

CYBER & INFORMATION SECURITY EXECUTIVE UPDATE

WHAT IS YOUR READINESS SCORE?

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Sassan S. Hejazi, Ph.D.

MAY 2021

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.**

Current State of Cyber Security

- Pandemic accelerators
- Dark web considerations
- Bitcoin - They can get paid now
  - Exploit kits …help desk?
- Ransomware as a service
- Data breach privacy concerns
- Operational continuity issues
- Legal and branding concerns

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Recent Event – PA Contact Tracing

- **Pennsylvania contact tracing breach impacts private info of 72K people.**
- Workers at Atlanta-based Insight Global "disregarded security protocols established in the contract".
- Insight Global acknowledged it mishandled sensitive data and apologized.
- The company has been directed to secure the records and has hired third-party specialists to conduct a forensic examination.

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Recent Event – Colonial Pipeline

- **Workers traditionally working from their offices within their corporate networks started working extensively from remote locations due to pandemic concerns.**
- Hackers were able to penetrate corporate systems through vulnerabilities in employee remote work connections.
- Colonial shutdown all their pipeline systems out of caution for protecting their systems, resulting in gas price spikes and shortages nationally and paid an estimated $5,000,000 in ransomware.

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

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

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

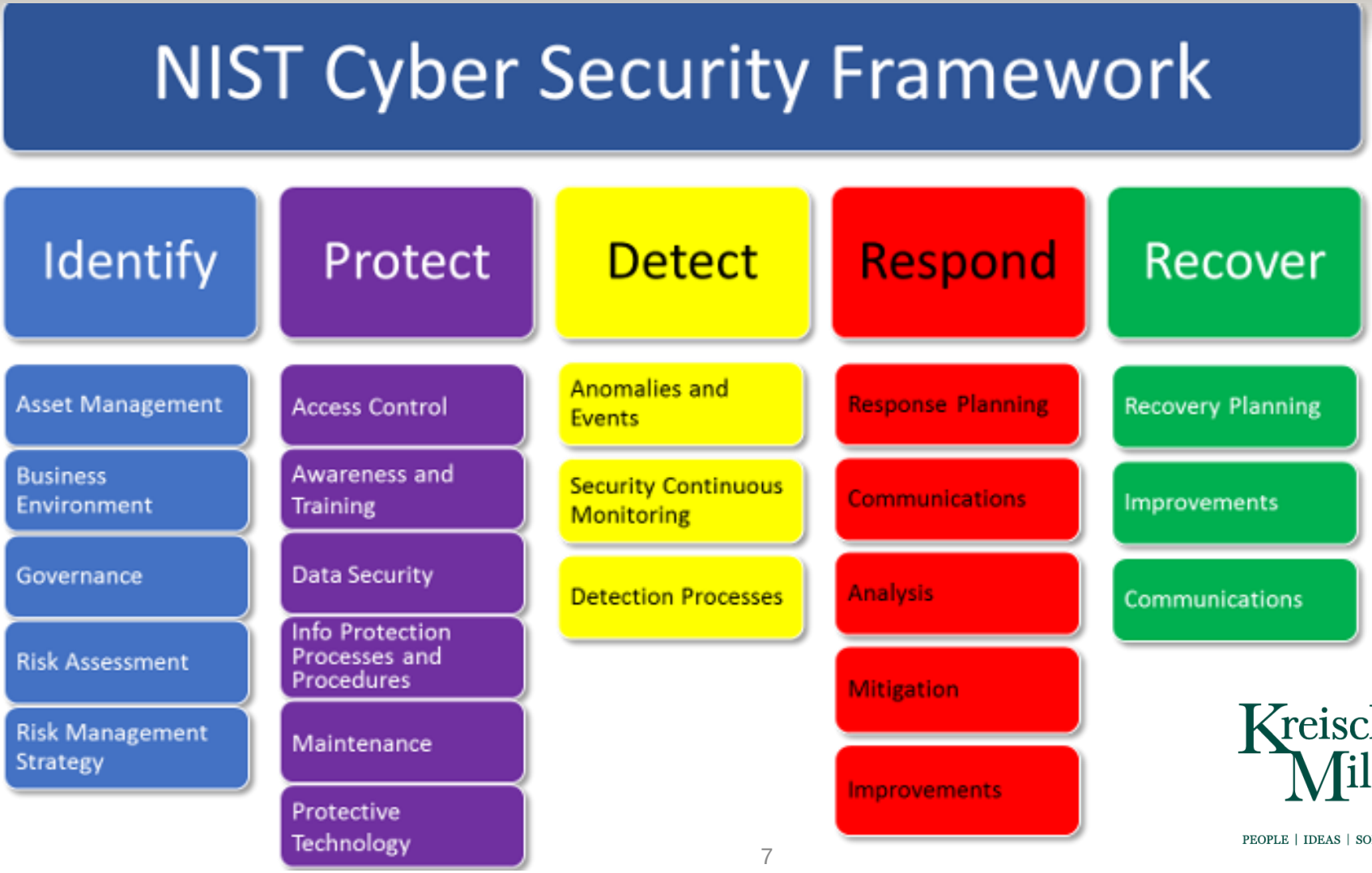
Holistic

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

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

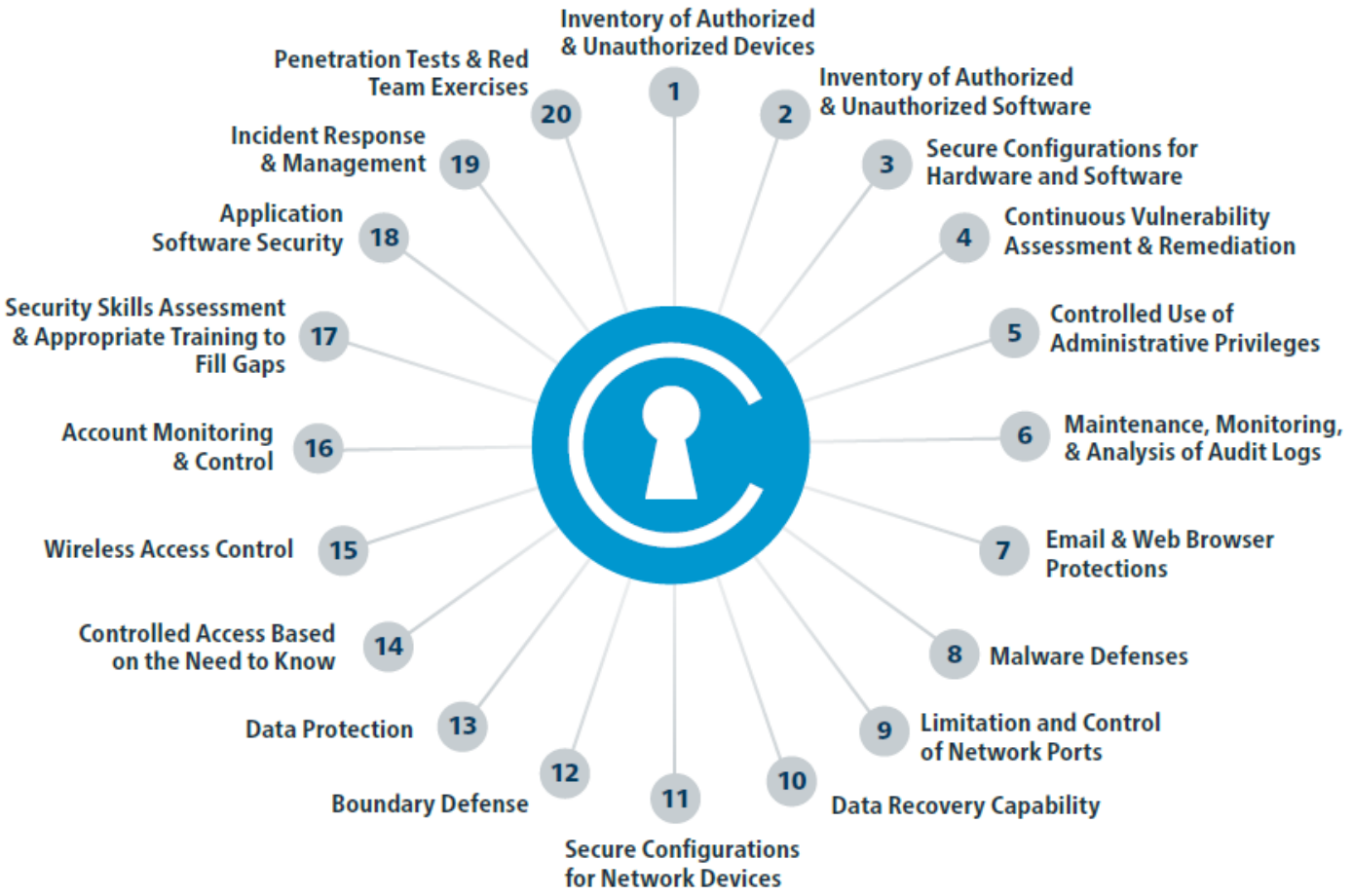
Leveraging Frameworks



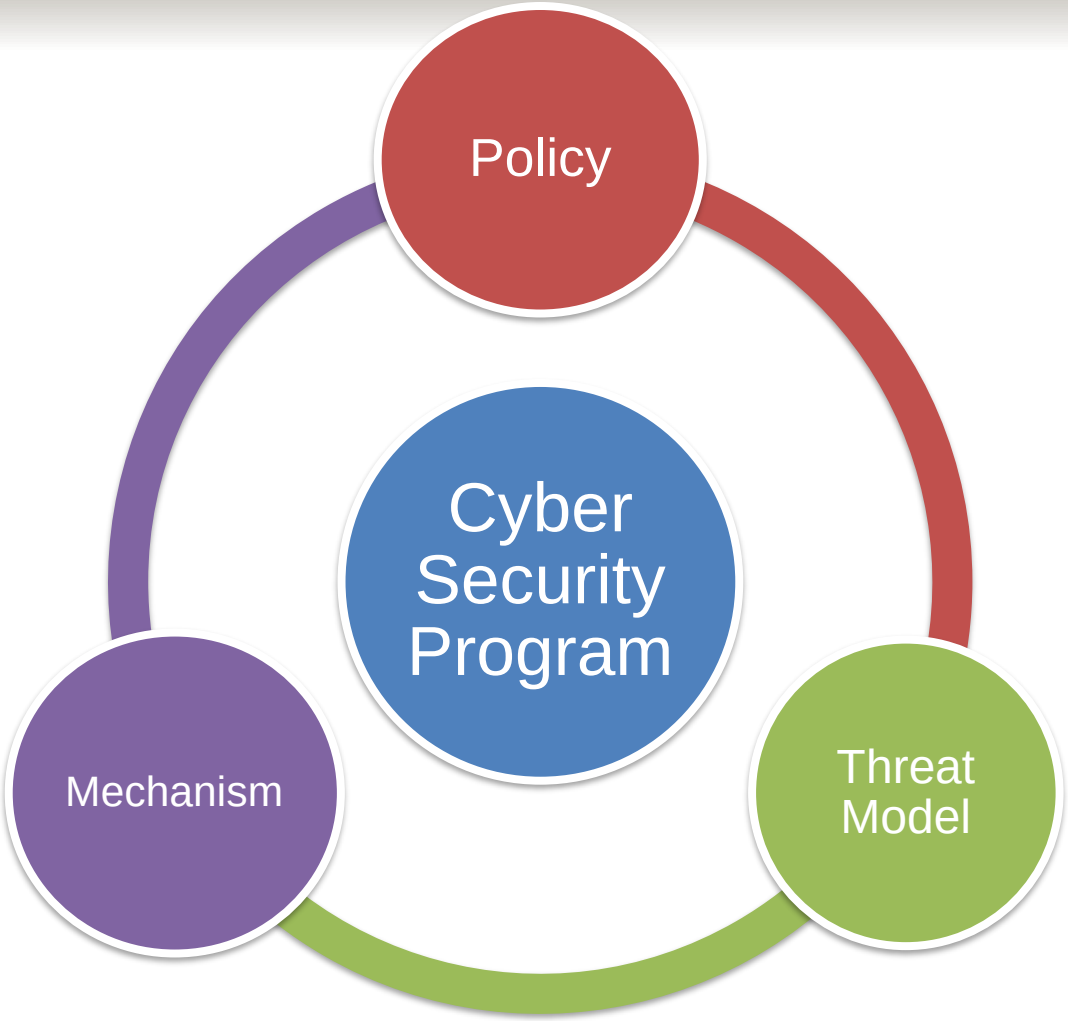
Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

CIS Top 20 for SMEs



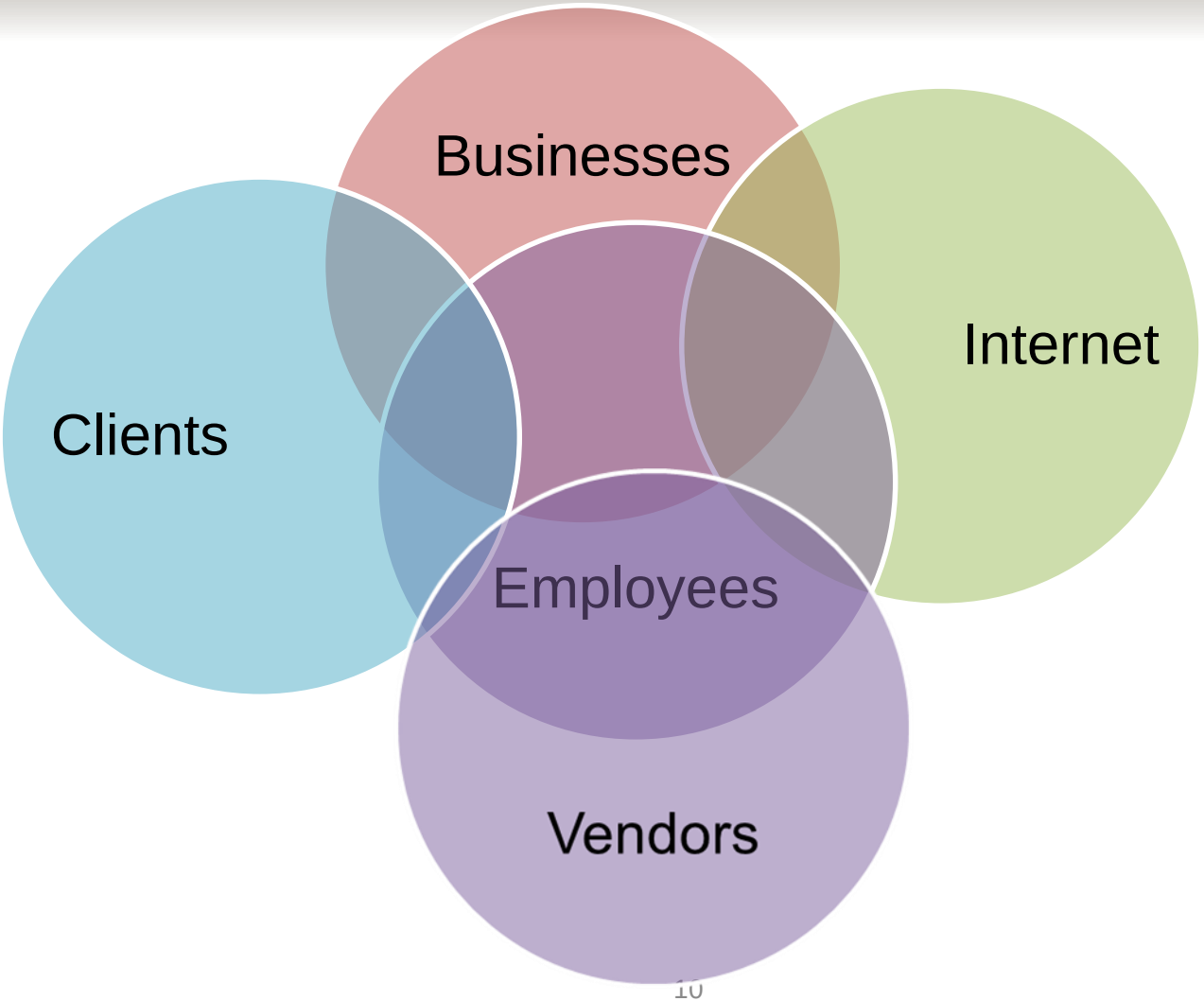
Cyber Security Program Triad



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Know Your Web of Trust



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

10 QUESTIONS TO ASK

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Ready to Develop Your Score?

- **Have a pen and paper or a blank spreadsheet ready.**
- For each question, use the following scoring model:
  - If your organization has not really addressed the issue or perhaps just a bit, record a 1/2 for this question.
  - If your organization in actively addressing this issue but could do better, record a 4/5 for this question.
  - If your organization is doing great for this question and simply needs minor tweaks, assign a 8/9 for this question.
- OK to assign a “0”, not OK to assign a “10”!
- Remember, this is a confidential, management awareness risk score, best to be totally honest with ourselves!!

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Do we have a cyber program?

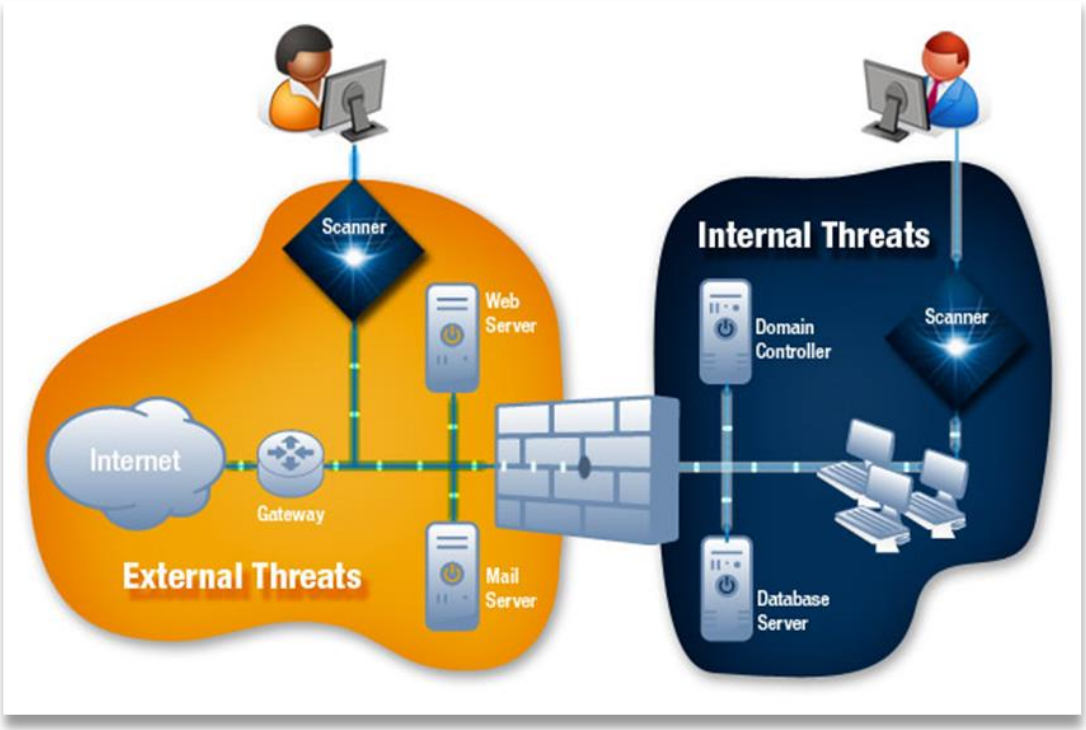
- Is it an active program?
  - Cyber versus Privacy
- Is it well planned/budgeted?
- Is it based on a methodology?
  - NIST
  - CIS
  - ISO
  - GDPR/HIPAA

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Do we know our vulnerabilities?

- How often do we 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?

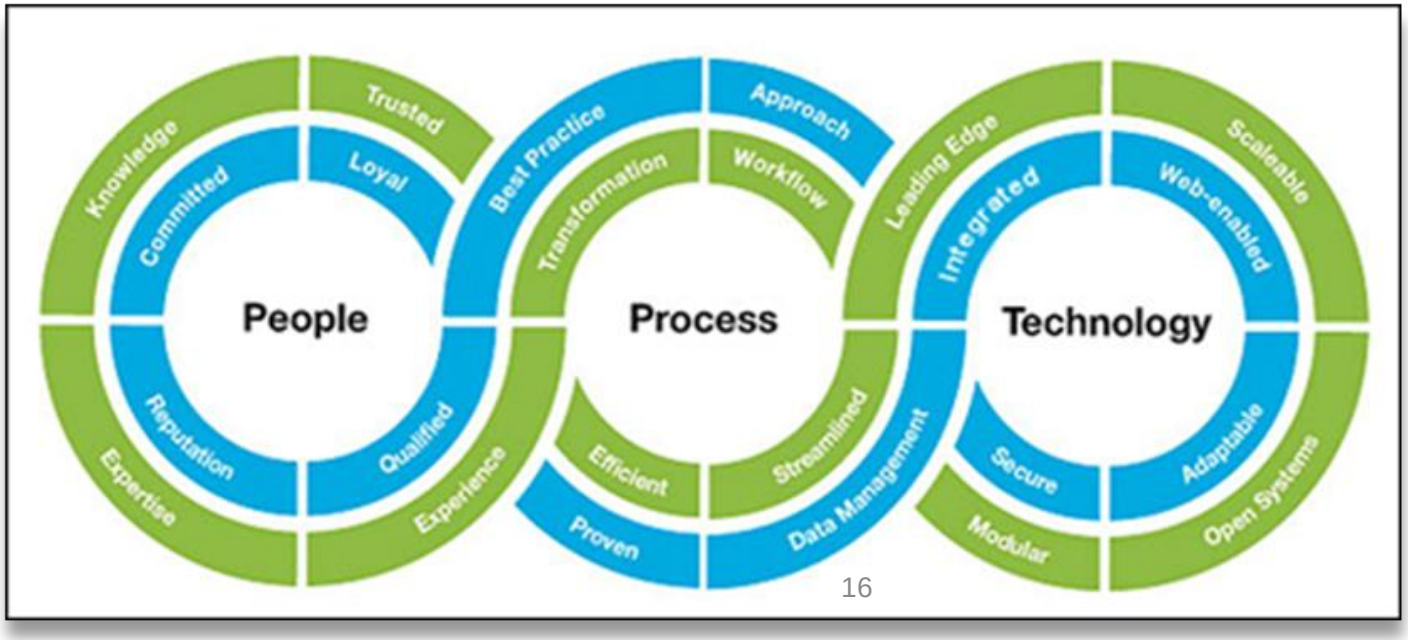
- Detecting potential intrusions?
- Review of user/insider activities?
- Staying on top of latest threats out there?

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Do we have updated policies?

- Employee on boarding, acceptable use, termination?
- Plan data handling and privacy considerations?
- Internal data confidentiality, access and protection?
- Vendor/contractor proper data handling and confidentiality?
- IT department/provider cyber policies & procedures?



Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Do we have a cyber training program?

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Are we validating user knowledge?

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

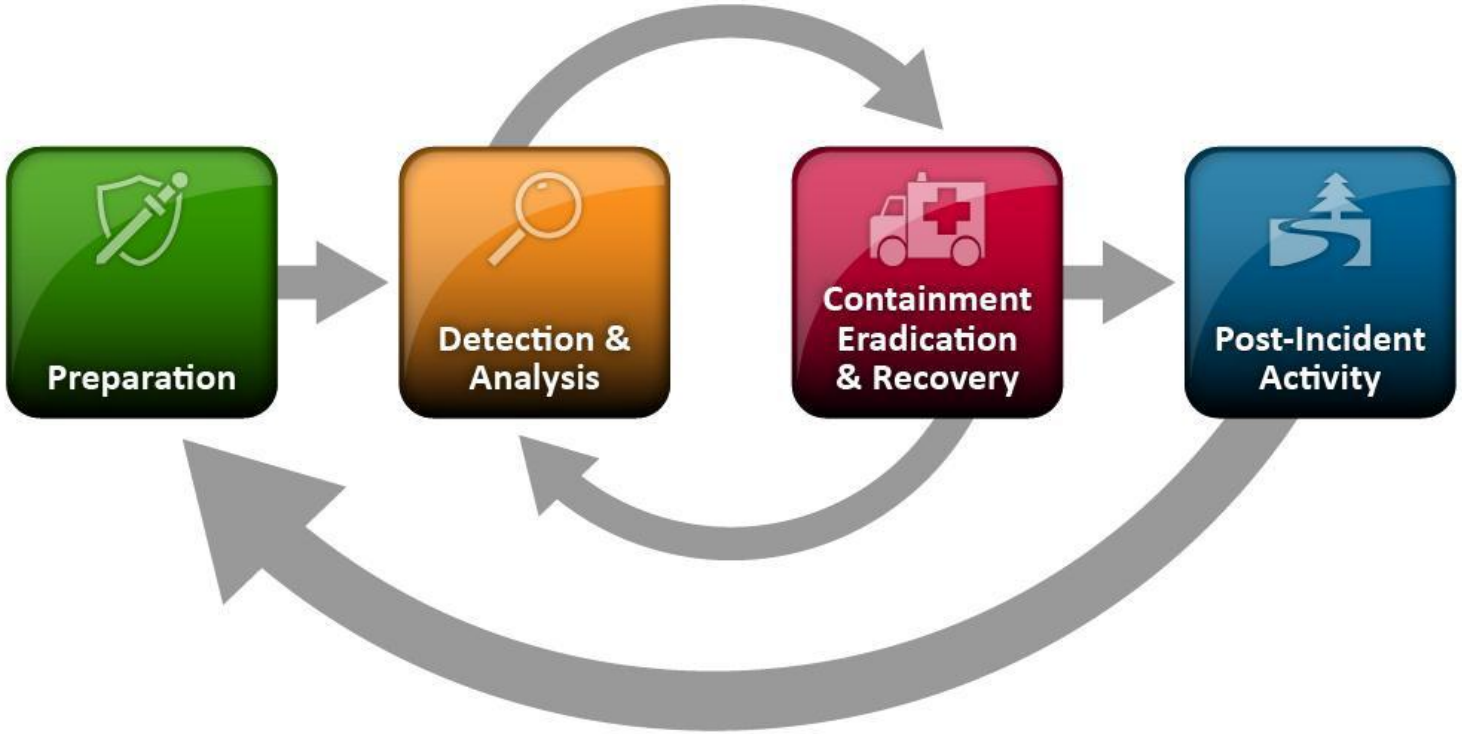
Users only access what they need?

- 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

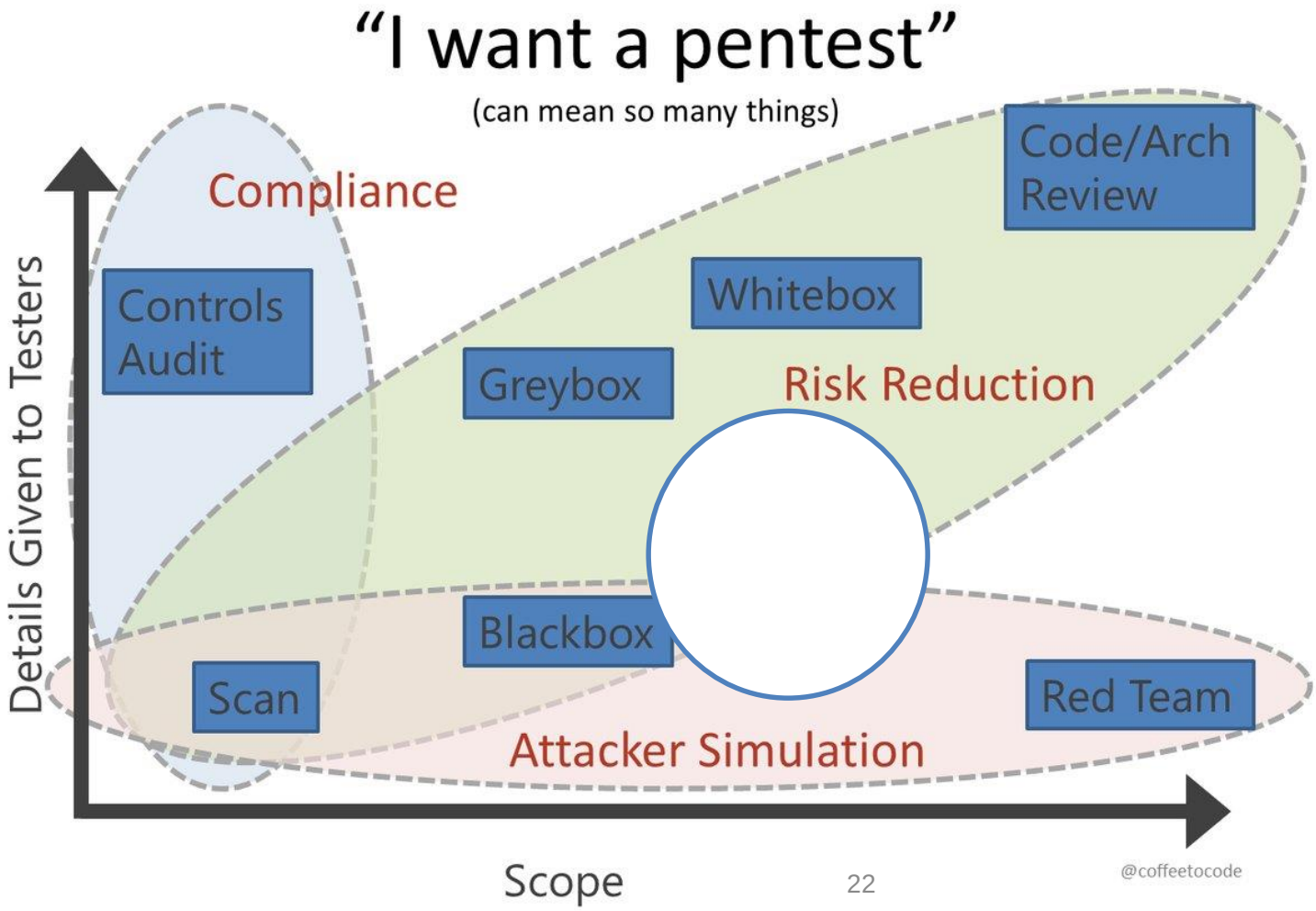
PEOPLE | IDEAS | SOLUTIONS

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 Readiness Score?

- **Add up your points from the 10 questions.**
- If you scored below 50, your organization is at a **CRITICAL LEVEL** of risk from a cyber related incident.
- If you scored between 50-70, your are at a **HIGH LEVEL** of risk from a cyber related incident.
- If you scored between 70-90, your organization is at a **MODERATE LEVEL** of risk from a cyber related incident.
- If you scored above 90, you are at a **MANAGED LEVEL** of risk from a cyber related incident.

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

Concluding Comments

- Executives are ultimately responsible for their organizations cyber security and information security readiness.
- Executives and Board members need to stay highly engaged in the cyber and information security readiness efforts to lead their organization's culture towards a security aware and empowered one.
- ***Increasing cyber hygiene and information privacy is not a costly endeavor. It could be accomplished if addressed in a systematic program fashion to best protect ongoing digital transformation efforts and assets.***

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS

THANK YOU FOR ATTENDING!

Sassan S. Hejazi, Ph.D.
shejazi@kmco.com

Kreischer Miller

PEOPLE | IDEAS | SOLUTIONS