An MSP's Guide to the Healthcare Industry

STEVE RUTKOVITZ
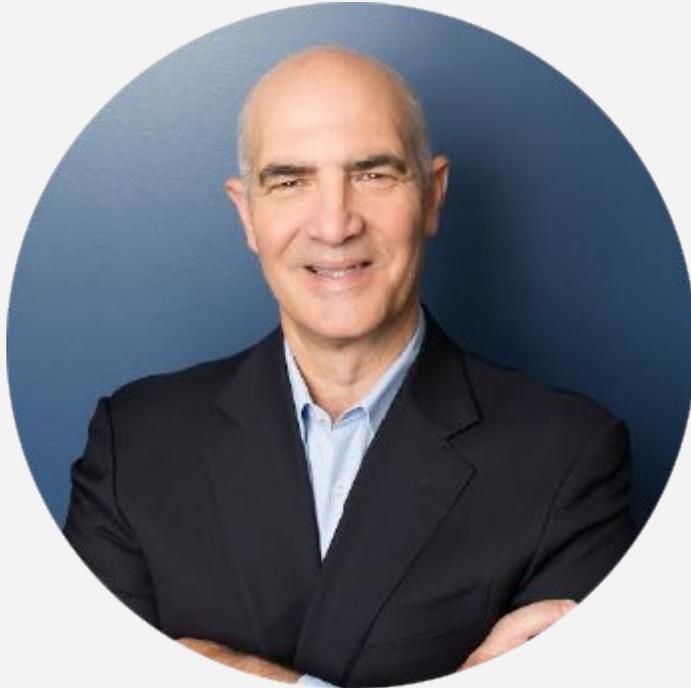
ABOUT STEVE RUTKOVITZ

For over 20 years, Steve owned and operated a very successful MSP business. With a clear understanding of the market needs, he developed an innovative IT and business process.

STEVE'S SKILLS

Security and Compliance

Risk Assessments

Educating

Management

PRESIDENT & CEO

CHOICE CYBERSECURITY

Expertise

Assess Address Maintain

Suite of Products and Services

MRR

Having been in the MSP industry, we understand the marketplace and its needs.

Our proven three step process has helped MSPs improve client relationships and increase MRR.

With a robust suite of products and services, you can put your clients' security and compliance worries at ease.

With minimal changes to your current offerings, MSPs can increase revenue by at least 40%.

THE VERTICAL WEBINAR SERIES

WHY FOCUS ON VERTICALS?

Each month, we will explore one vertical per month regarding security and compliance.

Our goal is to empower you to approach your customers in certain verticals with confidence.

A deeper understanding of a vertical industry offers:

- Subject matter expertise
- Trusted relationships
- Separation from the competition
- More opportunities for recurring revenue

Get paid for what you know—not what you do!

HEALTHCARE VERTICAL

- Healthcare accounts for **17.5%** of gross domestic product
- Americans spend about **$9,523 per person** on healthcare per year
- Total healthcare employment (2015): **12.4 million workers**
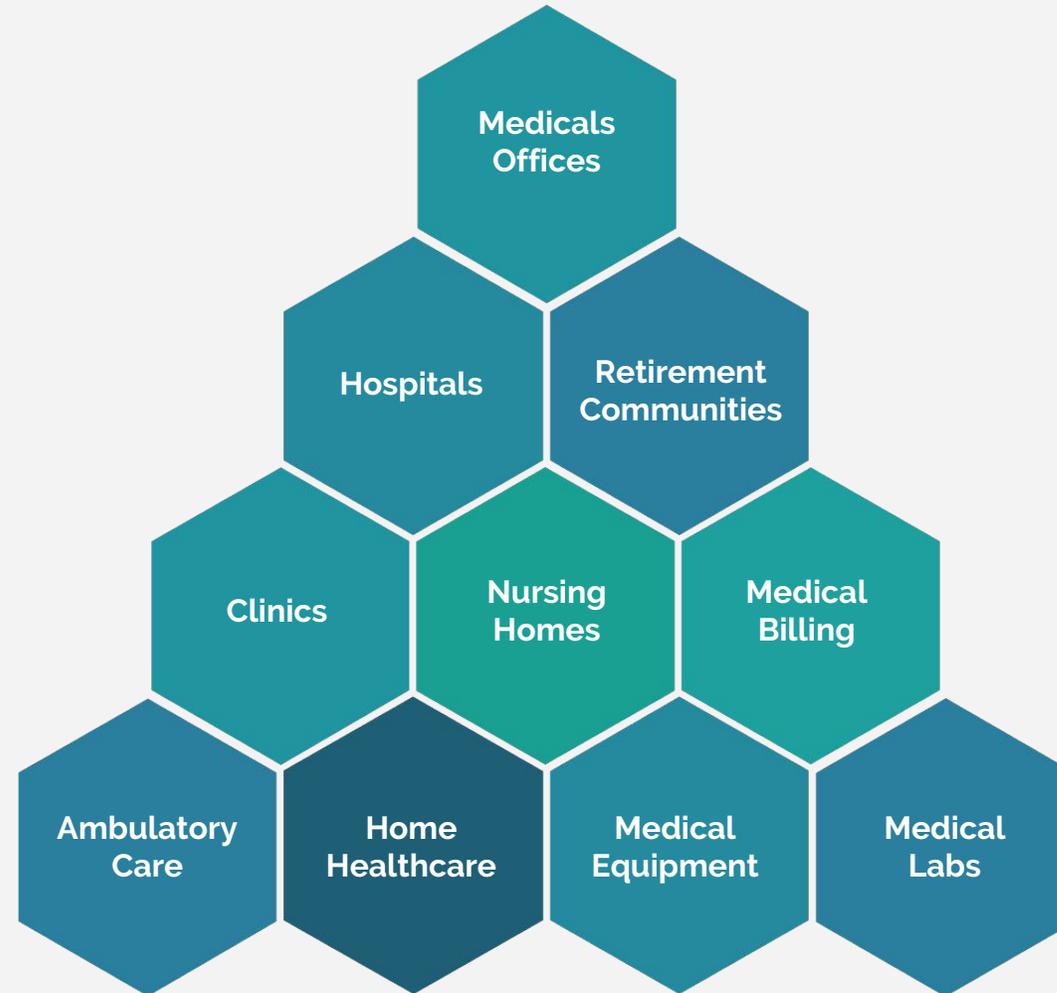
HEALTHCARE VERTICAL

1 **Covered Entity (CE)**
- Health plans, healthcare clearinghouses, and healthcare providers

2 **Business Associate (BA)**
- Person or entity that works with PHI on behalf of a CE (medical billing)

3 **Personally Identifiable Information (PII)**
- Data to identify a specific person

4 **Electronic Protected Health Info (ePHI)**
- Protected health information stored electronically

5 **Electronic Medical Records (EMR)**
- Digital version of a patient's medical records

6 **Electronic Health Record (EHR)**
- Digital version of a patient's overall health

HEALTHCARE IT HISTORY

2000
HIPAA electronic billing

2013
Omnibus Rule

2009
EMR Meaningful Use

2018
MIPS
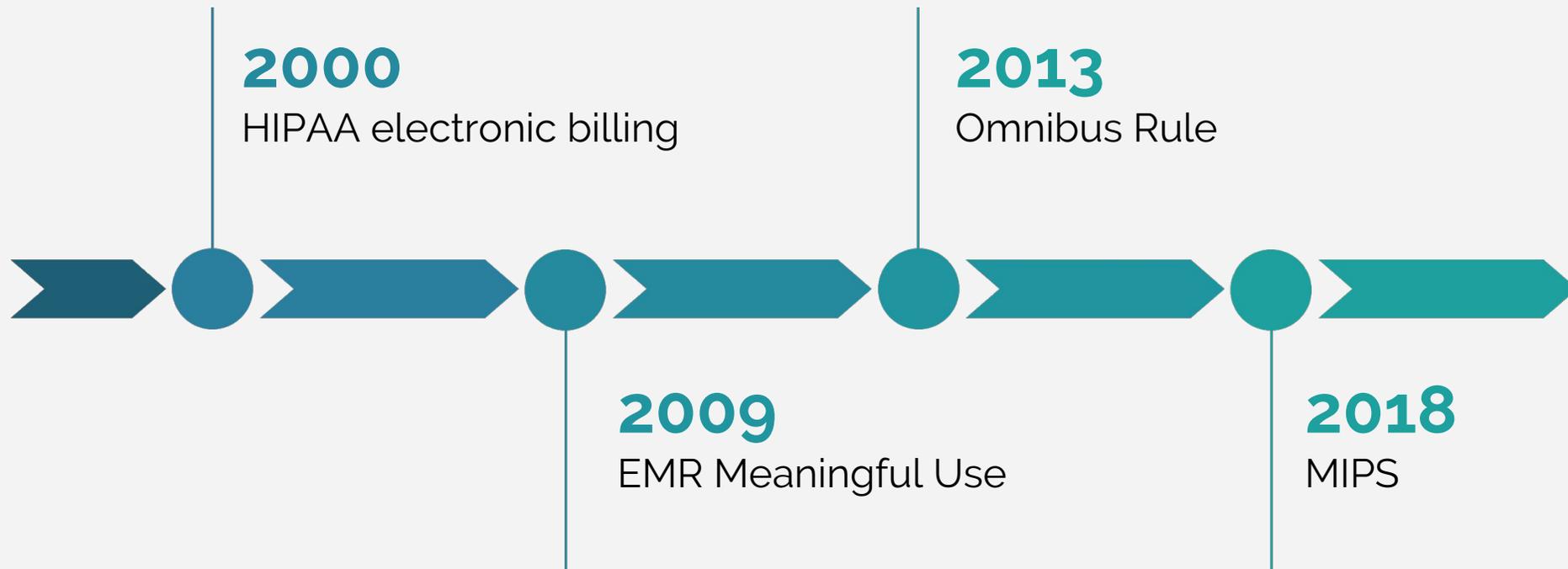
THE DIGITAL HEALTHCARE ROADMAP

ASSESS   ADDRESS   MAINTAIN

EHR
- Billing
- Electronic patient records

Patient Portal

Electronic Highway
- Information highway
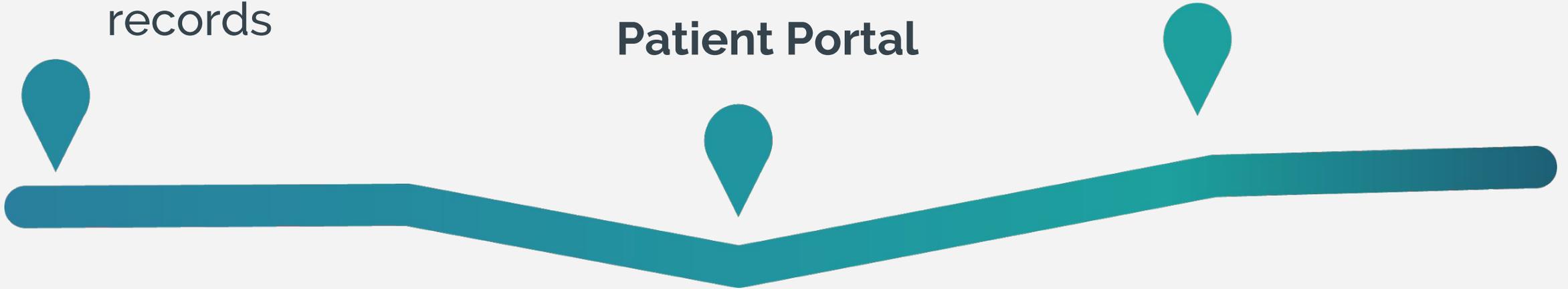
COMPLIANCES

PCI   **HIPAA**   **State PII Laws**   **PIPEDA**

PENALTIES

$50,000 per violation

- 1,000 records = $50M
- Capped at $1.5M for identical violations during a calendar year

- By patient record
- Safe Harbor rules

PENALTIES

Breach Report Results

| Expand All	Name of Covered Entity ⬍	State ⬍	Covered Entity Type ⬍	Individuals Affected ⬍	Breach Submission Date ⬍	Type of Breach	Location of Breached Information
●	Partners HealthCare System, Inc.	MA	Healthcare Provider	2450	02/05/2018	Hacking/IT Incident	Desktop Computer
●	City of Detroit	MI	Healthcare Provider	544	02/05/2018	Loss	Other Portable Electronic Device
●	Eastern Maine Medical Center	ME	Healthcare Provider	660	02/02/2018	Theft	Other Portable Electronic Device
●	Forrest General Hospital	MS	Healthcare Provider	1670	02/01/2018	Hacking/IT Incident	Email
●	Steven Yang, D.D.S., INC.	CA	Healthcare Provider	3202	01/26/2018	Theft	Laptop
●	Decatur County General Hospital	TN	Healthcare Provider	24000	01/26/2018	Hacking/IT Incident	Network Server
●	Rocky Mountain Women's Health Center, Inc.	UT	Healthcare Provider	1166	01/25/2018	Improper Disposal	Paper/Films
●	Zachary E. Adkins, DDS	NM	Healthcare Provider	3677	01/25/2018	Theft	Other Portable Electronic Device
●	Central States Southeast and Southwest Areas Health and Welfare Fund	IL	Health Plan	634	01/23/2018	Unauthorized Access/Disclosure	Paper/Films
●	RGH Enterprises, Inc.	OH	Healthcare Provider	4586	01/22/2018	Unauthorized Access/Disclosure	Paper/Films
●	Robert Smith DMD, PC	TN	Healthcare Provider	1500	01/22/2018	Hacking/IT Incident	Network Server
●	Westminster Ingleside King Farm Presbyterian Retirement Communities, Inc.	MD	Healthcare Provider	5228	01/19/2018	Hacking/IT Incident	Desktop Computer, Network Server
●	The Pediatric Endocrinology and Diabetes Specialists	NV	Healthcare Provider	1021	01/18/2018	Hacking/IT Incident	Desktop Computer, Electronic Medical Record, Laptop
●	Gillette Medical Imaging	WY	Healthcare Provider	4476	01/18/2018	Unauthorized Access/Disclosure	Paper/Films

DRIVERS

Meaningful Use

MIPS: 25% Risk Assessment HIPAA

$30,000 per year in medicare and or 100 medicare patients per year

OCR/HHS

RIsk Assessment form needs to be turned in annually

-

HIPAA
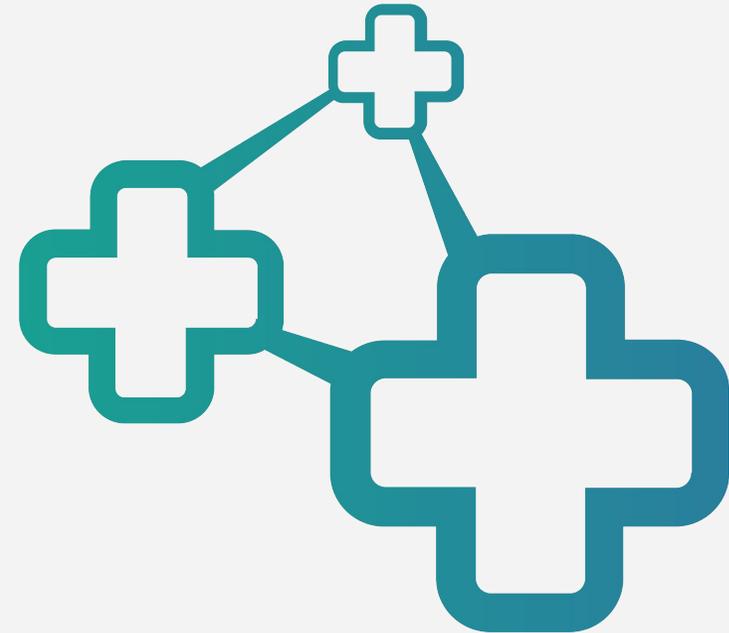
Annual risk assessment

Awareness training

Vulnerability scanning

Auditing and Logging

Encryption

Polices

WHO TO TALK TO

IT department?

Practice manager?

Officer manager?

Physician?

?
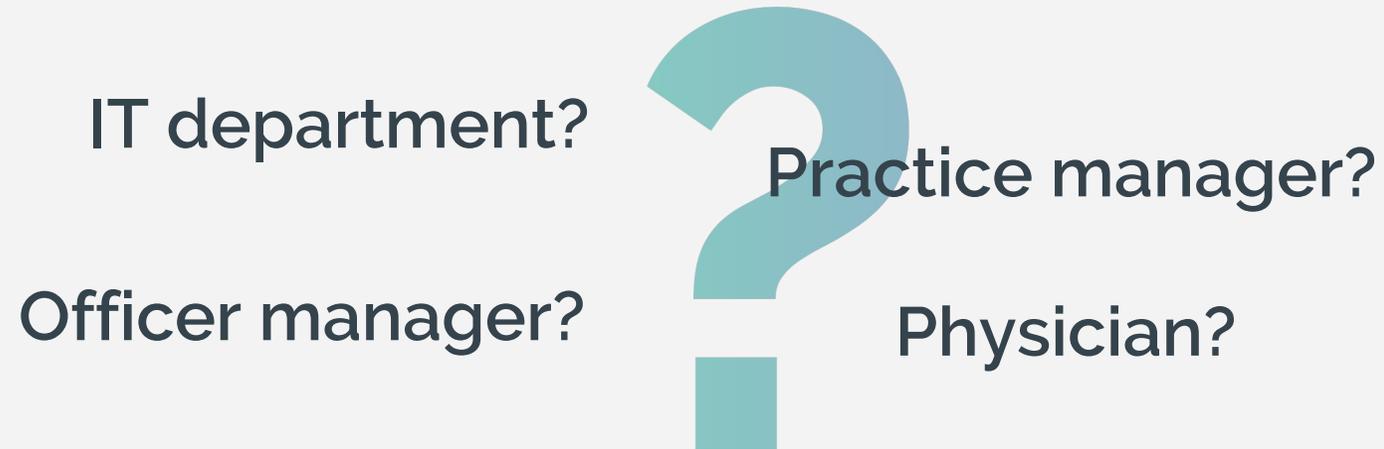
ANSWER

The Asset Owner

AUDITS

PRE-AUDIT

- Be audit ready at all times
- Collect appropriate documentation
- The more prepared you are, the less they bother you
- But the less prepared you are, the more they dig

POST-AUDIT

- Will provide you with list of "things" to fix
- Contract with organizations to fix issues
- Ensure you are up-to-date on recommended and required fixes

ASSESS   **ADDRESS**   **MAINTAIN**

RISK ASSESSMENTS

- Build a Baseline
- Uncover Gaps and Risks
- Expose Vulnerabilities
- Analyze Layers of Defense
- Identify Sensitive Data
- Missing Controls and Policies

ASSESS

RISK ASSESSMENTS

INITIAL RISK ASSESSMENT

**ANNUAL ASSESSMENT**

Who should perform the assessments?

Independent Contractors

MSPs

GOAL OF THE RISK ASSESSMENT
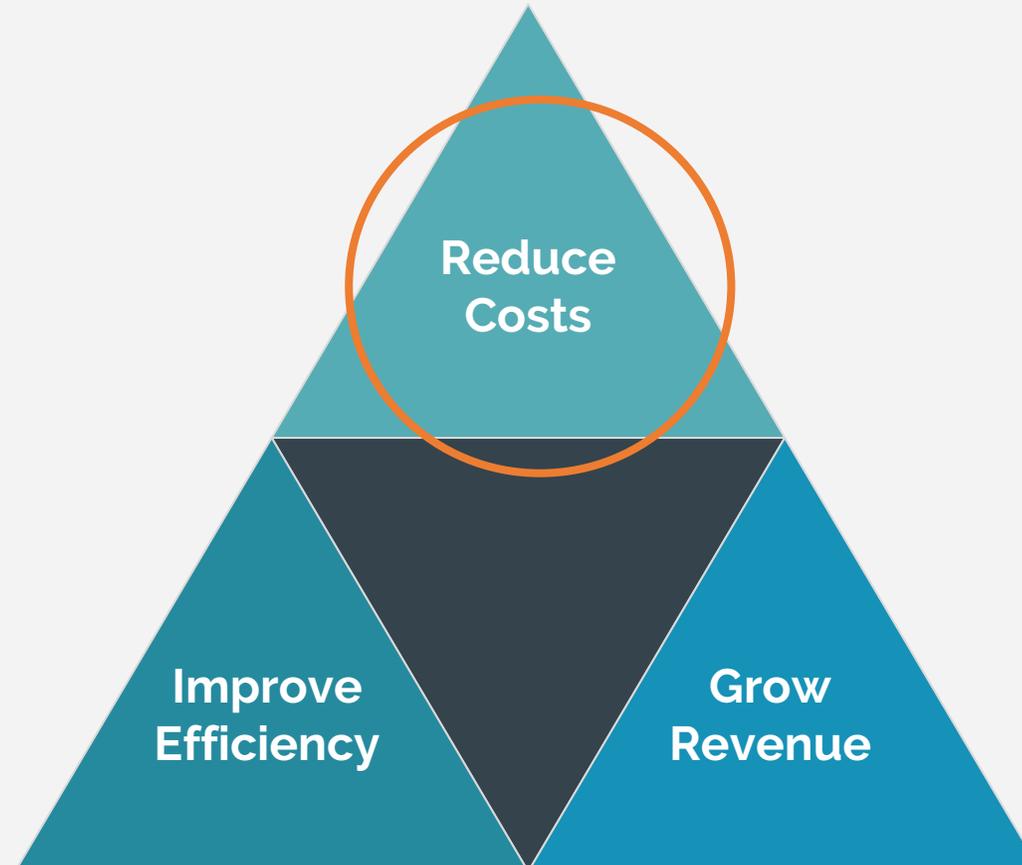
PII SCAN RESULTS

Total Liability: **$38.7 Million**

| **1,195** Credit Cards | **119,303** Social Security Numbers | **72,226** Date of Births | **19** Drivers Licenses |

HIPAA POLICIES GAP ANALYSIS

ASSESS   ADDRESS   MAINTAIN

Personally Sensitive Data Definition	Monitoring and Logging Operations	Access Controls and Logging	Organizational Policy and Process Documentation	Facility Management	Protection from Malicious Code
IT Asset Physical Security	Transmission Security	Uses and Disclosure of PHI with a Valid Authorization	Notice of Privacy Practices	Individual Rights to Uses and disclosure of PII	Encryption and Decryption
Disclosure Authorization	Physical and Environmental Security	Minimum Necessary and Limited Data Set of PHI	Amendment of PHI	Uses & Disclosure of ePHI General Rules	Incident Response and Disaster Recovery
HIPAA Privacy and Security Awareness Training	Contingency Plan	Business Associate Agreements	Individual Rights to PHI	Designating a HIPAA Privacy and Security Official	Social Media Policy
Complaints and Prevention of Retaliatory Acts	Sanctions	Risk Analysis and Management	HIPAA Terms and Definitions	Password Management	Mobile Device & Teleworking

BRING CLIENTS UP TO AN ACCEPTABLE LEVEL OF RISK

- Executive Summary

- Create New Projects

- Layers of Security 1.0 to 2.0

- Meet Client Compliances

- Action Plan/ Next Steps

- Best Practices

ADDRESS

CREATING NEW PROJECTS

SIEM

Encryption

Web Filtering

Mobile Device Management

Policy Development

Managed Firewall

Data Leak Prevention

Awareness Training

Remediation and Clean Up

Threat Detection

File Archiving
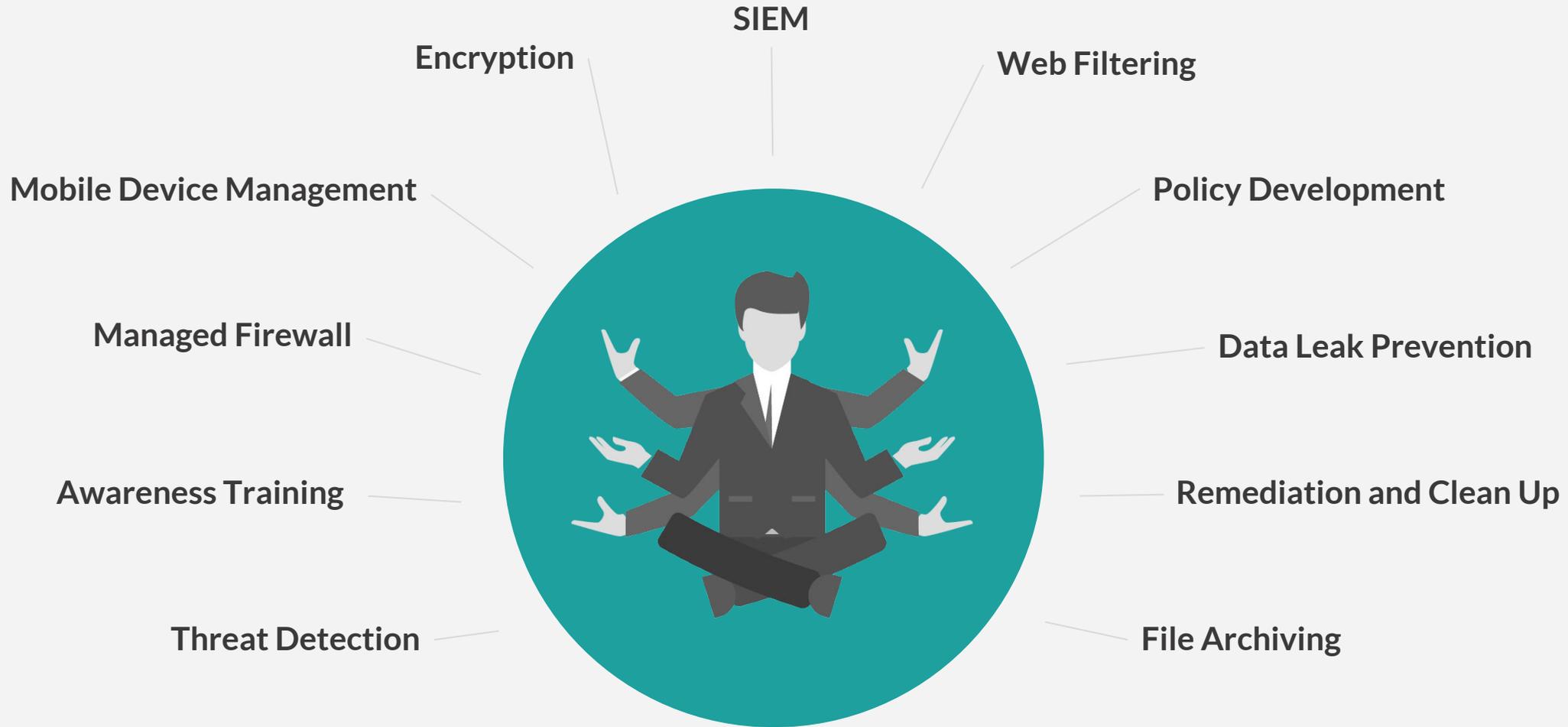
MAINTAIN AN ACCEPTABLE LEVEL OF RISK

- Monthly Recurring Revenue
- Continuous Alerting and Monitoring
- Comparison Reporting
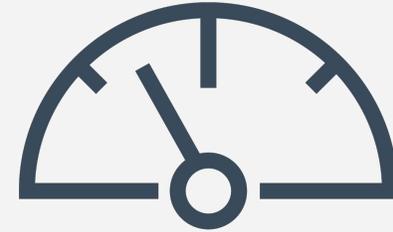
MAINTAIN

RECURRING REVENUE

Security as a Service

Vulnerability as a Service

Compliance as a Service

Dark Web & Credential Monitoring

SIEM Auditing and Logging

Awareness Training

Risk Assessments

NEXT STEPS
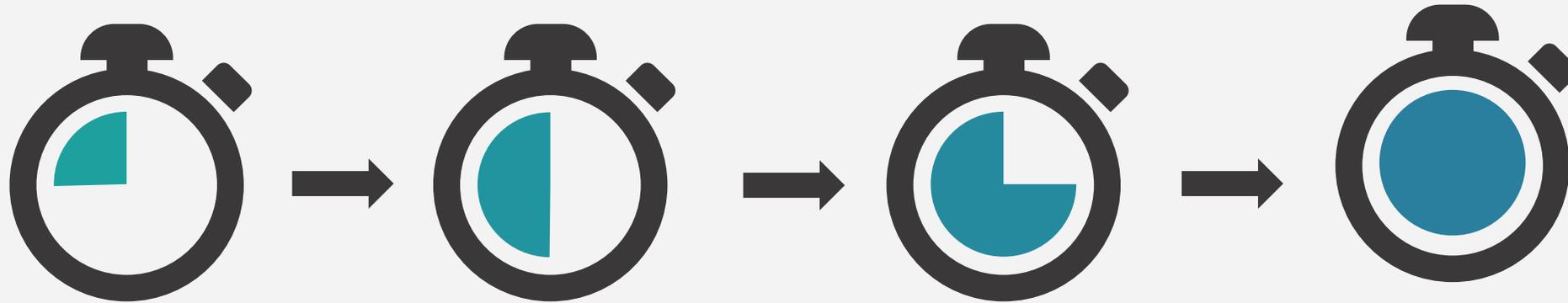
CONTACT US

Discover how to grow your business

CHOOSE THREE CLIENTS

Pick healthcare clients that needs security and compliance services

DEVELOP A STRATEGY

Create a strategy for approaching the client

PRESENT TO CLIENT

Present the risk assessment to your client

THANK YOU FOR ATTENDING

ASSESS   ADDRESS   MAINTAIN

CONNECT WITH US

If you're ready to expand your offerings and increase your monthly recurring revenue, let's start with a conversation.

10055 Red Run Blvd, Suite 140
Owings Mills, MD 21117

info@choicecybersecurity.com

+1 (410) 205-4980

choicecybersecurity.com

resources.choicecybersecurity.com

PRESIDENT & CEO