NCHICA INCIDENT RESPONSE 101 FORUM

Creating the IR Plan Using Playbook Scenarios

Jon Sternstein

Stern Security

ABOUT

JON STERNSTEIN

- Founder/Principal at Stern Security
- Author – Security Penetration Testing, The Art of Hacking (Cisco Press)
- Co-Chair Privacy & Security Workgroup at NCHICA
- Former Healthcare Security Officer

AGENDA

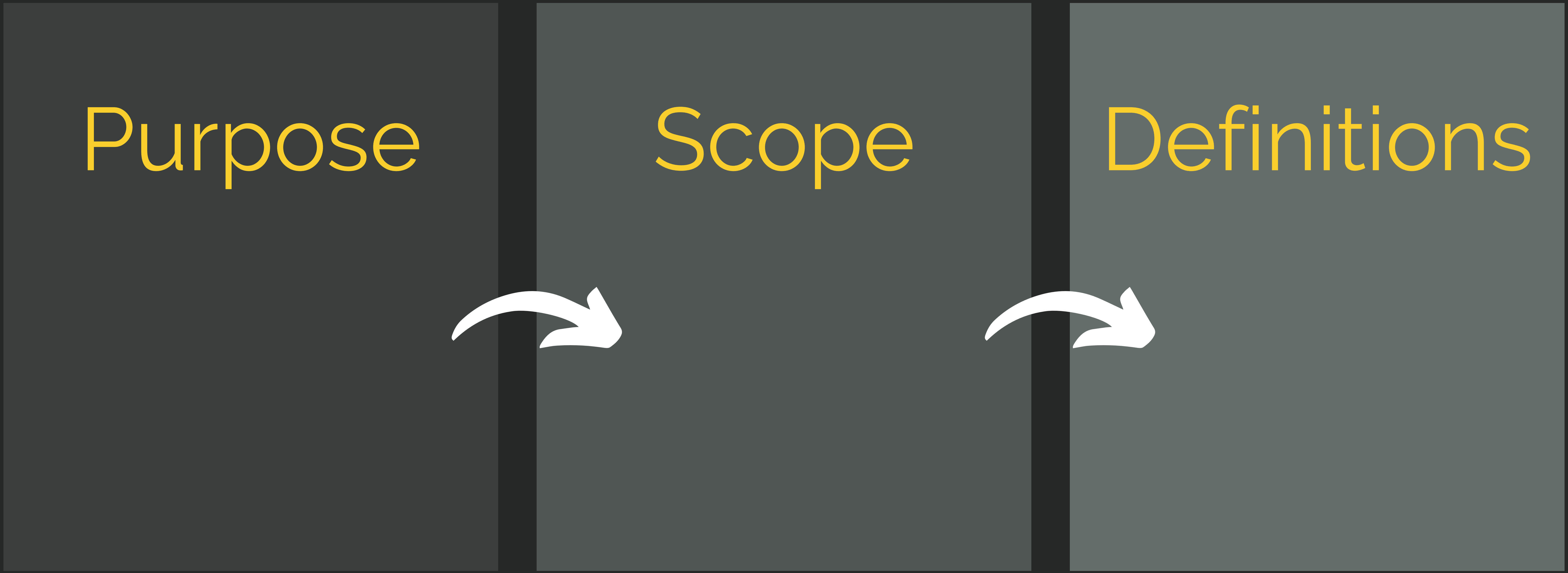
- Why Scenarios
- Plan Outline
- Choosing Scenarios
- Questions

Don't Get Overwhelmed

Creating the procedures is a large task, but you can do it :)

Why Scenarios?

Overall Outline



Purpose

Scope

Definitions

Overall Outline (cont.)

Team Roles

&

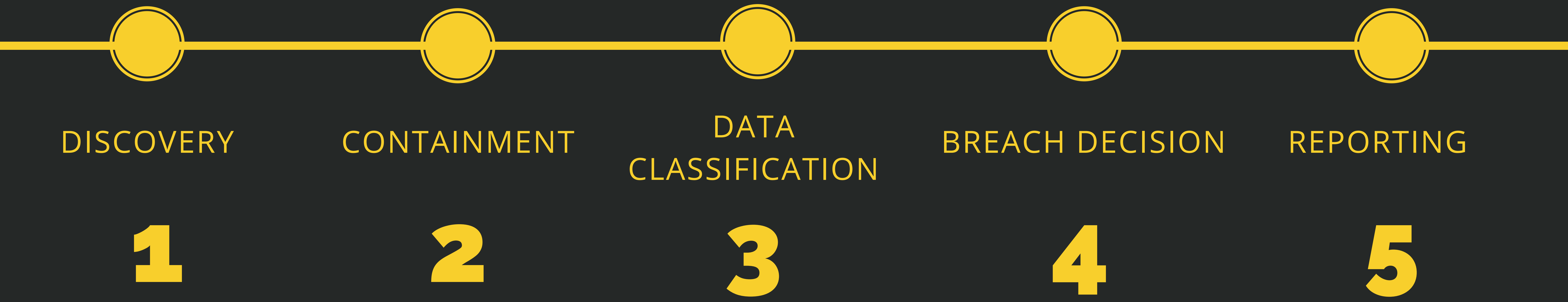
Responsibilities

Incident Response Team

- CIO
- Service Desk
- Security Team
- Various IT teams
- General Counsel
- Audit & Compliance
- Risk Management
- Police Department
- Public Relations

Overall Outline (cont.)

PROCESS FLOW



DISCOVERY
1

CONTAINMENT
2

DATA CLASSIFICATION
3

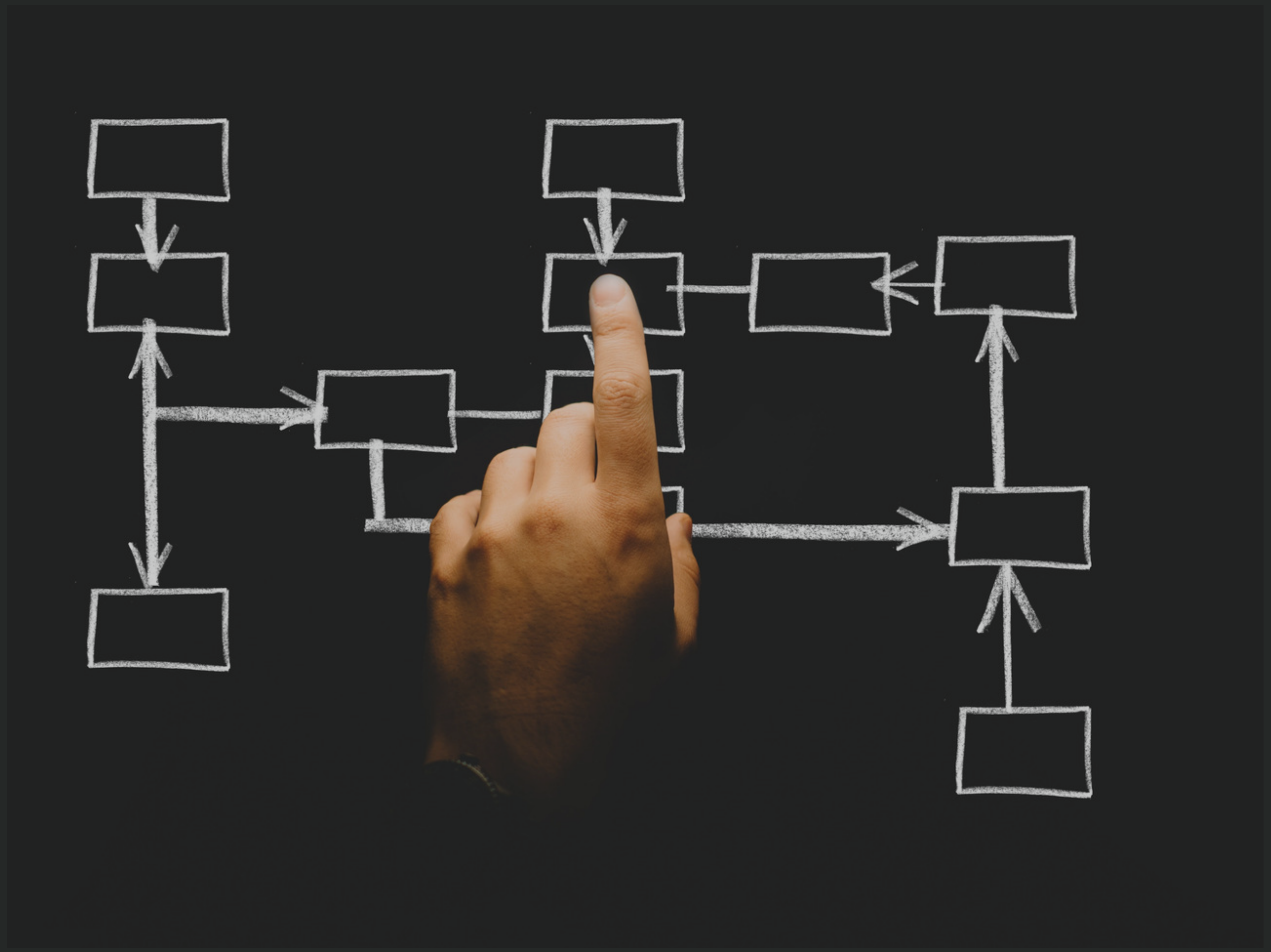
BREACH DECISION
4

REPORTING
5

Overall Outline (cont.)

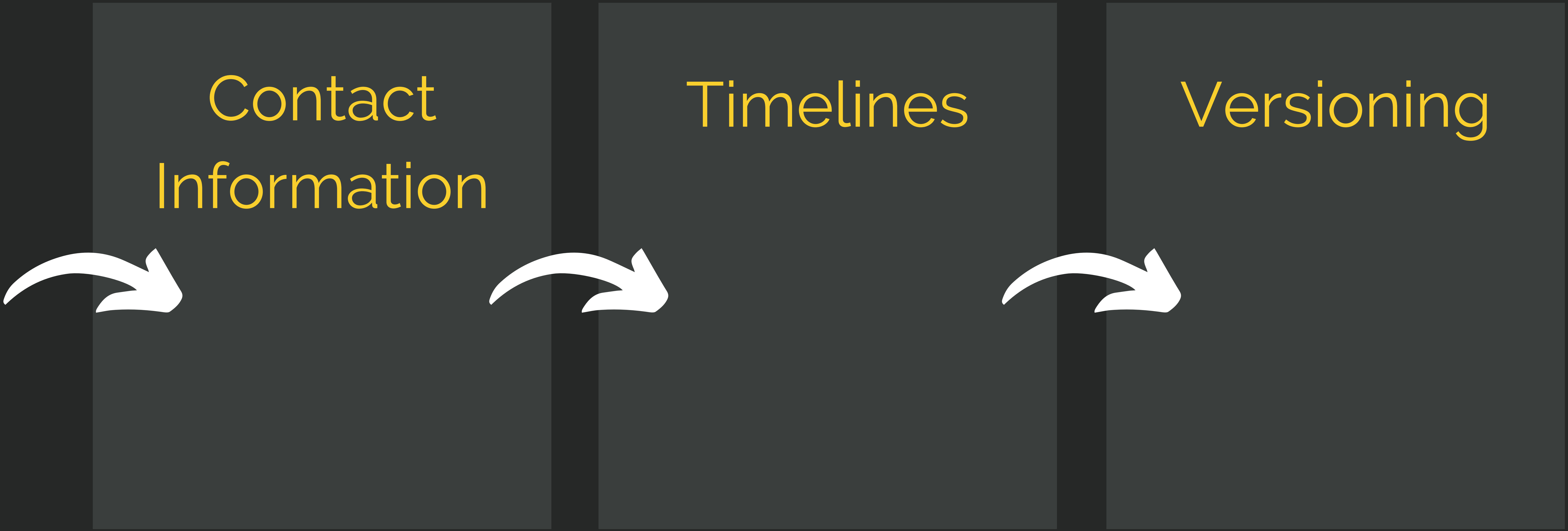
Scenarios

- Checklist
- Flowchart



Stern
Security

Overall Outline (cont.)



Contact Information

Timelines

Versioning

Choosing Scenarios

- Previous Incidents
- Breaches & Emerging Threats
- "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" Guide

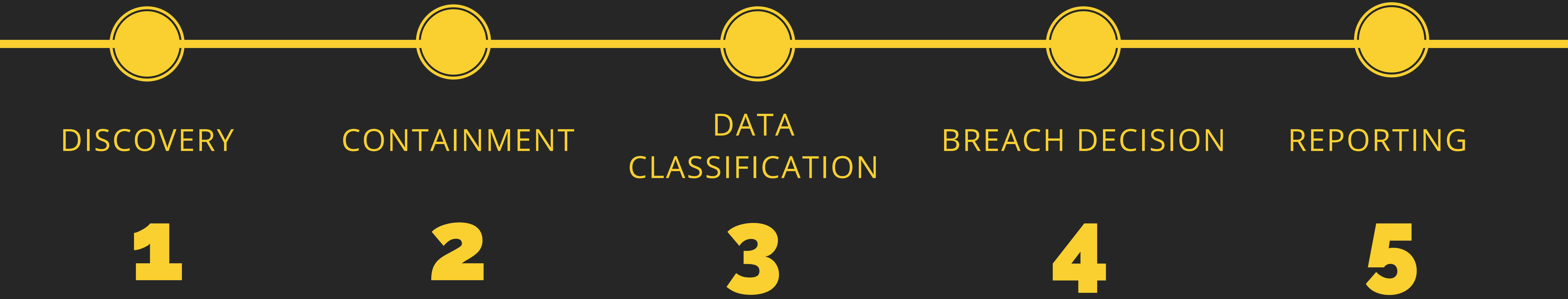
Choosing Scenarios (cont.)

HEALTH INDUSTRY CYBERSECURITY PRACTICES: MANAGING THREATS AND PROTECTING PATIENTS GUIDE

- Email Phishing Attack
- Ransomware Attack
- Loss or Theft of Equipment or Data
- Insider, Accidental or Intentional Data Loss
- Attacks Against Connected Medical Devices That May Affect Patient Safety

Ransomware Attack

INCIDENT RESPONSE PHASES



DISCOVERY

1

CONTAINMENT

2

DATA CLASSIFICATION

3

BREACH DECISION

4

REPORTING

5

Stern Security

Questions?

References

- Stern Security

  https://www.sternsecurity.com

- Healthcare Breaches Dashboard

  https://www.healthcarebreaches.com

- "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" Guide

  https://www.hhs.gov/about/news/2018/12/28/hhs-in-partnership-with-industry-releases-voluntary-cybersecurity-practices-for-the-health-industry.html