WOLF
& COMPANY, P.C.

CEO Roundtable

Information Security Threats

August 6, 2019

About Wolf & Company, P.C.

Established in 1911

Offers Audit, Tax, and Risk Management services

Offices located in:

- Boston, Massachusetts
- Springfield, Massachusetts
- Albany, NY
- Livingston, NJ

Over 230 professionals

As a leading regional firm founded in 1911, we provide our clients with specialized industry expertise and responsive service.

IT Assurance Services

Wolf's IT Assurance professionals have detailed knowledge of business operations and technologies.

- IT Audits
- Network Vulnerability Assessments
- Penetration Testing
- Social Engineering Assessments
- Cloud Security Reviews
- Security Framework Assessments
- SSAE16 & SOC Audits
- HITRUST Certifications
- PCI Compliance Attestations
- Business Continuity Planning (BCP)
- Incident Response Planning (IRP)
- Policy & Procedure Development

vCISO Advisory Services

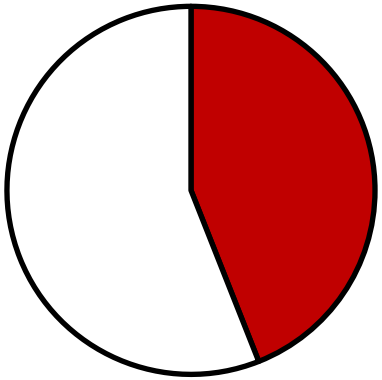
Today's Agenda

Introductions

Information security focus areas

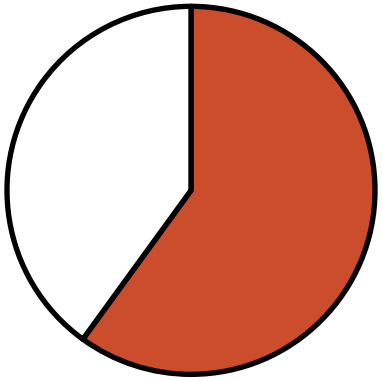
Summary / Q&A

We're On This… Right?



44% of security breaches are the result of known, unpatched vulnerabilities

- I.e. occur after vulnerabilities and solutions have been identified



60% of IT executives say their Security and Ops teams have little understanding of each other's requirements

What Will A Breach Cost ?

Smaller organizations have higher costs relative to their size than larger organizations. The total cost for organizations with more than 25,000 employees averages $204 per employee.

Organizations with between 500 and 1,000 employees have an average cost of $3,533 per employee.

$204

per employee

Breach costs at organizations with more than 25,000 employees averages $204 per employee.

$3,533

per employee

Breach costs at organizations with between 500 and 1,000 employees have an average cost of $3,533 per employee.

Source: 2019 Ponemon Cost of a Data Breach Report

Risk Assessment

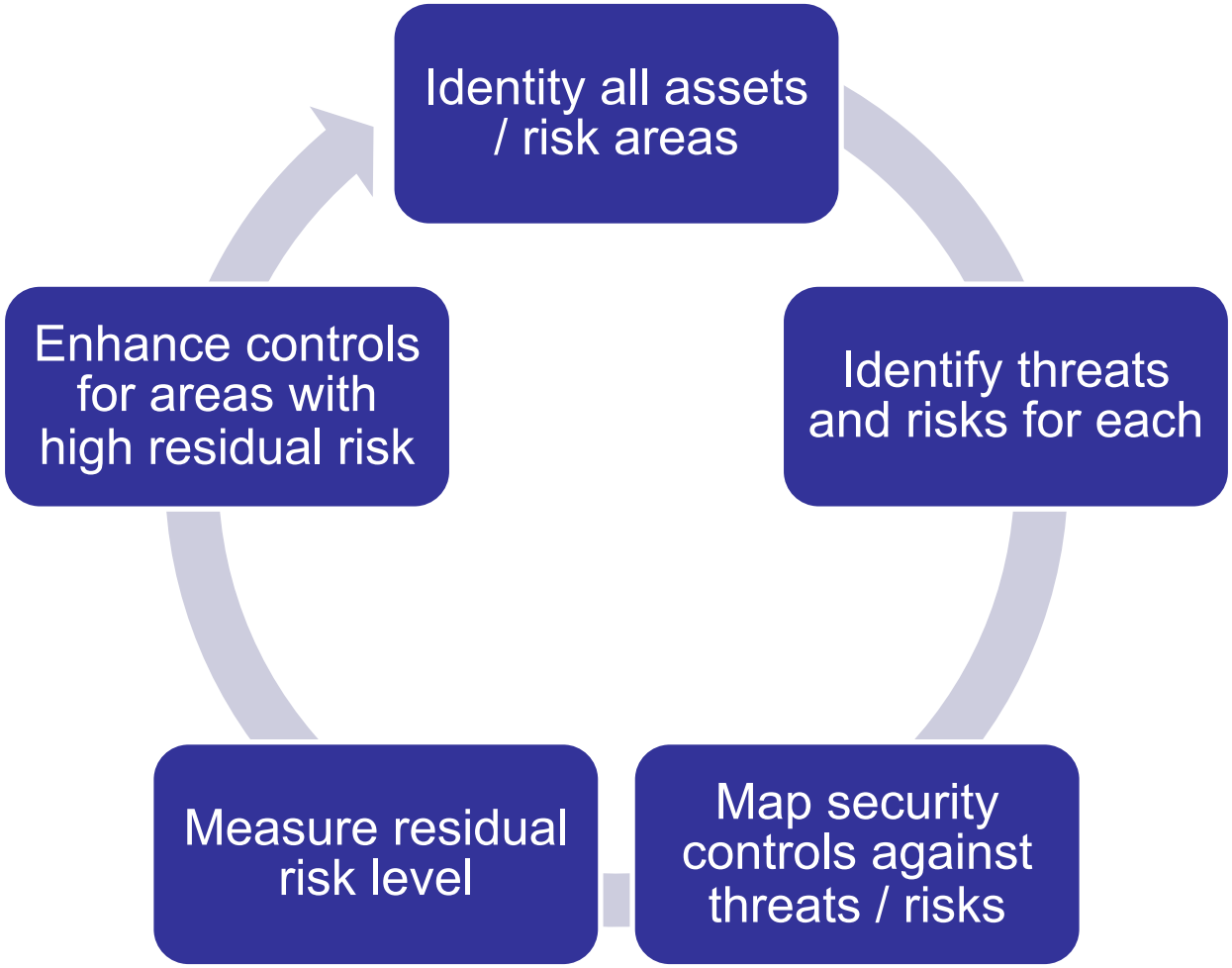
Foundation of any security program

Do you know everything you have? Do you know what you need to protect? Are you sure?

Basis for all risk and control decisions

Define your **inventory of assets, risks, and controls**, and their interrelationships

Risk Assessment



Social Engineering

Targets **people** rather than **systems**

Attackers often attempt to exploit a person's desire to be helpful

Threats may be disguised as legitimate entities

Types of Social Engineering

Phishing

Spear phishing

Pharming

Phone calls / pretexting

Physical Entry

Baiting

Many attacks use a **COMBINATION** of technical and social engineering tactics

Patch Management

Informed by Asset Management

Validated by Vulnerability Management

ALL hardware, software, firmware, appliances, IoT devices…

- Compare against your asset inventory

Commonly neglected:

- 3rd party software
- Desktop applications (user-installed?)
- Non-server/non-workstation hardware
- Databases
- Appliances
- “Test” machines on the network

Window of Opportunity for Attackers

Vulnerabilities remain until patches are applied

"Window of Opportunity" for attackers after disclosure, before patching

Missing patches = Susceptible to known CVEs!

Vendor Management

Documented vendor management program

Vendor **risk assessment**

Selection due diligence

- Financial condition
- Qualifications, experience, and capabilities
- Internal controls and audit reports
  - SSAE16, SOC1, SOC2, SOC3
- Business continuity plans
- Reputation
- Use of subcontractors and third-parties

Vendor Management

Contract requirements specific to cloud service

- Data privacy clause
- Incident response plan (for data breach)
- Compliance with applicable regulations
- Service level agreements (SLAs)
- Reporting and right to audit
- Also include “standard” contract elements

Incident Response Planning

Assign responsibility

Write out the game plan

Identify what data you possess that would classify as a breach

List consultants and providers that can help

- Network consultants / forensic analysts
- Attorneys
- Credit monitoring services

Which government agencies will you need to notify?

Create a public notification template

Test the plan

Incident Response Focus

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements
- Recovery Planning
- Improvements
- Communications

Summary

Security and Compliance are more important than ever

Outsourcing creates a downstream effect

Fundamentals / Common Pitfalls:

- Risk Assessment
- Cyber Hygiene
- Social Engineering
- Vendor Management
- Access Control
- Incident Response

Select and implement an appropriate security framework and measure against it

About

Matt serves as the Director of Wolf's Risk Management Services Group which provides Information Technology Assurance, Internal Audit, and Compliance and Enterprise Risk Management (WolfPAC) services for our clients. Additionally, Matt provides guidance to his clients around IT controls, information security, the development and implementation of critical technology processes, and strategic technology planning.

Matt has worked in the information technology field for over 20 years. Prior to joining Wolf, he worked with a medical information technology company where he was responsible for the programming, implementation, and support of medical information systems.

Renee serves as Senior Manager, VCISO Services for Wolf, where she develops, implements, and provides VCISO services for clients. She is a senior level healthcare executive with an extensive background in information security, strategic planning, information technology, HIPAA, data interoperability, and value based care. Renee has held the role of Chief Information Security Officer and Chief Information Officer in both hospital health systems and Managed Care Organizations (MCO).

Most recently, she served as AVP of Population Health Information Technology and Strategy at UMass Memorial Health Care in Worcester, MA; she was part of the leadership team that achieved $22 million in savings for the Accountable Care Organization, and was a member of the Cyber Security Executive Committee, which provided oversite to the health system on the execution of the data security strategy.