How to audit cyber incident response

ACUA WEBINARS

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education

- Don't forget to connect with us on social media!

ACUA SOCIAL NETWORKING

ACUA Virtual Learning Director
Wendee Shinsato, CPA, CIA
Assistant Vice Chancellor
California State University

ACUA Virtual Learning Volunteer
Christiana Oppong, CIA, CCSA
Senior Auditor
Princeton University

ACUA Virtual Learning Volunteer
Virginia L. Kalil, CIA, CISA, CFE, CRISC
Executive Director/Chief Internal Auditor
University of South Florida

CYBER INCIDENT RESPONSE

Presenters

Mike Cullen

Principal, CISA, CISSP, CIPP/US

mike.cullen@bakertilly.com

Morgan Mincy

Manager, CPA

morgan.mincy@bakertilly.com

Objectives

- Understand how auditors can get a seat at the table and engage with cybersecurity stakeholders
- Make the case for performing cybersecurity related audits or reviews
- Implement potential approaches for getting involved in post-breach remediation activities

Polling Question

- Do you have a role (e.g., seat at the table) for cybersecurity that is supported by your institution?

A. Yes

B. Sort of

C. No

D. Unsure

Agenda

- How to get a seat at the table and engage with cybersecurity stakeholders and make the case for performing cybersecurity related audits or reviews

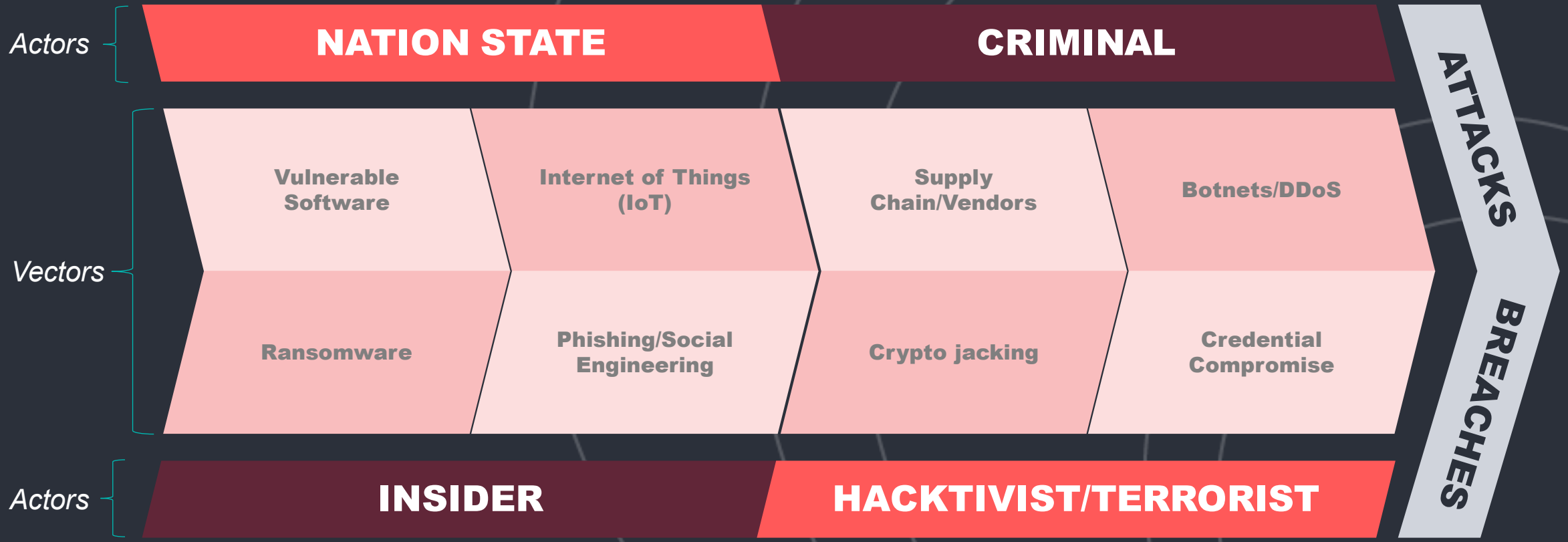
- How to audit cyber incident response

CYBER INCIDENT RESPONSE

How to get a seat and make the case

CYBER INCIDENT RESPONSE

Threats



Risks

Reputation

- Damage to brand/ negative publicity
- Damage to individual faculty/ researcher professional standing

Competitive

- Loss of intellectual property
- Damage to relationships with partners (e.g., research sponsors, other institutions)

Operational

- Loss of time spent to respond
- Loss of ability to operate or continue work

Financial

- Cost of response for incidents
- Loss of future funding

Regulatory

- Cost to address requirements
- Cost of fines, sanctions

Polling Question

- Does your institution follow a specific cybersecurity framework or standard?

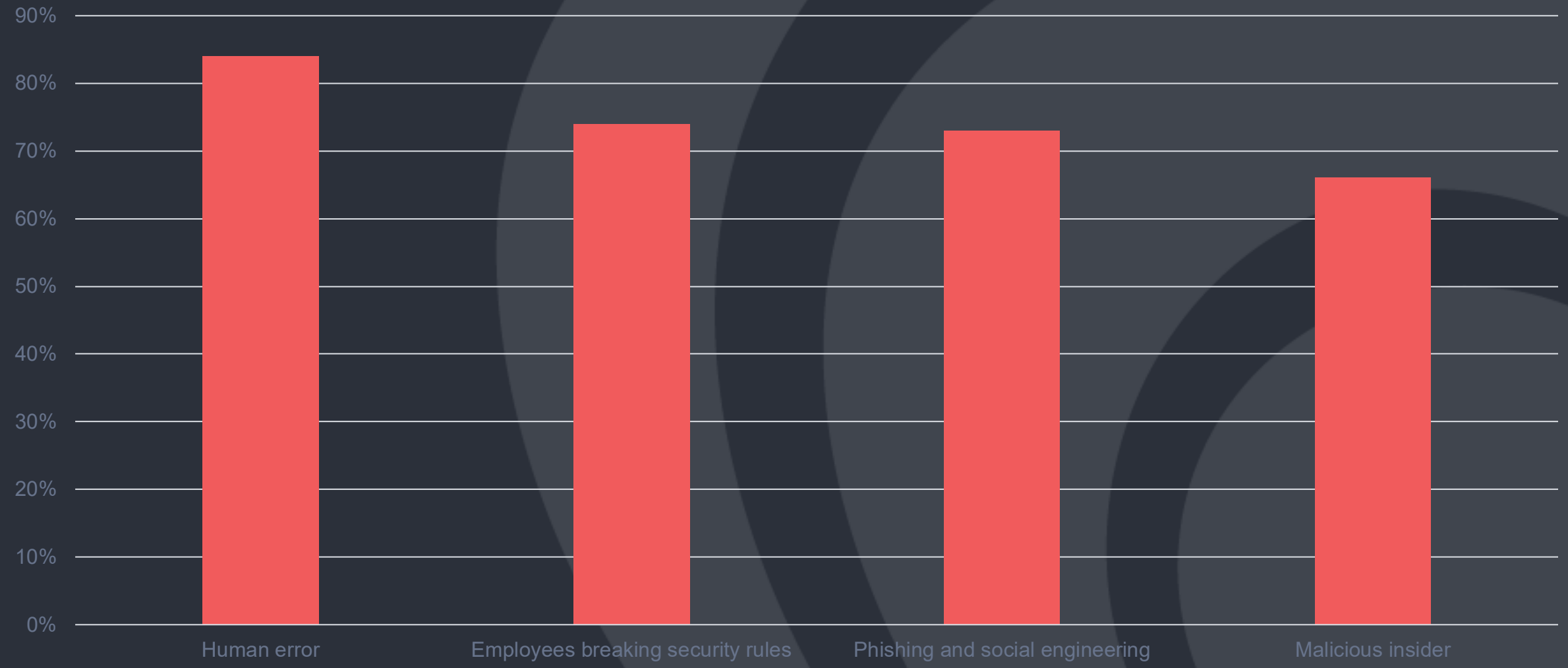
A. Yes

B. Sort of

C. No

D. Unsure

Incident rates



Insider Data Breach Survey 2021 (egress.com)

Recent incidents

A lawsuit filed in federal court alleges the University of Minnesota failed to "establish appropriate security safeguards" following leak of sensitive personal data from records dating back to 1989.

An annual Sophos study found that exploited vulnerabilities were the most common root cause of ransomware attacks in higher education (40%), with compromised credentials falling in second place at 37%.

The Colorado Department of Higher Education (CDHE) reported a massive data breach in August 2023 impacting a large group of students and educators dating back to 2004.

A report by IBM found that the average cost of a cybersecurity breach was $3.7 million at colleges or universities and related training and development companies between March 2022 and March 2023.

A two-day internet shutdown at University of Michigan in August 2023 affected campus IT systems used for research and fundraising, delaying financial aid reimbursements.

An Ohio community college notified 290,000 people of a data theft breach this spring that may have compromised their personal, financial and health information in September 2023.

Cyber insurance market

Causes

- Cybercrime (e.g., ransomware attacks)
- Frequency and cost of claims
- Complexity of threats / risks
- Rising claims costs

Impacts

- Significant rate increases
- Stringent approach to underwriting and risk acceptance
- Reduced capacity (i.e., lower limits, less cover)
- Increased excesses
- Inner limits imposed (e.g., ransomware, social engineering)

CYBER INCIDENT RESPONSE

How to audit cyber incident response

Polling Question

- Have you audited your institution's cyber incident response program?

A. Yes, in the last two years

B. Yes, sometime prior to two years ago

C. No

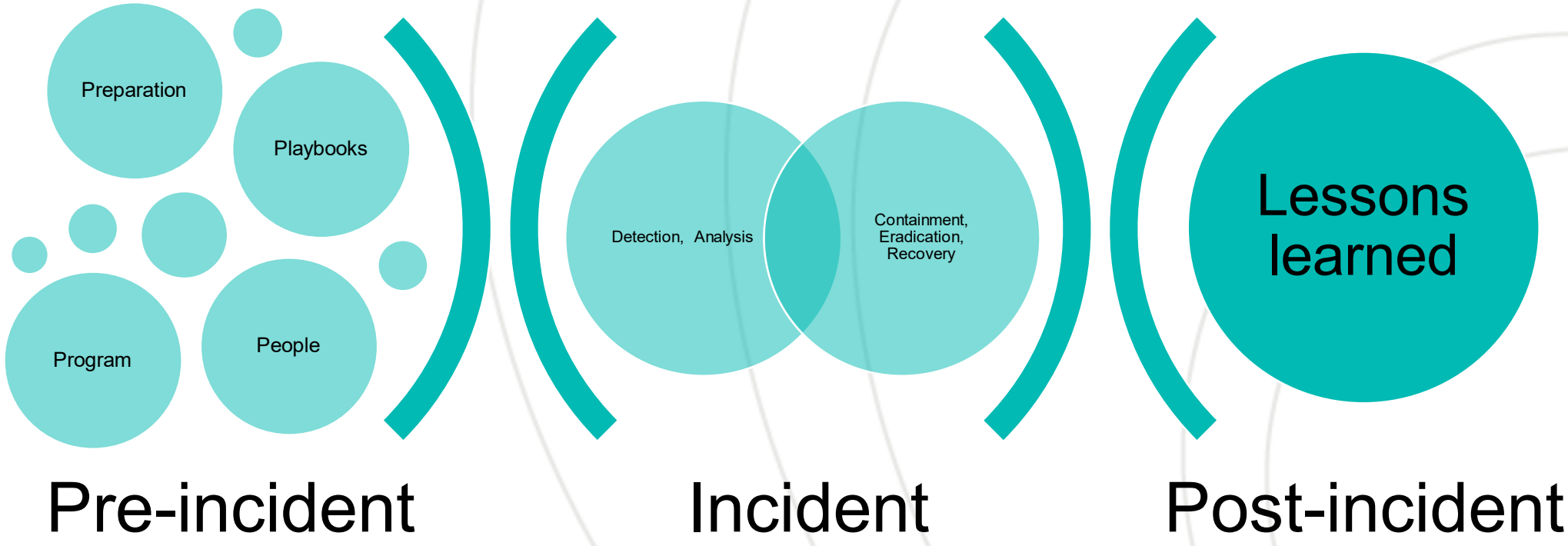
D. Unsure

What do you audit?

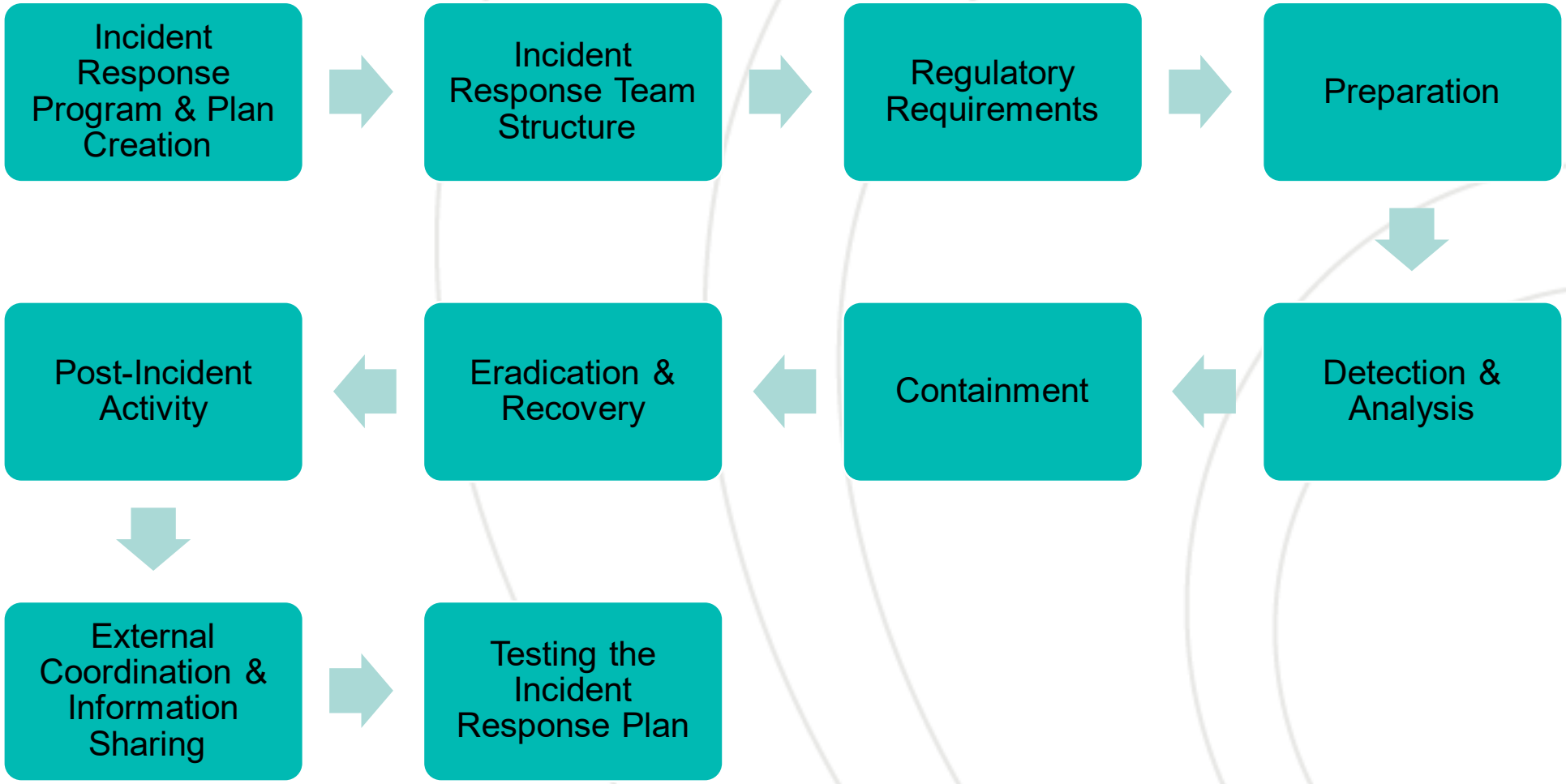
- Assurance vs. advisory
- Program vs. A plan
- All incidents vs. specific types
- Open vs. under-privilege

What is your audit criteria?

Incident Response Lifecycle (NIST SP 800-61)



What are the key controls?



Polling Question

- Do you participate in cyber incident response activities as a member of the team?

A. Yes, as an official member of the incident response team

B. Yes, as an advisor to the incident response team

C. Yes, as needed or in an unofficial manner

D. No

E. Unsure

What are the common findings?

Incident Response Program & Plan Creation	• No updated plan supported by full program elements (see other findings)
Incident Response Team Structure	• No involvement by risk management (insurance), public relations or board
Regulatory Requirements	• No coverage for new GLBA rules or HIPAA rules
Preparation	• No existing data inventory matched to systems
Detection & Analysis	• No SIEM tool for alerting
Containment	• No criteria for specific strategies
Eradication & Recovery	• No explicit alignment with IT recovery plans
Post-Incident Activity	• No updates to program based on lessons learned
External Coordination & Information Sharing	• No proactive coordination with law enforcement prior to incidents
Testing the Incident Response Plan	• No periodic testing with all team members participating

How else can audit be involved?

Area	Potential Internal Audit Activities (beyond traditional audits)
Pre-incident	• Join the team • Observe/participate in a table-top exercise to test the program
Incident	• Assess detection technologies, including retention of system data (e.g., logs) • Analyze event correlation methods, including distributed systems • Review incident tracking systems/methods • Review law enforcement involvement approach/method • Assess communication/public relations involvement • Assess institutional framework for key decisions (e.g., paying ransom)
Post-incident	• Analyze response for appropriate coverage beyond known incident impact • Collaborate with incident response team to craft lessons learned from incident • Develop metrics for incident response reporting

Stay in touch

Mike Cullen
Principal

mike.cullen@bakertilly.com

Morgan Mincy
Manager

morgan.mincy@bakertilly.com

Subscribe to receive higher education alerts and event invitations: https://connect.bakertilly.com/subscribe

Subscribe to our Higher Ed Advisor podcasts: https://connect.bakertilly.com/higher-ed-advisor-podcast

Questions & Answers

Announcements

Upcoming ACUA Webinar

December 7th - Best Practices in Research Documentation

See the ACUA website for more details

www.ACUA.org

New Kick Starter Available!

Cleaning and Transforming Data with Power Query

Download today in the members-only Audit Tools section of www.ACUA.org

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education

Next Kick Starter Release is November 15th!

Athletic Sports Camps

Will be available in the members-only Audit Tools section of www.ACUA.org

CONNECT WITH US

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Advancing Auditing in Higher Education

Working on a new audit subject? Looking for some best practices or insights from other higher education institutions? Connect with your colleagues on Connect ACUA! **Connect.ACUA.org**

Share your knowledge with others: Did you know that Connect ACUA allows you to post new messages directly from your email without logging in to the Connect ACUA website? Reply to a post today!

ACUA WEBINARS

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education

Stay Updated

- The College and University Auditor is ACUA's official journal. Current and past issues are posted on the ACUA website.
- News relevant to Higher Ed internal audit is posted on the front page. Articles are also archived for your reference under the Resources/ACUA News.

Get Educated

- Take advantage of the several FREE webinars held throughout the year.
- Attend one of ACUA conferences:

Audit Interactive

AuditCon

(Stay tuned)

- Contact ACUA Faculty for training needs.

Get Involved

- The latest Volunteer openings are posted on the front page of the website.
- Visit the listing of Committee Chairs to learn about the various areas where you might participate.
- Nominate one of your colleagues for an ACUA annual award.
- Submit a conference proposal.
- Present a webinar.
- Become a Mentor
- Write an article for the C&U Auditor.
- Write a Kick Starter.

Connect with Colleagues

- Subscribe to one or more Forums on the Connect ACUA to obtain feedback and share your insights on topics of concern to higher education internal auditors.
- Search the Membership Directory to connect with your peers.
- Share, Like, Tweet & Connect on social media.

Solve Problems

- Discounts and special offers from ACUA's Strategic Partners
- Kick Starters
- Risk Dictionary
- Mentorship Program
- NCAA Guides
- Resource Library
- Internal Audit Awareness Tools
- Governmental Affairs Updates
- Survey Results
- Career Center.....and much more.

ACUA WEBINARS

Join us for our upcoming webinar.