8

CYBER CHALLENGE

Eau Rapides Bank

FDIC | COMMUNITY BANKING INITIATIVE

1. VIGNETTE DESCRIPTION

THE BANK'S DATA CENTER WAS FLOODED.

After relocating the data center to the alternate site, management discovered that its new telecommunications provider was impacted by the same flood.

Management realized that:

1. **The telecom provider was not prepared for a natural disaster, which has left the bank unable to share data.**

2. **The telecom provider is uncertain how long service will be unavailable, which means connectivity between branches and outside the bank may be down for days.**

Currently, the bank cannot communicate up-to-date business information or transmit data, such as the cash letter, outside the bank.

2. INCIDENT ASSESSMENT

What are the possible financial and operational impacts to your institution resulting from a loss of connectivity for two days? Three days? Five days?

Are there other systems or services, besides communications, that could potentially have a similar impact?

Based on this discussion, is the bank's business impact analysis up-to-date?

QUESTIONS

3. INCIDENT RESPONSE

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

Does your incident response plan adequately address the loss of connectivity?

Does your incident response plan address other types of similar events, like power outages?

How are employees contacted if the primary contact mechanism (phone) is not working?

How are lessons learned documented and used to improve response in the future?

QUESTIONS

4. VENDOR

What factors, such as reputation, delivery capabilities, and disaster recovery/business continuity abilities, does your vendor selection process consider?

Are there contract provisions or agreements that address the vendor's responsibility for maintaining and testing plans to ensure critical services can be restored within acceptable timeframes?

Have you engaged critical vendors in joint disaster recovery/business continuity exercises?

Have you identified whether any internal procedures would need to be adjusted if the vendor invokes its plan?

QUESTIONS

5. RECOVERY

What immediate steps are necessary to manage this event?

What is the process for recovering from this incident?

How are recovery priorities established?

QUESTIONS

6. MESSAGING

With respect to the communications strategy, who are the critical audiences, and what are the main talking points that should be conveyed to each audience?

How would you reach the audience without telecommunication services?

What policies, procedures, and forms should staff members use to help 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?

What steps should employees and managers take to communicate internally, to develop and disseminate appropriate messages to clients, and to notify other external parties?

QUESTIONS

7. INSURANCE

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

Is insurance coverage adequate?

Has insurance coverage been added or expanded to account for changing infrastructure?

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

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

- **FIL-81-2000 FFIEC Guidance on Managing Risks Associated With Outsourcing Technology Services**
  https://www.fdic.gov/news/news/financial/2000/fil0081.html

EXTERNAL REFERENCES

- **Contingency Planning Guide for Information Technology Systems National Institute of Standards and Technology**
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf