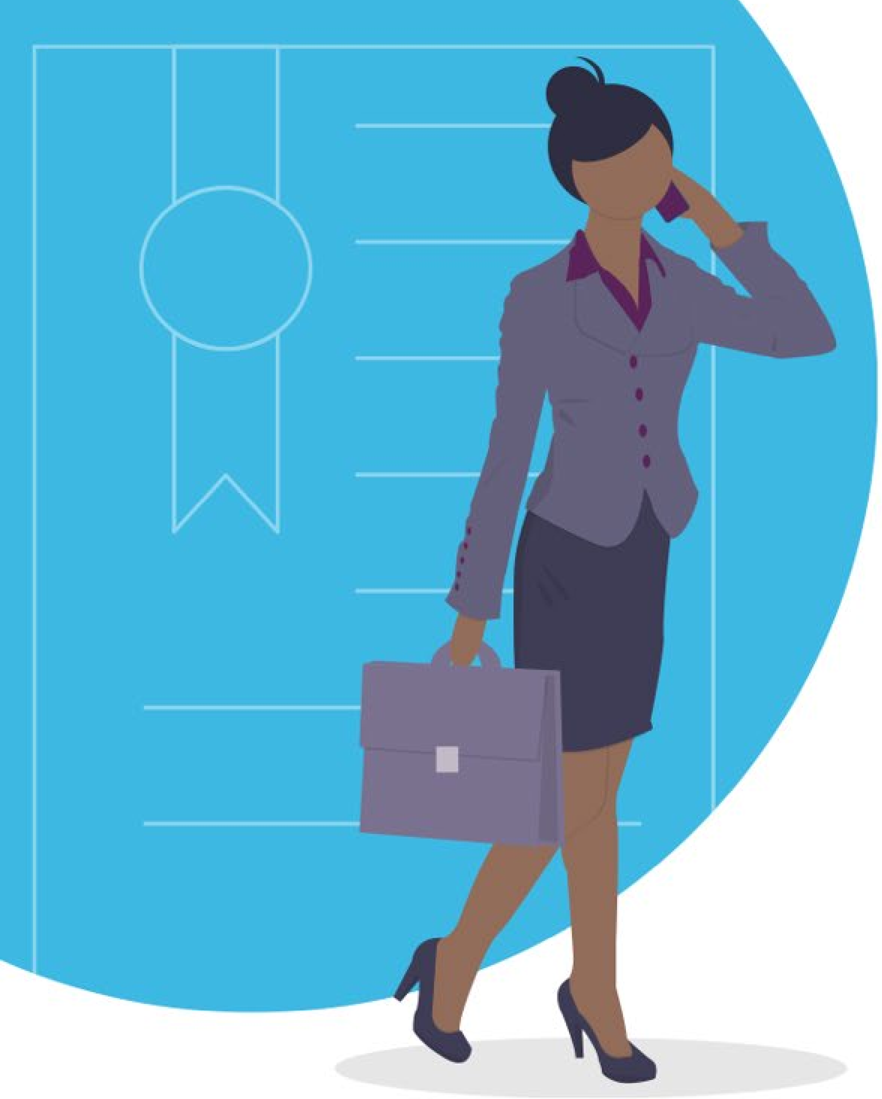


SVMIC

Cybersecurity: Are Your Secrets Safe?

Stephen A. Dickens, JD, FACMPE

Objectives

Highlight HIPAA Security Rule requirements and industry data outlining the risks you face from cyber criminals

Define the five key steps to an effective cybersecurity program including an effective security risk analysis

Outline a response plan for a security incident

Why is everyone talking about cybersecurity…

Data Breaches	2x	the level of 2018
Healthcare Data Breaches	3x	the level of 2018
Cyber Attacks	79%	of healthcare data breaches first 10 months of 2020
Cyber Attacks	45%	increase November/December 2020
Ransomware	$20.8B	downtime 2020
Healthcare Data Breaches	70%	breaches of 500 or more records reported to HHS were hacking/IT incidents
Outpatient Facilities & Specialty Clinics	⬆	Surpassed hospital systems in attacks the first half of 2021

Settlements & Civil Monetary Penalties (CMP)

$135, 328, 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.

It’s about more than just money…

69%

Delays in procedures & tests

63%

Patients diverted or transferred to other facilities

37%

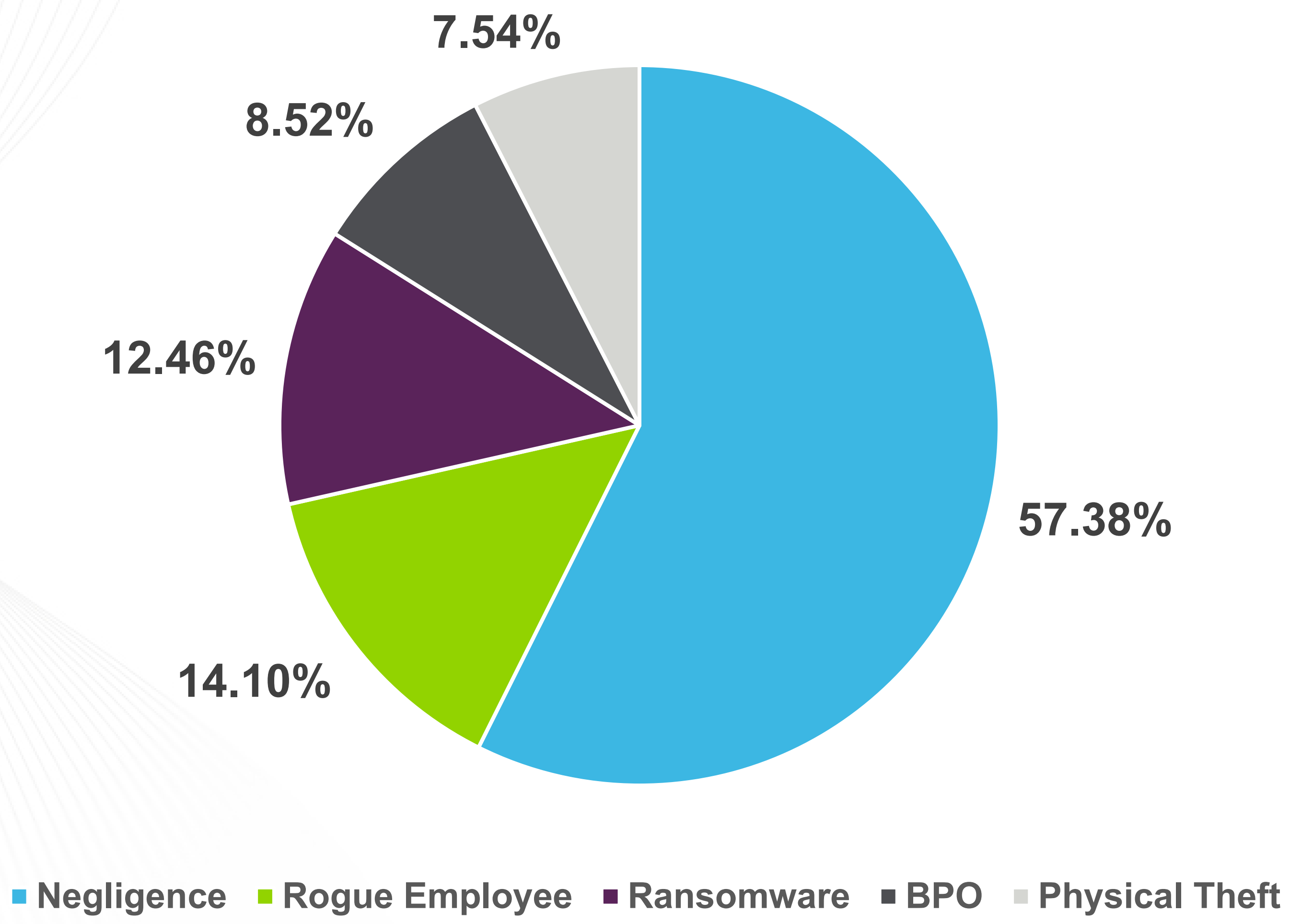
Increase in medical complications

23%

Increase in mortality rate

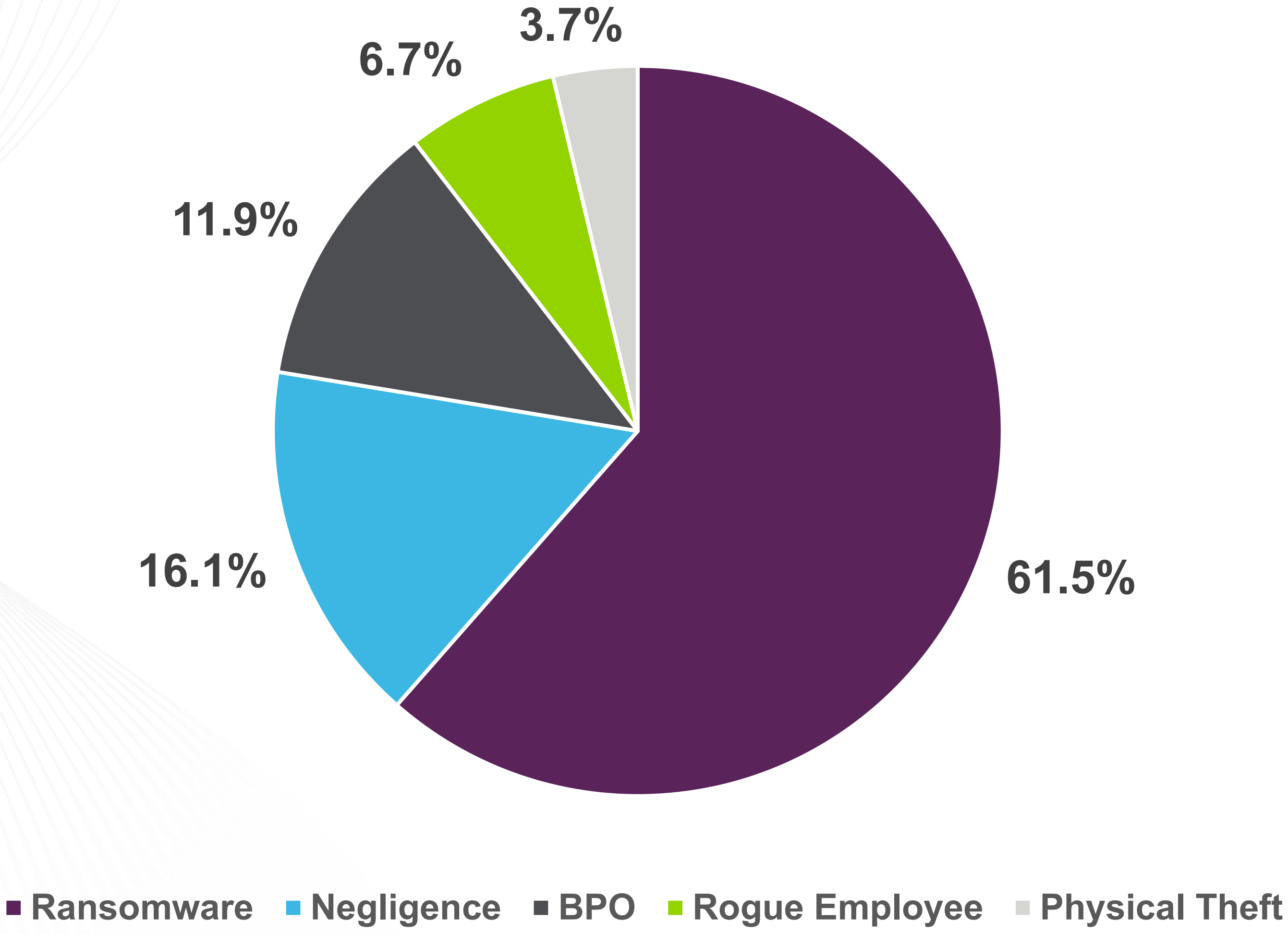
Modern Healthcare 09.22

SVMIC Claims by Type



2015 - 2019 Contract Years

SVMIC Claims Incurred by Cost



2015 - 2019 Contract Years

Common Pitfalls

Lack of proper Security Risk Analysis (SRA)

- Failure to assess potential threats
- Failure to properly address recognized threats

System vulnerabilities

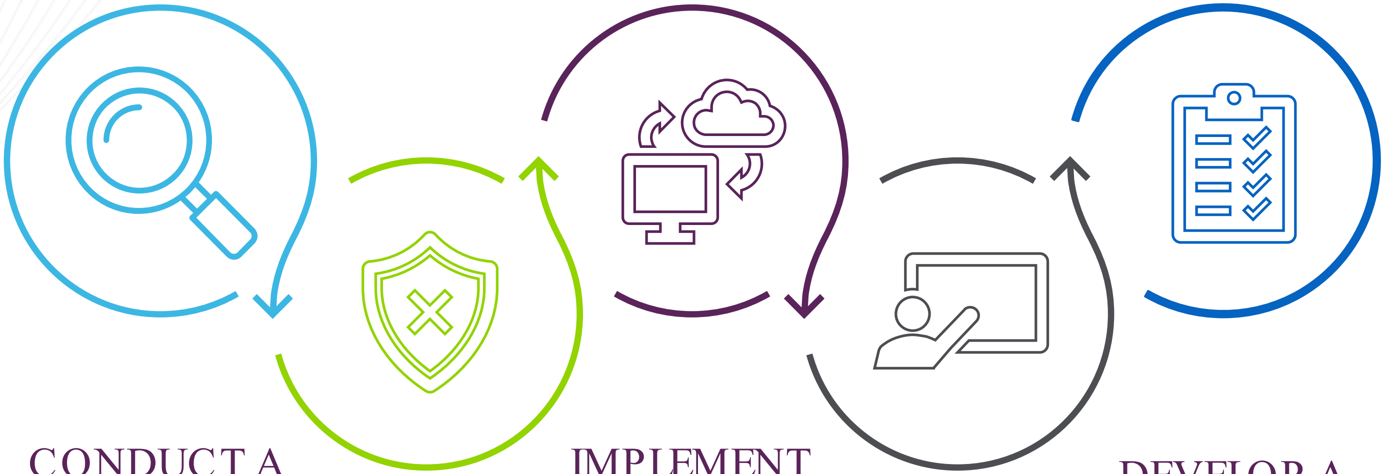
- Outdated software
- Inadequate backups

Lack of staff education

- Incident reporting & response
- Security awareness, phishing

So, what's a practice to do…

5 Step Practice Action Plan



CONDUCT A SECURITY RISK ANALYSIS

DEVELOP A RISK MANAGEMENT PLAN

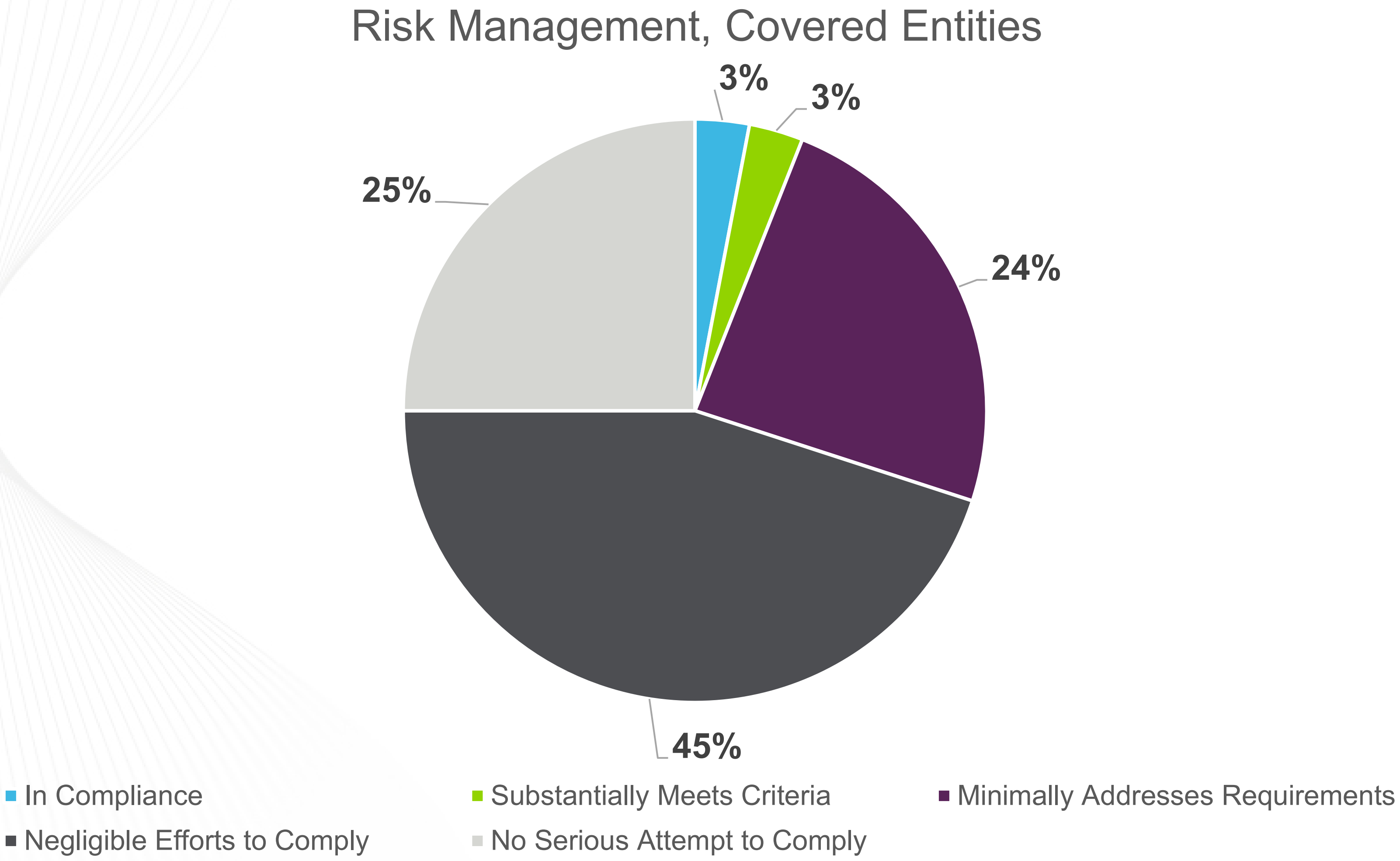
IMPLEMENT SECURITY TECHNOLOGIES

EDUCATE YOUR WORKFORCE

DEVELOP A RESPONSE PLAN

Cybersecurity Protection Begins with SRA

OCR Audit Results



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

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

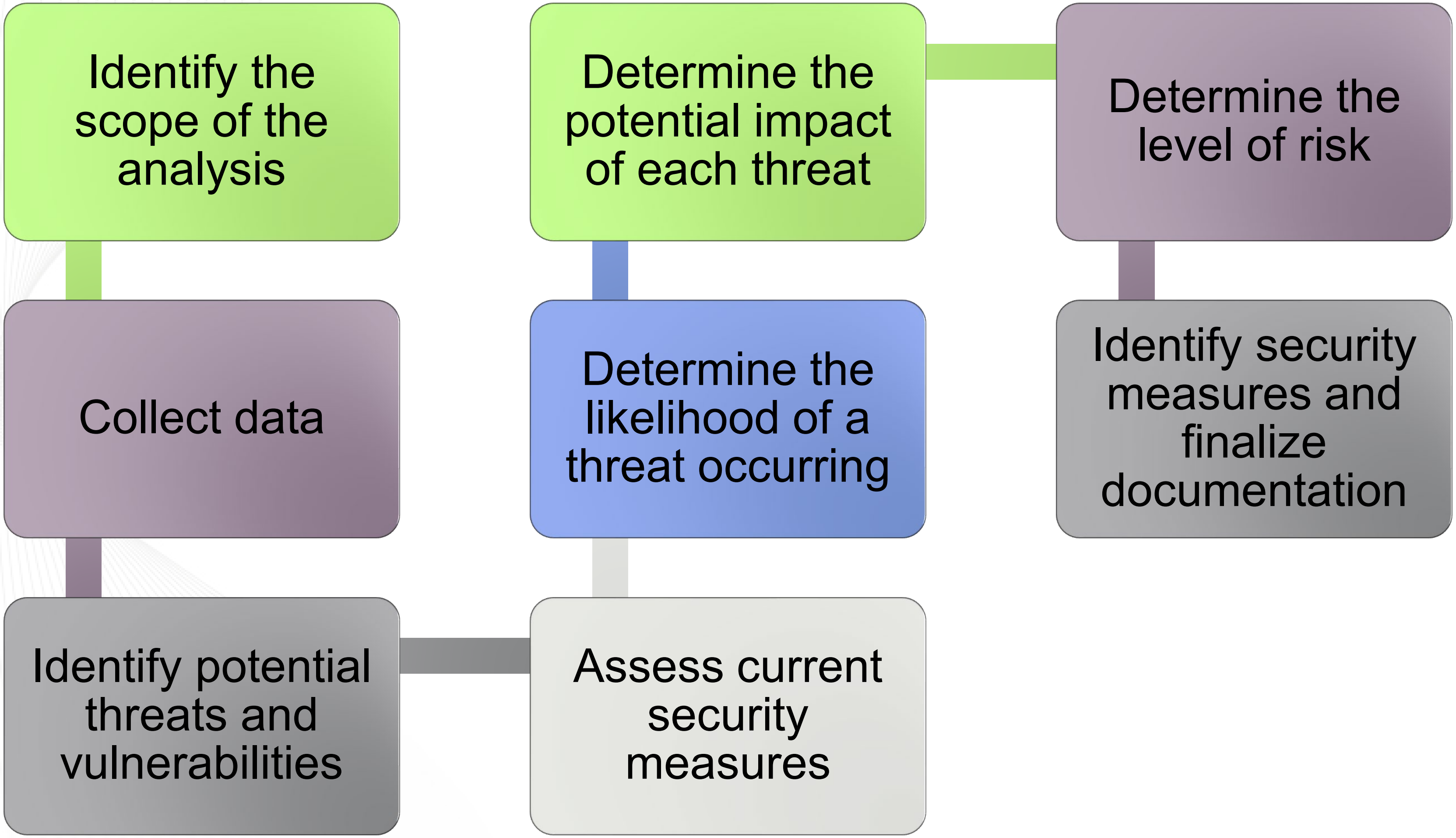
Scalable, but must be enterprise-wide

No required methodology, but guidance is provided

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.

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

Common Threats

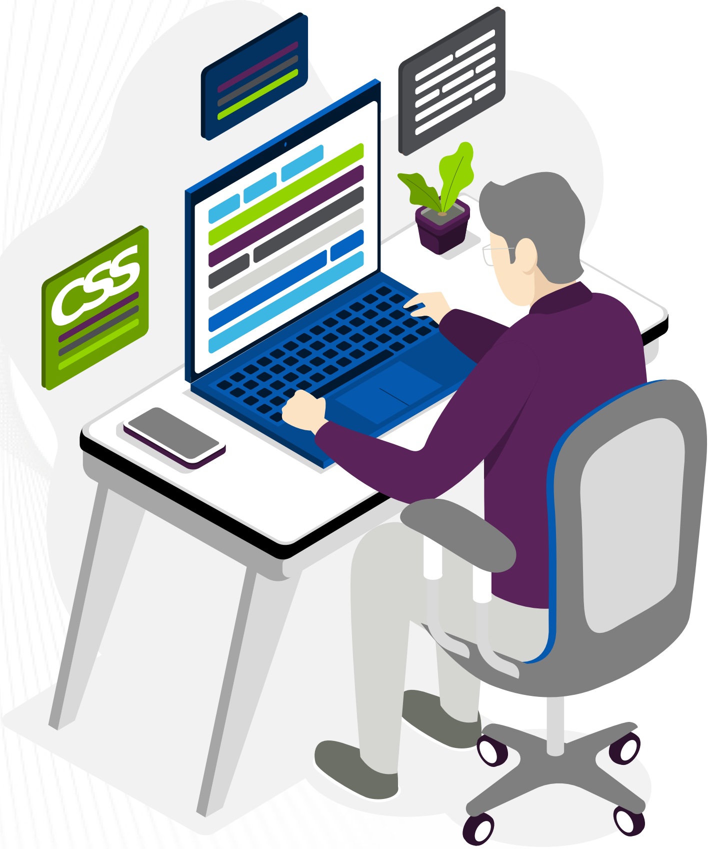
- Hacking
- Misuse
- Power loss
- Social engineering
- System errors
- Theft
- Malware
- Natural events

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



Phishing

- Staff awareness training
- IT resources & software to scan for malicious content & emails
- Sender domain & validation tools

Ransomware

- System backups & testing
- Malware detection & remediations tools
- Unpatched software

Devices

- Asset inventory & control
- Physical security
- Encryption

Assess Current Security Measures

Technical

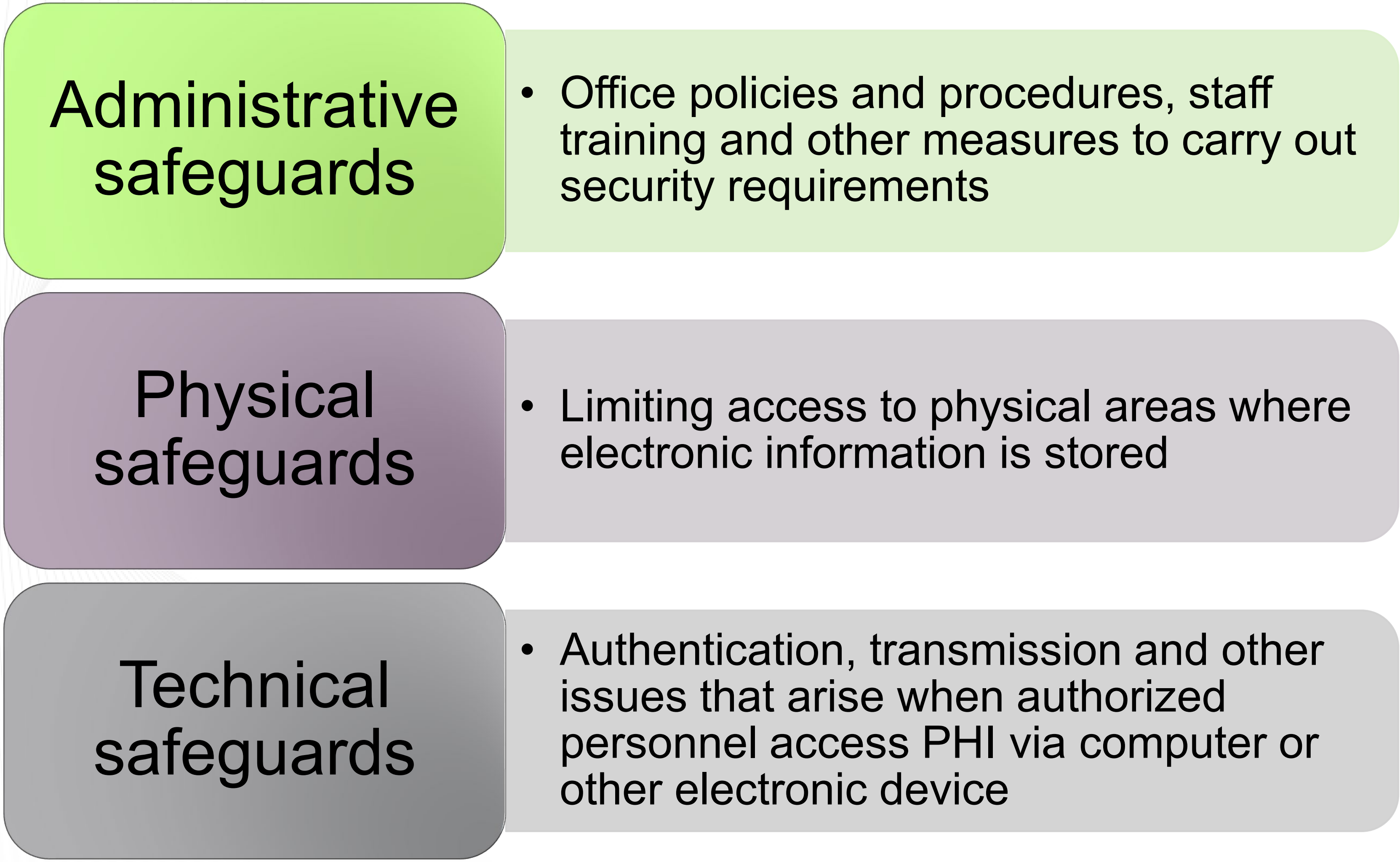
- Access controls
- Automatic logoff
- Encryption

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 Threat Likelihood & Impact

Threat
Asset
Vulnerability
Risk

Threat level

- Low - unlikely or rarely ever to occur
- Medium - could potentially occur
- High - most likely occur

Impact to confidentiality, availability and/or integrity of ePHI:

- Unauthorized access or disclosure
- Permanent loss or corruption
- Temporary loss or unavailability
- Loss of physical assets

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

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

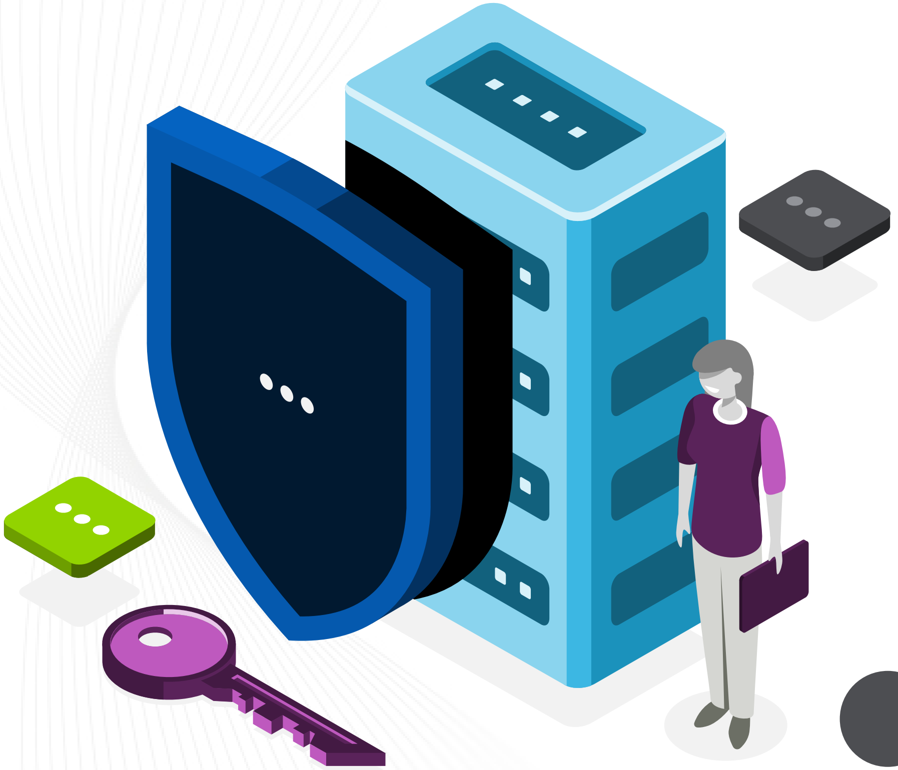
Documentation

- 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

Security Measures



- Two-factor authentication
- Offline backups
- Next generation anti-virus
- Spam filtering
- Phish training

Ongoing Process

Security measures must be reviewed & modified as needed

No timeline specified by the Security Rule, BUT…

- New technology
- Operational changes
- Personnel changes
- Existing security measures become obsolete

Review & update in response to environmental changes

MIPS & other programs may require annual assessment

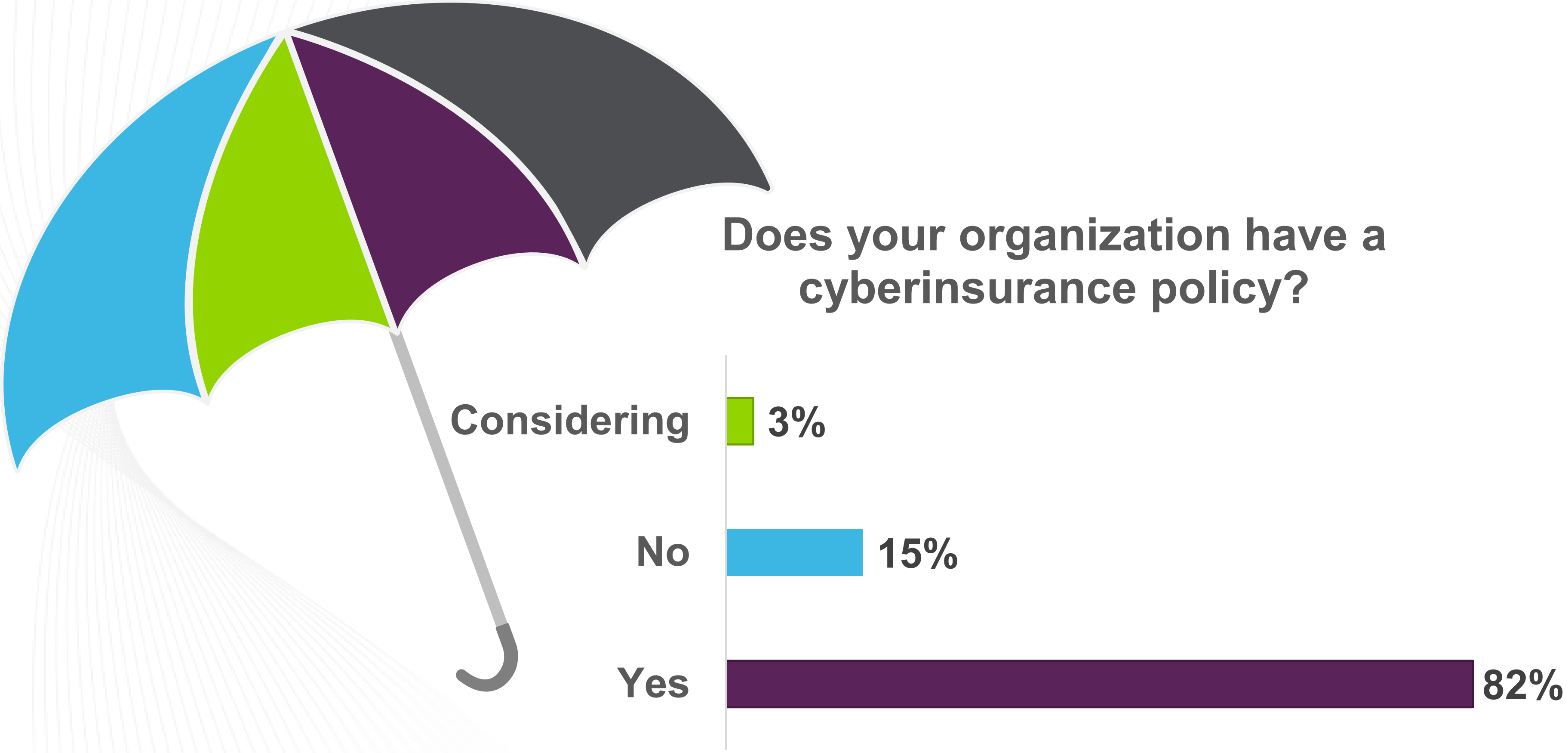
Staff Education & Training

- HIPAA & privacy
- Policies
- Phishing emails
- Breach reporting & response
- Limit access

Incident Response Plan

- **Keep it simple**
- **Define a security incident**
- **Identify who is to be notified**
- **Assemble an incident response team**
- **Identify external resources**
- **Determine documentation & reporting requirements**

Are You Protected



Does your organization have a cyberinsurance policy?

MGMA Stat 05.25.21, 810 responses

Insurance Is A Tool, NOT the Answer

Increasing premiums

Reducing limits

Implementing deductibles, coinsurance & exclusions

Requiring underwriting analysis

Cyber Incident Coverage

If the worst happens…

Know your policy

- Too good to be true pricing may have exclusions

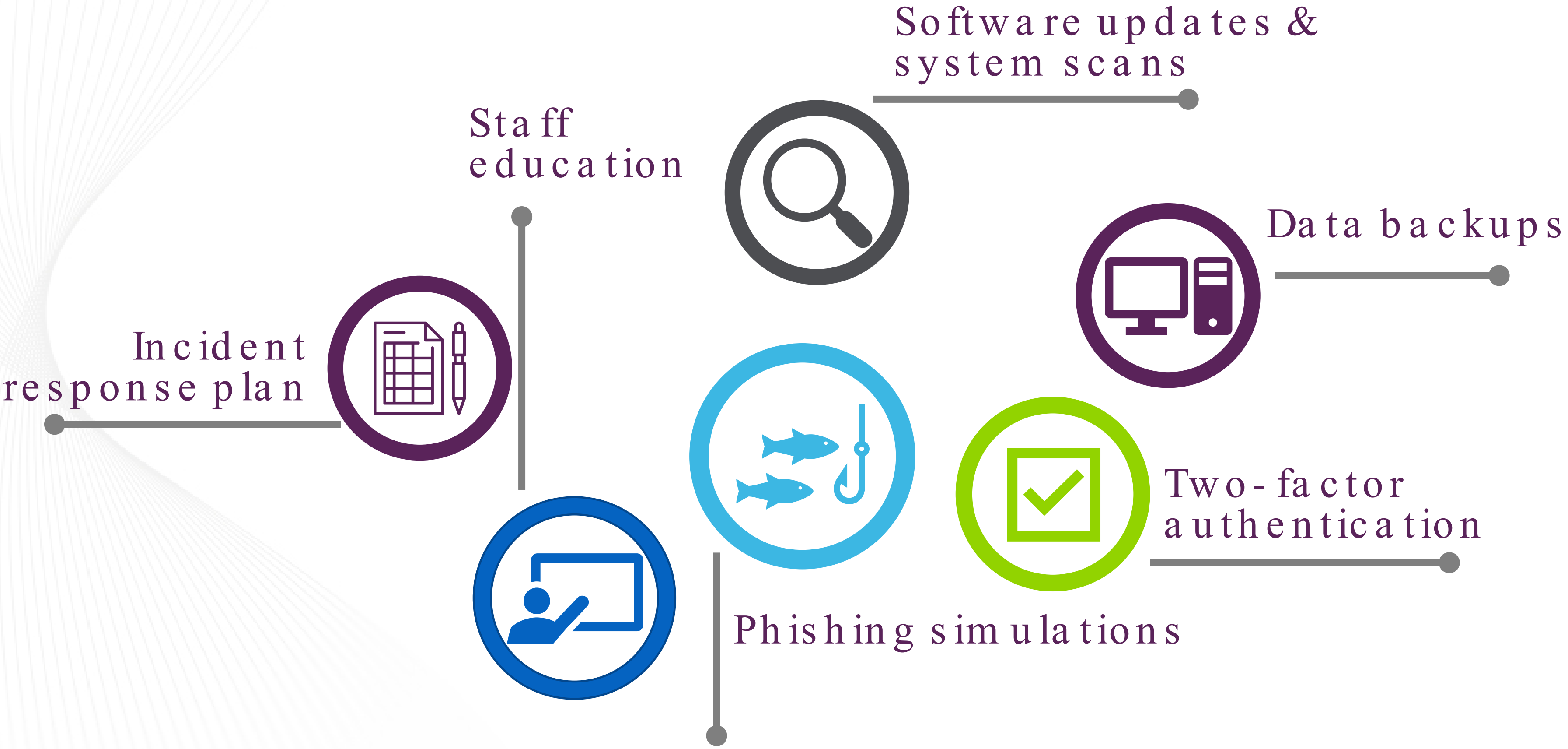
Ensure adequate limits

- If you are not undergoing an underwriting process, you probably do not have enough

Take advantage of education & resources

- There should be free online education, system scans, resources, checklists, etc. available

Practice Plan Key Elements



Incident response plan

Staff education

Software updates & system scans

Phishing simulations

Two-factor authentication

Data backups

Stephen A. Dickens, JD, FACMPE
Vice President
Medical Practice Services
steved@svmic.com

SVMIC®

Additional Resources

HHS Security Rule Guidance Materials

HealthIT.gov Security Risk Assessment Tool

HealthIT.gov Security Risk Assessment Videos

https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-videos

HHS Office of Civil Rights Hacking & Ransomware Resources

HHS Resources on Section 405(d) of the Cybersecurity Act of 2015:
•Health Industry Cybersecurity Practices: Managing Threats and Protecting Patientshttps://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
•Cybersecurity Reports and Tools
https://www.phe.gov/Preparedness/planning/405d/Pages/reportandtools.aspx
OCR Guidance:
•Ransomware https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
•Cybersecurity
https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
•Risk Analysis
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
HHS Security Risk Assessment Tool:
•https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
CISA Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches:
•https://www.cisa.gov/stopransomware
•https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf
CISA Ransomware Guide:
•https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf
FBI Ransomware Resources:
•https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
•https://www.ic3.gov/Media/Y2019/PSA191002