

Introduction to Cyber Resiliency

A460/A560, IT Auditing



KELLEY SCHOOL OF BUSINESS

INDIANA UNIVERSITY
IUPUI



Abstract

Organizations continue to implement cyber security defensive mechanisms to prevent an attack from occurring. Cyber Resiliency shifts the paradigm away from defense towards sustainability and returning to business operations. But is it clear what cyber security aspects focus on resiliency? What Cyber Resiliency areas can Internal Auditors provide value in assessing and consulting?

Cyber Resiliency

Learning Objectives

Distinguish between cybersecurity and cyber resiliency.

Gain a practical understanding of cyber resiliency.

Identify areas of assessing and consulting for cyber resiliency.

Agenda

This presentation covers the following topics:

- Cybersecurity versus cyber resiliency
- Aspects of cyber resiliency
- Cyber risk assessment and internal audit skillset
- How can internal audit add value?
- Appendix – Questions Auditors can ask?



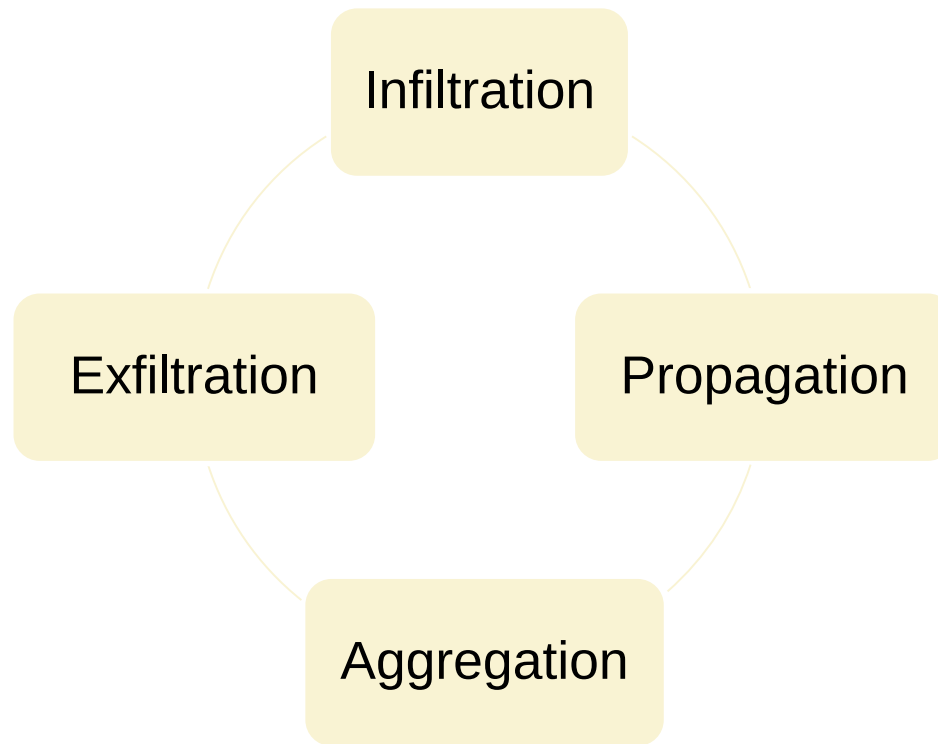
Cybersecurity vs. Cyber Resiliency

Cybersecurity

Reducing the risk to critical infrastructure by physical means or defensive cyber measures to minimize intrusions, attacks, or the effects of natural or manmade disasters.*

*As defined by Presidential Policy Directive 21 (PPD-21) (Homeland Security)

Breach Quadrilateral



Cyber Resilience

The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.*

As defined by Presidential Policy Directive 21 (PPD-21) (Homeland Security)

How do these terms differ?

Premise

- An organization will be attacked and a breach will occur

NIST SP 800-53R

- Contains over 860 controls
- 17% are focused on cyber resiliency

Why cyber resilience?

Breaches are inevitable

- Number of security incidents detected is rising

Breaches are costly

- Average total cost has increased

Security spending continues to increase

- The average trend in spend is upwards



Aspects of Cyber Resiliency



Aspects of Cyber Resiliency

Governance

User Access Permissions

Segmentation

Active Response



Aspects of Cyber Resiliency

Data Integrity Assurance

Monitoring

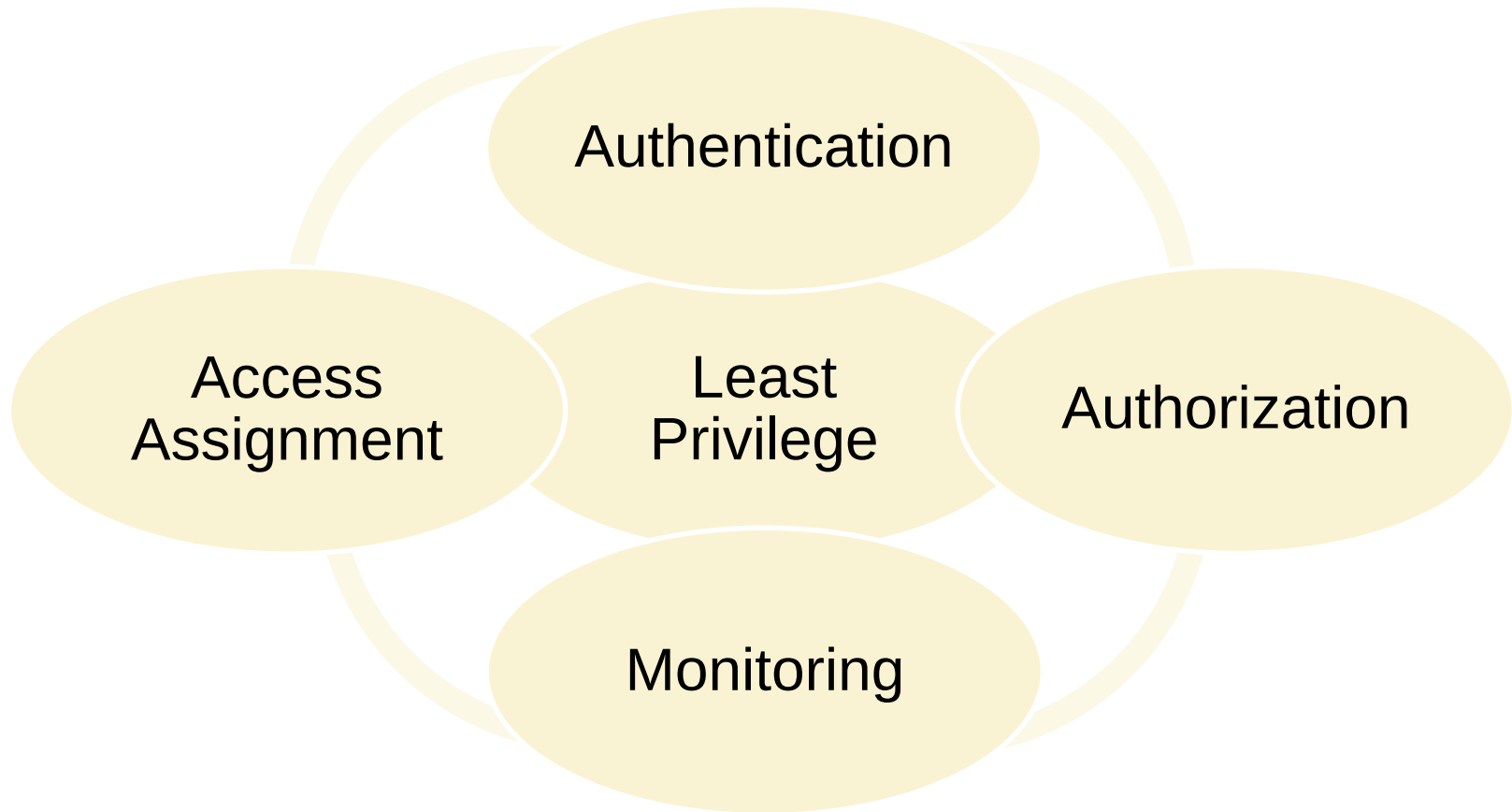
Coordinated Defense

Recovery Solutions

Governance

- Enterprise Risk Management
- Security Strategy
- Policies and Procedures
- Communication Strategy
- Awareness
- Frameworks

User Access Permissions



Segmentation

- Strategy
- Multi-layered Approach
- Multiple Domains
- Boundary Protection

Active Response

Modify based on threats:

- Privilege Capability
- Information Flow
- Incident Response
- Network Boundaries
- Recovery and Reconstitution

Data Integrity Assurance

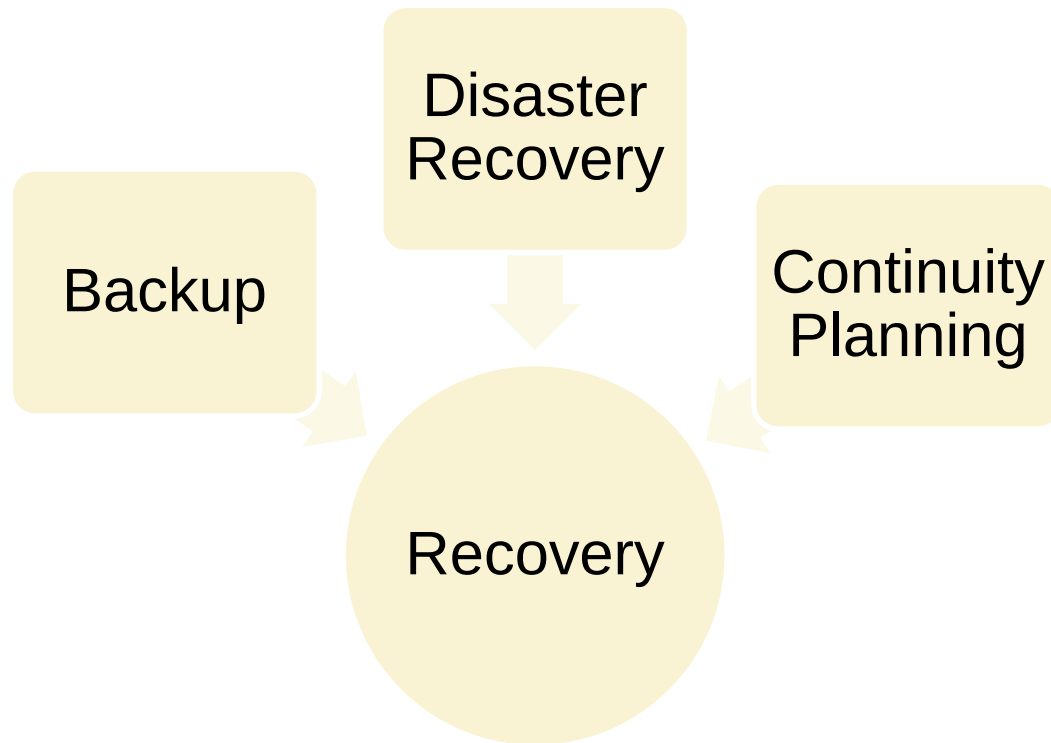
- Data Flow Protections
- Software & Hardware Integrity
- Procurement & System Development Protection
- Distribute Processing and Storage
- Input Validation
- Recovery and Reconstitution

Monitoring

- Track, Log and Alert
- Vulnerability Scans
- Penetration Tests
- Incident Response
- Threat Awareness Programs



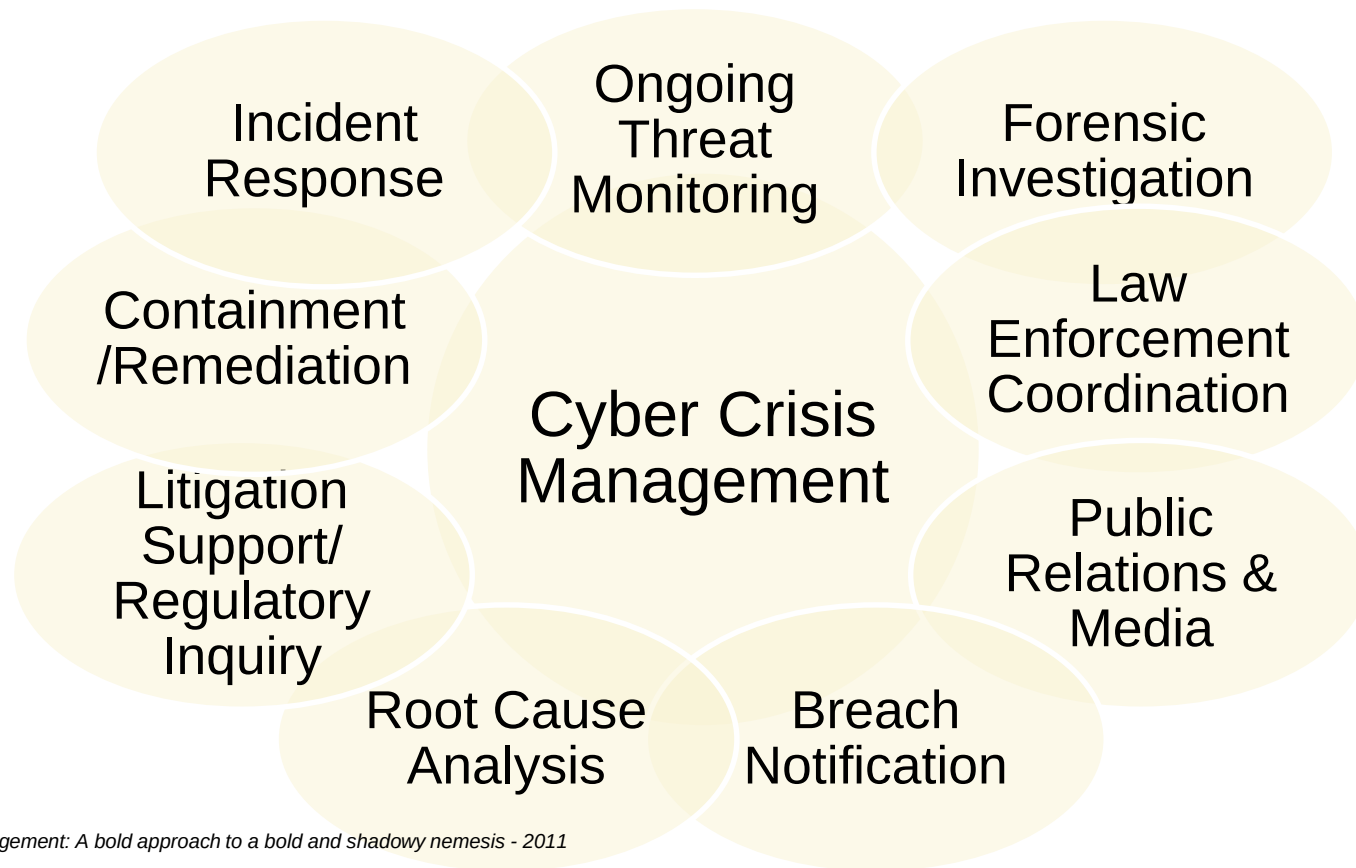
Recovery Solutions



Coordinated Defense

- Security Architecture and Strategy
- Security Training
- Diversity and Deception
- External Specialists
- Cyber Insurance
- Cyber Crisis Management

Necessary to manage all the moving parts...





Assessing Cyber Risk & Auditor Skillsets

Assessing Cyber Risk

- Understand cybersecurity practices
- Cyber resiliency perspective
- Historical audit results
- Historical cyber trends



Common Data Breach Root Causes

Stolen
Credentials

Unencrypted
Data

Phishing
Schemes

Malware

Unmanaged
Warnings
and Alerts

Technical Skills Gap?

- Assess staff IT and cyber knowledge
- Establish basic IT and cyber knowledge for all internal auditors
- Create formalized training program for internal auditors



What can Internal Audit do?

What Can Internal Audit Do?

Review Governance Processes:

- Communicate need for resiliency
- Review cyber resiliency using a known framework
- Review user awareness and training programs
- Review network resiliency strategy
- Review alignment of policies and procedures that govern resiliency to current security architecture and strategies

What Can Internal Audit Do?

Assess Access Permissions:

- Review privileged access capability
- Perform access management audits
- Review user account activation/deactivation processes
- Review transferred employees access capability
- Review processes that ensure access is periodically reviewed

What Can Internal Audit Do?

Review Segmentation Strategy:

- Review adequacy of network segmentation strategy to protect critical data and systems
- Review strategy for use of multiple domains
- Test to ensure network segments are protected

What Can Internal Audit Do?

Ensure Active Response Posture:

- Review IDS/IPS deployment and active response strategy
- Test appropriateness of strategy to limit data flow upon detection of attack
- Test to ensure response plans are updated as threat levels change

What Can Internal Audit Do?

Assess Data Integrity Assurance:

- Review administration of outbound filters
- Review manner data flows between domains or network segments
- Review adequacy of supplier/vendor management practices
- Validate whether Secure-SDLC is employed

What Can Internal Audit Do?

Ensure Active Monitoring Occurs:

- Test to ensure events are logged and timely follow-up occurs on alerts
- Employ third party expert to perform cyber assessment
- Test to ensure periodic vulnerability scan results are timely remediated
- Test effectiveness of threat awareness programs

What Can Internal Audit Do?

Assess Recovery Solutions:

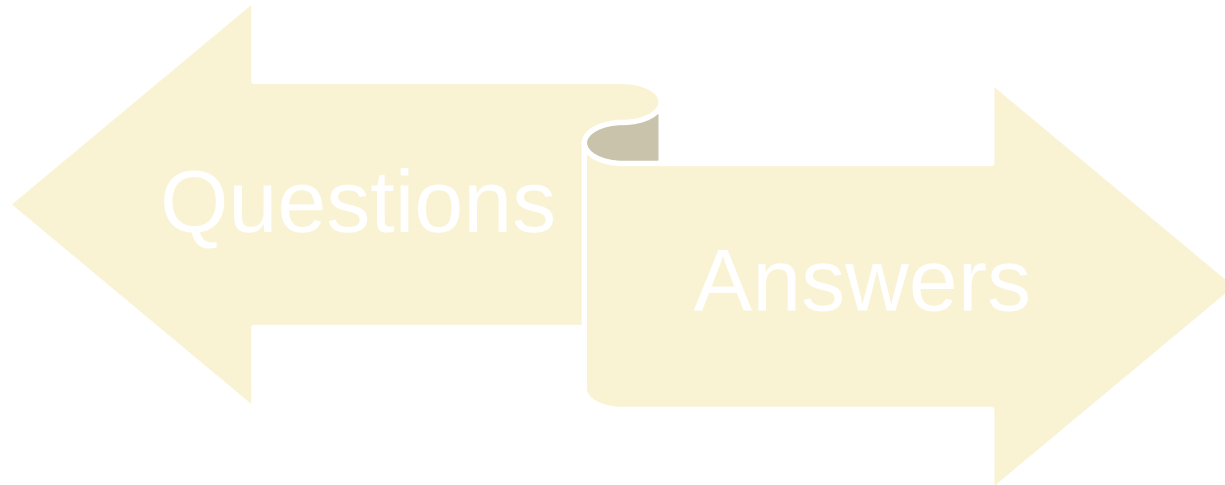
- Walk-through offsite storage facility
- Test to ensure regular backups of all systems occur
- Test to ensure tape restores are periodically tested
- Review redundancy of power and cabling
- Participate in disaster recovery and continuity exercises

What Can Internal Audit Do?

Ensure Coordination of Defense Posture:

- Review cyber policies and procedures
- Review cyber insurance coverage and requirements
- Review security strategy and architecture
- Test to ensure critical need external specialists are contracted in the event of breach

Cyber Resiliency





APPENDIX

Questions Auditors Can Ask?

Governance:

- Is cybersecurity assessed as part of enterprise risk management?
- Is a cyber-framework used to assess overall cybersecurity practices?
- Is defense-in-depth strategy deployed?
- Are cyber defenses coordinated?
- Do cybersecurity policies and procedures exist and maintained?
- Are users annually trained?
- Is user training tracked and monitored to completion?

Questions Auditors Can Ask?

User Access Permissions:

- Do all users with privileged access capability require it?
- Is monitoring of privileged activity tracked and alerts occur for suspicious activity?
- Are privileged users required to use 2-factor authentication?
- Do privilege users have 2 accounts one for normal usage and one for privileged activity?
- Is a user limited to least privilege within each application?

Questions Auditors Can Ask?

User Access Permissions:

- Is a user limited to least privilege amongst applications?
- Is a new user's set-up with least privileges and as authorized?
- Is new user passwords distributed to them in a secure manner?
- Is a termed user's access disabled timely upon termination?
- Is a transferred user's access removed upon transfer?

Questions Auditors Can Ask?

Segmentation:

- How resilient is the organizations network?
- Are domains separated by function?
- Does the network segment critical functions, systems or data?
- How is firewall configuration managed?
- How is IDS/IPS configuration managed?
- Is IDS/IPS in active mode?
- Who has access to network appliances?

Questions Auditors Can Ask?

Segmentation:

- Is change management required for network appliances?
- Are white and black lists residing on network appliances actively managed?
- Is data loss prevention deployed and outgoing data restricted based on predefined policies?

Questions Auditors Can Ask?

Active Response:

- Are network appliances (i.e., firewall, IDS/IPS, DLP, etc.) in active mode?
- For each network appliance in active mode, has a cost-benefit analyses been performed to ensure the level of protection is balanced with potential business disruption?
- Are incidents correlated and do responses timely occur based on threat?
- Is critical data restricted on the network based on threat level?

Questions Auditors Can Ask?

Data Integrity Assurance:

- What data and systems are isolated based the threat and are these the organization critical data assets?
- Are systems protected using integrity verification tools?
- Is hardware disposed in such a manner to ensure data cannot be stolen?
- Is secure SDLC employed?
- Is hardware and software acquired only from known sources?

Questions Auditors Can Ask?

Monitoring:

- Are all critical events logged?
- Are event logs secured?
- Are all events tracked to remediation and timely resolved?
- Are vulnerability and penetration tests performed and reported results reviewed and corrected?

Questions Auditors Can Ask?

Recovery Solutions:

- Are backups stored onsite or offsite in secure locations?
- Are alternate power sources employed?
- Are disaster recovery plans tested?
- Is cybersecurity incorporated into the continuity plan?

Questions Auditors Can Ask?

Coordinated Defense:

- Are diversity and deception processes used?
- Does the organizations continuity plan incorporate cybersecurity practices?
- Are external specialists on contract in the event required?
- Does cyber insurance provide appropriate coverage?



Questions