RIVIAL
DATA SECURITY

Incident Response Tabletop Exercise Report

Exclusively prepared for:

BCU

August 07, 2024

RIVIAL
SECURED

Table of Contents

Exercise Overview 3
Participants in Attendence: 3
Exercise Mission Statement 3
Exercise Goals 4
Exercise Objectives 4
Incident Scenarios 4
Incident Response Steps 4
Exercise Results 5
Objectives 5
Observations 5
Conclusion 5
Appendix A: Exercise Summary of Events 7

Exercise Overview

Rivial Data Security LLC (Rivial), in conjunction with BCU, conducted an Enterprise Information Security Incident Response Table-Top Exercise with the Incident Response (IR) Team and key employees to measure and evaluate the company's ability to adequately respond to an information security incident. The purpose of the exercise was to promote discussion around preparing, identifying, containing, eradicating, and recovering from a cybersecurity incident. Goals also included the evaluation of response processes, ensuring adequacy of technology tools, and validating roles and responsibilities.

Overall, the exercise was successful in pinpointing strengths and weaknesses in the process. The BCU IR Team did a good job working together and referencing the incident response plan to manage the scenario.

Participants in Attendence:

BCU

- Stephanie, CISO, Plan Administrator
- Kelli, Business Resiliency Director
- Mike, Admin Plan Coordinator
- Lisa, Admin Plan Coordinator
- Scott, Technology Plan Coordinator
- Jill, Communications Plan Coordinator
- Jim, Operations Plan Coordinator
- Steph, Security Plan Coordinator
- Megan, Alternate Admin Chair
- Dave, Alternate Admin Chair
- Pranay, Alternate Technology Chair
- Kourtney, Alternate Communication Chair
- Maggie, Alternate Operation Chair
- David, Alternate Operation Chair
- Rob, Alternate Security Chair
- Chuck, Alternate Finance Chair

Rivial Data Security

- Danny Rowell, Sr. Cybersecurity Consultant
- Molly Ford, Cybersecurity Consultant

Exercise Mission Statement

Ensure that critical information security events are properly identified, contained, escalated, and resolved in a timely manner.

Exercise Goals

- Promote discussion around preparation, identification, containment, eradication, and recovery.
- Exercise and evaluate the response process utilized during a potential incident.
- Ensure adequacy of technology tools available to the IRT.
- Ensure proper documentation and information are available to all members of the response team.

Exercise Objectives

1. Validate the incident response process
2. Increase awareness in participants of their role in the response process
3. Validate response strategies, tactical plans, and technology tools
4. Determine any weaknesses or deficiencies in the incident response process
5. Discuss and evaluate the situational outcomes

Incident Scenarios

The table-top exercise was led by Danny Rowell of Rivial Data Security. The exercise scenario that the team walked through was a Ransomware attack through phishing emails. Detailed descriptions of, and notes from, the scenario can be found in Appendix A of this report.

Incident Response Steps

Rivial used the organization's Incident Response Plan to create the scenario and guide the response process. The plan includes the following incident response steps:

- Detect
- Analyze
- Contain
- Eradicate
- Recover
- Post Incident Actions

Exercise Results

A summary of the exercise results is included in the Objectives table below.

Objectives

The objectives of the exercise were tracked, and their fulfillment documented.

Date	Scenario	Obj. 1	Obj. 2	Obj. 3	Obj. 4	Obj. 5	Obj. 6
07/22/2024	Malware on a patch from a vendor	√	√	√	√	√	√

Objectives

1. Validate the incident response process
2. Increase awareness in participants of their role in the response process
3. Validate response strategies and technology tools
4. Determine any weaknesses or deficiencies in the incident response process
5. Discuss and evaluate the problem outcomes
6. List observations and areas for improvement in the process

Observations

During the exercise, observations and areas for process/tool improvement were identified and documented.

#	Description	Recommendation
1	The team conducts a tabletop annually.	Rivial recommends that the team conduct quarterly exercises to keep the team aware of their respective duties and responsibilities and to keep readiness at a higher level. If "real world" incidents occur, document and conduct an after-action review in lieu of an exercise.
2	The team currently doesn't have formal criteria for declaring an incident but does have a robust IR Plan (Confidential) and IR Playbook. BCU is aware and working on developing a checklist based on objective and subjective criteria	Rivial recommends that BCU continue with plans to develop a formal checklist based on subjective and objective criteria to formalize the process of declaring an incident. **As discussed with the Credit Union, this is currently in progress.**

Conclusion

During the table-top exercise the organization's IR Team refreshed their understanding of the incident response plan and raised questions around the different steps. Throughout the scenario, excellent discussions were had, and important questions were voiced. Overall, the team did well at talking through

all possibilities of the scenarios they were given. We recommend that the team remain familiar with the plan, update notification procedures and timelines, and continue to apply the plan to different scenarios to prepare for an actual event. This team is very competent in their ability to resolve issues. It is important that the plan reflect a response mechanism that best serves the team and the organization. The team members were interactive and mutually supportive.

Appendix A: Exercise Summary of Events

Monday Early Morning (1.0)

Monday morning, Gordon is sequestered for Jury Duty this week.
During routine checks, an IT analyst notices some abnormal behavior on several servers
Patching and backups were completed over the weekend
AV systems report no anomalies
Log data indicates lots of traffic, but not necessarily *excessive* levels

Discussion Notes and Action Items

In part one, the team outlined how they would handle initial investigation of anomalous activity. Help Desk and the Security Team would try to gather more information by taking the following steps:

- review the logs
- work with SIEM (Arctic Wolf), CrowdStrike, Varonis
- contact vendor
- consider reaching out to IR Team
- reach out to the Director, Rob to see if there is any additional insight or guidance
- check Service Manager for Change Management to determine if changes were made during a specific timeframe.

The team has determined this is not an incident currently due to insufficient information.

Monday Mid-Morning (2.0)

Later in the morning an executive sends an email to the IT Team asking about the tech reports on Acme
The organization uses Acme applications to manage their servers
The IT Team reads on the Interwebs that Acme is having large scale issues

Discussion Notes and Action Items

Communications

In response to the change of events, the team discussed how information is disseminated into and throughout the organization. There are formal and informal means of tracking industry standard notices, security news and events. Formal means include newsletters and vendor notifications sent via email and posted online. Informal channels also exist, which rely on strong vendor relations.

The team noted that the organization has strong vendor relationships established that may give timely insight on potential incidents. Overall, the team has many channels of important security information set up for the organization. There is also an automated ticket created for major vendor updates.

Internal communications would take place in form of Teams chats, Teams video, and email. The team determined that if there is an event that potentially affects members, Chris and the security team would be brought in to meet additional needs.

Classification

The team also discussed the classification process for declaring an event, suspicious event, incident, etc. There are categories of criticality outlined (Critical, High, Medium, Low) which require to different

responses. For anything considered Critical or High for Business Services, a formal P1 or P2 is kicked off. For anything considered Medium for Business Services, it is declared no higher than a P3 (Outage) and is kept withing the teams that can troubleshoot.

Monday Late Morning (3.0)

Further log scrutiny reveals that some of the Acme applications show abnormal traffic patterns
Some of the servers failed to backup over the weekend as files were "locked out"
Two of the servers appear to be operating, but IT cannot access them directly through Acme

Discussion Notes and Action Items

The team discussed how DevOps and System Engineers would be brought in to take a deeper look at the servers. Their primary means of communication is through Microsoft Teams and Office 0365 email. The Security Team would continue to monitor for alerts and see if there was any additional information surrounding this anomalous behavior.

DevOps and System Engineers would focus on bringing the clusters, host, and virtual machines back up. They discussed going into Azure to detach the disks, drill into the directory structure, clean up, and migrate the disks back. If they find anything that is infected, they will reach out to the Security Team. The team also specified if there was a big outage, they would be working closely with Security from the beginning.

Every application or asset owner will lead the charge with internal communication and streamlining communication with other teams.

Declaring an Incident

The team also discussed how and when to escalate an "event" to an "Incident". They determined that it would be a collective effort in declaring an incident. Once an incident is declared, the *Incident Plan* kicks in. For P1/P2 events, IT Technicians, Managers, and all people who are listed in the process are brought in for a Teams meeting to work through the issue, normalize communications, sort out troubleshooting, and try to determine root cause. If there becomes a transition from a technology major event to an incident that is governed by the IR plan, then an additional parallel process will take place.

Documentation

There is a documentation process that brings in information from the ticketing system, ServiceDesk, Teams meetings recordings and transcriptions. Gordon or Ellie would create a timeline.

Monday Early Afternoon (4.0)

Shortly after the lunch hour, a key vendor has contacted the organization noting an issue
The scheduled routine data transfer failed to initiate over the weekend
The IT Team finds that this affects the same servers that failed to complete backups

Discussion Notes and Action Items

The team discussed the importance of bringing in IT Ops to help provide insight on the data transfers. IT Ops are responsible for data transfers in the Organization (FTP, etc.) from 5AM-5PM. They monitor jobs for failure and recovery all day long. If they note if files are not received or sent, they would work with the

owner and vendor to determine why the files were not transferred correctly. IT Ops escalates to the owner of the data to see why the files were not transferred correctly.

This has not been declared an incident yet and has not been raised to management. The team would bring in managers if the server is member facing or if it has a big impact. They would also notify members through online postings and social media.

Monday Mid-Afternoon (5.0)

The two servers in question appear to be "talking" to a non-US based IP address
Logs reveal that the traffic volume is low, but consistent
IT remains unable to use Acme to access the servers, though the agents appear to be online

Discussion Notes and Action Items

What actions would you take if you cannot get into the server and there is traffic going out of the country:

The team discussed the following action items:

- disable the NIC from the backdoor and isolate the asset to stop the traffic. Isolation would allow the team to be able to still work on the server without it providing traffic outwards
- search through Firewall logs that for information on inbound and outbound traffic
- search through logs and metadata. Log retention is 1.5 weeks and metadata retention go back for months for on-prem servers
- have a pretty good idea what type of data is on what server. The operations team would tell the rest of the team what data is on what file and on what server.
- This is still not declared an incident. The team still needs to know what data was being exfiltrated.

If declared an Incident

- The team would work a governance process parallel to the troubleshooting
- There are predefined criteria in determining an incident. If it affects PII, then there is 72-hour timeframe to notify NCUA that they were researching the incident.
- Notify Legal
- IR team would work with Stephanie, marketing, legal, and others. They would consider what is required from a state perspective and determine what notifications are required.
- CrowdStrike logs would show some information
- up to the committee before deciding to use their forensic services
- great established relationship with Beazley

Monday Late Afternoon (6.0)

Acme reaches out directly and informs IT that an old vulnerability has resurfaced after a recent patch
If the Acme agent version in use was released after April 2024 but is not the most current version, the agent may be susceptible to a brute force attack with a high rate of success.
A successful brute force has led to known data exfiltration

Discussion Notes and Action Items

After the announcement from the vendor that an old vulnerability resurfaced after a recent patch, the team decides to check CrowdStrike or Qualys for their software inventory to see which version they're currently running in efforts to determine whether the servers are susceptible to the vulnerability.

The team does not declare this an incident because they still cannot determine what data was exfiltrated. They also collectively determined that the risk of further data exfiltration is lower because the servers have been isolated. For added protection, they decided to continue to closely monitor activity on the servers moving forward.

Exercise Conclusion

- BCU has accomplished the following:
    - Followed processes to triage, categorize, and prioritize an anomalous event.
    - Ensured all participants accessed the IR playbook to manage an event.
    - Relied on personnel expertise to augment the response.
    - Confirmed proper evidence gathering and documentation through the ticketing system were implemented.
    - Identified the Incident Commander/Manager who properly led the response. Determined the collaborative nature of working across teams to triage event.
    - Recognized and followed established communication protocols.
    - Contacted the necessary third parties at the appropriate stage of the response.
    - Generated ideas to improve and streamline both the plan and the process.

End of Exercise