Apple Bank Cyber Table Top Exercise

Lessons Learned and Awareness Training

July 2021

Cyber Table Top Exercise Overview

Cyber Table Top Overview

On June 9th 2021 Apple Bank conducted a cyber table top exercise with the Incident Response Team ("IRT") and the Executive Management Steering Committee ("EMSC")

- The table top exercise was facilitated by the Bank's cyber insurance broker Willis Towers Watson;
- The objective was to provide insight into how the Bank would respond to a real cyber attack;
- EMSC and the IRT were presented with a cyber attack scenario;
- The cyber attack scenario was based on the emerging threat of ransomware; and
- The EMSC and IRT had to respond to the attack scenario.

Cyber Table Top Exercise: Lessons Learned

During the exercise the EMSC and IRT were presented with several questions regarding how the Bank would respond and recover during a real cyber attack. Action items have been identified to improve the process.

Action Items

Action ID	Actions	Owners	Due Date
1	Train employees not to communicate any information about the incident to customers or the press.	Corporate Training	TBD
2	Provide quarterly reminders through the Privacy Perspectives newsletter, as well as develop tips that can be displayed on screensavers and posters to enhance awareness.	Information Security	8/31
3	Appropriate training for primary, secondary and all delegated backup IRT members.	Information Security	10/31
4	Ensure that the Incident Response Plan ("IRP") has clearly defined delegated backup contacts in the event the primary contact is not available.	IRT Members	TBD
5	Provide hard copies of the IRP to all primary, secondary and all delegated IRT members, in the event systems are down.	BCP/DR	TBD
6	Create and distribute wallet cards with instructions and dial-in information to help assemble the IRT members.	Information Security /Marketing	9/30
7	Determine the method of out of band communication for IRT members in the event email has been compromised.	BCP/DR	TBD
8	Engage a forensic firm on a retainer to make sure in advance of an event that the forensic company would have a working knowledge of the Bank's environment. ***(Budgeted for 2021)***	Information Security	11/30
9	Use crisis management tools to effectively communicate with employees and provide instructions on how to respond to an incident.	BCP/DR	TBD
10	Develop a call tree for all departments, and consistently perform call tree drills.	BCP/DR	TBD
11	Work with the Bank's public relations firm to develop a public relation plan in the event of a cyber incident.	Consumer Banking	9/30
12	Develop procedures for business departments to operate in the event of a security Incident where the Bank is unable to process transactions (i.e., C&I and RELC transfer funds on a loan).	EMSC	TBD
13	Coordinate with external legal counsel to enhance the understanding of the strategy and approach to ransomware payments.	Legal	TBD

EMSC Incident Response Awareness Training

Incident Response Plan ("IRP") Awareness Training

The IRP establishes procedures for the Bank's incident response process, including steps for identifying, reporting, investigating, analyzing, resolving and recovering from an incident.

IRP Purpose and EMSC Roles

The incident response plan facilitates a centralized process that focuses on organizational coordination, communication and escalation activities enabling a seamless dynamic to effectively and timely respond to and recover from a data security incident.

The Incident Response Team ("IRT") will promptly alert the EMSC of a data security incident based on the severity of the incident according to parameters defined in the Plan.

- The role of the EMSC:
  - Provide executive perspective, feedback, and effective challenge, as well as weigh in with decision making on escalated matters (i.e., paying a ransom).
  - Participate in after-action reviews to contribute to identifying lessons learned and assist in suggesting improvements to the IRP.

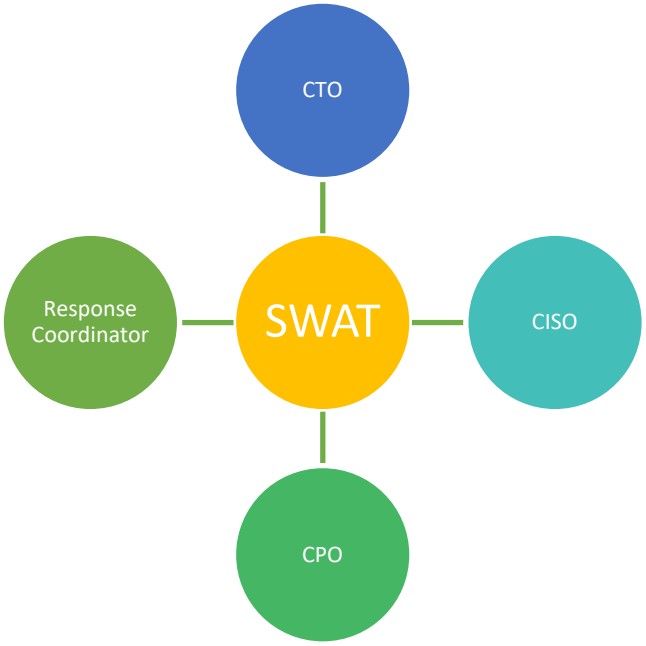
Incident Response Team Structure

The IRP organizes incident response in a tiered approach based on appropriate escalations.

Structure of the IRT

The SWAT team is engaged first in the initial escalation process, to assess and determine if a substantial, organized response is required.

– SWAT is comprised of CTO, CISO, CPO and Response Coordinator



Incident Response Team Structure

Continued

Structure of the IRT

As warranted, SWAT thereafter further escalates to the full IRT to determine the appropriate steps necessary to respond to the incident.

- IRT Standing Membership is SWAT plus CEO/Chairman, General Counsel, Chief Risk Officer and Chief Retail Banking Officer
- Non-Exclusive list of additional personnel who are engaged on a fact-dependent or SME needed basis, in addition to external SMEs as needed

Non-Exclusive list of additional personnel
Chief Financial Officer
Chief Compliance Officer
IT Infrastructure and Support Manager
Chief Human Resources Officer
Director of Marketing
Director of Digital Banking
Director of Deposit Operations
Business Continuity Officer
Vendor Management
Head of Financial Crimes Compliance & BSA Officer

Incident Response Strategy

Take Charge and Determine Facts

Apple Bank Incident Response Strategy

Take Charge Quickly:

- It is imperative in any incident situation for Apple Bank and its leadership to recognize the nature of the incident and begin to manage it as soon as possible.
- It is incumbent upon the SWAT Team to make the decision whether or not to activate the IRT as soon as possible.

Determine the Facts:

- It is critical that all members of the SWAT Team and IRT are assessing the incident with the same set of facts – a common operating picture of the issues.
- This begins by gathering information about what specifically has occurred that has created the potential incident.
- The activation of the IRT will provide the structure within which enterprise-wide facts, developments and messaging can be gathered and included in situation reports to inform the IRT on a regular cadence.
- The IRT will then provide updates to the EMSC and Board at appropriate intervals and as needed on an escalation basis

Incident Response Strategy

Awareness and Communication

Apple Bank Incident Response Strategy

Maintain Persistent Awareness of Situation and Impacts:

- Typically, an incident evolves quickly and it is important to have ongoing situation monitoring activities and an attitude of persistent awareness to ensure that employees notice and escalate critical events, issues, or impacts as soon as possible.

Communicate quickly but responsibly:

- The Communications Guide section of the Plan outlines the strategy for communicating to employees, customers, regulators and the public.
- When the image and credibility of Apple Bank is potentially questioned or threatened due to the reaction and response to an incident situation, it is critical that Apple Bank let concerned entities know what its posture and response actions are.
- There should not be a rush to communicate, however, until sufficient facts are developed.

Incident Response Strategy

Isolate, Contain and Follow-thru

Apple Bank Incident Response Strategy

Isolate and Contain the Problem:

- There is immediate tension between acting quickly to stay in front of the incident and knowing that the IRT needs accurate factual information to support solid deliberative decisions.
- Apple Bank's priority in responding to an incident will be to contain – to not allow the incident to grow or worsen.

Relentless Follow-thru:

- The Response Coordinator will track action items which are underway, as well as open action items to be undertaken, and IRT will meet at frequencies necessary to track progress in resolving items/issues.
- The IRT members must be committed to being accountable to meeting milestones and incident resolution deadlines.
- Apple Bank executives and managers will foster a similar attitude of follow-through and accountability to all employees and contractors involved in incident response and recovery efforts. This is where the tone from the EMSC can play a critical role.