Coordinated RESPONSE

Why Plan?

August, 2015

Prepared by: Jim Bothe & Jim Meyer

Incident Response – Why Plan?
It's good business!

Coordinated RESPONSE

Ponemon Institute surveyed 62 companies over 16 industries that experienced a data breach last year.

- $217 – the average cost per compromised record.
- $259 – the average cost per record in financial services.
  NOTE: the cost was higher in part due to lost customers.
- $6.5 Million the average total cost of a breach.
- 11% – cost reduction due to effective incident response plan.
- $715,000 – average savings due to the plan.

Ponemon Institute, 2015 Cost of a Data Breach: United States, May 2015, sponsored by IBM. Retrieved 08/15/2015 from: http://www-03.ibm.com/security/data-breach/.

The Incident Response – Why Plan?
It is a recognized best practice.

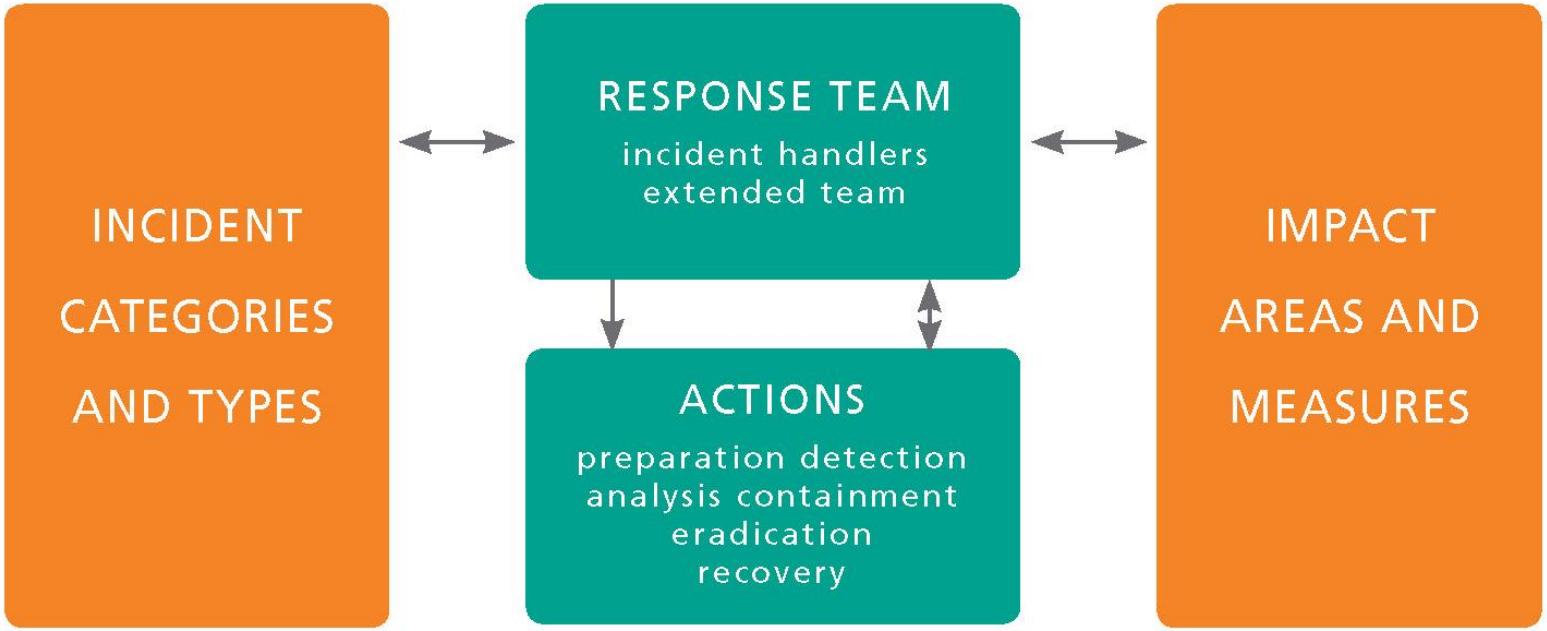
Coordinated RESPONSE

Everyone Agrees an Incident Response Planning is a critical control.

- **National Institute of Standards and Technology (NIST)** Special Publication SP 800-53 Rev 4 – identifies Incident Response (IR) as 1 of the 18 families of information security controls: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
- **NIST SP 800-61 Rev 2:** Computer Security Incident Handling Guide, August 2012: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.
- **The Internal Standards Organization** defines ISO 27035:2011 as the standard for Information Security Incident Management: http://www.iso.org/iso/catalogue_detail?csnumber=44379.

Coordinated RESPONSE

Four Dimensions of Incident Response



Coordinated RESPONSE

Four Dimensions of Incident Response

1. **Scope:**
   identify incident categories & types addressed by the plan.
2. **Team:**
   identify the core team – hands on;
   extended team – specialists, e.g., legal; and
   external team – managed security services.
3. **Impact & priority:**
   identify impact areas, e.g., financial, legal, etc.;
   identify associated impact levels or metrics;
   link to priority, escalation, and notifications.
4. **Response actions:**
   for each category and type identify associated actions, e.g., examine log files, seek legal direction, etc.

Coordinated RESPONSE

Possible Incident Categories and Types

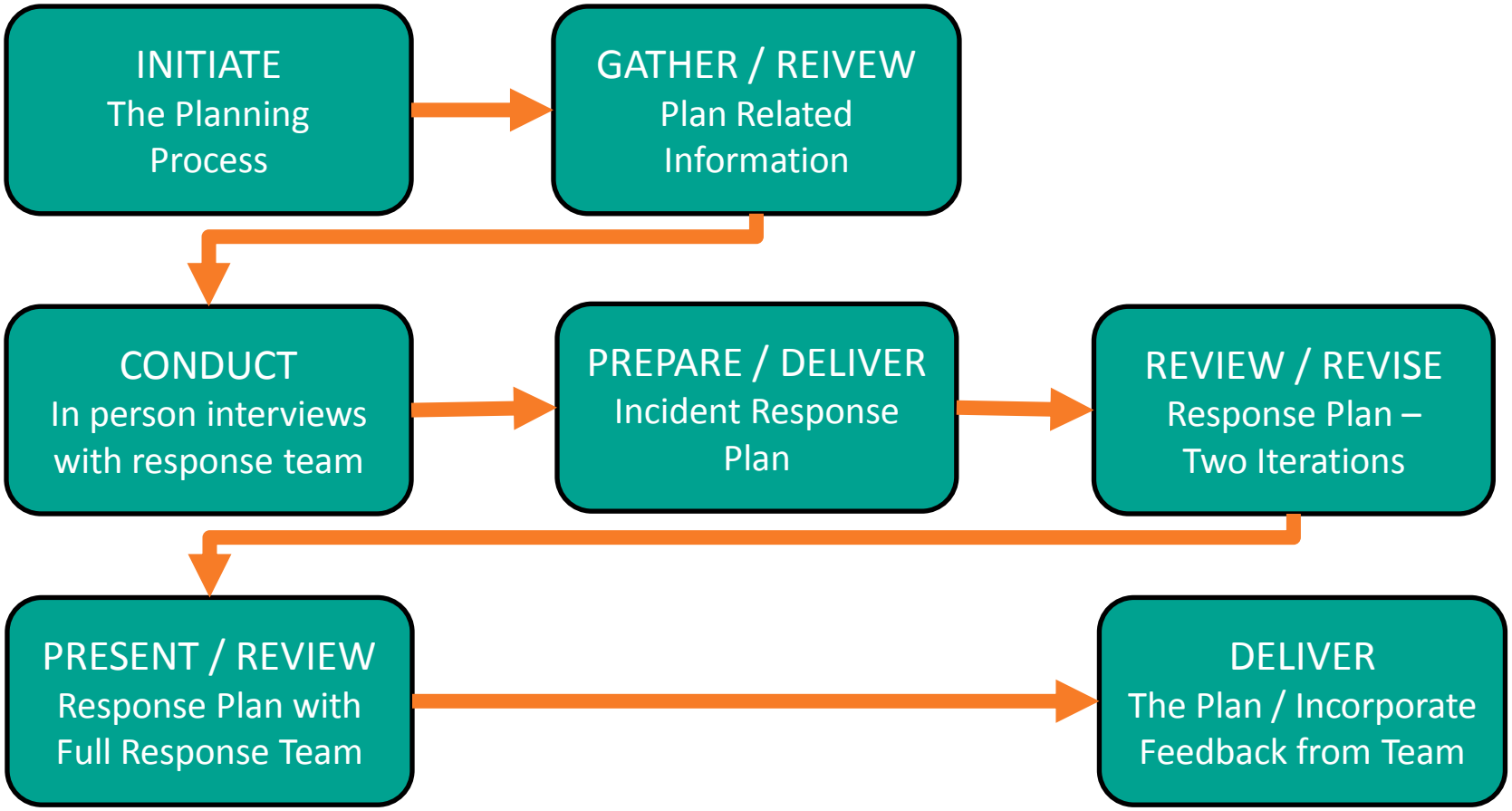
Incident Categories	Incident Types
Compromised Asset	✓ Data breach or other data compromise ✓ Fraud or fraudulent transaction ✓ Compromised system
External Internet	✓ Denial of service (DoS) or Distributed DoS (DDoS) ✓ Network probing / logical attack ✓ E-mail spamming / phishing / social engineering ✓ Threat intelligence
Malware	✓ Malware including Trojans, worms, viruses, et al.
Equipment Loss	✓ Loss of equipment or phone ✓ Loss of credential
Internal / Personnel	✓ Improper email usage ✓ Improper internet usage ✓ System or network misuse
Information Security Services	✓ Other incidents not categorized above ✓ Other services as required, e.g., legal support

Response Planning Process

- Start with a template reflecting the 4 dimensions.
- Interview response team members, solicit input, explore “what if” scenarios.
- Build out the plan and review with the team, iteratively.
- Hold group meetings to discuss the final plan.

Coordinated RESPONSE

Seven Steps for Response Plan Development



Coordinated RESPONSE

Table of Contents

Key Benefits of the Planning Process

- First and foremost, develop and document an incident response plan.
- Socialize and exercise the plan.
  - Team members are aware of the plan, their role and responsibility.
- Gap analysis – with the plan in hand identify areas for improvement.

Coordinated RESPONSE

Additional Resources

The Incident Response – Why Plan?
It is a recognized best practice.

Additional resources

- **The SANS Institute** identifies Incident Response (IR) as 1 of 20 Critical Security Controls:

  https://www.sans.org/critical-security-controls/

- **CERT/CC**, Carnegie Mellon University, Software Engineering Institute (CME/SEI), Handbook for Computer Security Incident Response Teams: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

Coordinated RESPONSE

ISACA – Incident Management and Response

ISACA's paper makes key points that help strengthen a response plan including:

- The importance of identifying **business value** in a good response plan;
- The importance of supporting **enterprise governance** in the response plan; and
- The importance of the link between **risk planning** and **response planning**.

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Incident-Management-and-Response.aspx