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

Presented by:
Stacy Scott & Lucie Hayward
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 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

Tweet along: #Sec360 www.Secure360.org
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)

Plan Components

In Your Plan:

• An incident should be clearly defined.
• Your IRP should clearly state who has the authority to declare an incident.
• Declaring an incident invokes the Incident Response Plan and convenes the Incident Response Team (IRT)
• Your definition may be different than NIST
Incident Response Plan (IRP)

Severity Levels

• How do you establish severity levels for an incident?
• Trick Question – You Don’t!
• Severity levels = the risk that you’ll mis-label an incident.
  • Don’t go by what your AV vendor says.
• Incident Declared = top priority, all hands on deck
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)

Communication

• Create a communication flow

• 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)

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. Mike 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)

The Process

• Clearly outline all steps in the process

• Start with incident reporting and end with lessons learned
  • Caveat: Don’t get bogged down with internal status reports

• Clearly indicate when the team is convened
  • Make sure IT/Security knows this by heart.
  • Don’t delay.
Note: some or all of these activities may be performed. The IRT will make the decision based on the nature and scope of the incident.
Incident Response Plan (IRP)

Reviewing & Testing the Plan

- Review the plan quarterly and make updates
  - Did roles change?
  - Update contact/resource information
- Plan should be tested annually to identify gaps

Tweet along: #Sec360
www.Secure360.org
Incident Response Plan (IRP)

What It’s Not
Questions?