It’s Not If…But When
How to Build Your Cyber Response Plan

Michael Quinn

Lucie Hayward

September 25, 2017

Incident Response Plan (IRP)

Key Questions

- Why is it important to define an incident?
- How do you define an incident?
- How do you define an event?
- How do you define a breach?

- What's the difference between them? Why should I care?

Incident Response Plan (IRP)

Definitions

- Incident Definition (NIST 800-61 r2)
  - NIST says… ”A *computer security incident* is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.”
- If we used this definition, we would always be in incident response mode. We all have users! ☺
- Consider appending with: “that *has significant potential* to lead to the following:
    - Negative impact to the company’s reputation
    - Inappropriate access to PII or PHI or customer data
    - Loss of IP or Funds

Incident Response Plan (IRP)

Definitions

- Event Definition
  - NIST says… ”An ***event*** is any observable occurrence in a system or network.”
  - “***Adverse events*** are events with a negative consequence, such as system crashes, packet floods (DDoS), unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.”

Incident Response Plan (IRP)

Definitions

- Breach Definition (The “B Word”)
  - “…a security breach in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.”
  - Be very careful when using that word in communications around an incident.
  - Generally occurs when an organization has lost control of certain types of sensitive data
    - PII, PHI, customer data
  - Talk to your counsel.

Incident Response Plan (IRP)

Roles and Responsibilities

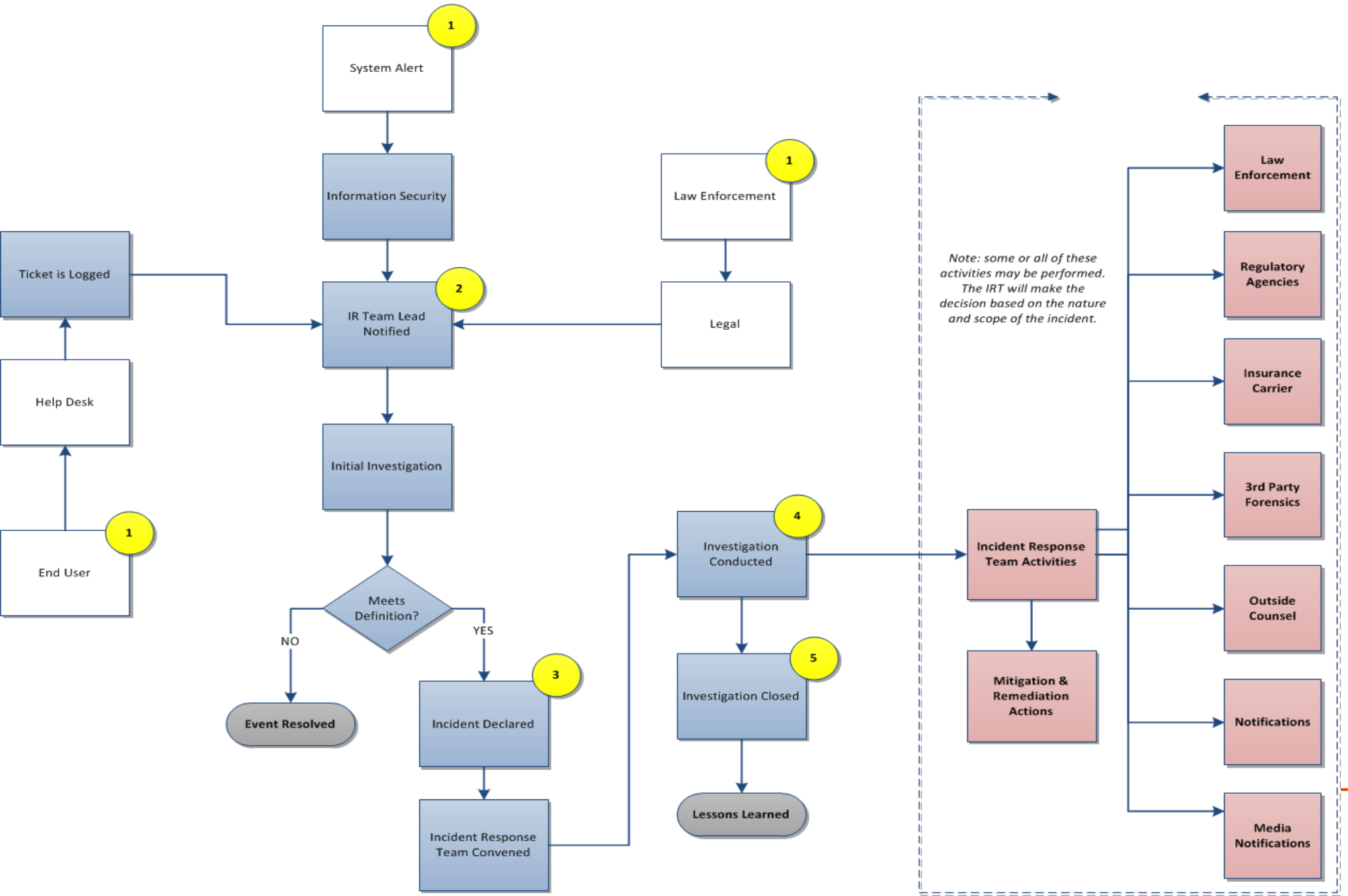
- Identifies each member of the Incident Response Team (IRT)
- Outlines the role of each member
- Details each team member’s responsibilities
- Can define as one single team, or a core team + ad hoc members as needed

Incident Response Plan (IRP)

Roles and Responsibilities

- Team Members to include / consider:
  - General Counsel (Legal)
  - CISO / CIO (Management / technical)
  - Technical leads (Network / infrastructure)
  - HR
  - PR/Marketing
  - Risk Management/Insurance
  - Business Leads
- Know who is driving the bus. There are tough decisions ahead.

Incident Response Plan (IRP)



Questions?