Kroll | A Division of DUFF & PHELPS

It’s Not If But When: How to Build Your Incident Response Plan

Matthew Dunn & Lucie Hayward

September 7, 2018

Introductions – Who We Are

Matthew Dunn

Associate Managing Director

Lucie Hayward

Director

Kroll | A Division of DUFF & PHELPS

Incident Response Plan (IRP)

Definition

The instructions and procedures an organization can use to identify, respond to, and mitigate the effects of a cyber incident.

- NIST SP 800-34 Rev.1 Contingency Planning Guide for Federal Information Systems

Incident Response Plan (IRP)

Key Components

- Incident definition
- Designated team members
- Clearly defined roles & responsibilities
- Severity levels

Incident Response Plan (IRP)

- 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) – Key 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, customer data, research data
    - Loss of IP or Funds

Incident Response Plan (IRP) – Key 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) – Key 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 & 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 & 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
  - Project Manager
  - Business Continuity Planning
- Know who is driving the bus. There are tough decisions ahead! (In other words – who is in charge?)

Incident Response Plan (IRP) – Roles & Responsibilities

- Team should NOT be IT centric – Why?
  - Inherent conflicts of interest
  - Too many ‘hats’ for one person, team or role
    - Increased complexity of technology
    - Increased complexity of threats and vulnerabilities
    - Different skills, education and training paths
  - Frequently follows tool-based, defense-only strategy
  - May minimize or miss subtle clues of exposure
    - More important to ‘keep the lights on’
  - Incident Recovery
    - What happens during a real crisis?
    - IT is often busy leading recovery efforts

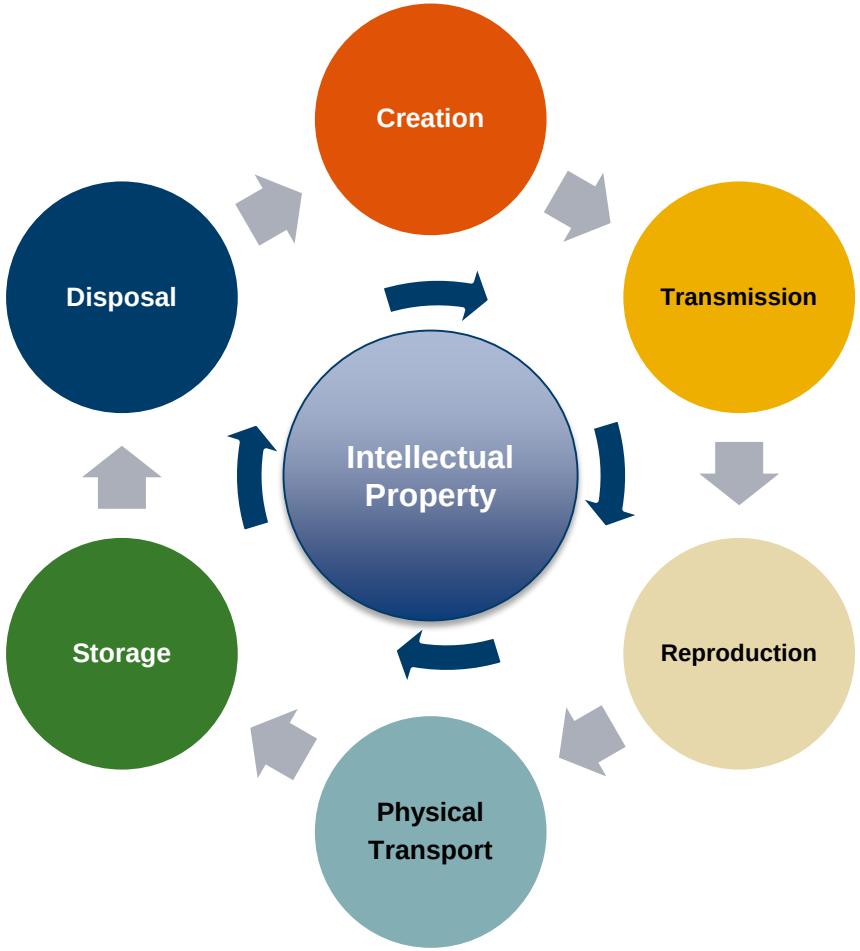
Incident Response Plan (IRP) – Communications

- Create a communications matrix
- How will the team communicate securely?
  - Where will you meet? (War rooms)
  - Is it safe to use corporate e-mail?
  - What is verbal, what is written?
- Define who owns communications with external parties
  - Outside counsel, Insurance, Law enforcement, the media, regulators
- Define who owns communications with the C-Suite

Incident Response Plan (IRP) – Associated Materials

- Contact Lists
  - Should include contact information for the IRT, key stakeholders
  - Consider critical vendors/service providers
    - When do we bring in outside help (e.g. Matt and Lucie ☺)
  - Should include out of hours contact information
  - Review and update quarterly
- Network and Critical Application Diagrams
  - Lack of this information kills response times
  - How can data get in and out of the organization?

Incident Response Plan (IRP) – Associated Materials



Incident Response Decisions – Severity Levels

- How do you establish severity levels for an incident?
- Severity levels = the risk that you'll mis-label an incident.
  - Don't go by what your AV vendor says.
  - Make sure your definitions are clear and understood by everyone
  - Make sure you re-evaluate the severity level as you uncover more information
- Incident Declared = top priority, all hands on deck
- OK to establish a severity level for reporting purposes

Incident Response Decisions - Insurance

- Advantages of a cyber insurance policy
  - Access to third party support and discounted rates
  - Coverage for your incident, which can include loss and business interruption
- When do you notify your insurance carrier about an incident?
  - As soon as you think something is going on!
  - Be aware that an informal call usually is not considered “formal notice” by the carrier.

Incident Response Decisions – Third Party Support

- When do you bring in third party assistance? (Law Firm, Forensics, Crisis Communications)
- Remember “The 3 Cs”!
  - Capability – do you have the skillset to do the work?
  - Capacity – do you have enough resources to do the work?
  - Conflict – would it be a conflict of interest to conduct your own investigation?

Incident Response Decisions – Ransomware

- Would you ever consider paying ransomware?
  - Under what circumstances?
  - Who makes this decision?
  - What does your cyber insurance policy cover?

Incident Response Decisions – Law Enforcement

- When should I call Law Enforcement?
  - What is our goal when we find attackers in our network?
  - What is the goal of law enforcement?

Incident Response Plan - Testing

- Table Top Exercises
  - To test the readiness of your organization to respond to cyber incidents
  - Key Objectives:
    - Identify gaps in the current IRP
    - Strengthen communication between stakeholders
    - Familiarize all participants with key definitions and decision making criteria
    - Enable participants to adapt the IRP to the dynamic nature of cyber incidents

Incident Response Process

- Clearly outline all steps in the process
- Understand how an incident might be reported and how it should be escalated
- Clearly indicate when the team is convened

Incident Response Life Cycle