Cyber Security
Industry Best Practices

An Introduction & Overview

Charles Sgrillo C|EH CISSP

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

www.kmco.com

What's on Tap

- Key Terms Overview
- Current State of Information Security
- The Basics of a Vulnerability Assessment
  - Leveraging Frameworks
- The Basics of a Penetration Test
- The Human Element in Information Security
- Q & A

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Key Terms Defined

- Vulnerability
  - A flaw or weakness in system security procedures, design, implementation, or internal controls
- Control
  - A measure taken to prevent, detect, minimize, or eliminate risk to protect the Confidentiality, Integrity, and Availability of information (CIA Triad)
- Risk/Vulnerability Assessment
  - The process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system or organization
- Penetration Test
  - is the practice of testing a computer system, network or Web application to find vulnerabilities
- Exploit
  - a sequence of commands that takes advantage of a vulnerability

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability

2016 Global State of Information Security Survey - *Burg*

"There is no one-size-fits-all model for effective cybersecurity. It's a journey toward a future state that starts with the right mix of technologies, processes, and people skills. With those components in place, cybersecurity can potentially serve as an indispensable, ongoing business enabler."

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Current State of Cyber Security

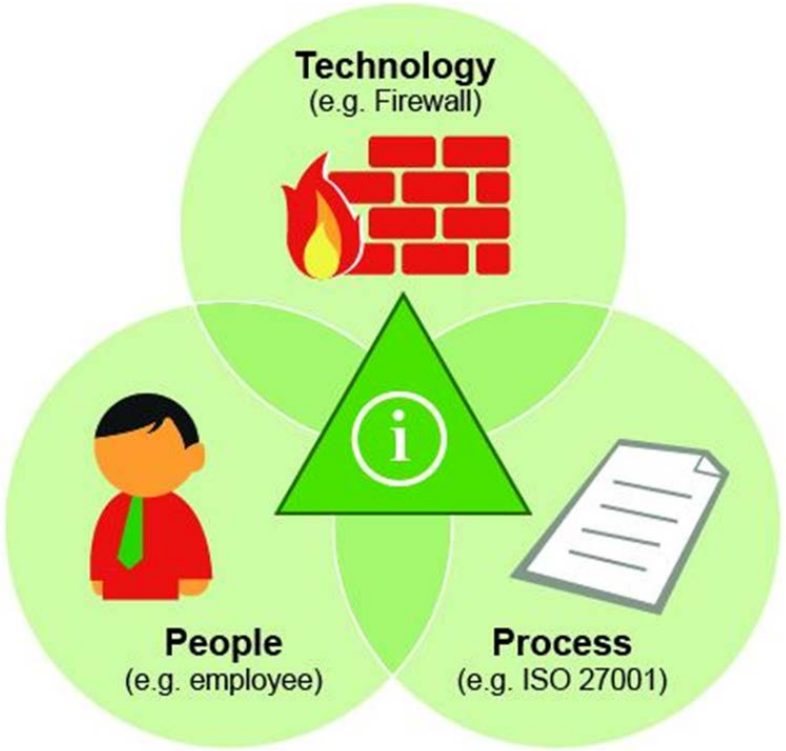
- Ransomware
- IoT
- Bitcoin
  - They can get paid now
- Exploit Kits…….Help Desk?
- Good hacker discounts?
- Tax fraud
- Data breaches
- Legal ramifications
- Traditional InfoSec Clients
- The New Wave

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Middle Market & InfoSec

- State of current resources
  - Internal resource realities
  - External IT eco system
  - Scope and reach extends beyond IT
  - Information Security vs IT Security vs Cyber Security
- Controls based on specific situations and the risks unique to the organization
- Risk Assessments should help guide organization's implementation of security controls



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

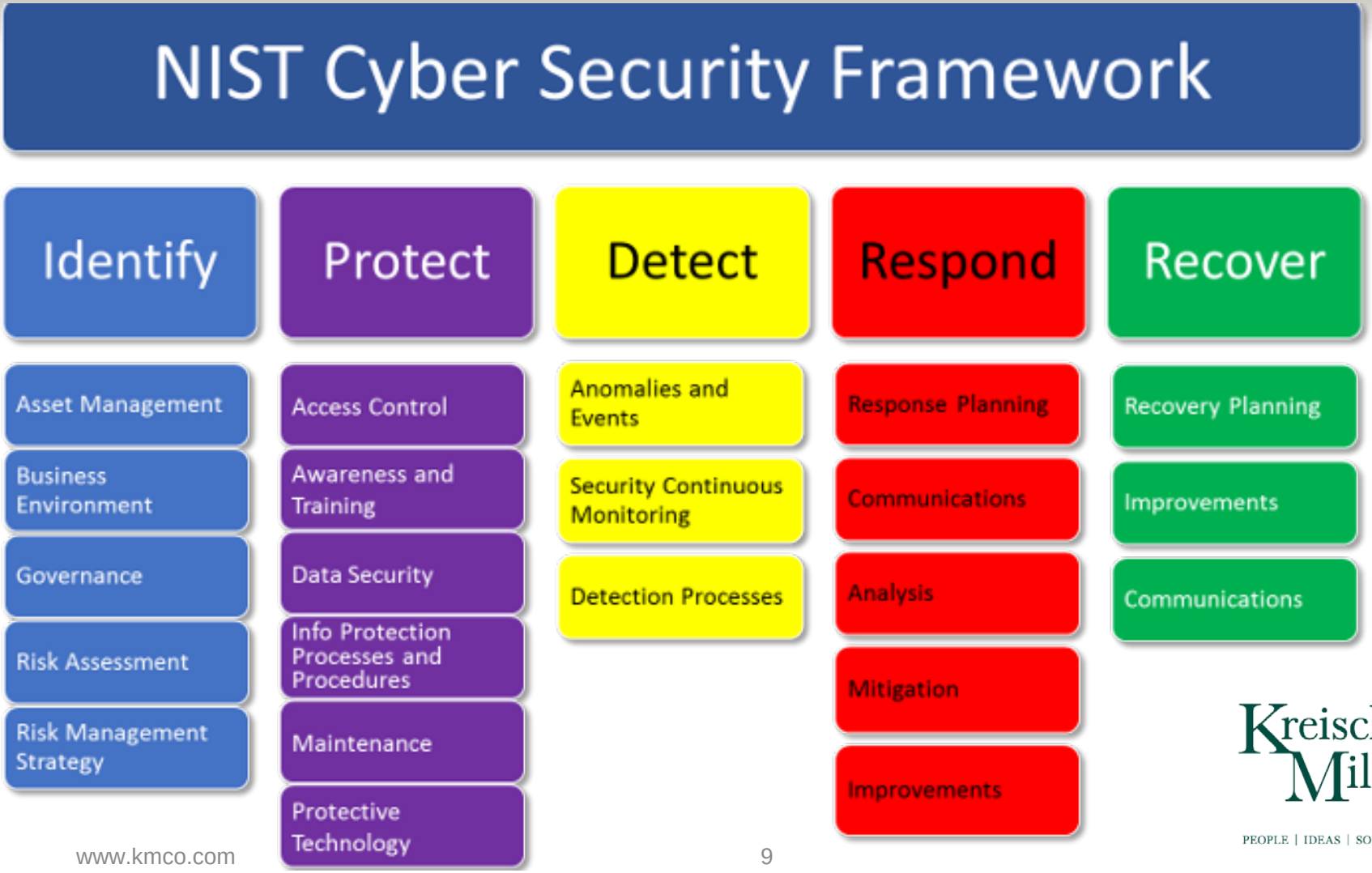
The Basics – Vulnerability Assessments

- Classically general in scope
- Foreseeable – The bad guys will arrive at 12pm
- Vulnerability Scan is not a Risk Assessment
  - Reaches beyond just IT systems
    - People, Policy, Process
- Report to serve as guideline for **<u>remediation</u>**

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Leveraging Frameworks



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Phases of the Assessment

- System Characterization
  - Defining the scope and approved targets for testing
- Threat/Vulnerability Identification
  - Conduct vulnerability identification against approved scope
    - People , Process, Technology
- Analysis
  - Control
  - Likelihood
  - Impact
- Risk Determination & Classification
- Solution Roadmap Development & Recommendation
- Roadmap Delivery for Management & IT Review

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Assessment Benefits

- Non-Intrusive scan can **discover valuable information** regarding the current infrastructure
- **A proactive approach to problems** –business that takes a proactive approach will be able to identify potential safety risks and resolve these problems before it is too late
- High/Med/Low vulnerability ranking allows an organization to **address critical concerns 1st**

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

The Basics – Penetration Testing

- Concentrated and detailed scope
  - External, Internal, Wireless, Physical, Social Engineering
- Path of least resistance
- Objective based approach
- How? When?
- Penetration Testing = PoC against vulnerabilities

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Penetration Testing Benefits

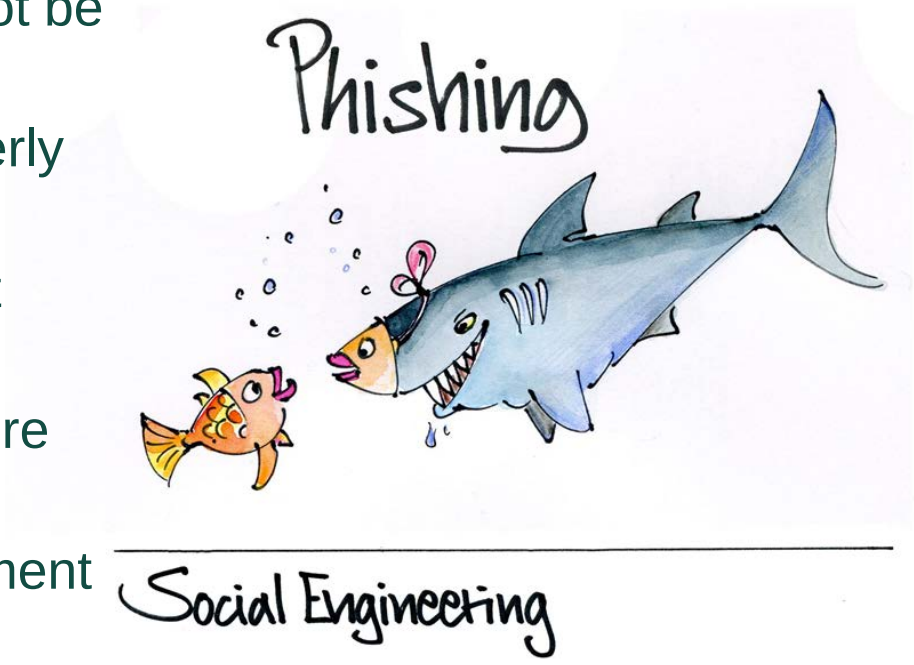
- What are the vulnerability scanners missing?
- Does your organization practice what they breach?
- Physical Security
  - The best firewall does not stop someone from walking in the front door
- Advances security awareness
- Delivers Management a true view of their current security posture
- If we can break it, the bad guys can

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Social Engineering - The Human Element

- Any act that influences a person to take an action that may or may not be in their best interest
- Organizations struggle with properly training their employees
- Employees with never care about data
- Teach employees how to be secure and they will be secure workers.
- It's a life style not a work requirement
  - Security cannot be a 9 to 5
- Ensure current policies are being executed



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

InfoSec Checklist

- ❑ Conduct vulnerability scans of all internal and external IT systems on a periodic basis?
- ❑ Review key business processes and identify and address potential information management security related risks?
- ❑ Perform annual penetration testing to validate information system security defenses?
- ❑ Provide ongoing information security training to all staff?
- ❑ Conduct random social engineering trials to validate staff training effectiveness?
- ❑ Maintain and validate updated information security policies and procedures?
- ❑ Established proper information security governance and control mechanisms in place?

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Q & A

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS