RIVIAL
DATA SECURITY

Incident Response Tabletop Exercise Report

Exclusively prepared for:

BCU

August 19, 2024

RIVIAL
SECURED

Table of Contents

Stay Ahead of Risk. Maintain Compliance. Solidify Peace of Mind.

Exercise Overview

Rivial Data Security LLC (Rivial), in conjunction with Baxter Credit Union (BCU), conducted an Enterprise Information Security Incident Response Ransomware discussion with key employees to determine how to best move forward in creating an Official Ransomware Strategy.

The purpose of the exercise was to discuss plans on how to best respond to a Ransomware attack. Goals also included the evaluation of response processes, ensuring adequacy of technology tools, and validating roles and responsibilities. Additional goals included:

- Define the security function and align it to the goals, mission, and objectives of BCU.
- Planning horizon for long-term goals and vision for the future are discussed in a strategic plan.

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

Create a Ransomware Strategy that accounts for critical security events to ensure everything is effectively managed, identified, contained, escalated, and resolved in a timely manner. The goal of containment and mitigation is to bring all Business Functions up to full capacity and protect member data.

Exercise Goals

- Promote discussion around preparation, identification, containment, eradication, and recovery.
- Exercise and evaluate the response process utilized during a potential incident.
- Ensure proper documentation and information are available to all members of the response team.
- Review cyber insurance policy and third-party support in the case of a ransomware attack.
- Review communication between internal teams.
- Review PR strategy and consider lessons learned from Patelco and CrowdStrike.

Exercise Objectives

1. Begin tailoring an Enterprise Ransomware Strategy
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

Molly Ford and Danny Rowell of Rivial Data Security led the table-top exercise and discussion. Danny presented the team with an overview of the lifecycle of a ransomware attack. Molly led a discussion covering key topics and considerations that will aid in creating a thorough ransomware strategy. Detailed descriptions of, and notes from, the scenario are in Appendix A of this report.

Rivial and BCU will work together on an official Ransomware Strategy.

Observations

After reviewing the content from the exercise, Rivial recommends the following when creating BCU's official Enterprise Ransomware Strategy.

#	Category	Recommendation
1	Cyber Insurance	*Rivial recommends ensuring there is effective communication between Cyber Insurance, Legal, and Security. Rivial also recommends revisiting current policy to ensure appropriate coverage. Cyber Insurance will connect BCU with additional third-party support.*
2	Back-up Communication: SMS	*Rivial recommends deploying an SMS communication solution within the employee environment to establish redundancy in communication.*
3	TruState	*Rivial recommends adding TruState to the Incident Response Plan. Currently, there are no notification requirements. Further clarification is needed to determine notification requirements.*
4	PR Firm	*Review contract and services of PR firm to determine whether to use BCU's internal resources to create drafts for the public, members, and media or rely on the PR firm to provide communication material.*
5	Communication: Branch Managers	*Rivial recommends amending the Incident Response Policy to include guidance for Branch Managers on how to handle member and public questions.*
6	Post-Incident	*Rivial recommends ensuring there is increased Security Awareness and Technical Controls in place in the high likelihood attackers will target members and employees after a Ransomware Attack. Consider creating and promoting Security Awareness Training that focuses on post-incident frauds that can be available over social media, email, and website.*

7	Post-Incident Controls	*Rivial recommends creating a secure process for members to communicate with the credit union that limits the likelihood of a bad actor successfully deceiving members into providing PII.*
8	Physical Controls	*Rivial recommends determining how and when to lock down physical facilities in the case of a cyber-attack.*
9	Access to Ransomware Strategy and IR Plan	*Rivial recommends ensuring all essential employees have access to the IR Plan and Ransomware Strategy that is not dependent on network access.*
10	Vendors	*Rivial Recommends continuing to strength ties to all vendors, in addition to nurturing current connections with cyber insurance. There is an increase in supply-chain risk as more systems are outsourced. It is vital to have strong vendor relations and contacts. Ensure BCU has an up-to-date call tree to reflect those responsible for vendor relations and communications.*
11	Call Center	*The team noted that their policy provides a call center which would help in the case of an overload. This guidance should be for members who physically show up at branches and synchronize the phone systems with a call center to offload traffic.*

Appendix A: Ransomware Strategy

MEETING NOTES

Communication

The team reviewed reporting and how, when, and what to communicate to third-party support and cyber insurance. They reviewed their relationship with cyber insurance and noted BCU's main points of contact. The team noted that there would be a collaboration between Legal and Security on communicating with cyber insurance. They would look to cyber insurance for guidance on additional support, including law firms, and forensic specialists.

Reminder: The earlier you can communicate to cyber insurance, the better and the more support that you may be able to get. Additionally, by communicating early with insurance you will be more likely to follow all mandates by the insurance vendor.

Communication outside of the network:

There are redacted policies stored online.

Communication Redundancy: SMS

There is current access to employees' network and phone number that does not require a BCU login. There is an SMS platform that BCU is trying to get employees to adopt, but there is still room for improvement with off-net network communication. The team discussed building more redundancies in their processes.

Forensics

The team discussed the that forensics work would be collaborative in nature, which would allow for Security personnel including Stephanie and the team to add their expertise.

Coverage

The team mentioned coverage from TruState and their role in a potential class action lawsuit. The organization would prefer to avoid a class action lawsuit in the first place. *We are looking for lessons learned: who to contact, when, to contact, and what order they are going to talk about it from Patelco attack.*

Communicating to the Public

There are templates for diverse types of communication intended for different audiences in the case of an incident. BCU is still developing new playbooks to ensure broad coverage and consideration of different scenarios. The team recommended referencing the security updates from the Patelco website and the information from their FAQs section developed in response to the Ransomware attacks.

Communication to the Press

The team discussed processes around communication with the press and their current coverage that would give them access to publicity firms. They discussed that those services are part of a benefits package accessible on day one.

Communication: Social Media

The team also discussed the need to account for social media in the overall Ransomware Strategy and IR Response. In different case studies during a major service outage, members and the public have taken to social media to reach out to the credit union. The team discussed the use of PR firms to provide a playbook for what and how to communicate to members or the public, including through social media.

The team discussed their Business Continuity Resiliency Committee group and highlighted their excellence in collaborating with different departments and helping members. There was emphasis on prioritizing support for the branch leaders who will have direct access to members and the public.

Review contract and services of PR firm to determine whether to use your internal resources to create drafts for the public, members, media, etc.

Post-Incident Risks

The team discussed that new risks emerge after incidents occur and cited a case where a credit union suffered a ransomware attack. The credit union paid the ransom, decrypted their files and restored operations; however, the credit union's members were faced with another attack. There was a large phishing campaign where the malicious actors said they were from a financial institution and wanted to ensure the members' accounts were secure. They verified the social security number and other PII.

The credit union in this scenario responded by creating tighter controls over how members communicated with the credit union to lessen the likelihood a malicious actor could successfully mask as an official credit union representative.

Physical Security

The team discussed whether to consider physically locking down facilities in the case of a Ransomware Cyber Incident.

Best Practices

One of the final considerations was about the importance of asset inventory, patching vulnerabilities, and keeping up with security updates on all devices. The team noted that this needs attention and needs to be updated. There was heightened importance on looking at security and patching update, tools, and monitoring.

- Creating a whitelist of applications and restricting or severely limiting downloading unauthorized applications.
- Continuing Security Awareness Training.
- Reviewing vendor contracts and making sure there is an awareness of what the vendor is responsible for, and breach or incident disclosure.
- The team discussed the importance of continual phishing assessments for employees and whether BCU should adopt a termination of employment policies for employees who fail tests over a predetermined number of times after a predetermined number of Security Awareness Training sessions.