



# Mastering Incident Response

## A Guide for IT Professionals

# Agenda

Introduction ~ Why Incident  
Response Matters

Phase 1: Preparation

Phase 2: Identification

Phase 3: Containment

Phase 4: Eradication

Phase 5: Recovery

Phase 6: Lessons Learned

Phase 7: Prevention



# Incident Response Matters?

# Incident Response

## What Why & How?

- Structured iterative methodology for handling security breaches, cyberattacks, and cybersecurity defensive measures
- Goal: Manage incidents to minimize damage, reduce recovery time and costs, and mitigate exploited vulnerabilities
- Ensure confidentiality, integrity, and availability (CIA) of data and systems Business Continuity (BCP) & Disaster Recovery (DR)
- Develop policies, plans, and preventive measures to remove threats and return systems to an operational state
- Integrated into security operations, including continuous monitoring, threat intelligence, and defense strategies
- Collaboration across IT, security, legal, HR, and communications



# Setting the Stage



## Cyberattack Mitigation for Rural K-12 Public School District





# NOTES ~ FERPA:

## Family Education Rights & Privacy Act

- Data Protection and Access Controls

Ensuring only authorized individuals can access or modify student data

- Incident Reporting and Response

Compliance with guidelines

- Training and Awareness

- Vendor Management & 3<sup>rd</sup> Party Security

- Communication Plan



# Phase 1:

## Preparation

- Incident Response (IR) Team Formation
- Tool and Access Preparation

Patch Deployment, SIEM, EDR,  
Network Analysis/Monitoring, Firewall,  
IPS, IDS, SOAR, Vulnerability Scanners, Forensics

- Secure Infrastructure
- Security Awareness, Culture, and Training
- Communication Plan

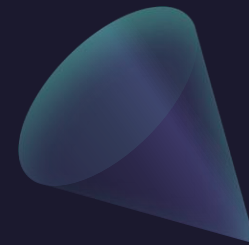
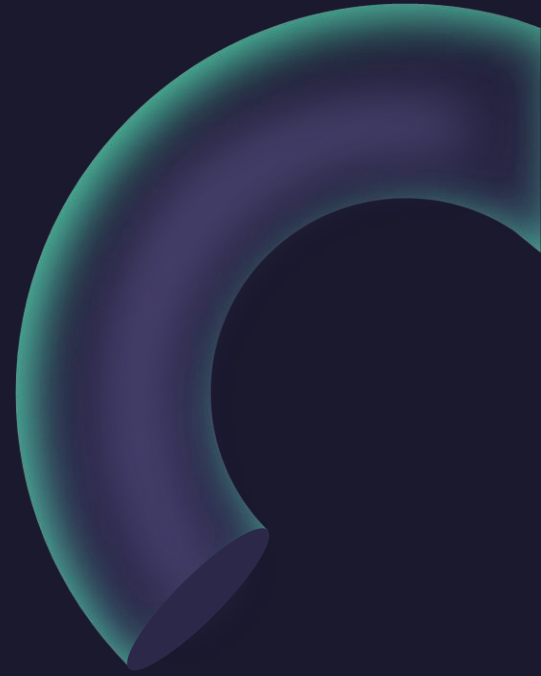




# Phase 2:

## Identification

- Incident Identification
- Breach Confirmation
- Assessment of Scope
- System & Network Monitoring
- Incident Documentation



# Phase 3:

## Containment

- Immediate Actions

Disconnect, Segregate, and Isolate

- Quarantine

Intercept and Restrict

- Long-Term Containment

Passwords and Credentials

Stricter Rules

Multifactor Authentication



# Phase 4:

## Eradication

- Remove Threats

Antivirus, Antimalware, EDR

Reimage, Reinstall, Redeploy

- System Updates

Patch Deployment

Updating antivirus/antimalware definitions

& firewall rules

# Phase 5:

## Recovery

- Restore Systems & Services

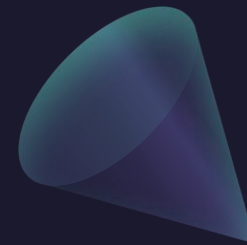
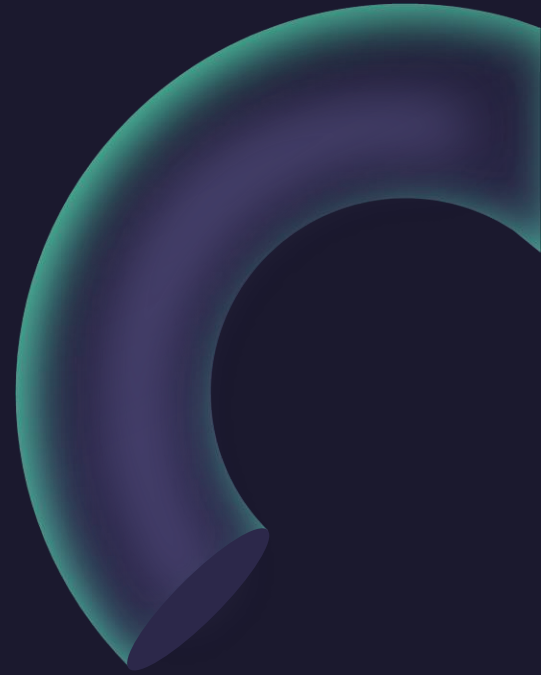
Deploy Backups & Gradual Restoration

Ensure no unauthorized modifications  
or lost data

Regulatory adherence

- Monitoring

Enhanced and Continuous





# Phase 6:


## Lessons Learned

- Review, Document, & Analyze
- Policy Update
- Training Improvements
- Communication
- Legal & Regulatory Compliance



# Phase 7:

## Prevention

- Regular Audits
  - Red-Team, Vulnerability Assessments, Penetration Tests
- Community Engagement
  - Law Enforcement & Cybercrime Units
- Resilience Planning
  -  NIST Cybersecurity Framework
- Cybersecurity Insurance



Incident Response Matters!



# The Stage

## Purdue University Security Incidents & Compromised PHI



Adler, S. (2018, May 31). *Purdue University uncovers data security incidents that potentially ...* The HIPAA Journal. <https://www.hipaajournal.com/purdue-university-uncovers-data-security-incidents-that-potentially-compromised-phi/>





HUNGRY  
FOR  
APPLES?

# Thank you

Brock 'INIT 6' Warner

brock.warner@pm.me

<https://linktr.ee/brockwarner>

