Example Co.

Managed Threat Complete – D&R Readiness Assessment

Prepared for:

John Customer

Prepared by:

Jane Consultant

The following document is a demonstration D&R Readiness Assessment deliverable from Rapid7. This report provides a limited overview of what will be included in a final Rapid7 D&R Readiness Assessment.

Rapid7 Contacts

Consultant

Jane Consultant
Senior Consultant
Jane_Consultant@Rapid7.com

Leadership Team

Mike Kaplan
Senior Director, Security Services
mike_kaplan@Rapid7.com

Brian Carey
Senior Manager, Security Services
brian_carey@Rapid7.com

Rick Bremer
Manager, Security Services
rick_bremer@Rapid7.com

Table of Contents:

Executive Summary

Rapid7 reviewed the Incident Response program for Example Co.; designed to provide Example Co. with an independent, point-in-time assessment based on reviewing business, IT, and security program elements that provides actionable recommendations to improve Example Co.'s operational resiliency.

Assessment Synopsis

Rapid7 performed a review of business, IT and Security components at Example Co. with an objective of identifying optimal changes that can be implemented to ensure Example Co.'s incident response program is relevant and sustainable.

The assessment considers internal processes and security controls to support the organization's ability to respond to an incident while also leveraging Rapid7's Managed Detection and Response.

The recommendations within this report are common controls that can increase security efficiency and effectiveness contributing to overall IT efficiency. Testing of individual controls to determine effectiveness and adequacy was out of the scope for this assessment, and any testing performed was for information-gathering purposes only.

Scope

Rapid7 worked remotely with Example Co. from November 30th to December 1st, 2021.

Assessment Data

Dates: 11/30/2021 to 12/01/2021

Level of Effort: 2 days

Consultant(s): Jane Consultant

Incident Response Assessment Findings

The following section provides a high-level overview of key assessment findings and recommendations for Incident Response:

Key Observations

- In recent years, Example Co. has made significant strides in improving its security program and overall incident response processes and practices. The organization has made tangible investments in technology and staff to support the overall security program. For example, the organization created a distinct Information Security team and invested in a third-party Managed Detection and Response technology and service. Overall, Example Co. has a solid foundation for further improving its security posture bolstering incident response capabilities.
- Example Co. has an Incident Response Plan, which includes key elements, such as the response lifecycle, Security Incident Response Team (SIRT) definition, as well as internal and external contacts. The plan has been well-circulated to all key stakeholders within Information Technology and beyond. However, stakeholders on the SIRT, namely those outside of IT, are not confident in their roles and responsibilities during an incident.
- The current Incident Response Plan could be further enhanced and improved upon through greater detail related to chain of custody, criticality methodology, and identification of critical data and systems.

Key Recommendations

- Further expand upon roles and responsibilities defined and communicated in the Incident Response Plan. Consider leveraging a RACI matrix approach to delineate who should be responsible, accountable, consulted, and informed during each phase of incident response. Work collaboratively with all SIRT members to complete a RACI matrix to ensure there is buy-in and understanding across the lines of business. Moreover, once these roles and responsibilities are more clearly defined, continue efforts to test the plan. Once the tabletop exercise with Rapid7 is complete, revise the RACI matrix based on lessons learned during the exercise. Moreover, consider performing internal tabletop exercises to regularly test the plan.
- Continue efforts to revise the current Incident Response Plan with the goal of incorporating lessons learned from this assessment and tabletop exercises. Example Co. could benefit from implementing a chain of custody program as well as adding

greater detail to its criticality methodology, and critical data and systems. Examples of each of these can be found in the appendices.

(This is a limited depiction of this section. Each final report includes a selection of Key Observations and Recommendations of each D&R Readiness Assessment finding.)

Areas of Evaluation

Incident Response

Governance & Organizational Information

How information is documented, updated, and disseminated to individuals within an organization, and the roles and responsibilities of IT and Security personnel.

Business Goal

Organizations must have a clear and documented understanding of their assets, network topologies, relationships with other teams, stakeholders, and solid IT and Security policies. Additionally, documentation must be tested and reviewed on a frequent basis.

Security Threat

A clear understanding of an organization's footprint is critical when responding to an incident. Missing or outdated organizational information could result in a communication breakdown during an incident.

Positive Observations

- Example Co. has a Cyber Insurance policy.
- Example Co. undergoes an annual SOX compliance audit.
- The organization created a formal Information Security team in recent years, and this has propelled Example Co.'s security program and overall security posture.
- Information Security manages and maintains a robust set of policies to support Example Co.'s information security program. These policies provide governance controls as well as the foundation for further security coordination.

Identified Gaps

- Example Co. has a well-developed Incident Response Plan with role and responsibilities documented at a high level. However, stakeholders outside of Information Technology and Information Security are less comfortable with their responsibilities during an incident.

- While response coordination and communication methods are discussed in the Incident Response Plan, internal and external communication plans are not in place.
- It does not appear that Example Co. has a process for chain of custody. Without this program, incidents that may require federal or regulatory authority assistance will be inconsistent and could allow for evidence to not be handled properly.

Recommendations

- Consider creating more clear roles and responsibilities matrix for incident management to include stakeholders beyond IT and IS. This list of roles and responsibilities should avoid personnel names, and instead include the role (for redundancy) which can perform the task. This would also include the primary coordinator for incident management. This role's responsibilities would include developing a standard for incident documentation, and coordination between business units and external parties to ensure the incident is contained and the business recovers within the opportune time defined within the SLA This could also allow the analyst to ensure containment and eradication to the highest standard. See Appendix A for a RACI matrix to further refine and define roles and responsibilities during IR efforts.
- The Security Incident Response Team should work collaboratively to clearly document internal and external communications templates to be used during an incident. The organization should engage its external legal counsel and public relations teams in the development of such communication templates.
- Continue efforts to regularly perform a tabletop exercise to evaluate how the IRP meets organizational needs. If Example Co. desires to perform internal testing in addition to third party-facilitated tabletop exercises, it should consider using readily available resources, such as templates provided by CISA. Developing a first tabletop can be a daunting task, so using templates, can facilitate development of an initial internal tabletop. For additional information, see: 'https://www.cisa.gov/publication/cybersecurity-scenarios'. When performing the tabletop, ensure that all contacts are easily reachable and still with Example Co.
- Leverage the appendices within the IRP to create a chain of custody program. This could provide a standardization across the business to handle digital evidence if authorities need to be involved.
- Consider further expanding the criticality methodology within the Incident Response Plan. See Appendix B, which serves as an example of a comprehensive criticality methodology.