

Cyber & Information Security Executive Update

Managing in an Increased Risk Environment








Sassan S. Hejazi, Ph.D.
Robert Rittich, CISSP

www.kmco.com

**Kreischer
Miller**

PEOPLE | IDEAS | SOLUTIONS

Global Threat Levels

Center for Internet Security		GUARDED	LOW GUARDED ELEVATED HIGH SEVERE
Centre for Cyber Security		MEDIUM	VERY LOW LOW MEDIUM HIGH CRITICAL
MI5 Security Service		SUBSTANTIAL	LOW MODERATE SUBSTANTIAL SEVERE CRITICAL
Europol		ACUTE	ACUTE
Australia Cyber Security Centre		PROBABLE	NOT EXPECTED POSSIBLE PROBABLE EXPECTED CERTAIN

<https://www.cisecurity.org/cybersecurity-threats/alert-level>

<https://www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html>

<https://www.mi5.gov.uk/threat-levels>

<https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/terrorism>

<https://www.nationalsecurity.gov.au/national-threat-level/current-national-terrorism-threat-level>

Sources:

- Verizon DBIR 2021
- IBM Ponemon Study 2021
- CrowdStrike Global Threat Report 2021



PEOPLE | IDEAS | SOLUTIONS

Trends & Statistics

348.3

↑ 76

Global eCrime Index (CrowdStrike)

year-over-year 321.3 Lo, 831.5 Hi

The CrowdStrike 2022 Global Threat Report
CrowdStrike Holdings, Inc.
<https://www.crowdstrike.com/>

4,971

↑ 300

US Global Terrorism Index Score

28 of 93 ranked, 163 total worst 10 average 8,243

2022 Global Terrorism Index
Institute for Economics & Peace
<https://www.economicsandpeace.org/>

900

↑ 21

Advanced Persistent Threat Groups

900+ identified and tracked, numbers vary by source

APT annual review 2021
AO Kaspersky Lab
<https://apt.securelist.com/>

\$1.79M

↑ \$0.69M

Avg. Ransom Payment for those who paid
plus avg. \$792K additional extortion fees after ransom pmt.

CrowdStrike Global Security Attitude Survey
CrowdStrike Holdings, Inc.
<https://www.crowdstrike.com/>

287

↑ 7

Number of days to discover a breach

on average, a breach occurring on Jan. 1 is found Oct. 14

Cost of a Data Breach Report 2021
IBM Corporation
<https://www.ibm.com>

Sources:

- Verizon DBIR 2021
- IBM Ponemon Study 2021
- CrowdStrike Global Threat Report 2021

**Kreischer
Miller**

PEOPLE | IDEAS | SOLUTIONS

Threat Factors Outlook



CONTINUED PROLIFERATION OF 'INITIAL ACCESS BROKERS': advanced persistent threat actors will buy initial network access from cybercriminals, hackers and by bribing or extorting



INCREASED TARGETING OF NETWORK APPLIANCES: by directing malicious activities against VPN appliances threat actors attempt hijacking VPN sessions and obfuscate knock-on attacks.



THE EMERGENCE OF 5G VULNERABILITIES: as the technology is adopted, it will increase the attack surface of mobile platforms (by numbers) and provide launchpads for attacks.



EVOLUTION OF VICTIMOLOGY: 'enhanced' ransomware tactics will include blackmailing victims for public release of sensitive information and added pressure from secondary malware.



MORE DISRUPTIVE ATTACKS: orchestration of events will continue to evolve to take advantage of secondary effects such as short selling industry's stocks prior to attacks on integrated supply chains.



CONTINUED USE OF THE PANDEMIC TO LEVERAGE TO EFFECT: the initial confusion of the pandemic continues to provide pretext for social engineering and for exploitation of quick fixes that were never revisited after the initial rush to implement them.



PROLIFERATION OF SURVEILLANCE GEAR AND SOFTWARE: image processing capabilities of body, gait, face and identifying marks will continue to evolve intelligence gathering and inform action.

Sources:

- Verizon DBIR 2021
- IBM Ponemon Study 2021
- CrowdStrike Global Threat Report 2021

Threat Factors Outlook *(Continued)*



EFFORT AND FOCUS OF ATTACKERS DIRECTED AT MOBILE DEVICES, SPECIFICALLY iOS: advanced persistent threat actors and governments are investing heavily in zero-day (silent) malware.



MORE SUPPLY CHAIN ATTACKS: threat actors will continue to evolve the supply chain attack playbook for 'big game hunting' through trusted partners of their target's ecosystem.



CONTINUED EXPLOITATION OF WORK-FROM-HOME: threat actors will continue to seek the weakest link through which to attack corporate networks through poorly trained employees.



EXPLOSION OF ATTACKS AGAINST CLOUD SECURITY AND OUTSOURCED SERVICES: proliferation of microservices and use of 3rd party infrastructure continues to breed complexity and vulnerabilities. Compromise of API keys will continue to proliferate.



RE-EMERGENCE OF OFFENSIVE AND DESTRUCTIVE MALWARE: cyber weapons such as worms designed for destruction will affect businesses and may cripple global networks and supply chains.

Sources:

- Verizon DBIR 2021
- IBM Ponemon Study 2021
- CrowdStrike Global Threat Report 2021

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.



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

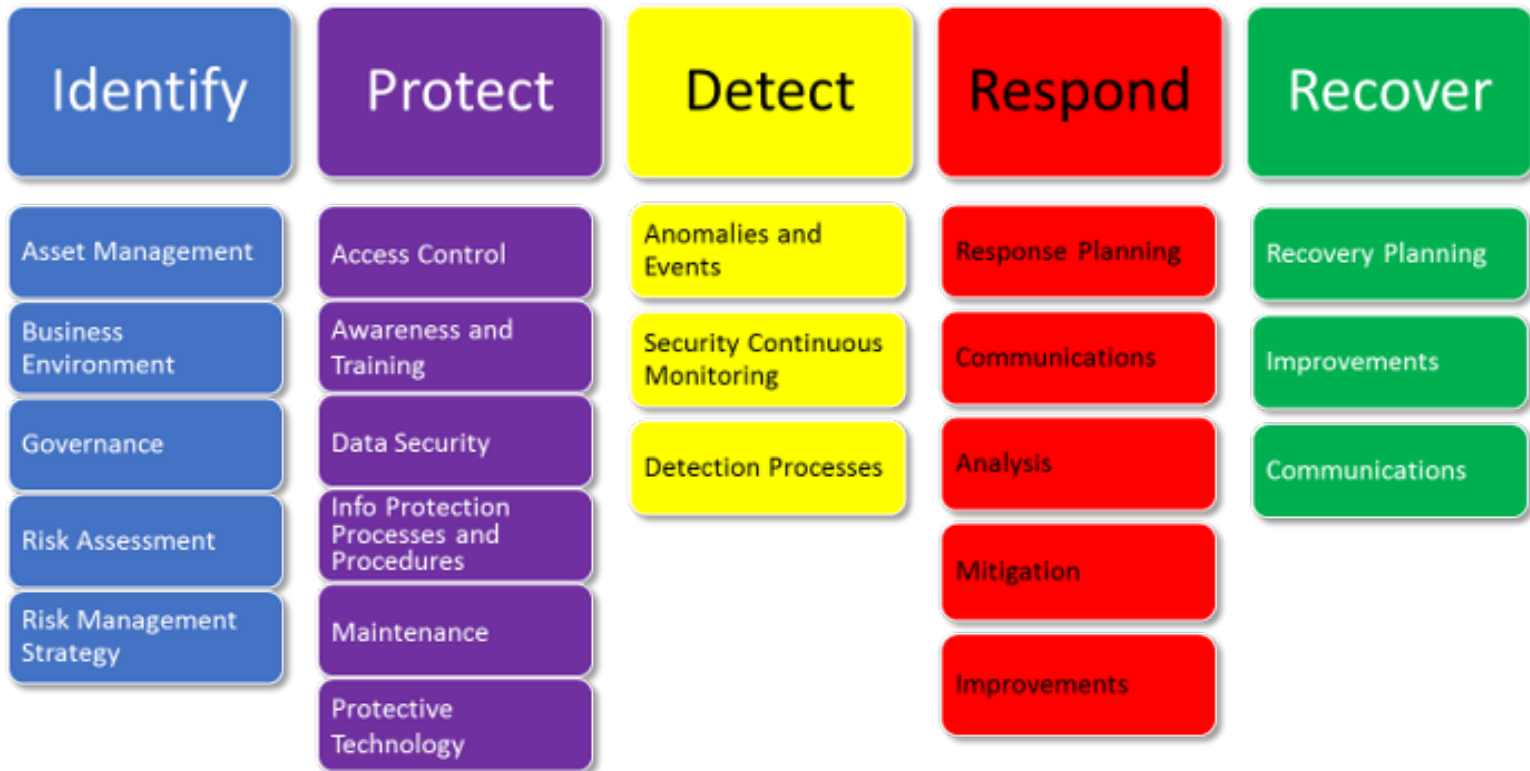
- Active cyber program in place
- Leveraging leading industry practices
- Close and active collaboration between IT and management



PEOPLE | IDEAS | SOLUTIONS

Leveraging Frameworks

NIST Cyber Security Framework



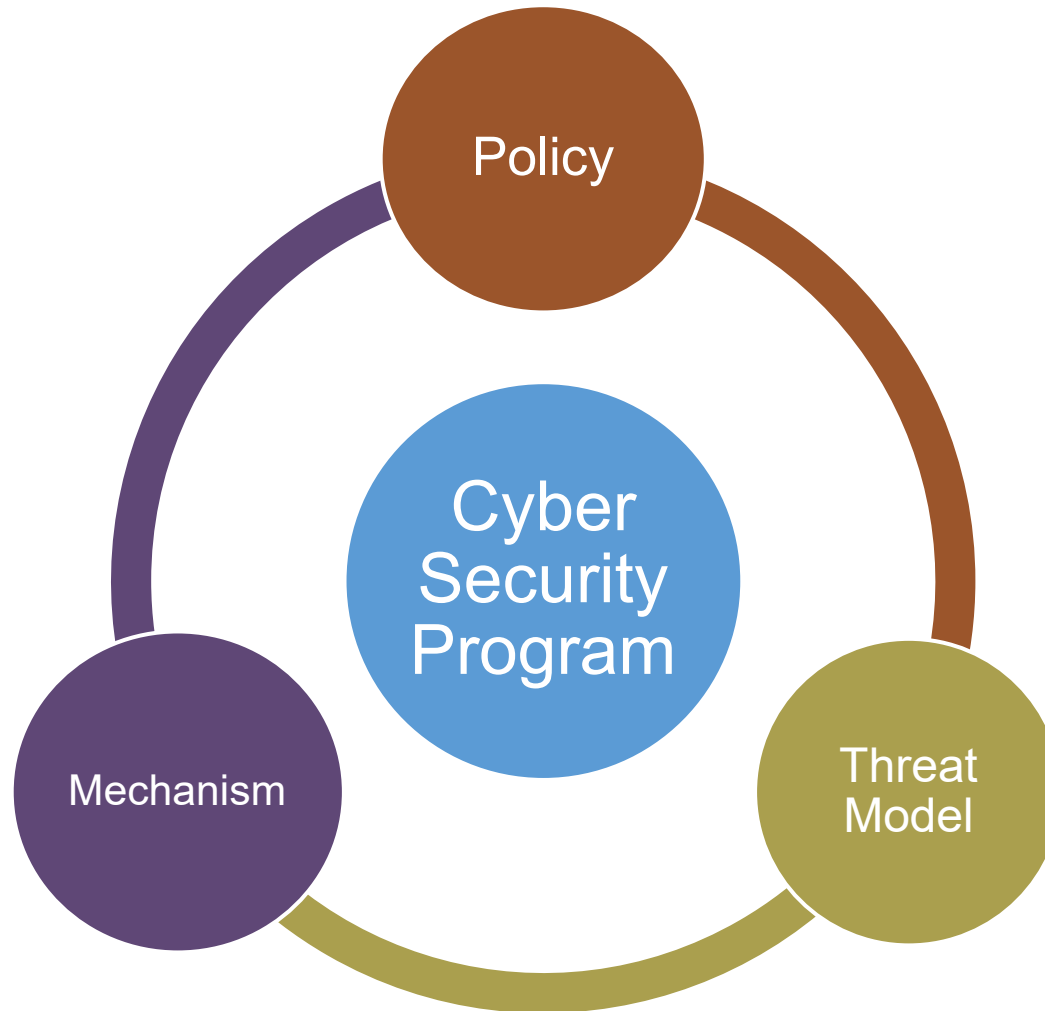
Leveraging Frameworks



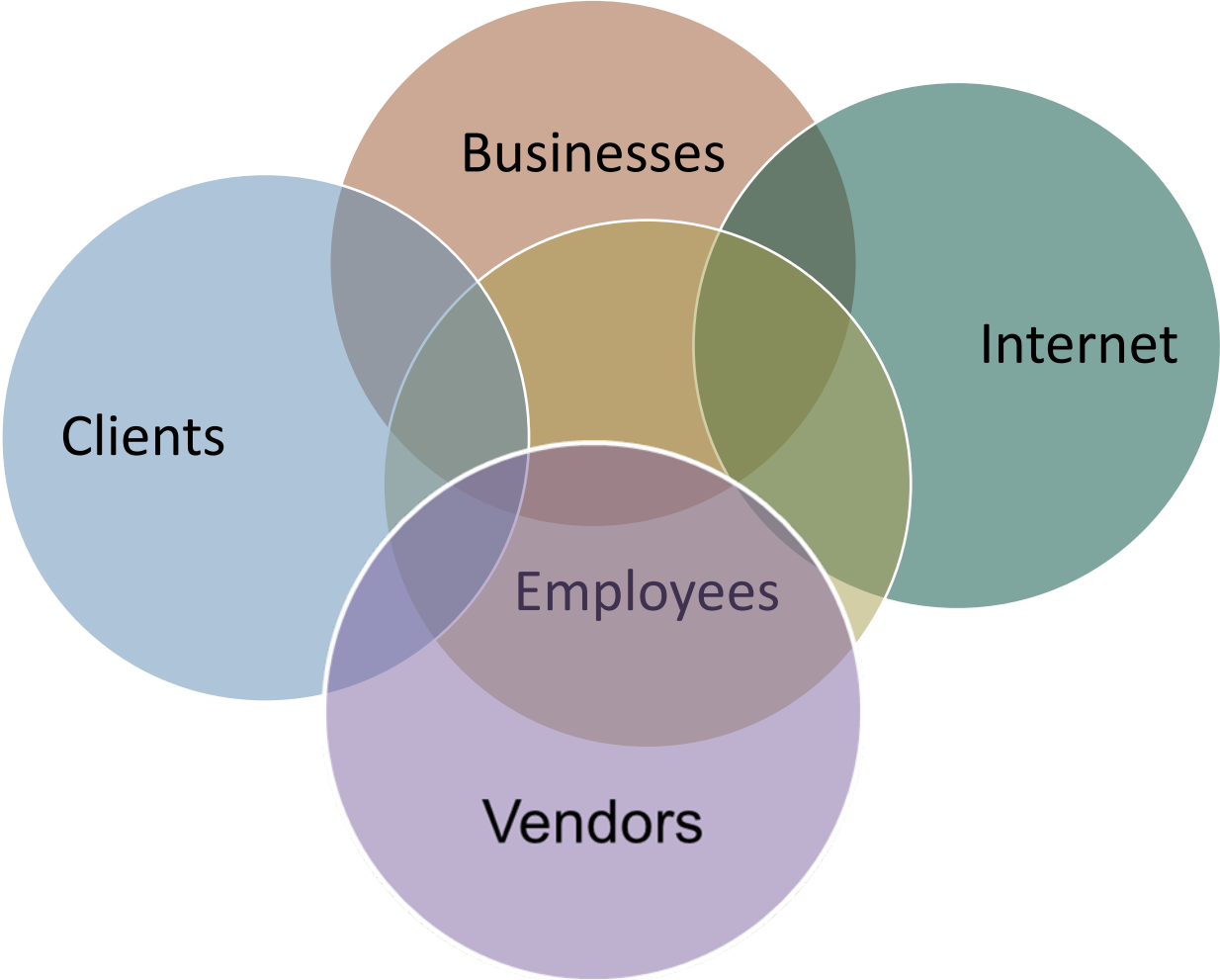
CIS Controls Overview



Cyber Security Program Triad



Know Your Web of Trust



What is Your Risk Profile?



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

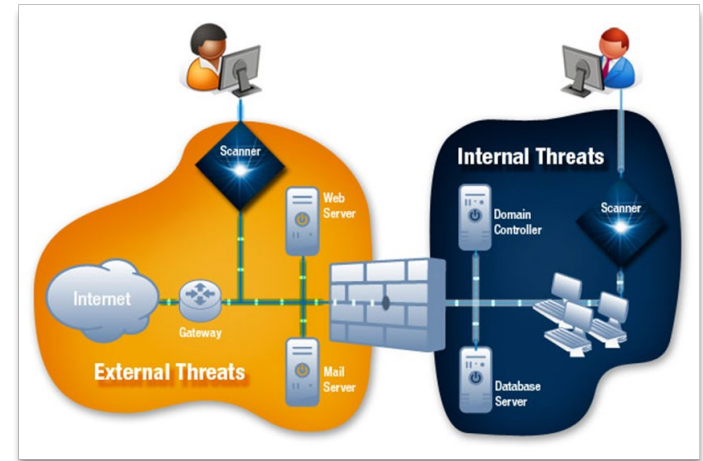


**Kreischer
Miller**

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?



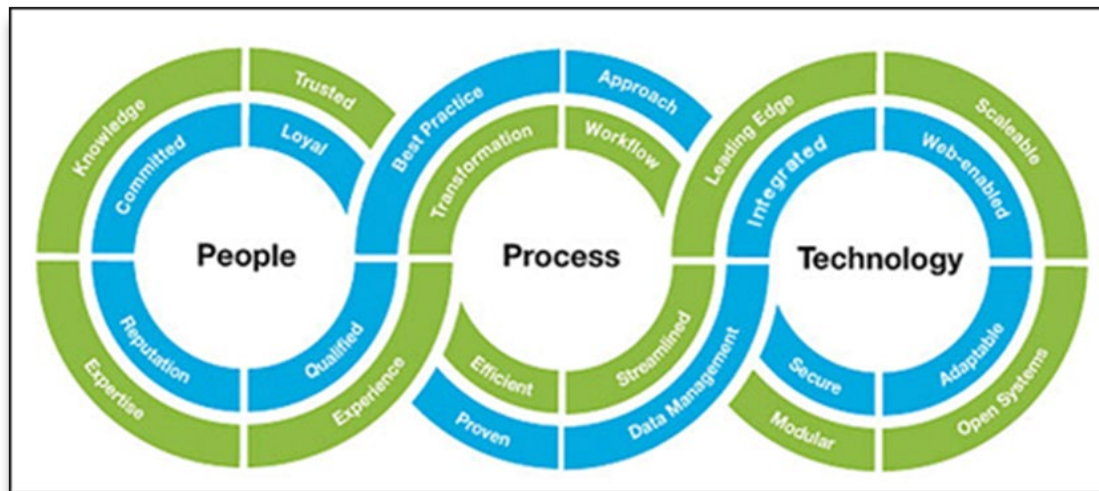
© iStockphoto.com • 307337962

**Kreischer
Miller**

PEOPLE | IDEAS | SOLUTIONS

Do We Have Updated Policies?

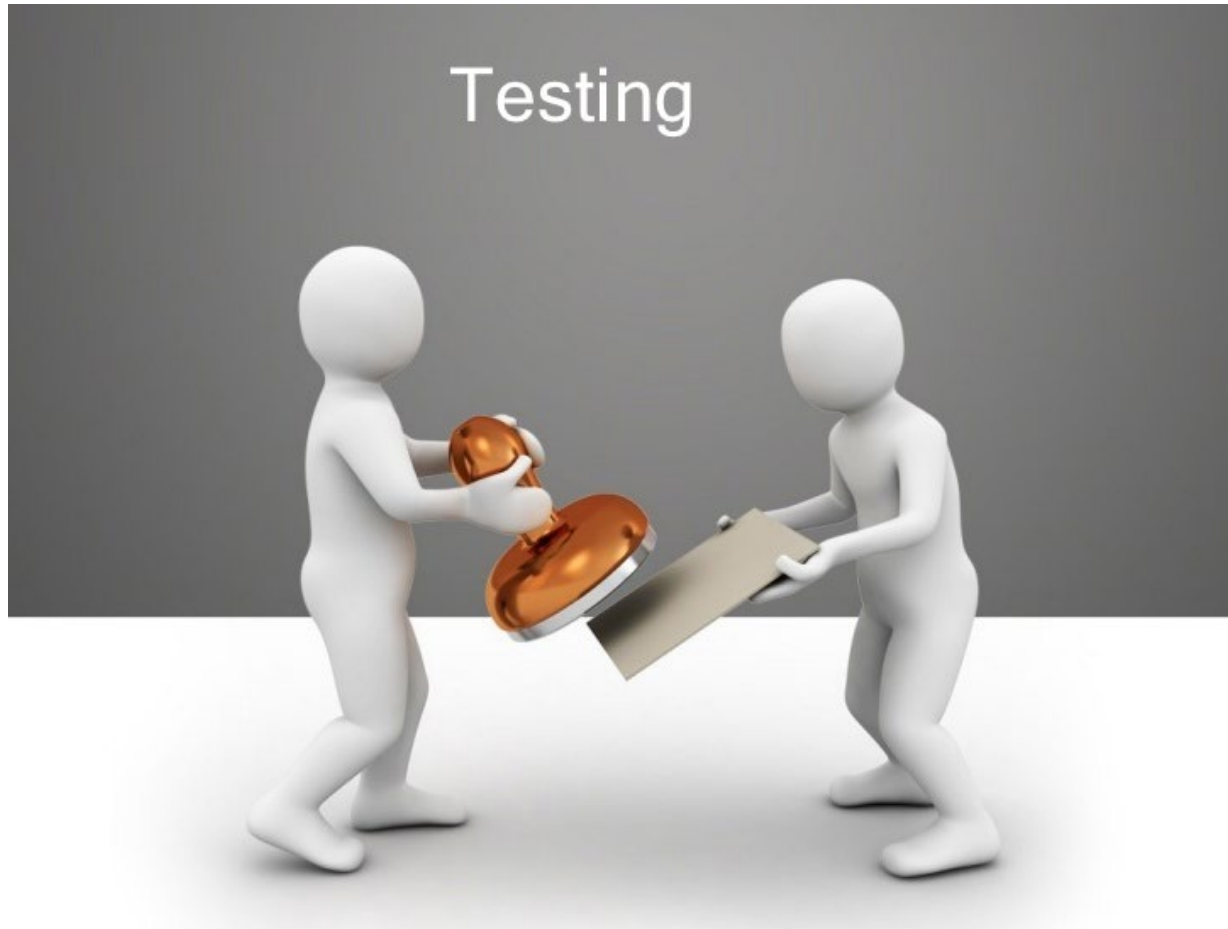
- Employee onboarding, acceptable use, termination?
- Data classification, access and protection?
- Data handling and privacy considerations?
- Vendor/contractor proper data handling and confidentiality?
 - IT department/provider(s) considerations?



Do We Have a Cyber Training Program?



Are We Validating User Knowledge?



Users Only Access What They Need?

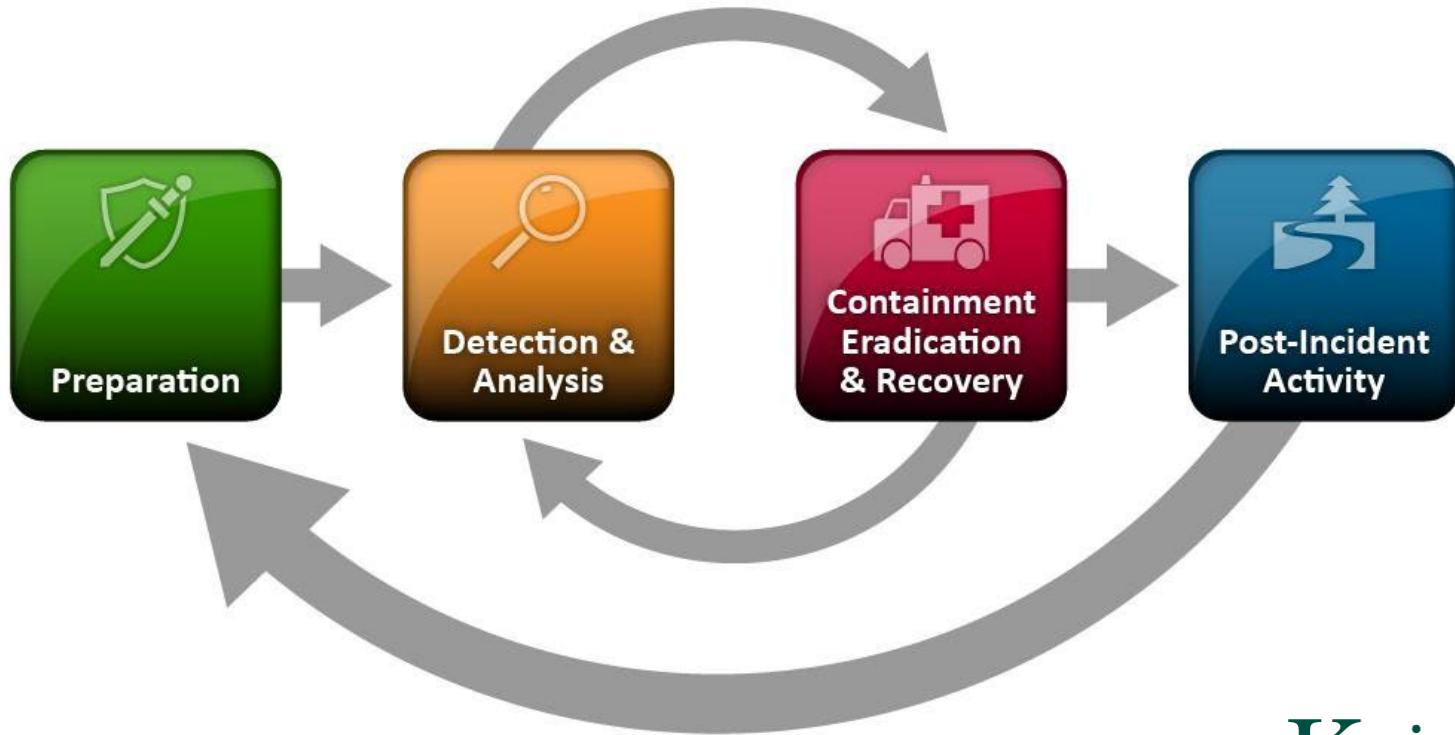
- Principle of least privilege
 - A user or a program (depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose
- Review access levels and have proper change control procedures in place
- Apply this principle to all employees and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



**Kreischer
Miller**

PEOPLE | IDEAS | SOLUTIONS

Do We Have an Incident Response Plan?



Cyber Insurance Considerations

**Kreischer
Miller**

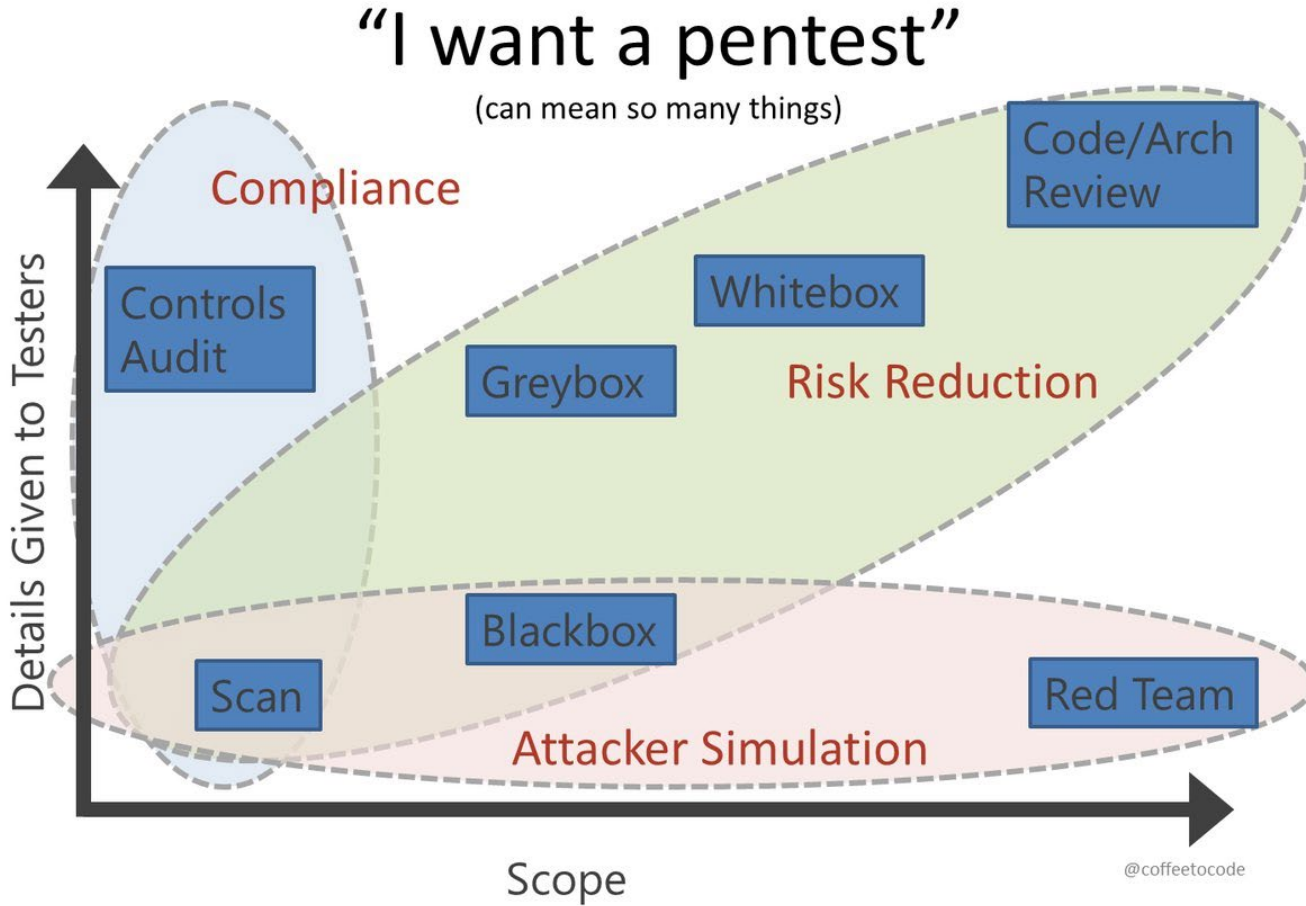
PEOPLE | IDEAS | SOLUTIONS

Do We Have a Recovery Plan?



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**



PEOPLE | IDEAS | SOLUTIONS

White House Crisis Recommendations

- Enable and mandate the use of multi-factor authentication.
- Deploy modern security and monitoring tools on all computers and devices.
- Leverage internal or external cybersecurity 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) so you are prepared to respond quickly in the case of an attack.
- Educate employees on common attack vectors.



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.



PEOPLE | IDEAS | SOLUTIONS

Thank You for Attending!



Sassan S. Hejazi, Ph.D.
Robert Rittich, CISSP

**Kreischer
Miller**

PEOPLE | IDEAS | SOLUTIONS