7

CYBER CHALLENGE

FDIC

1. VIGNETTE DESCRIPTION

A cyber-attack has taken place at the bank. Word processing files are being held hostage, and the attacker is demanding payment. The IT department was backing up data on the network file servers nightly. However, data on workstations were not backed up. The bank invokes its Incident Response Plan. Management decides to replace all machines that were compromised in the attack. When the bank president questions the effectiveness of anti-virus and anti-malware programs, management discovers that critical patches were not installed on the infected computers.

7

CYBER CHALLENGE

FDIC

2. SOFTWARE PATCHING

Many forms of malware, including ransomware, take advantage of known vulnerabilities in unpatched systems. What is your institution's process for identifying security vulnerabilities and patching them in a timely manner?

QUESTION(S)

7

CYBER CHALLENGE

FDIC

3. BACKUPS

Some viruses and malware destroy or make original data unrecoverable. How does your institution ensure that all critical data can be recovered?

- **Has the bank conducted a Business Impact Analysis (BIA), including end-user systems?**
- **What data and systems are critical?**
- **Are back-up strategies sufficient to address cyber-attacks?**
- **What steps are taken to ensure that report-generating systems and customizations to standard reports can be restored?**
- **Which data and reports are produced and verified during tests of the business continuity or disaster recovery plans?**

QUESTION(S)

7

CYBER CHALLENGE

PEOPLE'S STATE

PSBM

BANK OF MORELLO

FDIC

4. EMPLOYEE TRAINING

Malicious emails and websites are common initial entry points for attackers. What kind of employee training is in place to increase awareness of proper cyber-safety practices and to protect employees who use email and the Internet?

What support do you provide employees when they receive a suspicious email?

QUESTION(S)

7

CYBER CHALLENGE

FDIC

5. INCIDENT RESPONSE

What tasks does your institution perform during the initial incident response?

Identify the roles and responsibilities for implementing the Incident Response Plan.

How are typical phases of incident response, such as containment, eradication, recovery, and evidence protection, accomplished?

How are these tasks documented in the Incident Response Plan?

How are lessons learned used to improve cybersecurity?

QUESTION(S)

7

CYBER CHALLENGE

FDIC

6. POLICY

Under what circumstances would your institution pay ransom to regain access to critical files or data?

How are malware attacks mitigated?

What factors should be considered before notifying customers of a cyber-attack?

QUESTION(S)

7

CYBER CHALLENGE

PEOPLE'S STATE

PSBM

BANK OF MORELLO

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)

7

CYBER CHALLENGE

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?**

7

CYBER CHALLENGE

FDIC

9. REFERENCES

- **FIL-13-2015 FFIEC Joint Statements on Destructive Malware**
  https://www.fdic.gov/news/news/financial/2015/fil15013.html

- **FFIEC IT Examination Handbook, Business Continuity Planning**
  http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

EXTERNAL REFERENCES

- **Ransomware on the Rise**
  Federal Bureau of Investigation
  http://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise/ransomware-on-the-rise

- **Computer Security Incident Handling Guide**
  National Institute of Standards and Technology
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- **Crypto Ransomware (Alert TA14-295A)**
  United States Computer Emergency Response Team
  https://www.us-cert.gov/ncas/alerts/TA14-295A