Establishing an Incident Response Plan

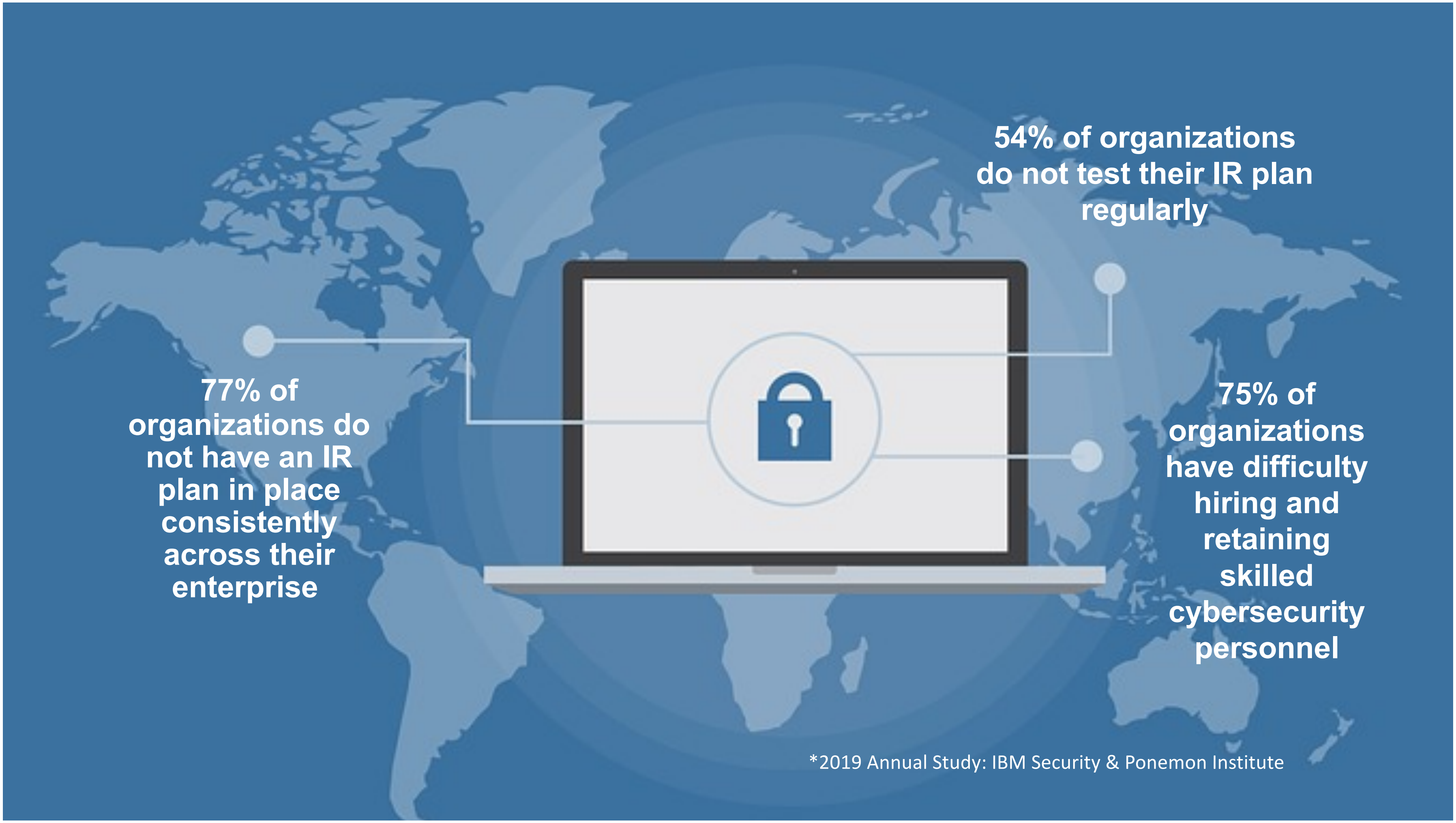
Michael McCartney

President, Avalon Cyber

- Co-founder of the Western New York Regional Computer Forensic Lab
- Former Assistant Chief Investigator for the New York State Attorney General’s Office Internet Crime Bureau
- Expert in Computer Crime Investigations and Computer Forensics

AGENDA

- Incident Response Landscape
- Incident Response Considerations
- NIST Framework
- Elements of an IR Plan Lifecycle
- Q&A



54% of organizations do not test their IR plan regularly

77% of organizations do not have an IR plan in place consistently across their enterprise

75% of organizations have difficulty hiring and retaining skilled cybersecurity personnel

*2019 Annual Study: IBM Security & Ponemon Institute

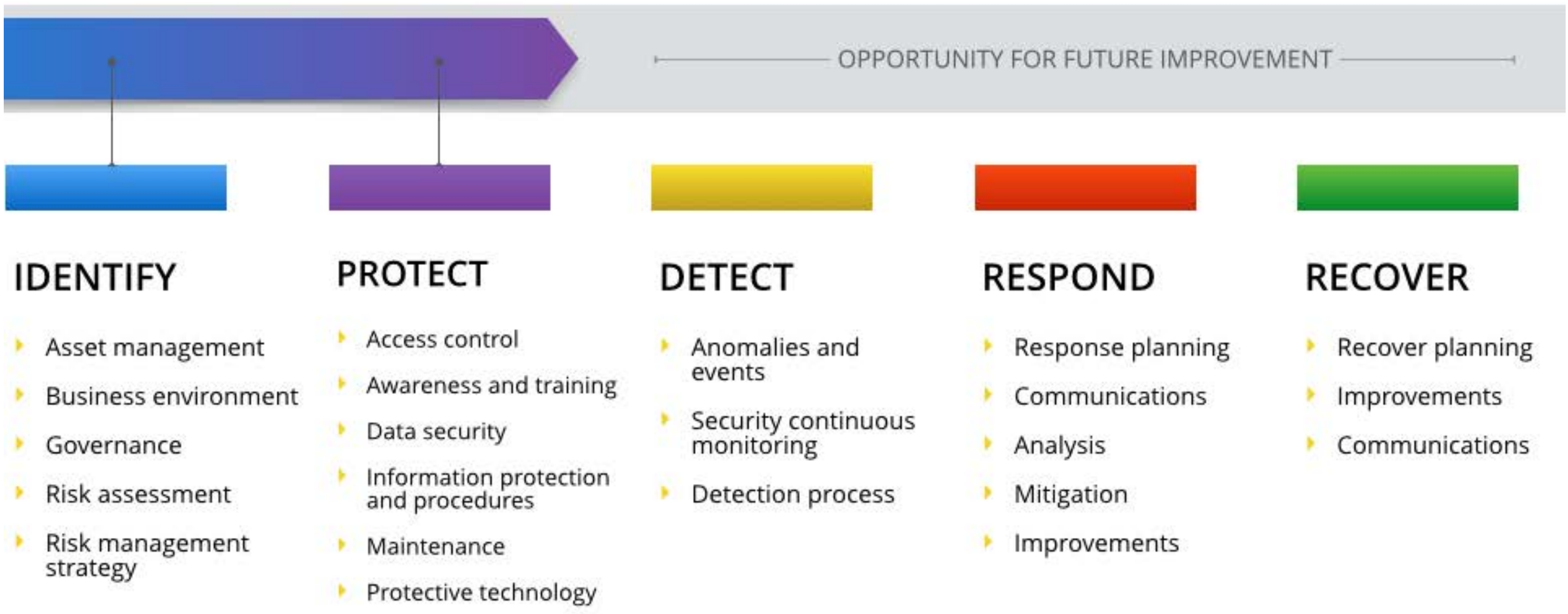
Internal Organizational Considerations

- Building an IR plan that fits business objectives
- Acceptance that incidents will occur
- Gaining management engagement
- Employees and other stakeholder education
- How to work together in together in a crisis
- Understanding the potential pitfalls in writing an IR plan

Information Governance Considerations

- Who are you?
- What kind of data do you have?
- Where is your data?
- How are you protecting your data?

NIST Cybersecurity Framework



OPPORTUNITY FOR FUTURE IMPROVEMENT

IDENTIFY

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT

- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology

DETECT

- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND

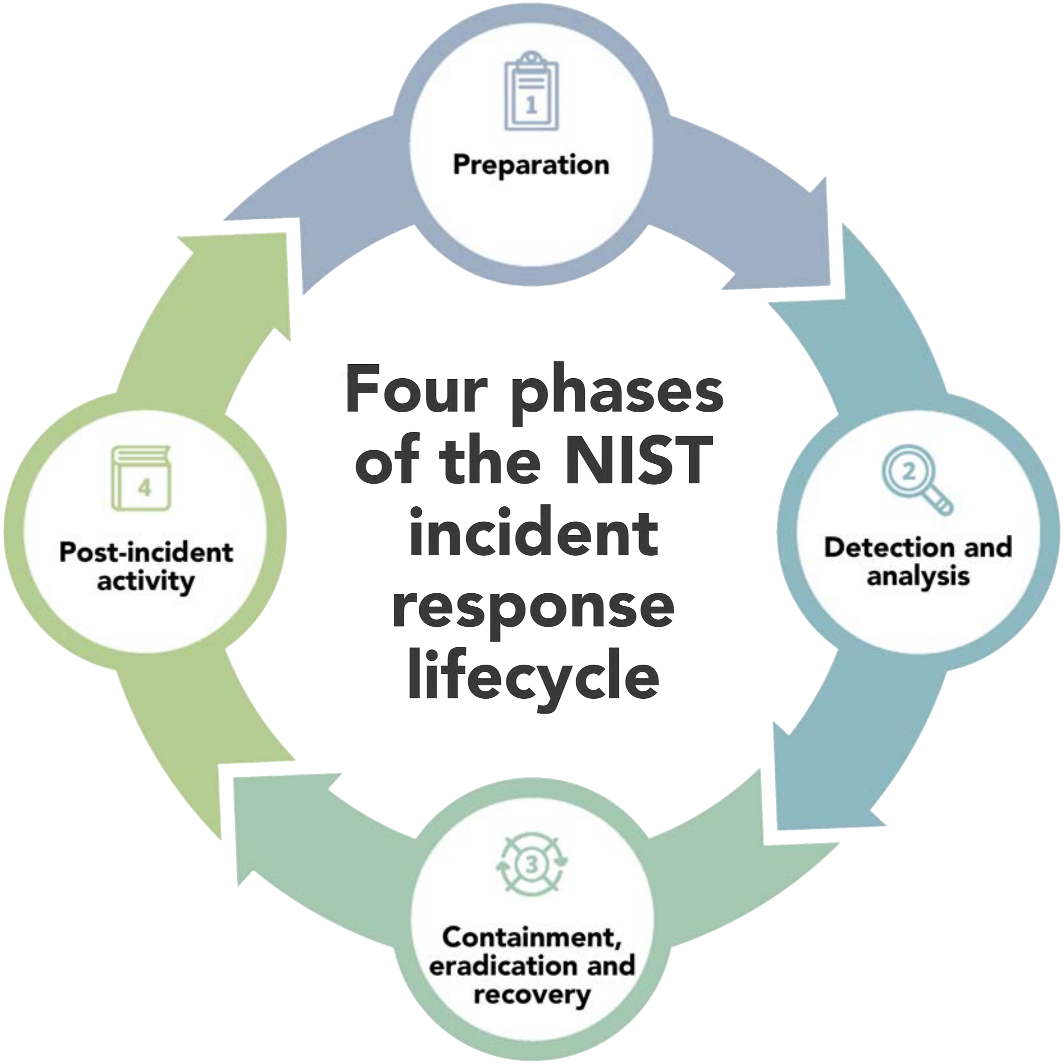
- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

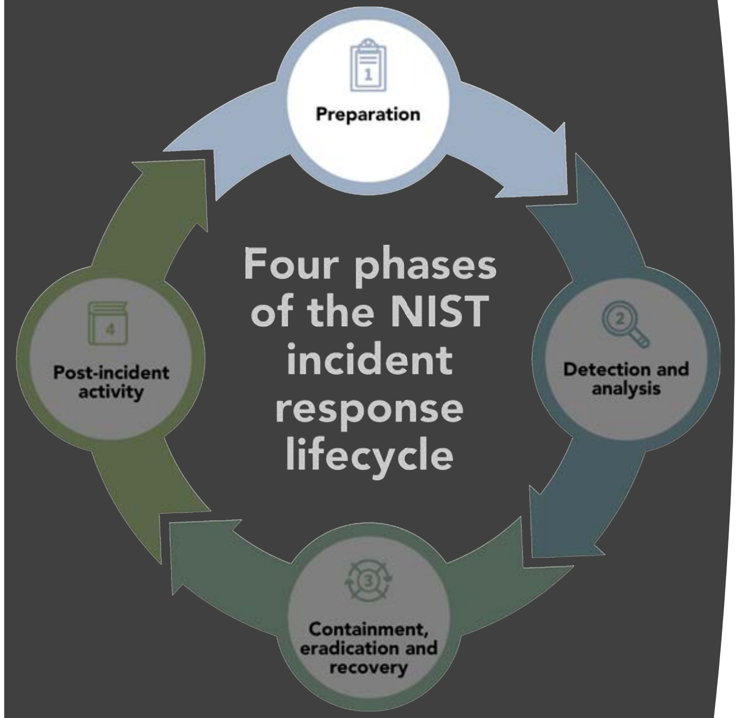
RECOVER

- Recover planning
- Improvements
- Communications

NIST IR Lifecycle

Incident management is NOT linear – new threats lead to new policies and procedures and will inform each other constantly.

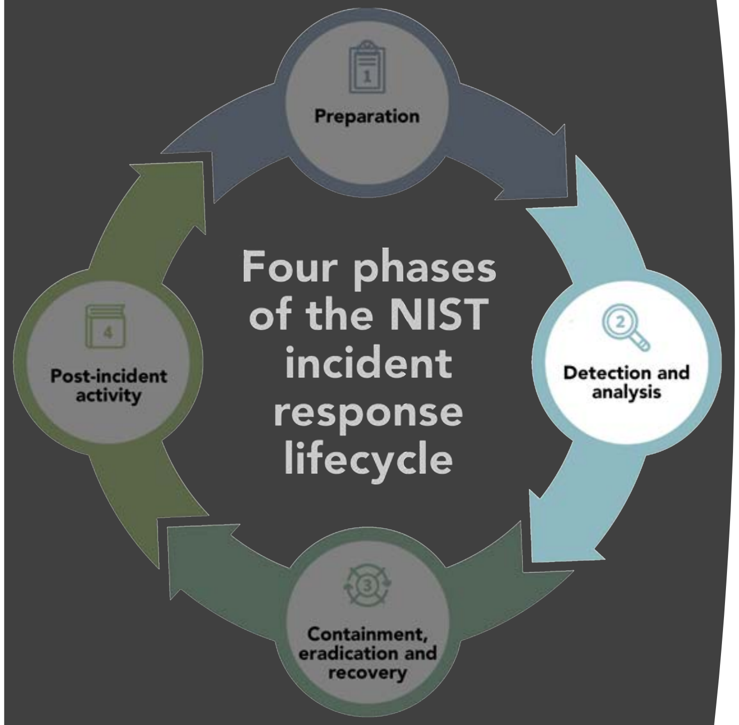

1
Preparation
2
Detection and analysis
3
Containment, eradication and recovery
4
Post-incident activity
Four phases of the NIST incident response lifecycle


Preparation
Detection and analysis
Containment, eradication and recovery
Post-incident activity
Four phases of the NIST incident response lifecycle
1
2
3
4

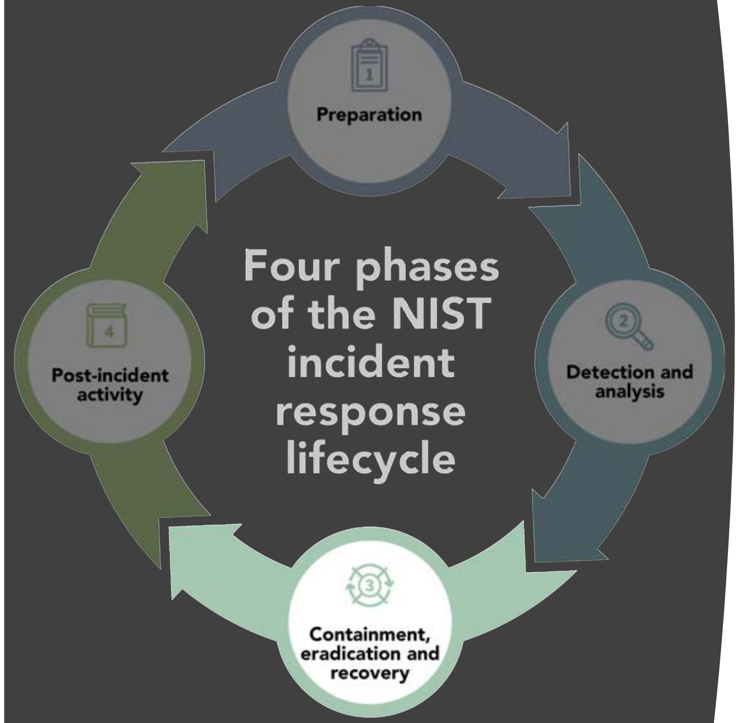
- Risk Assessment
- Identify Team, Define Roles, and Train
- Threat Modeling
- Establish Policies, Procedures & Agreements
- List Assets
- Develop Playbooks & Communication Plans
- Prepare Incident Log

IR Simulation Exercises

- Nominate the Simulation Architect & Facilitator
- Planning: Number of scenarios, timing, location, participants, establishing goals
- Design an effective scenario
  - Format/Structure
  - Scenario
  - Props/Tools
  - Scenario inspiration can be found on The Office of Cyber Security for the State of Washington


Four phases of the NIST incident response lifecycle
1
Preparation
2
Detection and analysis
3
Containment, eradication and recovery
4
Post-incident activity

- Do you have the tools/technology to identify root cause issues?
- Who, What, Where, When, How?
- Endpoint Analysis
- Threat Hunting
- Defense in Depth
- Vulnerability Management
- Purple Team



Four phases of the NIST incident response lifecycle

1 Preparation

2 Detection and analysis

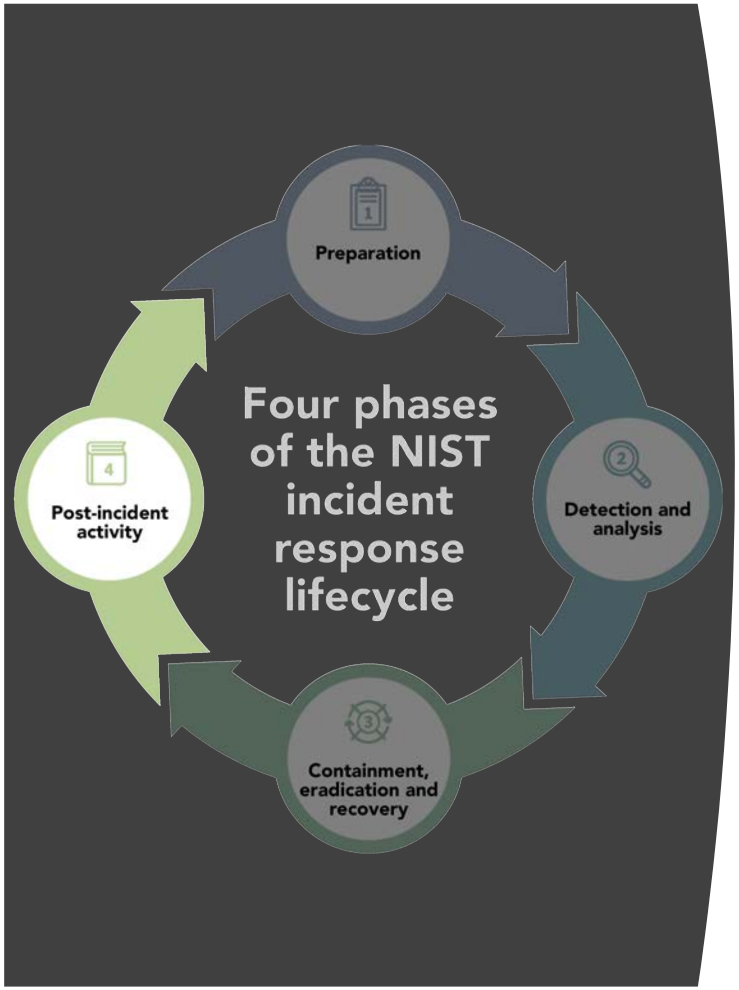
3 Containment, eradication and recovery

4 Post-incident activity

With your current technology, how can you **contain** a bad actor, malware, etc.?

How will you ensure that the root cause AND incident artifacts are **eradicated**?

Do you currently possess the capability to **recover** from a breach/ransomware outbreak, security event, etc.?

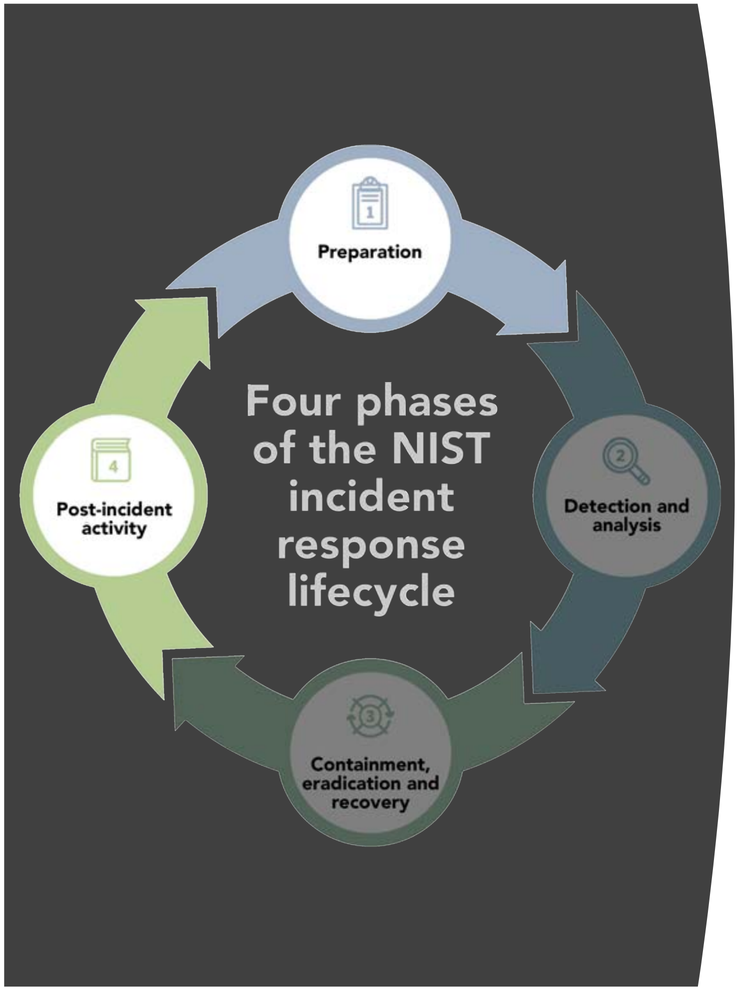

Four phases of the NIST incident response lifecycle
1
Preparation
2
Detection and analysis
3
Containment, eradication and recovery
4
Post-incident activity

Postmortem update with key stakeholders

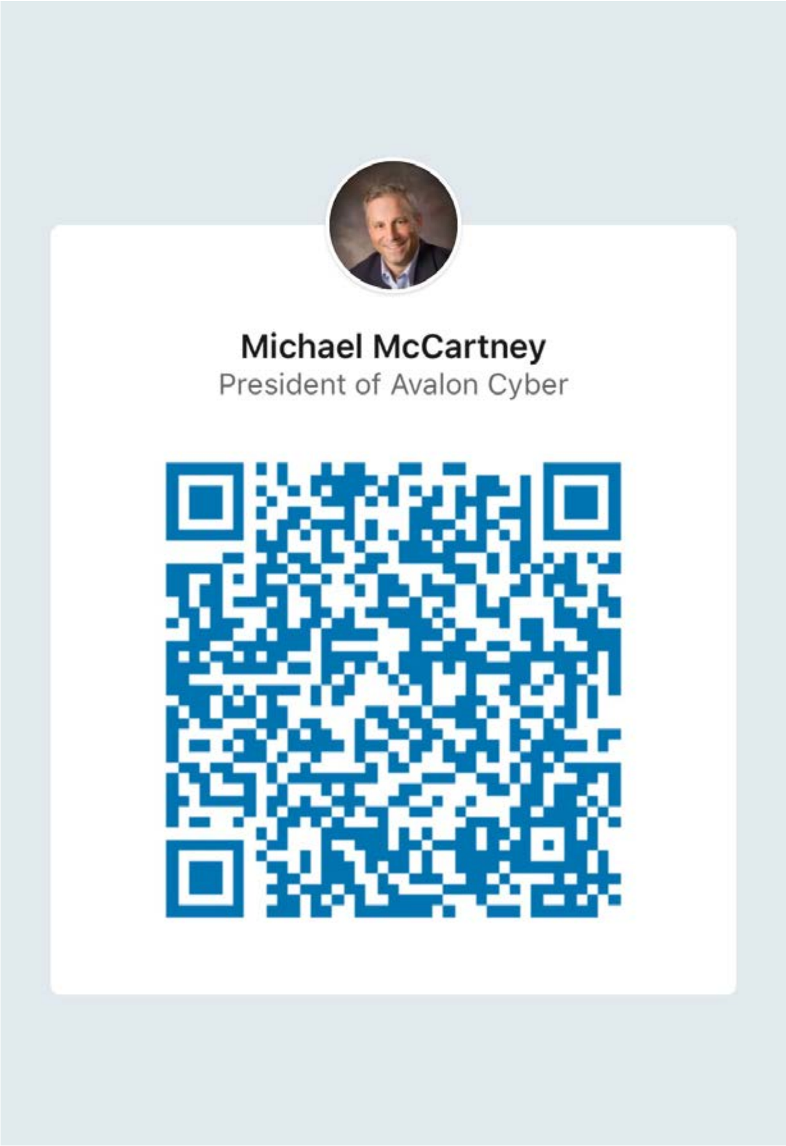
Root Cause Analysis (RCA) of incident

Questions to drive a “Lessons Learned” discussion:

- What changes need to be made to the cybersecurity posture?
- How should employees and incident responders be trained differently?
- What weaknesses did the breach exploit? (Hard and soft included)
- How will you ensure a similar breach doesn’t happen again?
- What changes are needed to the IR plan based on outcome?


Preparation
1
Detection and analysis
2
Containment, eradication and recovery
3
Post-incident activity
4
Four phases of the NIST incident response lifecycle

- Update Risk Assessment
- Revise Team, Define Roles, and Update Training Materials
- Threat Modeling
- Revise Policies, Procedures, and Agreements
- List Assets
- Update Playbooks and Communication Plans
- Prepare Incident Log



Michael McCartney

President of Avalon Cyber

Q
A

Thank you for listening!