Incident Response

Incident Response Roundtable Testing

On [DATE] [BANK] personnel including [LIST PARTICIPANTS] conducted an incident response roundtable as 2015’s incident response test.

The purpose of the incident response test is to review the current incident response plan, to utilize a scenario to verify the validity of the plan, and to update the plan based on the roundtable test.

Scenario: On Tuesday, December 1, 2015, [Personnel Name] noticed an abnormal slowdown in computer performance. Additionally, [Personnel Name] noticed a number of files being deleted.

Questions:

1. What actions should [Personnel Name] take at this point?
2. What actions should others take as they are notified?
3. How will the bank contain a potential breach?
4. How will the bank investigate to identify whether a breach has occurred?
5. Who will be responsible for initiating and maintaining documentation of all steps?
6. What potential forensics investigators will be utilized if deemed necessary?
7. At what point would customers be contacted?
8. Likewise, at what point would the bank’s primary regulatory agencies be contacted?

Review:

[BANK] utilized information found in VISA What to do if Compromised to provide training and action items to [PARTICIPANTS]: https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf . Pertinent areas to review (relevant sections only) can be found on pages 3 and 7+.

[BANK] viewed one of the vignettes as presented by the FDIC. https://www.fdic.gov/regulations/resources/director/technical/cyber/cyber.html

Employees Attended