3

CYBER CHALLENGE

THE STATE BANK OF
TOWN CITY

FDIC

1. VIGNETTE DESCRIPTION

PHISHING AND MALWARE PROBLEM

A bank employee informs the bank president that she followed up on her email request to check the bank's website, and it looks ok. However, the president stated that she did not send an email requesting the employee to check the website. The bank soon discovers that its Voice over Internet Protocol (VoIP) server is down and none of the phones are working. Two work stations have also crashed. The bank is informed by its technology service provider that it has detected malware coming in over the bank's connection. The bank invokes its incident response plan.

3

CYBER CHALLENGE

THE STATE BANK OF
TOWN CITY

FDIC

2. TECHNICAL MEASURES

A spear phishing attack compromised a workstation with malware that replicated to some servers and workstations. What technical measures should be taken to prevent further contamination, to preserve evidence, to detect fraudulent transactions, and to assess damage?

Does your incident response plan address these measures?

QUESTION(S)

3

CYBER CHALLENGE

THE STATE BANK OF
TOWN CITY

FDIC

3. COMMUNICATIONS

What steps should employees and managers take to communicate internally, to develop appropriate messaging to clients, and to notify external parties such as law enforcement?

What policies, procedures, and forms should staff members use for guidance?

QUESTION(S)

3

CYBER CHALLENGE

THE STATE BANK OF
TOWN CITY

FDIC

4. LONG-TERM CORRECTIVE MEASURES

What measures are necessary to ensure that the malware is completely removed from the network?

Would recovery include network design changes?

Do data backups exist in a format or location that is protected from self-replicating malware?

QUESTION(S)

3

CYBER CHALLENGE

THE STATE BANK OF
TOWN CITY

FDIC

5. ADMINISTRATIVE CONTROLS

What administrative controls contribute to preventing malware infections? Consider employee training and policies.

How often are administrative controls reinforced through awareness initiatives such as reminders in staff meetings, posters, and updated training?

QUESTION(S)

3

CYBER CHALLENGE

THE STATE BANK OF
TOWN CITY

FDIC

6. TECHNICAL CONTROLS

What technical controls contribute to preventing malware infections and to limiting the spread of attacks throughout the network? Consider technical controls that supplement anti-malware software such as user access controls, network design, data backup, and patch management.

To what extent does your audit program validate that these controls have been implemented and are working as intended?

QUESTION(S)

3

CYBER CHALLENGE

THE STATE BANK OF
TOWN CITY

FDIC

7. INSURANCE

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?

QUESTION(S)

3

CYBER CHALLENGE

THE STATE BANK OF
TOWN CITY

FDIC

8. SOLUTION DEVELOPMENT

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?**

QUESTION(S)

3

CYBER CHALLENGE

THE STATE BANK OF
TOWN CITY

FDIC

9. REFERENCES

REFERENCES

- FFIEC IT Examination Handbook, Information Security Booklet

  http://ithandbook.ffiec.gov/it-booklets/information-security.aspx
- FIL-43-2003 Computer Software Patch Management

  https://www.fdic.gov/news/news/financial/2003/fil0343.html
- FIL-103-2004 Interagency Informational Brochure on Internet "Phishing" Scams

  https://www.fdic.gov/news/news/financial/2004/fil10304.html
- FIL-27-2005 Final Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

  https://www.fdic.gov/news/news/financial/2005/fil2705.html

EXTERNAL REFERENCES

- Computer Security Incident Handling Guide; National Institute of Standards and Technology (NIST) Special Publication 800-6; www.nist.gov
- National Cyber Security Alliance; www.staysafeonline.org
- OnGuard Online; www.onguardonline.gov
- Anti-Phishing Working Group; www.apwg.org
- Internet Crime Complaint Center; www.ic3.gov