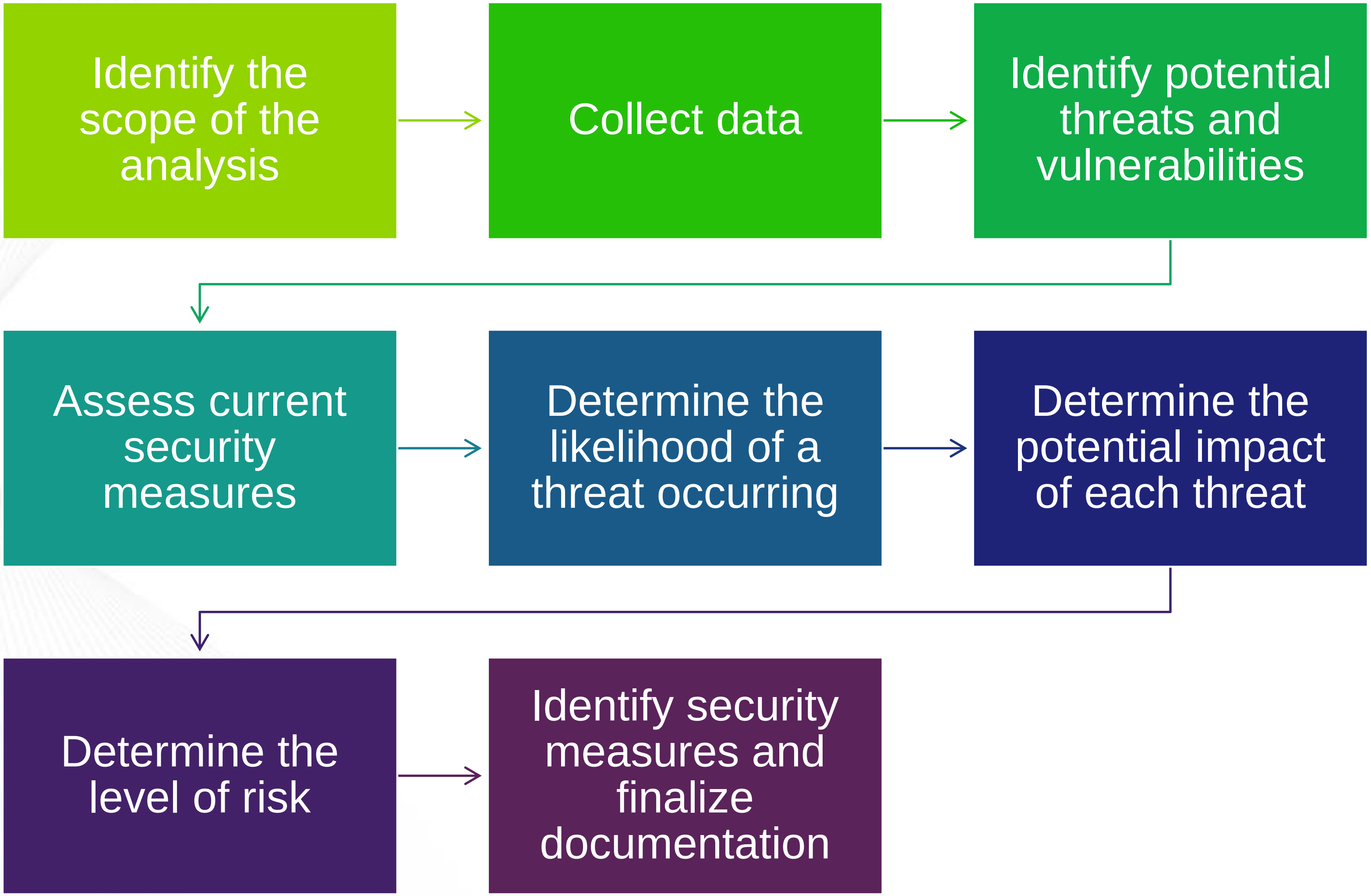
Security Risk Analysis

An assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ALL electronic PHI created, received, maintained, or transmitted

Scalable, but must be enterprise-wide

No required methodology, but guidance is provided

Steps of a Security Risk Analysis



Identify the scope of the analysis

Collect data

Identify potential threats and vulnerabilities

Assess current security measures

Determine the likelihood of a threat occurring

Determine the potential impact of each threat

Determine the level of risk

Identify security measures and finalize documentation

Scope

ALL electronic PHI created, received, maintained, or transmitted

Must be documented as a part of the SRA

Will vary based on size/complexity of organization

May require review of multiple locations and processes for use and disclosure

Collect Data

Interview

Conduct interviews of all workforce members

Identify

Conduct on-site reviews to identify ePHI

Review

Review past and existing projects that involved ePHI

Develop

Develop an inventory of all hardware, software, portable media, and other devices that are used to create, receive, maintain, or transmit ePHI

Commonly Overlooked ePHI

VoIP telephone systems

Email applications

Medical equipment

Digital faxing services

Cloud storage

Personal devices

Identify Threats and Vulnerabilities

Threat

- Potential for a specific vulnerability to be triggered or exploited
  - Natural
  - Human
  - Environmental

Vulnerability

- Flaw or weakness in systems or processes

Common Threats

- Hacking
- Misuse
- Power loss
- Social engineering
- System errors
- Theft
- Malware
- Natural events

Identifying Vulnerabilities

Previous risk analysis

Audit reports

Assessing information systems

- Vulnerability scans
- Penetration testing

Vulnerability lists and advisories

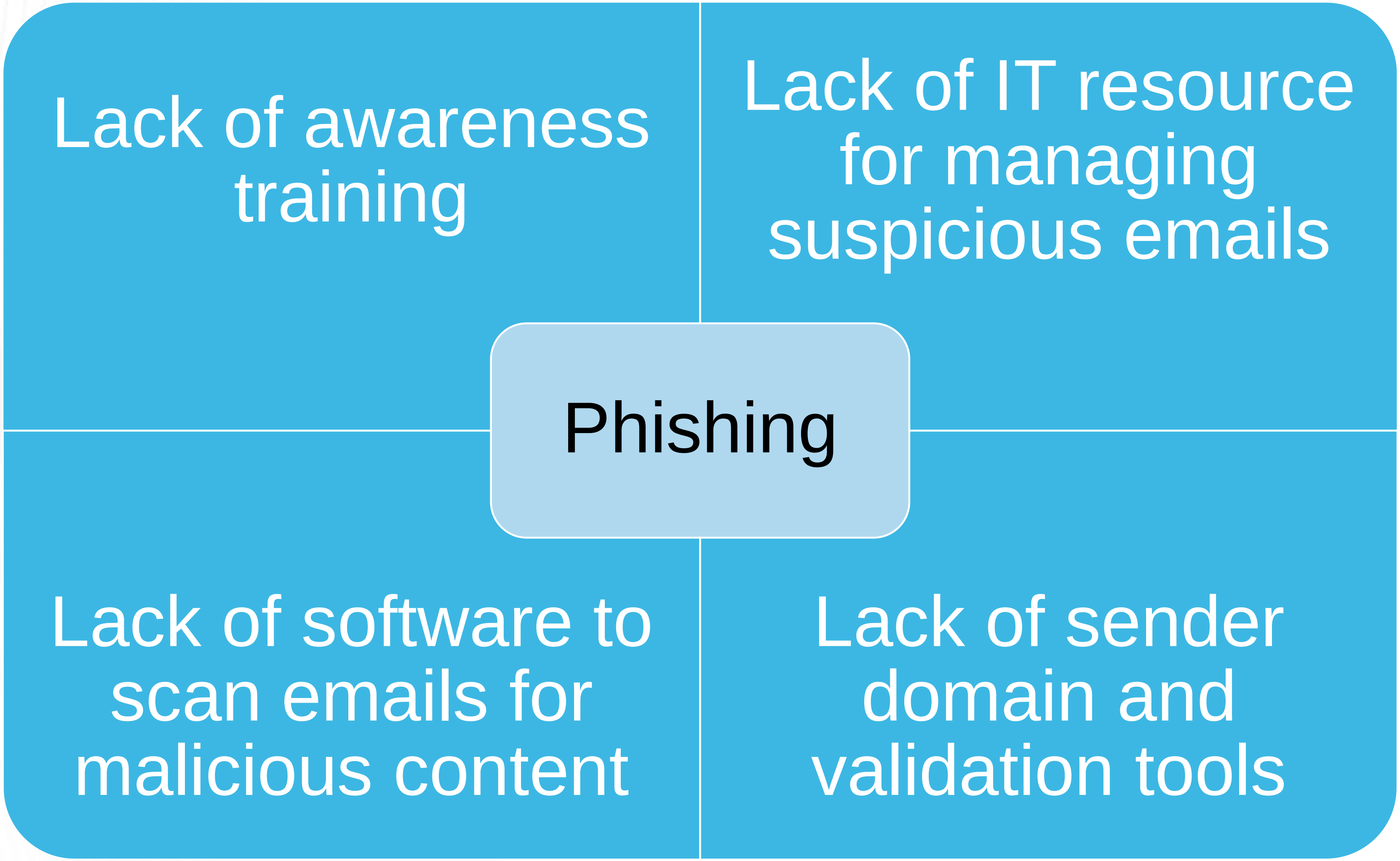
- HHS Cybersecurity Updates
- FBI Internet Crime Complaint Center (IC3)

Threats to the Healthcare Industry

- Email phishing
- Ransomware
- Loss or theft of equipment or data
- Insider, accidental or intentional data loss
- Attacks against connected medical devices

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Vulnerabilities



Lack of awareness training

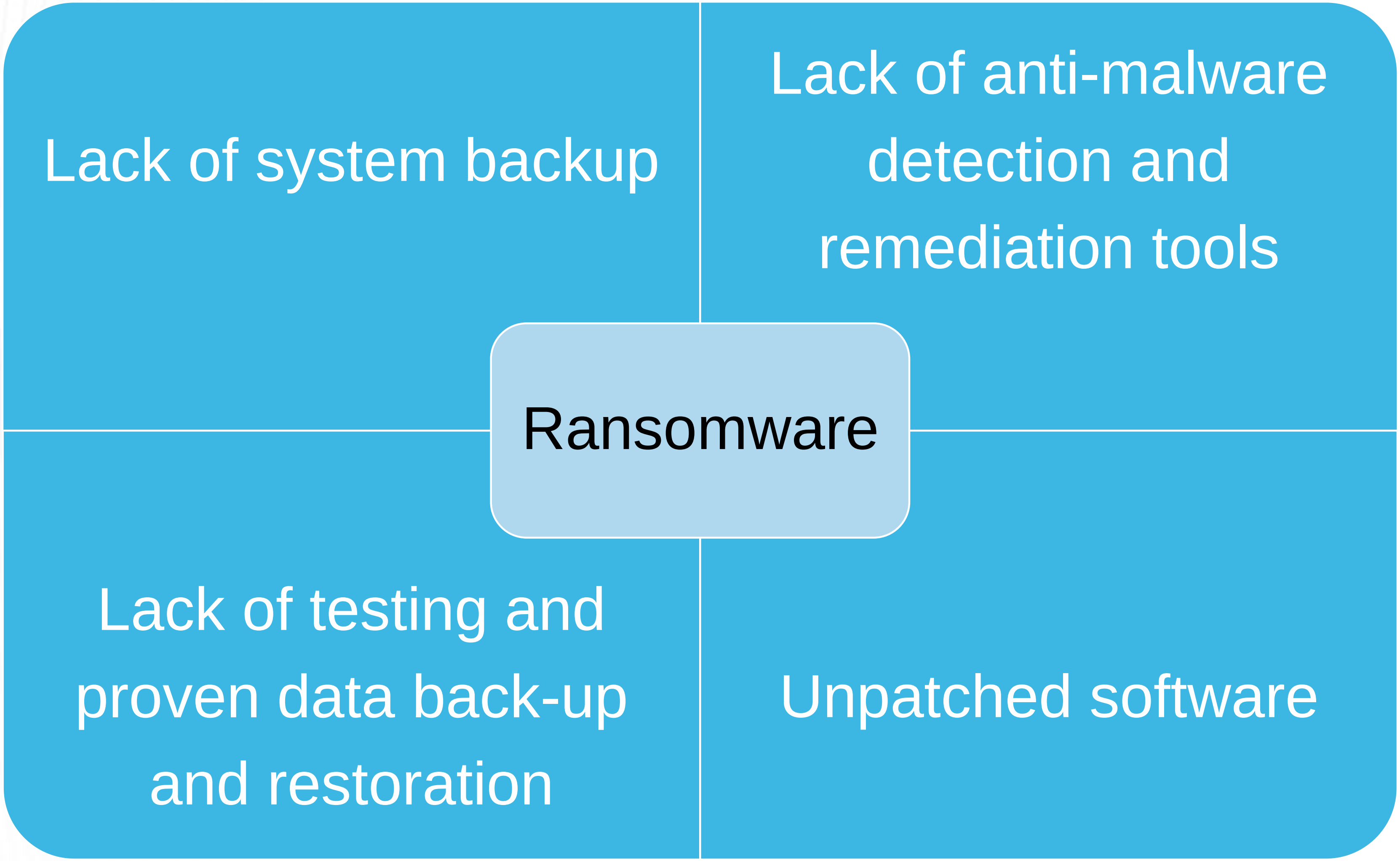
Lack of IT resource for managing suspicious emails

Phishing

Lack of software to scan emails for malicious content

Lack of sender domain and validation tools

Vulnerabilities



Lack of system backup

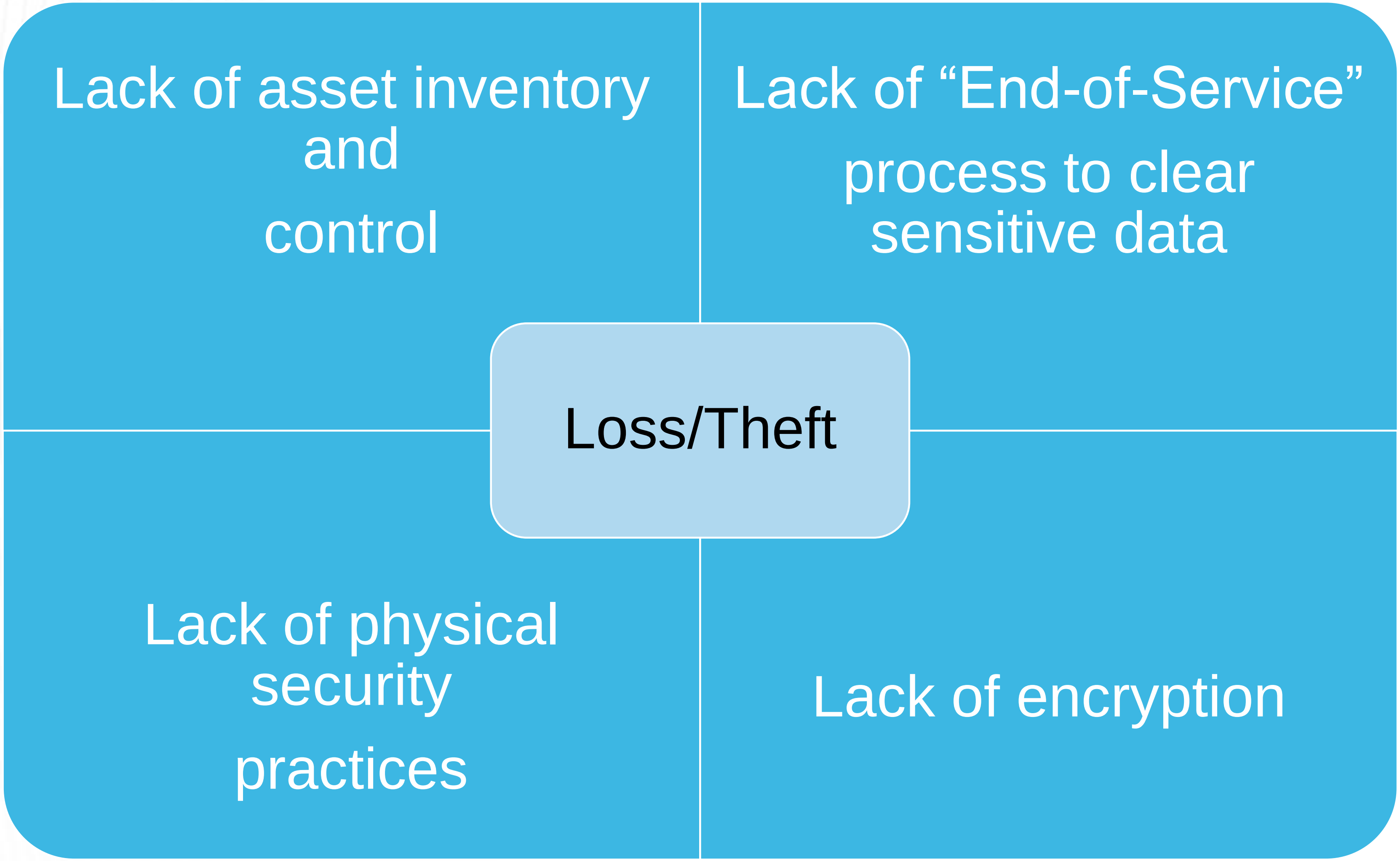
Lack of anti-malware detection and remediation tools

Ransomware

Lack of testing and proven data back-up and restoration

Unpatched software

Vulnerabilities



Lack of asset inventory and

control

Lack of “End-of-Service”

process to clear sensitive data

Loss/Theft

Lack of physical security

practices

Lack of encryption

Assess Current Security Measures

Technical

- Access controls
- Automatic logoff
- Encryption

Non-technical

- Policies and procedures
- Standards and guidelines
- Physical security measures

Identify security measures required by the Security Rule

Security Standards

Administrative safeguards

- Office policies and procedures, staff training, and other measures to carry out security requirements

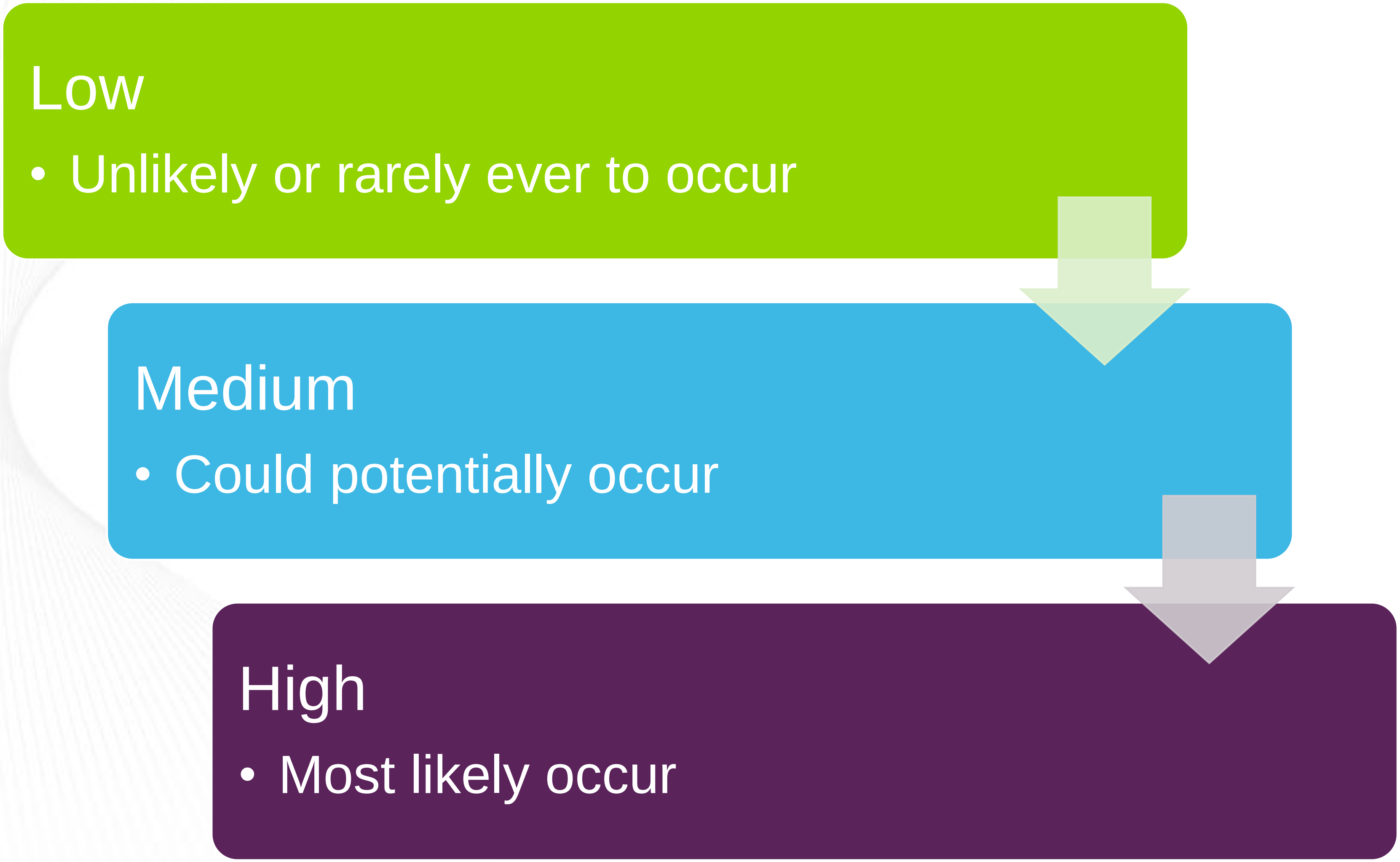
Physical safeguards

- Limiting access to physical areas where electronic information is stored

Technical safeguards

- Authentication, transmission and other issues that arise when authorized personnel access PHI via computer or other electronic device

Determine Likelihood of Threats



Low

- Unlikely or rarely ever to occur

Medium

- Could potentially occur

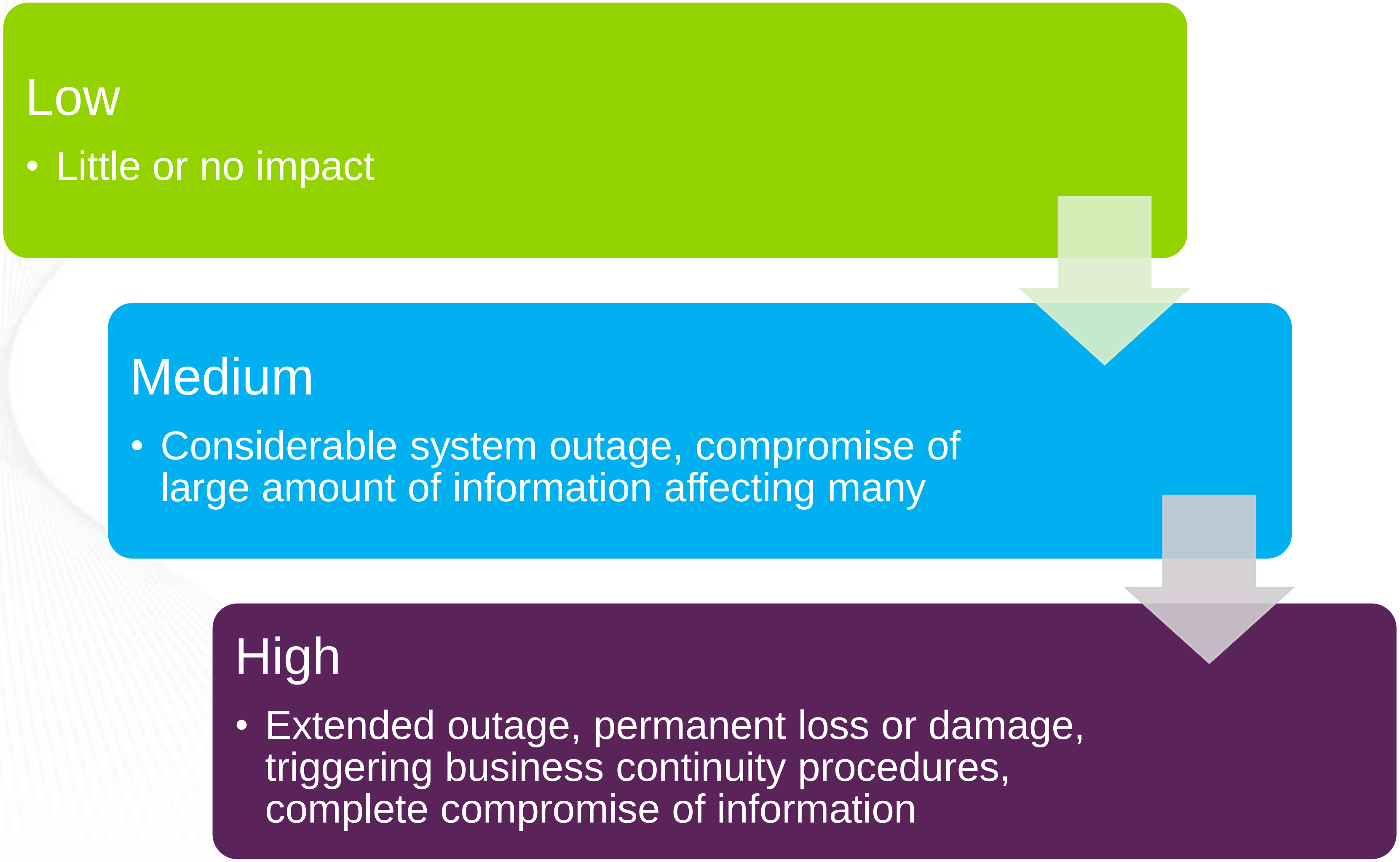
High

- Most likely occur

Determine Potential Impact

- Most common outcomes that could impact the confidentiality, availability and integrity of ePHI:
  - Unauthorized access or disclosure
  - Permanent loss or corruption
  - Temporary loss or unavailability
  - Loss of physical assets

Impact Severity Levels



Low

- Little or no impact

Medium

- Considerable system outage, compromise of large amount of information affecting many

High

- Extended outage, permanent loss or damage, triggering business continuity procedures, complete compromise of information

Determine Level of Risk

Risk Levels			
Impact Severity	Likelihood of Occurrence		
	Low	Medium	High
Low	Low	Low	Low
Medium	Low	Medium	Medium
High	Low	Medium	High

Identify Security Measures & Finalize Documentation

Identify actions that can reduce risk to a reasonable and appropriate level

Important considerations

- Required regulatory security measures
- Effectiveness of security measure
- Existing policies and procedures

All steps must be documented and retained for six years

SVMIC

Risk Management

Risk Management Plan

Develop and implement a risk management plan

- Evaluate and prioritize actions identified in risk analysis
- Implementation will vary by organization
- Cost can be considered, but cannot be the only factor

Documentation

- Required resources
- Assigned responsibilities
- Start and completion dates

Implement Security Measures

- Begin implementation
- Document scope, timeline, and budget
- Consider internal and external resources/vendors
- Covered entity is ultimately responsible, even if task is outsourced

Utilize Best Practices

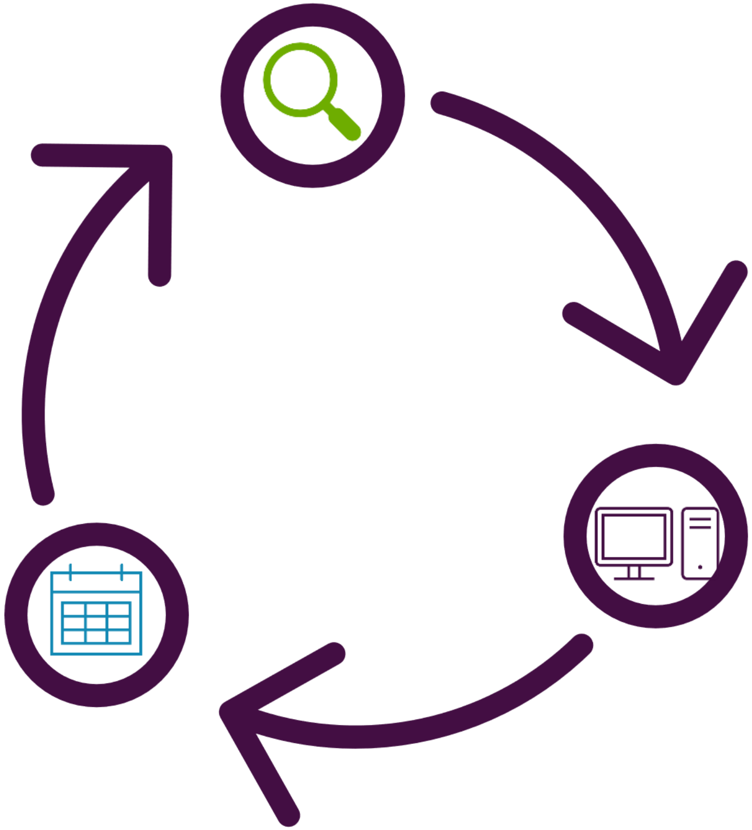
HR 7898

An Act to amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes.

- ❑ NIST Cybersecurity Framework
- ❑ CSA of 2015 Section 405(d)

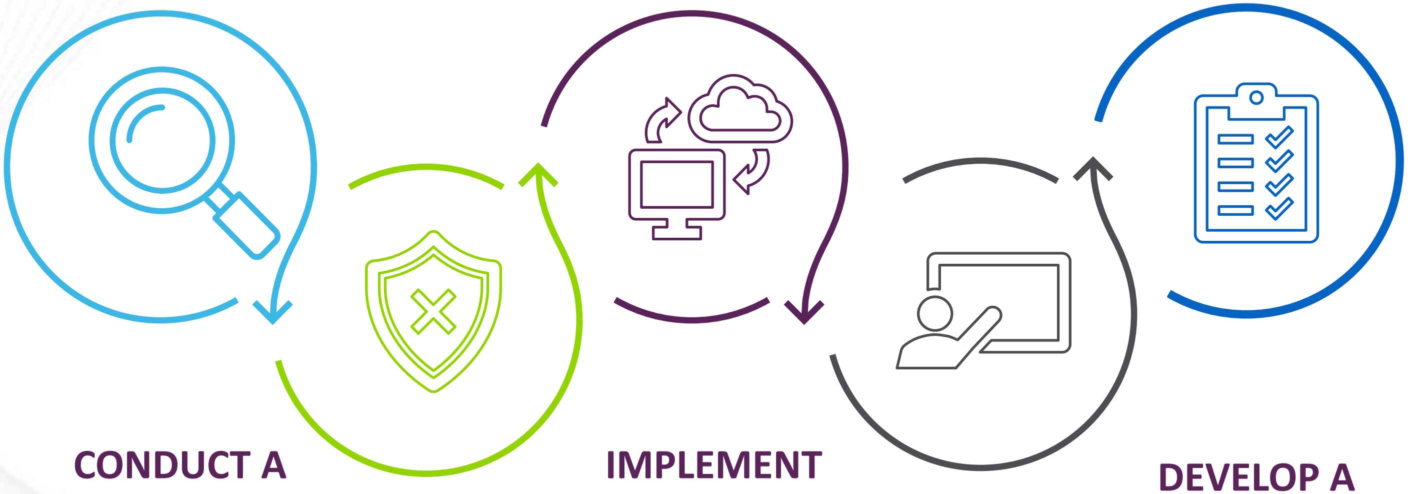
Ongoing Process

- Security measures must be reviewed and modified as needed
- No specified timeline by Security Rule
- Other programs may require regular assessment
- Review and update in response to changes in the environment
    - Addition of new technology
    - New business operations
    - Key staff turnover
    - Existing security measures become less effective



Resources

5 Steps to an Effective Cybersecurity Program



CONDUCT A SECURITY RISK ANALYSIS

DEVELOP A RISK MANAGEMENT PLAN

IMPLEMENT SECURITY TECHNOLOGIES

EDUCATE YOUR WORKFORCE

DEVELOP A RESPONSE PLAN

SVMIC Upcoming Webinars & Resources

Using Technology to Secure Your System

Friday, August 20, 2021

12:00 PM CST

Planning for the Worst - Security Incident Response

Friday, September 10, 2021

12:00 PM CST

SVMIC Cybersecurity Resources

Additional Resources

HHS Security Rule Guidance Materials

HealthIT.gov Security Risk Assessment Tool

HealthIT.gov Security Risk Assessment Videos

Thank you!

Call 800-342-2239 and ask for Medical Practice Services for more information or questions about the content covered in this presentation.

You may also email Contact@svmic.com.

SVMIC®