Creating Incident Response Plan and Playbooks

RVTEC 2025 San Diego

Nov 3, 2025

Ishan Abhinit

Senior Security Analyst @ IU


Incidents happen
to the best of us
Have a cyber incident response plan.

Incident Response Plan

- Scope
- Definitions
- Goals
- Roles and Responsibilities
- Communications
- Pre- and Post-Incident Activities

Scope

- Describe the intended scope of the document.

- Consider Special Scenarios
  - Multi-institution policies
  - Parent organization policies

Definition of an Incident

- What is an Incident?
  - A cybersecurity incident is an event that compromises the CIA of information systems or data.

- Why it is important?
  - Defining an “incident” is critical in determining which events trigger the application of this policy.
  - The definition of incident is an organizational decision as it determines the scope of when and how this policy is applied.

Consideration when defining an Incident

- Mission Impact
- Time Sensitivity
- Workforce
- Clarity

Events - Incident or not?

1. Malware Infection
2. Data Breach
3. Forgotten Password
4. DoS Attack
5. Network Latency Issues
6. Compromised email account
7. Employee's Unlocked computer
8. Hard drive failure
9. Unusual network traffic

Incident Response Goals

- Maintain system operability
- Protect CIA of critical data
- Protect org's reputation
- Protection from legal liability
- Collecting and preserving information related to the IN
- Preserving evidence for Law enforcement

Roles and responsibilities

- Incident Response team or Personnel
- Cybersecurity lead/CISO
- Senior Leadership
- Communication personnel

Communication

- Communication with the media
- Communication with law enforcement
- Communication with external stakeholders
- Communication with Parent institution
- Communication with ISACs

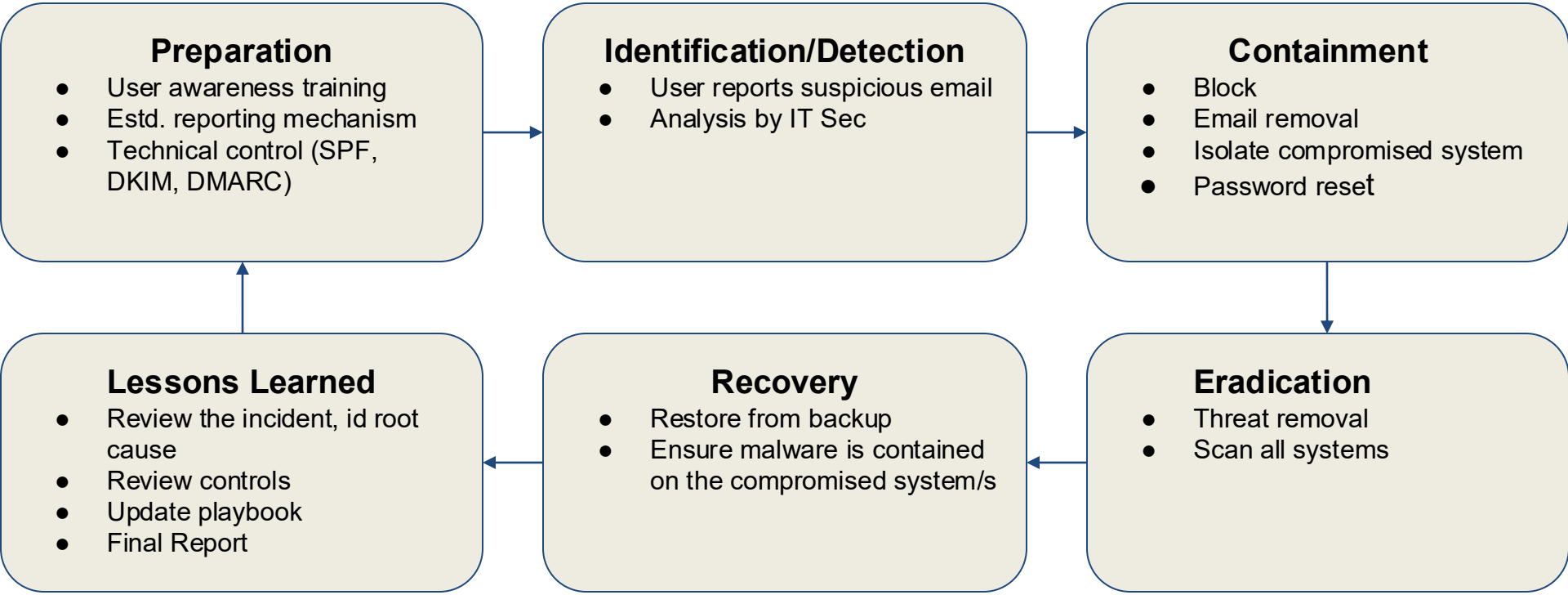
Pre- and Post-Incident Activities

- Pre-Incident Activities
  - Training
  - TTX
  - Policy and Procedure
  - Tool
- Post-Incident Activities
  - Incident Post-Mortems
  - Training
  - Policy and Procedure revision - periodically

Incident Response Process - PICERL

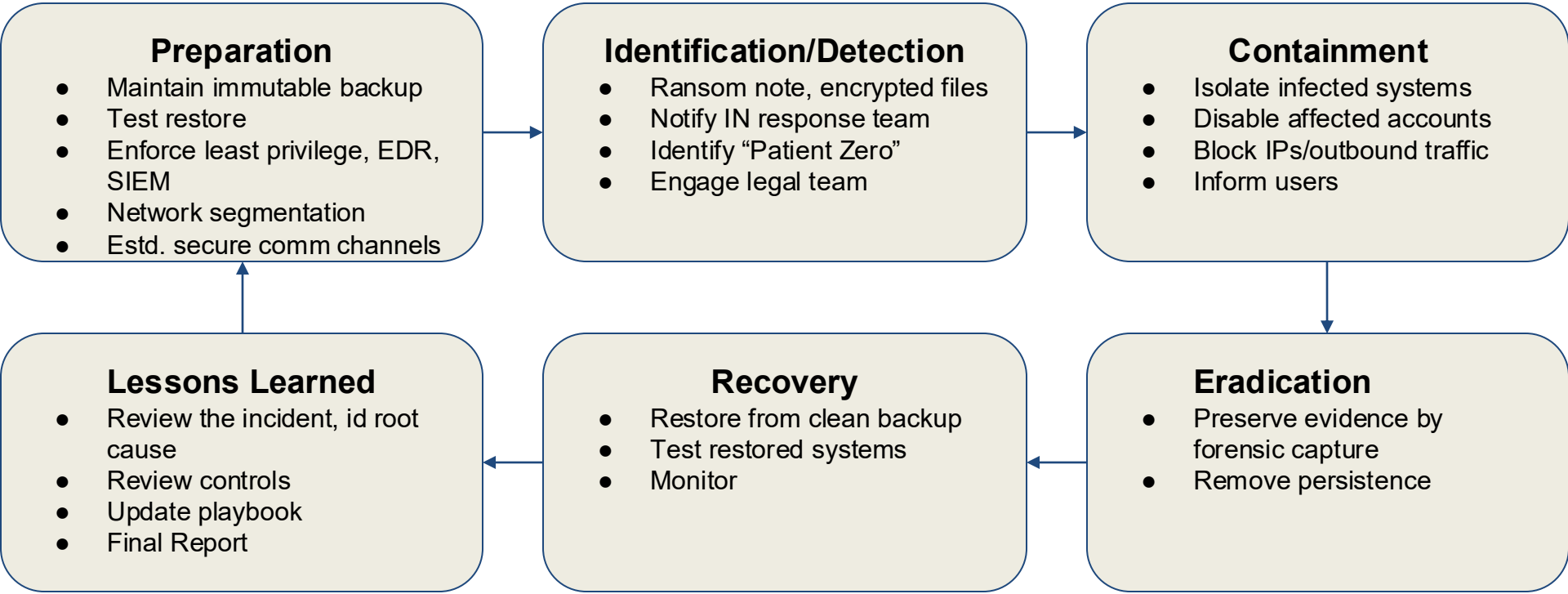
- P - Preparation
- I - Identification (and Analysis)
- C - Containment
- E - Eradication
- R - Recovery
- L - Lesson Learned

Playbook: Phishing



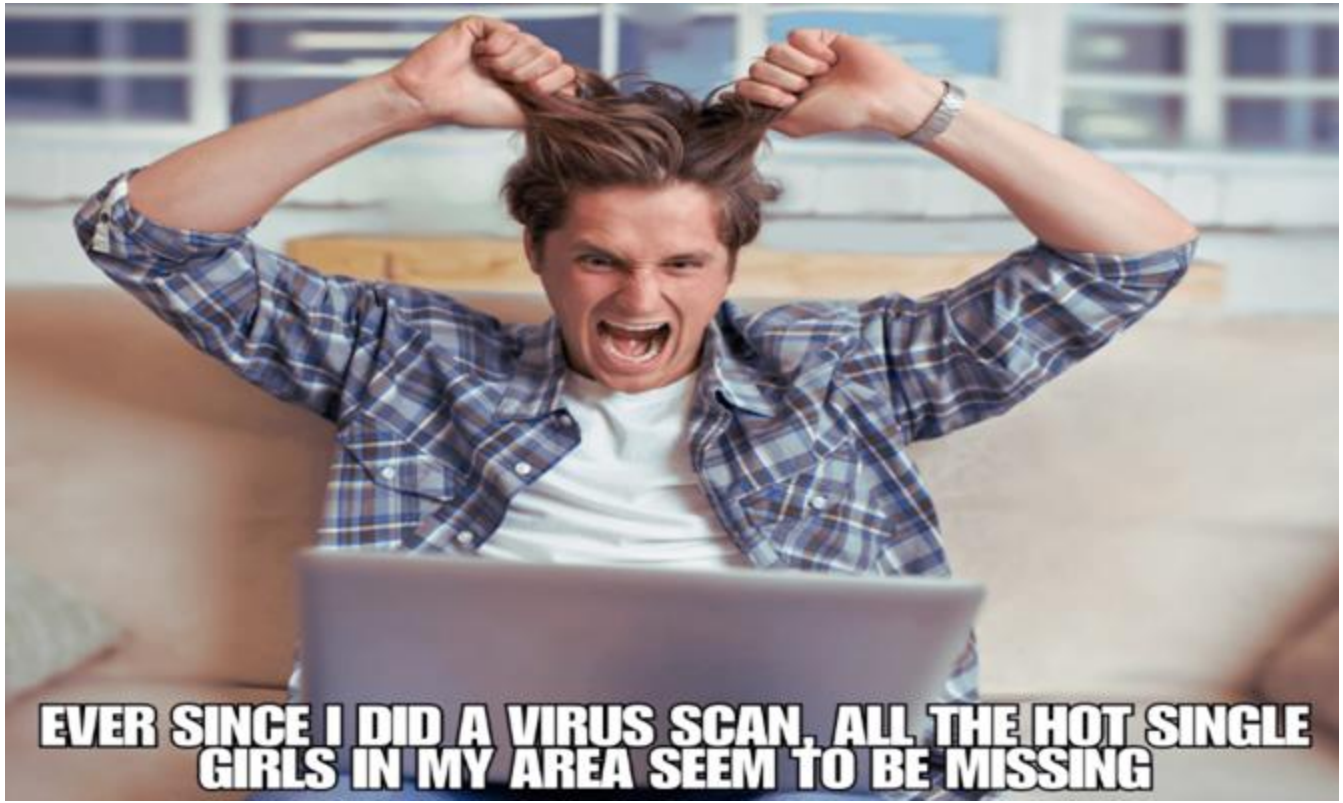
Phishing Meme

Playbook: Ransomware



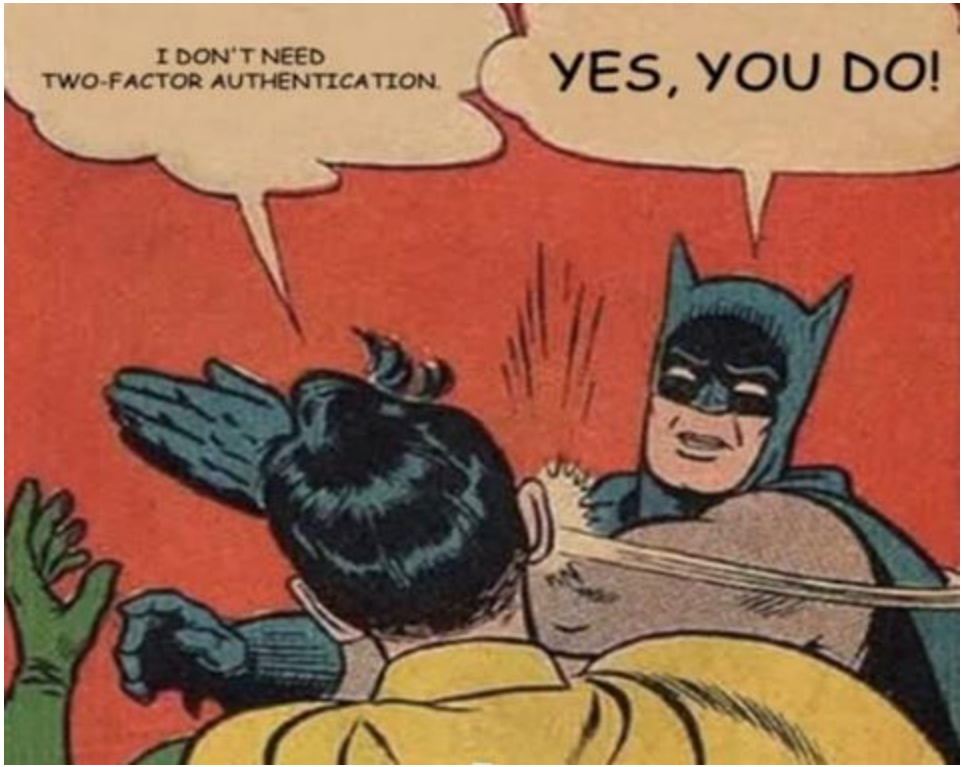
Ransomware Memes

Memes


EVER SINCE I DID A VIRUS SCAN, ALL THE HOT SINGLE GIRLS IN MY AREA SEEM TO BE MISSING

More Memes


SOMEONE FIGURED OUT MY PASSWORD,
NOW I HAVE TO RENAME MY DOG.


I DON'T NEED TWO-FACTOR AUTHENTICATION.
YES, YOU DO!

Template

U.S ARF Incident Response Template

Thank you

email: ARFSEC@IU.EDU