Cyber & Information Security Best Practices

Establishing a Sustainable Risk Management Approach

Sassan Hejazi, Ph.D.,
Director-in-Charge,
Technology Solutions,
Kreischer Miller

Robert Rittich, CISSP,
Affiliated Cyber
Security Consultant

www.kmco.com

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Cyber Security Hot Topics

5 months of ChatGPT/AI's impact on cyber security

- New levels of targeted phishing and deepfakes
- Moderately complex technical hacks executed by amateurs
- The tip of the iceberg, evolving ever faster…

Merck $1.4b insurance award for NotPetya attack

- 'Hostile or warlike action by sovereign power' exclusion not applicable for property insurance
- 'Historic definitions applicability in new world' debate continues

Dobbs decision cyber security ramifications

- >50 lawsuits filed to date over tracking pixels
- 99% of all US nonfederal acute care hospital websites use pixels

Law enforcement chalks up big wins in 2023

- Medusa operation takes down 20-year-old Russian malware
- Dark web marketplace 'Genesis' shutdown

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

2022 Trends & Statistics

84 minutes

Average time from foothold to full breach

95% increase

Cloud exploitation in 2022 & 3x increase in cloud focused threats

212 advanced persistent threats

Number of organized, well-funded, active cybercrime operations

112% increase, >2500 ads

Initial access broker ads for already compromised entry

277 days

Average time to identify and contain a breach

$10.2 billion

Damages reported to FBI from cybercrime in 2022

Sources:

- Microsoft Digital Defense Report 2022
- IBM Cost of a Data Breach Report 2022
- CrowdStrike Global Threat Report 2023
- FBI 2022 Internet Crime Report

High Value Target Assets

- Personally Identifiable Information (PII) such as employee and customer social security numbers, dates of birth, electronic protected health information (EPHI), email addresses, compensation and credit card numbers
- Product and service intellectual property data, product design, engineering, manufacturing, marketing, regulatory and competitive data
- Operational continuity and reliability capabilities, reputational and legal risk concerns

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**

Cyber Readiness Approaches

Minimal

- Keeping up with latest patches and fixes at best
- Highly reactive in nature
- Lack of cyber related plans and budgets

Traditional

- Having a formal cyber program in place
- Leveraging applicable industry methodologies
- Highly IT focused and driven

Holistic

- Active cyber program in place
- Leveraging leading industry practices
- Close and active collaboration between IT and management

Kreischer Miller

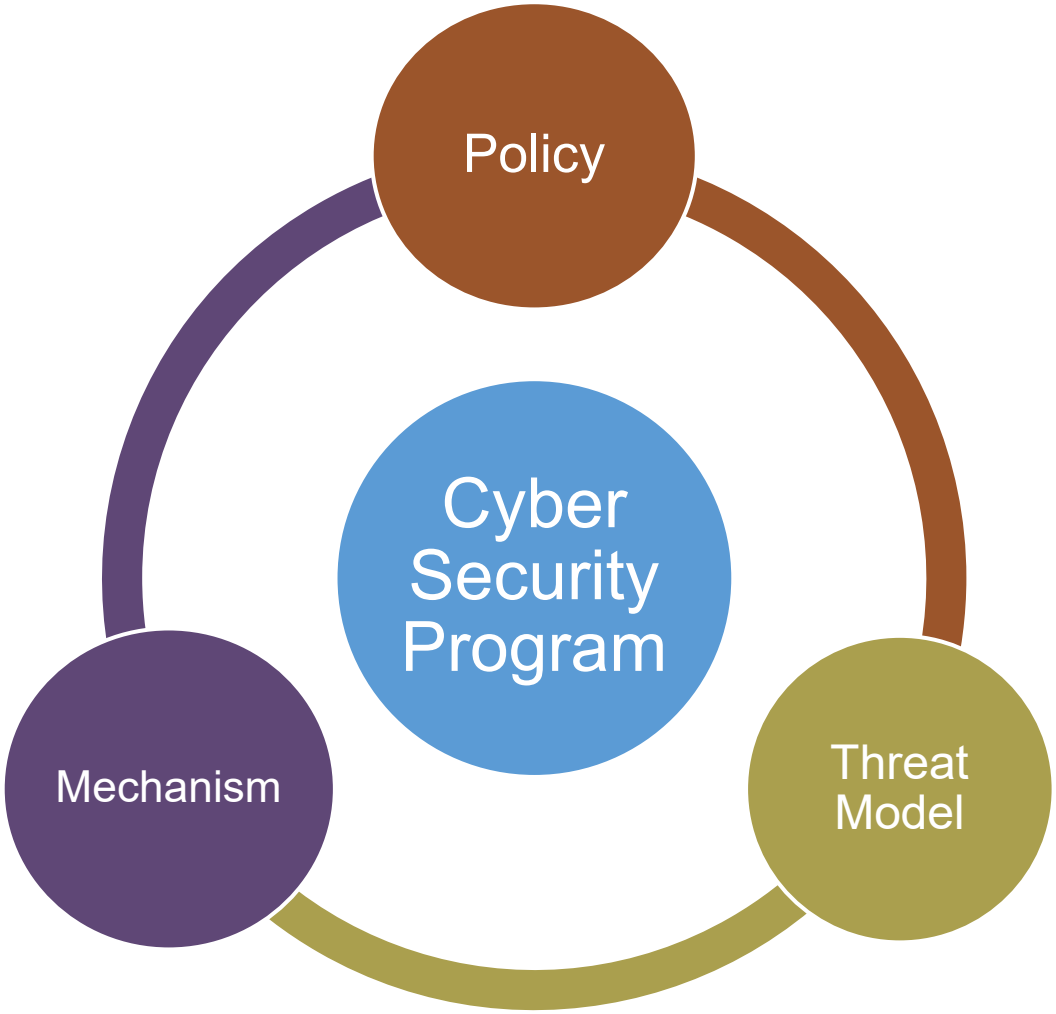
PEOPLE | IDEAS | SOLUTIONS

Leveraging Frameworks - NIST

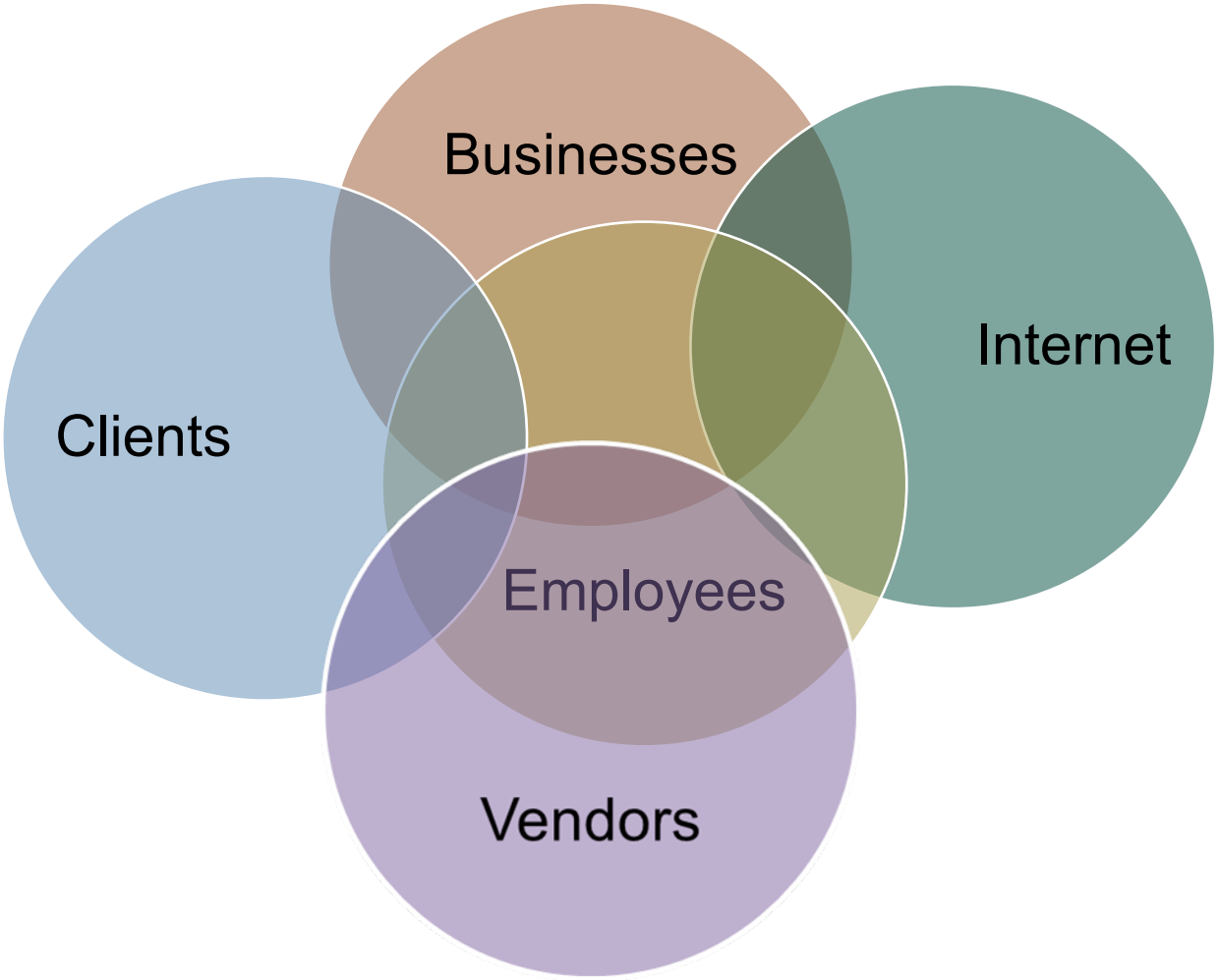
[NIST Cybersecurity Framework | NIST]

CIS Controls Overview

Cyber Security Program Triad



Know Your Web of Trust



What is Your Risk Profile?

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Do We Have a Cyber & Privacy Program?

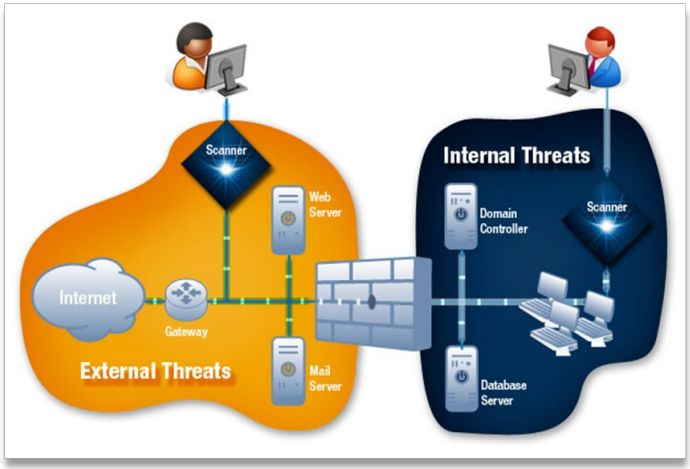
- Is it an active program?
  - Committee in place?
- Is it well planned/budgeted?
- Is it based on a methodology?
  - NIST/CMMC/CIS
  - ISO
  - GDPR/HIPAA

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Do We Know Our IT Vulnerabilities?

- Do we periodically conduct a vulnerability scan?
  - New vulnerabilities are discovered daily
  - Internal vulnerability scans occur from within the network
  - External vulnerability scans simulate the effect of Internet users attempting to access a network



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Are We Monitoring Threats?

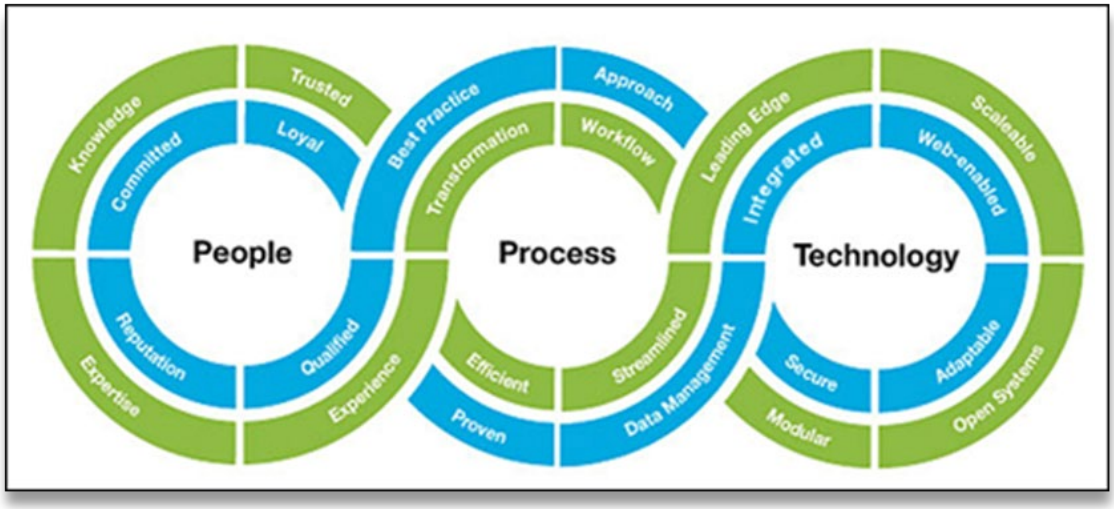
- Detecting potential intrusions?
- Review of user/insider activities?
- Staying on top of latest threats out there?

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

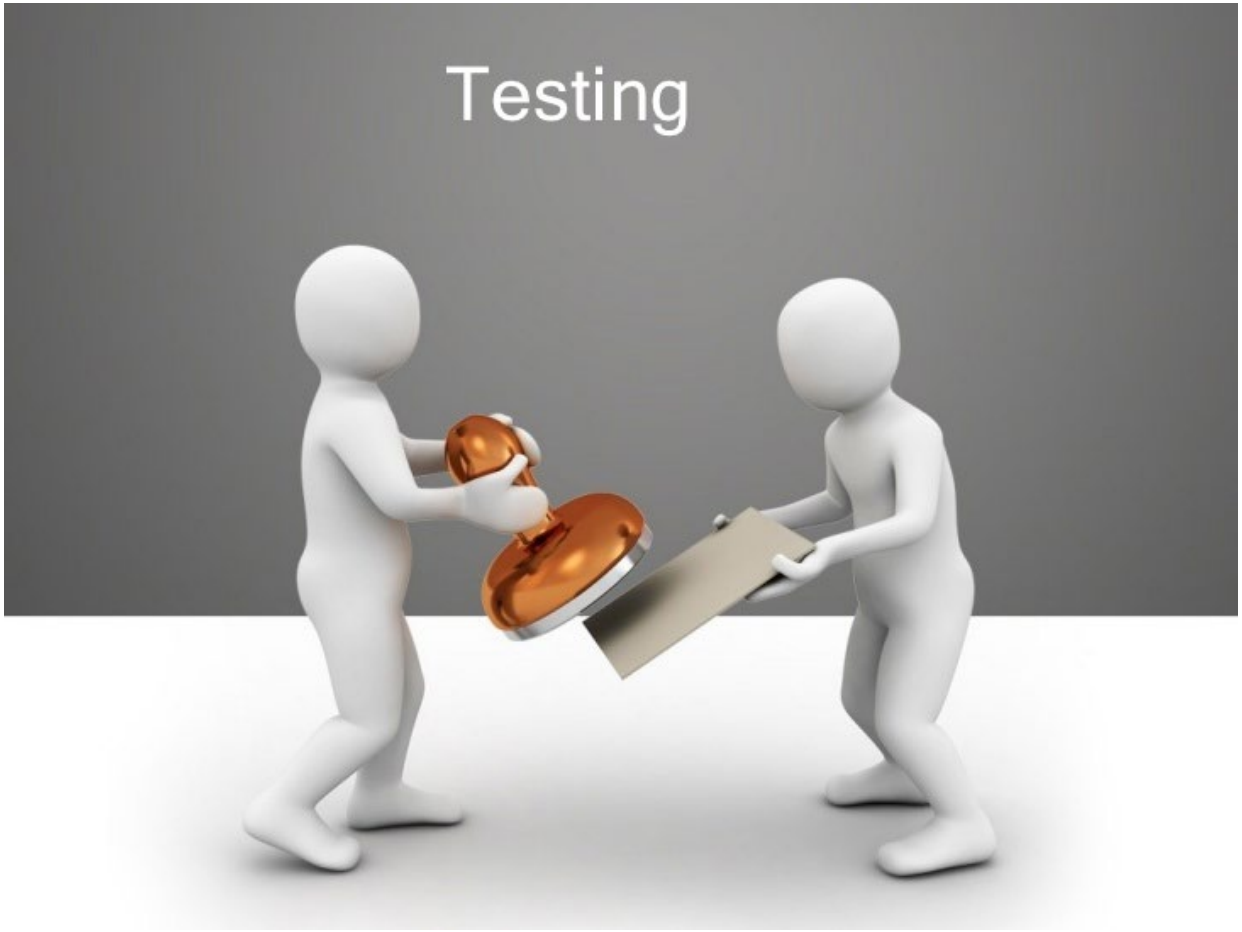
Do We Have Updated Policies?

- Employee onboarding, acceptable use, termination?
- Data classification, access and protection?
- Data handling and privacy considerations?
- Vendor/contractor proper data handling and confidentiality?
  - IT department/provider(s) considerations?



Do We Have a Cyber Training Program?

Are We Validating User Knowledge?



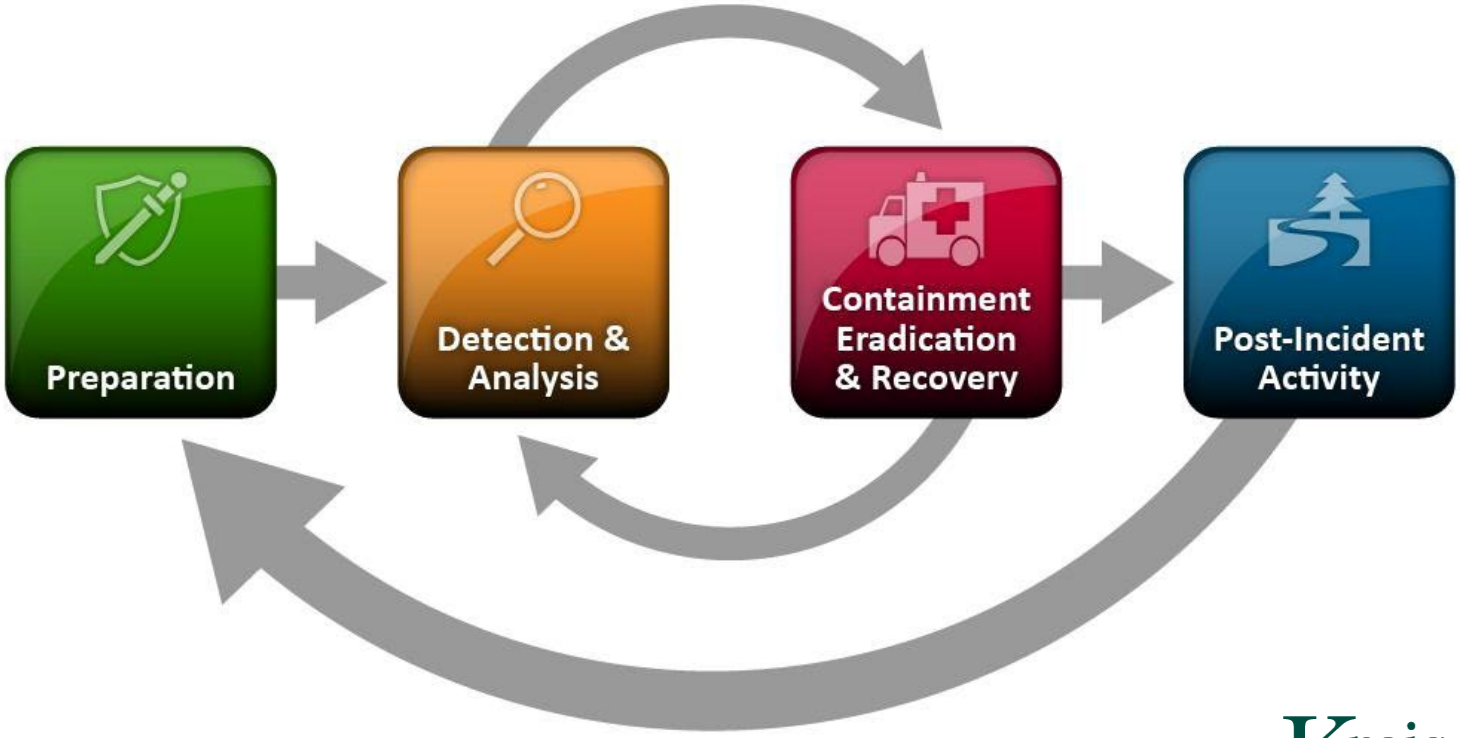
Users Only Access What They Need?

- Principle of least privilege
  - A user or a program (depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose
- Review access levels and have proper change control procedures in place
- Apply this principle to all employees and third parties

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Do We Have an Incident Response Plan?



Cyber Insurance Considerations

Kreischer Miller

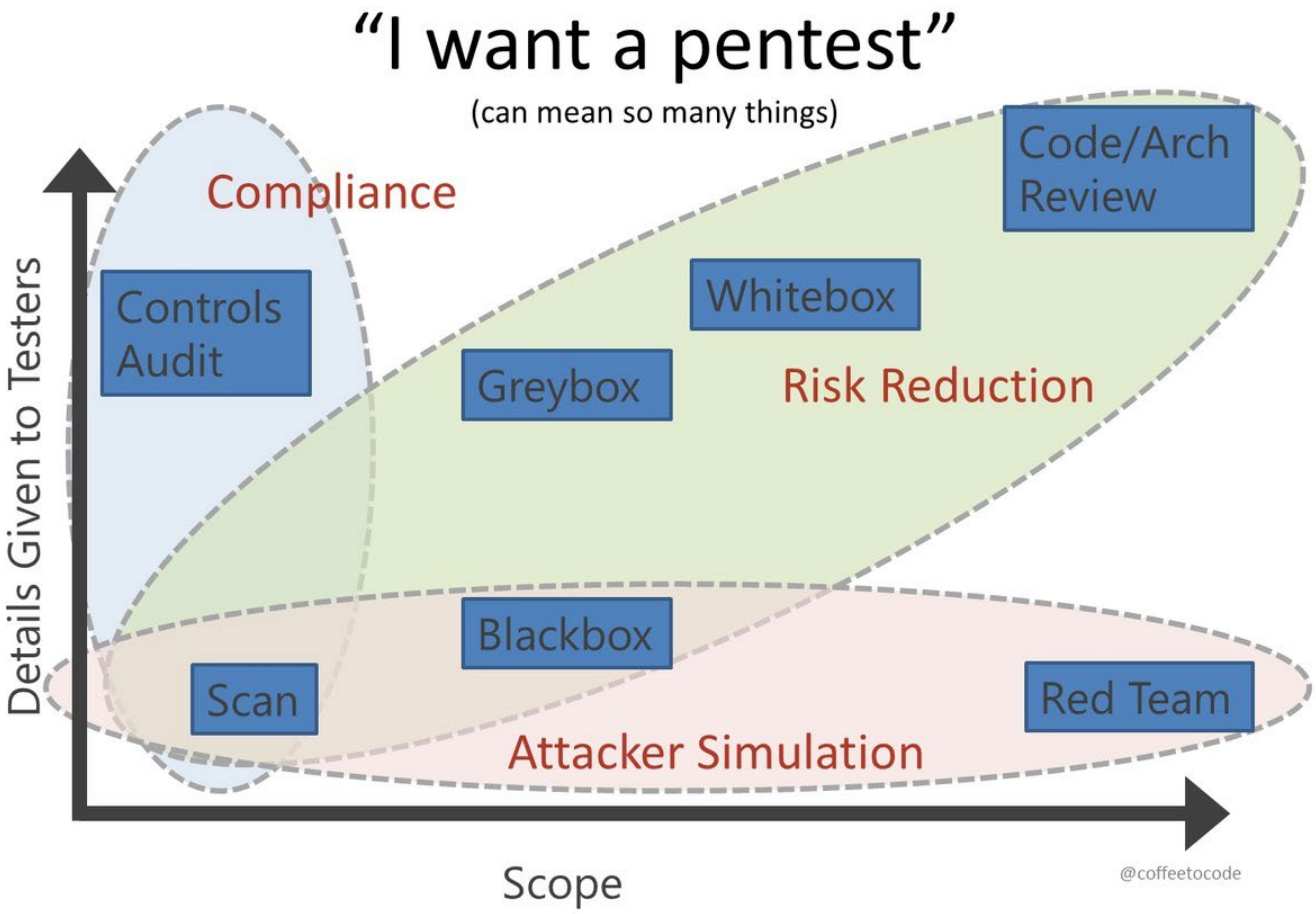
PEOPLE | IDEAS | SOLUTIONS

Do We Have a Recovery Plan?

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Have We Paid Someone to Break In?



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

What is Your Risk Profile?

- **Assign a 10 to all YES responses**
- **Assign a 5 to all SOMEWHAT responses**
- **Assign a 0 to all NO responses**
- **Add up all your points from the 10 questions**
  - Scored below 50, organization at a **CRITICAL RISK LEVEL**
  - Scored between 50-70, at a **HIGH RISK LEVEL**
  - Scored between 70-90, at a **MODERATE RISK LEVEL**
  - Scored above 90, at a **MANAGED RISK LEVEL**

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Management Recommendations

- Establish an active cyber program and ensure hygiene practices such as following are in use:
  - Enable and mandate the use of multi-factor authentication
  - Deploy modern security and monitoring tools on all computers and devices
  - Leverage internal or external cyber security resources to ensure that your systems are patched and protected against all known vulnerabilities
  - Establish and enforce a password change regiment across your networks on a regular basis
- Have emergency plans (practice/validate) in place
- Educate employees on common attack vectors

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Concluding Comments

- Executives are ultimately responsible for their organization's cyber security and information security readiness
- Current increased threat levels require executives and board members to stay highly engaged in the organizations cyber and information security readiness efforts to protect their key assets and lead their organization's culture towards a security aware and empowered one
- Having an active and effective cyber readiness program could be leveraged as a source of competitive advantage!

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Thank You for Attending!

Sassan Hejazi, Ph.D.,
Director-in-Charge,
Technology Solutions,
Kreischer Miller

Robert Rittich, CISSP,
Affiliated Cyber
Security Consultant

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS