9

CYBER CHALLENGE

Bank of **Lieferkette**

FDIC

1. VIGNETTE DESCRIPTION

THE BANK IS EXPERIENCING SLOW NETWORK RESPONSE TIMES.

Network operations staff discovers that several files on the core banking server have been encrypted and transmitted out of the bank. Staff learns that the bank's core banking software update contained malware. The vendor used third-party programmers, unknown to the bank, who provided the corrupted code. Bank staff is having problems accessing core banking information; however, other network functions appear to work. Management invokes its incident response plan. Manual operations can sustain operations temporarily, but the core banking server needs to be cleaned and rebuilt to return to normal operations.

2. INCIDENT ASSESSMENT

What are possible financial, operational, and reputational impacts to your institution resulting from an incident like this?

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

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

QUESTIONS

3. PATCH MANAGEMENT

Does management evaluate the impact of installing patches and updates by assessing technical, business, and security implications?

Are there procedures in place for testing patches and updates before installation to minimize operational disruptions?

Are there appropriate backup and back-out procedures in place to allow for recovery if problems arise during or after installation?

QUESTIONS

4. VENDOR MANAGEMENT

What factors, such as the use of subcontractors, does your vendor selection process consider?

Are there contractual provisions that address the vendor's responsibility for maintaining and testing the integrity of updates before issuance?

QUESTIONS

5. RECOVERY

What is the process for recovering from an incident like this?

What immediate steps are necessary to manage the recovery from this event?

How are recovery priorities established?

QUESTIONS

6. MESSAGING

Does the incident response plan guide the development of messages (e.g., press release, customer notification) so they can be drafted quickly and appropriately for the situation?

Who is authorized to discuss the incident with the service providers, consultants, law enforcement, regulators, and the public?

QUESTIONS

7. INSURANCE

Does insurance coverage protect against losses associated with the scenario described?

Is insurance coverage adequate?

QUESTIONS

8. SOLUTION DEVELOPMENT

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

- **What types of actions could be taken?**
- **Who would act?**
- **What decisions need to be made, by whom, and at what points in time?**
- **Who has the authority to make and carry out these decisions?**

QUESTIONS

9. REFERENCES

REFERENCES

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

- **FFIEC IT Examination Handbook, Outsourcing Technology Services**
  https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx

- **FFIEC IT Examination Handbook, Development and Acquisition**
  https://ithandbook.ffiec.gov/media/274741/ffiec_itbooklet_developmentandacquisition.pdf

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

- **FIL-13-2014 Technology Outsourcing: Informational Tools for Community Bankers**
  https://www.fdic.gov/news/news/financial/2014/fil14013.html

- **FIL-44-2008 Guidance for Managing Third-Party Risk**
  https://www.fdic.gov/news/news/financial/2008/fil08044.html

EXTERNAL REFERENCES

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