Crowe Horwath®

Advancing Healthcare
Crowe Healthcare Summit 2017

Financial Decisions, Risk Management, and the Impact on Cybersecurity

September 20, 2017

Mike Porter
Jared Hamilton

Smart decisions. Lasting value.™

Learning Objectives

Learning Objectives

- Identify key risk factors to consider when budgeting for cybersecurity.
- Recognize potential pitfalls of investing in the wrong priorities.
- Evaluate the role insurance, finance, risk management and IT plays in managing cybersecurity costs.

Introductions

Jared Hamilton, CISSP
Senior Manager & Healthcare Cybersecurity Solutions Leader
Indianapolis, IN

Mike Porter, CISSP
Healthcare Cybersecurity Manager
San Francisco, CA

Agenda

- Discussion
- Where to Invest?
- Cyber Insurance
- Take-aways

Any other topics you would like us to touch on?

~$80 Billion

Worldwide information security spend

$3.62 Million

Average cost of a breach according to the IBM/Ponemon
“2017 Cost of Data Breach Study”

$200,000

Median cost of a breach according to a Oxford University Press
“Examining the Cost and Causes of Cyber Incidents” Study

What's the point?

It Depends…

Breach costs (on commensurate investment) varies significantly based upon the:

- Scale of the data
- Number of potential patients impacted
- Risk appetite
- Technology strategy
- Business interruption (lost or delayed)
- Regulatory fines
- Legal costs

Discussion Topic

Is your organization specifically budgeting for cybersecurity?

Discussion Topic

How do you think about ROI on cybersecurity spending?

Increasing compliance?

Preventing breaches?

Increasing patient confidence?

Reducing insurance costs?

Where to Invest?

Case Study – Windows XP Migration

- Windows XP is end of life and must be upgraded
- When IT requests financial support, message of risk is lost
- CFO is not able to see the risk and cost relationship and denies the request
- Thousands of systems are susceptible to a PREVENTABLE vulnerability now costing the organization more in downtime and malware exposure.

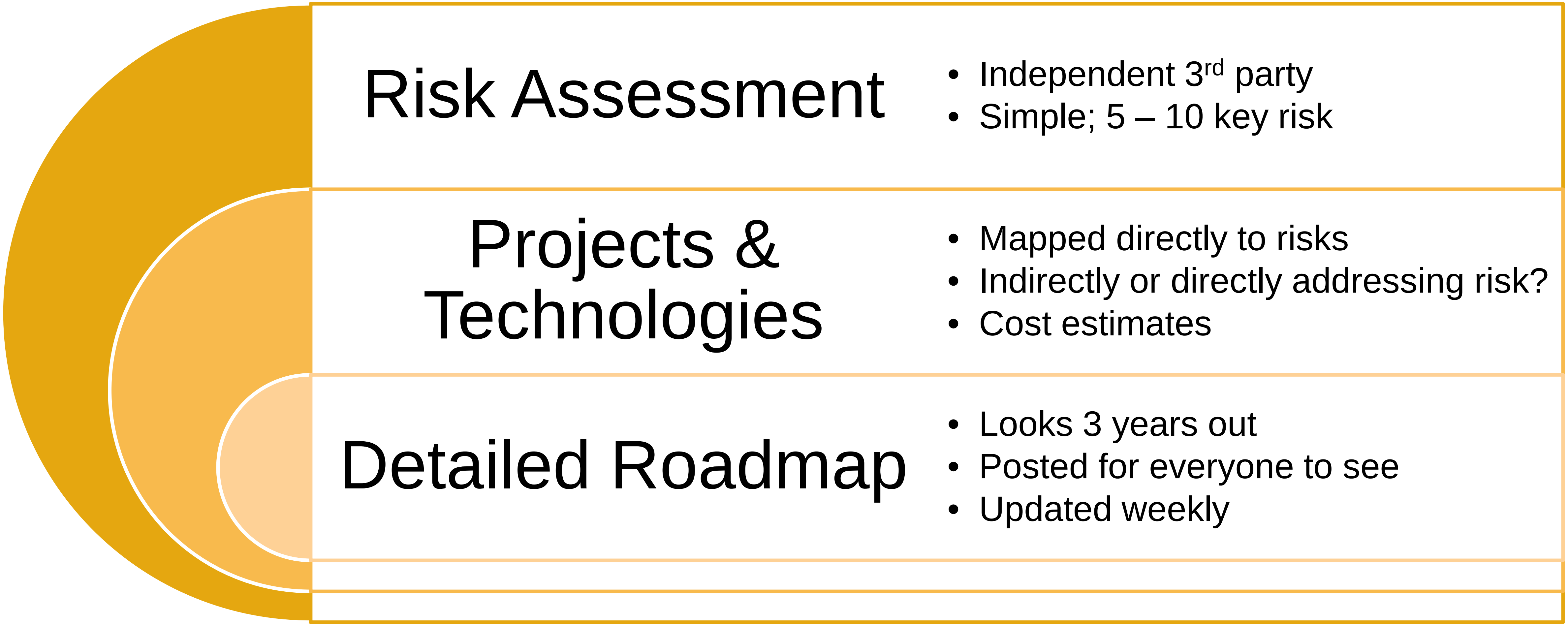
Lesson Learned: IT needs to frame risks in business terms; business needs to be savvy to help bring visibility of risk impact in financial decisions

Case Study – Doing it wrong

- Meet and Greet Setup with IT Security Officer
  - Background
  - Team
  - Projects
  - Goals

“A Goal Without a Plan is Just a Wish”

Case Study – Doing it right



Risk Assessment

- Independent 3rd party
- Simple; 5 – 10 key risk

Projects & Technologies

- Mapped directly to risks
- Indirectly or directly addressing risk?
- Cost estimates

Detailed Roadmap

- Looks 3 years out
- Posted for everyone to see
- Updated weekly

Why is it so difficult?

Risk Velocity for cybersecurity risks is high

- The time between a risk scenario occurring and the organization realizing the impact is short.

The direction for most cybersecurity risks is increasing

- This is due to heightened awareness (both internally and externally) increased threat activity, and awareness of multiple attack vectors.

There is still a lack of understanding, even amongst IT professionals, on the true impact of even ‘low’ risk systems.

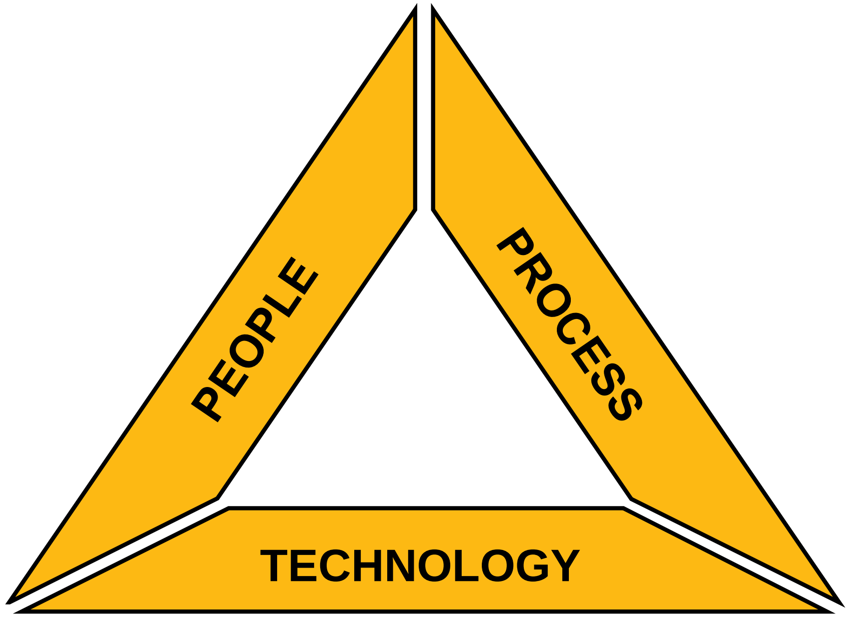
- This is often times due to the inability to understand how an attack could traverse the environment.

General Considerations for Spending

Understanding **Total Cost to Implement**

- "Cost" is often considered only for the specific software or technology product
- This does not consider "Sustainability" of the solution

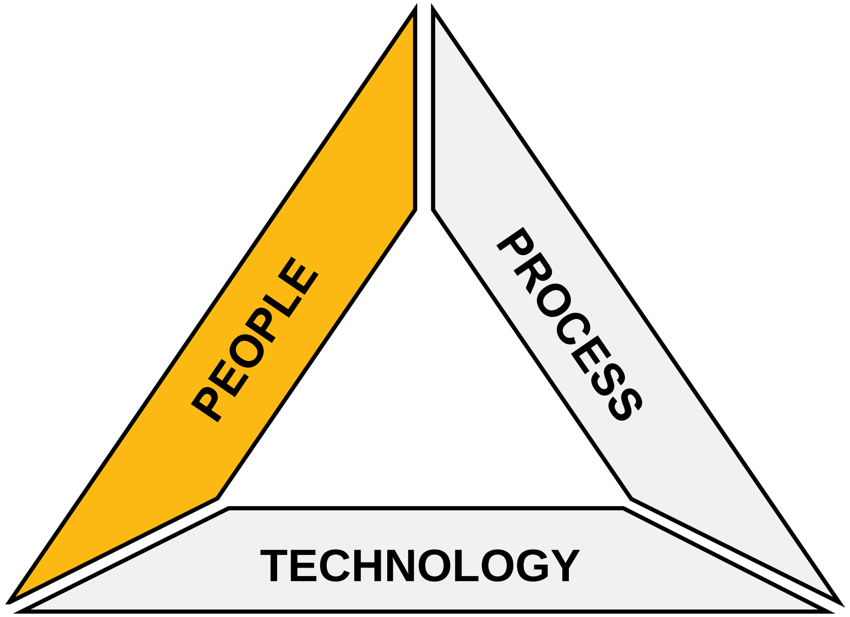
All solutions have **People, Process and Technology** components



People

In our opinion, investing in a strong team is the best predictor of a successful cybersecurity program

- Leadership: as always, messaging from the top is critical
- Build a team: easier said than done with skills gap but…
  - A good team can develop good processes and use technology effectively
  - A team has the potential to outlast any process or technology
- Know what your organization's core competencies are
  - Boost their strengths
  - Compensate for weaknesses with training or outsourcing where necessary
- Know what your organization's IT/Security core requirements to maintain internally
  - Outsource where able based on function, capability
  - Effort can result in cost-savings in people and technology pending smartly outlined strategy

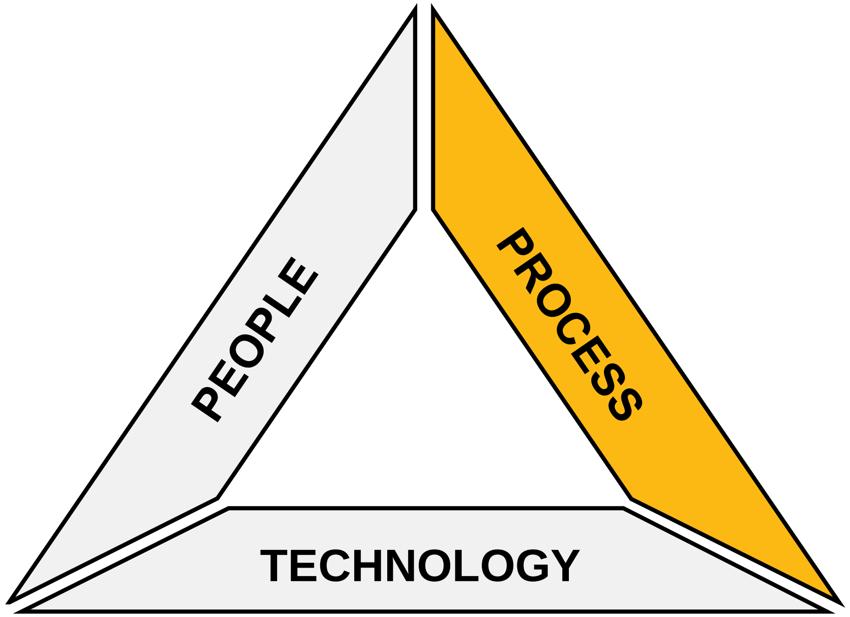


A 2016 Kapersky report estimated that the cost of a breach can be reduced by a third or more with strong IT security talent.

Process

Always consider process **before** technology

- Start with the basics…
  - Effective password policies
  - Strong account management procedures and monitoring
  - Secure configuration standards
- Effective, efficient, and well communicated processes can in some cases **negate/minimize the need for technology**
- **Policies ≠ Processes**



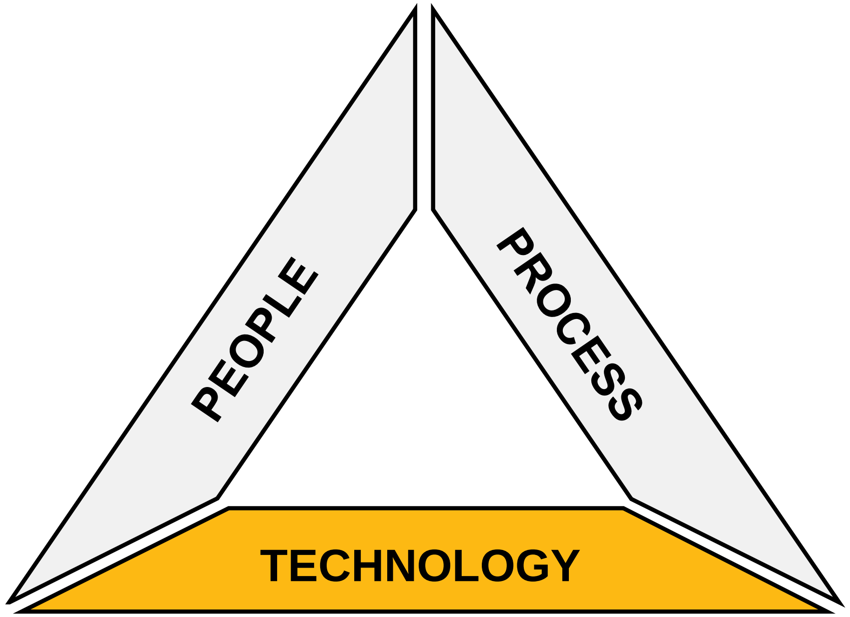
Process is highly integrated with People concerns. Effective processes bring together multiple teams:

- Clinical teams
- Audit
- Vendor management
- Risk management

Technology

Some key tips:

- First and foremost, **there are no silver bullets**
- Seek to leverage additional features and functions of your current technologies before investing in new ones
- Always consider **integration** (both in relation to processes and other technologies), technology solutions should not exist in a vacuum
- Always keep in mind **who will own and operate** new technologies
- We have often seen expensive tools go unutilized because the initial implementation was not properly planned or there is not enough staff to support
- **Do not solely rely on vendor** for implementation of new technologies, they do not know your organization like you do
- Look at **complimentary and/or enhancement capabilities** for existing technology; do not consider technology in an issue silo (one technology for one issue)



Trends in Managing Costs

Clouds Service

- More and more organizations are looking to get out of the hardware business
- Often can be more cost effective
- Also can introduce additional risk to the organization

Consider cybersecurity from the outset

- It is much more effective than trying to secure a system after implementation or after an incident occurs

Too many hats

- Security leaders often also filling operational, privacy, or compliance roles
- Can cause conflict of interests

Establish IT Risk Management Process

- Risk Assessment & Objectives
- Controls and Assessment
- Analysis and Treat Risks

Establish Scorecard with Frameworks

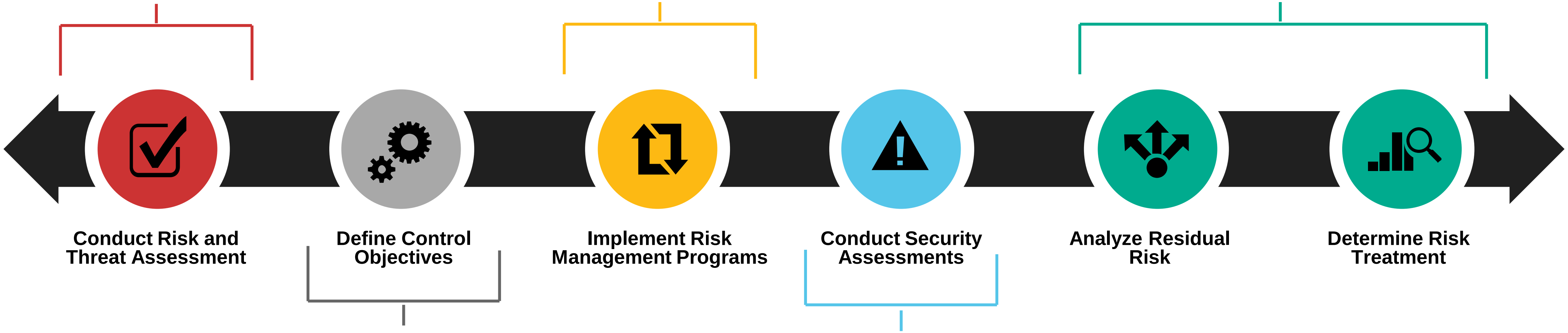
- Organize
- Report
- Measure

Understand Your IT Risk Management Processes

- Threat Likelihood and Capability
- Asset Classification
  - Technology Assets
  - Applications
  - Infrastructure
  - Endpoints
  - Third Parties

- Information Security Program
  - Data Protection
  - Threat and Vulnerability Management
  - Third Party Risk Management
  - Logging and Monitoring

- Risk Appetite and Tolerance
- Risk Treatment
  - Mitigate
  - Transfer / Share
  - Accept
  - Avoid



Conduct Risk and Threat Assessment

Define Control Objectives

Implement Risk Management Programs

Conduct Security Assessments

Analyze Residual Risk

Determine Risk Treatment

- Industry Standards
  - NIST, ISO, COBIT, etc.
- Regulatory Requirements
  - HIPAA, PCI, FFIEC, etc.

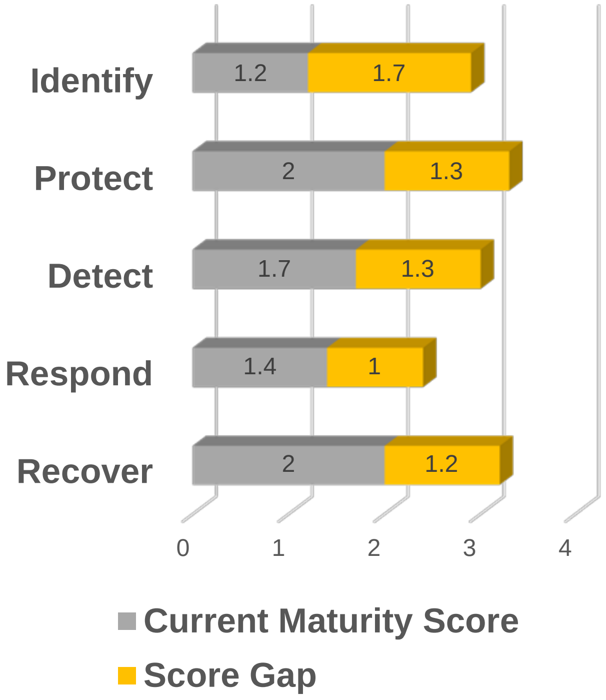
- Cybersecurity Assessment
- Penetration Testing
- Internal and External Audit

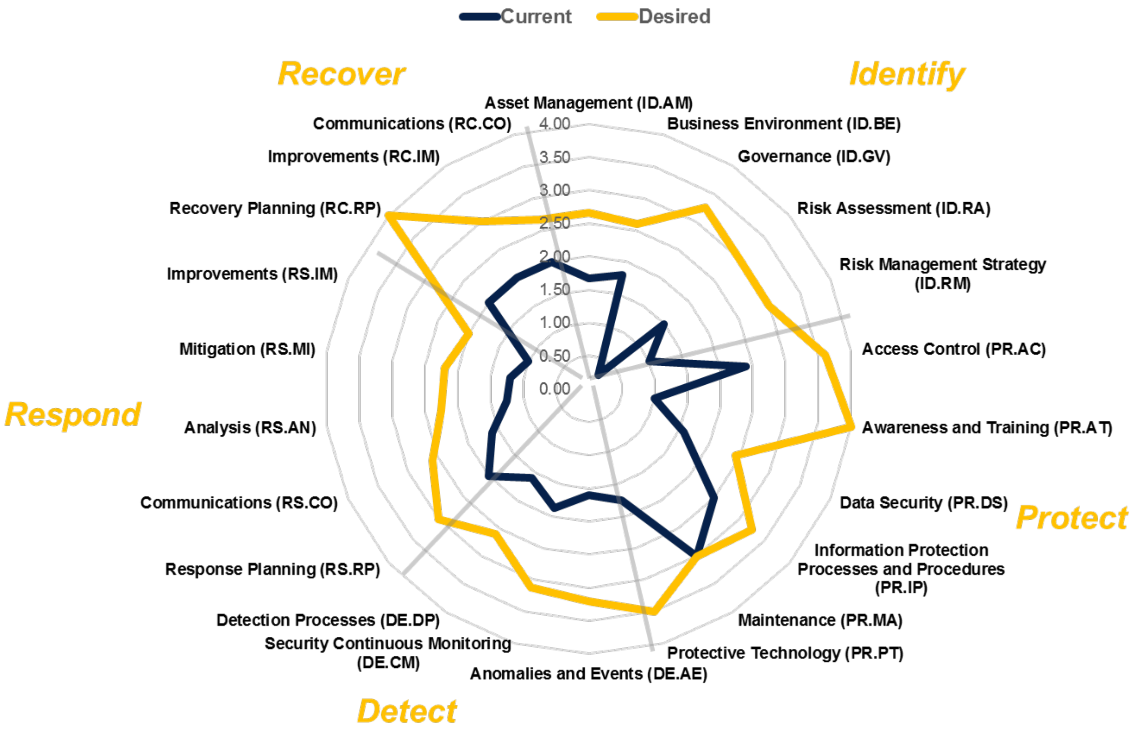
Organizing Controls around Frameworks

- What Frameworks Provide:
  - Align and organize IT Security controls
  - Can provide reporting metrics for organizations to apply proper levels of IT security controls

- Common IT Security Control Frameworks:
  - ISO 27001
  - NIST Cybersecurity Framework (800-53 Controls)
  - COBIT
  - HITRUST
  - Cloud Security Alliance (CSA)
  - Center for Internet Security (CIS)
  - HIPAA Security Rule
  - Payment Card Industry Data Security Standard (PCI-DSS)
  - AICPA Trust Services Principles Criteria
  - Crowe Cybersecurity Risk & Control Framework

NIST Cybersecurity Framework Example





NIST CSF Maturity Scale

1 = Partial

2= Risk Informed

3=Repeatable

4=Adaptive

Analyze Cost

Continue to Revise

- Each incident offers an opportunity to re-evaluate
- Changes in services, technologies, and business strategies
- Monitor the threat landscape

Start with what you know

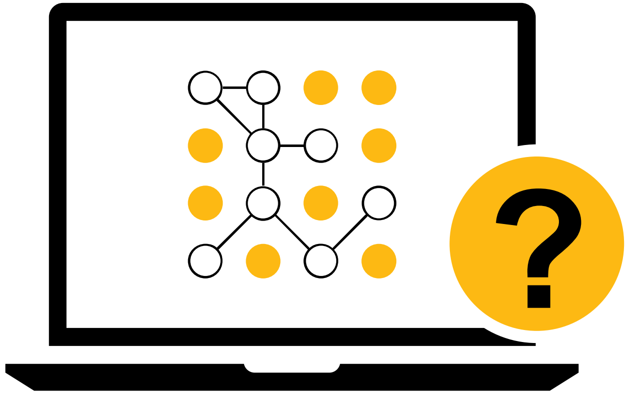
- Business Impact Analysis (BIA)
- Downtime cost analysis
- Organization’s historical breach or incident reports
- Observe your peers

Fill in the Gaps

- Risk Assessment
- Start asking the questions
- Form a committee

Cyber Insurance

Questions to Consider



Were IT or other technical teams involved in evaluating the policy?

- These teams can help spot potential gotchas and pitfalls

Does your policy reflect current and emerging threats? How are threats defined in general?

- Is ransomware specifically addressed?
- Does you policy cover instances of insider threats on only external threats?

What technical considerations would cause a claim to be denied?

- Unpatched systems?
- Poor system configuration?
- Gaps in software licensing?

Practices to Consider

- Be sure to incorporate insurance into cost models to map mitigation of specific risks to your policy
- Do not count on your policy to cover reputational damages, regulatory fines, or internal cost of response
- Find a policy that covers specific external costs such as:
  - Forensic investigation
  - Outside legal representation
  - Public relations or crisis management

Take-aways

5 Key Points

1. **Be intentional** about analyzing cybersecurity spend
2. **Actively engage** with IT
3. **Stay focused** on the highest risks
4. **Measure & report** your progress
5. **Don’t overestimate** the value of cyber insurance

Questions / Open Discussion

Crowe Horwath.

Thank you

Mike Porter

Phone +1 (415) 590-3916

Mike.Porter@crowehorwath.com

Jared Hamilton

Phone +1 (317) 706-2724

jared.hamilton@crowehorwath.com

In accordance with applicable professional standards, some firm services may not be available to attest clients.

This material is for informational purposes only and should not be construed as financial or legal advice. Please seek guidance specific to your organization from qualified advisers in your jurisdiction.