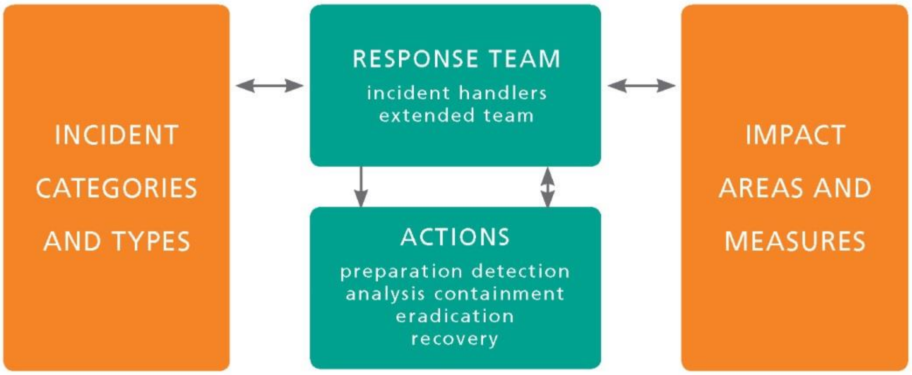
Why Plan? Why not?

A cybersecurity incident response plan is considered to be 1 of the top 20 security controls by a number of respected authorities. Industry research indicates an effective response to a cybersecurity incident reduces the actual cost by 11%. Developing an incident response plan is not only a best practice, it is good business. Besides, it is often a legal or regulatory requirement. See **References and Research**.

The Dimensions of Incident Response

A good plan addressed four key dimensions of incident response:

1) Scope: identify incident categories and types addressed by the plan.
   For example, a plan may address malware, compromised assets (including breached data), and lost equipment or credentials.
2) Team: start with the core individuals responsible for handling the incident; add extended team members required in select situations, for example, human resources or legal; identify third parties who support the response, for example, an Internet Service Provider or a forensics firm.
3) Impact & priority: identify impact areas that might be effected by an incident, for example, financial, reputational, and legal; identify impact levels or measures for each of these areas; this supports setting appropriate incident impact; and this should align with enterprise risk assessments.
4) Response actions: for each category and types, identify actions for responding to the incident. For example, examining log files, requesting a legal review, or involving a consultant.



The elements of the 4 dimension interact throughout the incident response. The response team identifies the likely incident category and type. This informs their action plan. As they execute the plan, information is collected and analyzed. Impact is measured to establish the priorities and communicate with management. Additional resources and actions are invoked as needed and as authorized. Ultimately, the incident is contained and the cause is eradicated. Finally, the organization benefits from the lessons learned.

The Incident Planning Process

The incident planning process starts with the template reflecting the 4 dimensions. An iterative approach is used to interview team members, solicit their input, and build out the plan. The plan is distributed to the team. After review, 1 or more group meetings are held to discuss the plan. Then a final draft is prepared for review and approval.

The planning process serves a number of key objectives.

Develop the plan – first and foremost, the incident response plan is developed and documented.

Socialize and exercise – the planning process "socializes" the incident response plan as well as the roles and responsibilities of the response team members. Team members learn from the planning process. The interviews and group sessions exercise the plan. Team members working together consider "what if" different events our outcomes occur.

Gap analysis – the planning process often identifies short comings in the response capability. Filling the gaps might be as straight forward as training team members or acquiring equipment needed for response. Filling the gaps may also require working with service providers to acquire additional resources when needed.

References and Research

National Institute for Standards and Technology

National Institute of Standards and Technology (NIST) Special Publication SP 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, identifies Incident Response (IR): http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

NIST also provides SP 800-61 Rev 2: Computer Security Incident Handling Guide, August 2012 to help organizations develop their incident response program: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

International Standards Organization

The International Standards Organization defines ISO 27035:2011 as the standard for Information Security Incident Management: http://www.iso.org/iso/catalogue_detail?csnumber=44379.

Ponemon Institute

Ponemon Institute performs an annual survey of organizations that experienced a data breach in the past year. The survey is global, but the numbers provided here are for the United States. The survey included 62 companies, across 16 industries.

- $217 – the average cost per compromised record
- $259 – the average cost per compromised record in the financial institutions
- $6.5 million – the average total cost
- 11% – cost reduction realized by organizations with an incident response program
- $715,000 – the average savings realized by organizations with an incident response program

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/.