VIGNETTE DESCRIPTION

Customer Account Takeover

A long-time valued corporate customer is questioning withdrawals from its cash management/payroll account. The bank's loan officer contacted the customer and told the customer it would have to use its line of credit to make payroll. The company thought it had sufficient funds and reviewed its account statement, which showed several withdrawals for under $10,000 over the last month and one large withdrawal for $250,000. The bank researched the matter and determined that the withdrawals were made through the online cash management system by an authorized user. The customer states that it did not make the withdrawals and indicates that the withdrawals started shortly after the company received an email from the bank asking it to update the company's account information. The bank informs the customer that it did not send the email.

INCIDENT ASSESSMENT QUESTIONS

What information should be gathered from the customer for investigation of the suspicious transactions?

Does your incident response plan include current contact information for local police, FBI, and U.S. Secret Service?

What computer hardware devices and logs might contain useful forensic information, and how would your institution protect this evidence?

AWARENESS QUESTIONS

This customer fell prey to a phishing email and followed links to a malicious website. How does your institution promote awareness of phishing and educate customers about avoiding scams that target your institution?

RECOVERY OF FUNDS QUESTIONS

What actions should be taken to attempt recover of funds and to prevent additional unauthorized transactions?

Do you verify that all security procedures required by the blanket bond and riders have been implemented at each renewal?

What regulations, account agreements, and circumstances would your institution consider when determining whether to refund financial losses that result from online fraud?

MULTIFACTOR AUTHENTICATION QUESTIONS

Has your institution implemented a layered security program that meets the 2011 updated guidelines for multifactor authentication?

How does your institution detect and respond to anomalies?

Does the program include enhanced controls for system administrators?

If device identification and challenge question(s) are used, does the system use complex identification and out-of-wallet questions as described in FIL-50-2011?

RISK ASSESSMENT QUESTIONS

Does your institution review and adjust the layered security program at least annually to respond to changes in the online functionality that you offer to customers and to protect against the loss experience at your institution and throughout the industry?

INSURANCE QUESTIONS

Will your current insurance coverage provide adequate protection against loss associated with impacts from the scenario described?

Is the amount of your insurance coverage commensurate with the amount of potential loss?

Has insurance coverage been added or expanded to account for new activities?

SOLUTION DEVELOPMENT QUESTIONS

Select one or more characters in the vignette. Discuss the options these individuals could consider in response to the scenario.

- What actions could be taken?
- Who would conduct these actions?
- What decisions need to be made, by whom, and at what point in time?
- What are the authorities for making and carrying out these decisions?

REFERENCES

References

- FIL-103-2005 Authentication in an Internet Banking Environment
  https://www.fdic.gov/news/financial/2005/fil10305.html
- FIL-50-2011 FFIEC Supplement to Authentication in an Internet Banking Environment
  https://www.fdic.gov/news/news/financial/2011/fil11050.html
- FIL-65-2005 Guidance on Mitigating Risks From Spyware
  https://www.fdic.gov/news/news/financial/2005/fil6605.html

External References

- National Cyber Security Alliance;
  www.staysafeonline.org
- OnGuard Online;
  www.onguardonline.gov
- Internet Crime Complaint Center;
  www.ic3.gov