5

CYBER CHALLENGE

FARMERS BANK OF
WESTBURG

1. VIGNETTE DESCRIPTION

The IT Manager believes the bank is experiencing a Distributed Denial of Service (DDoS) attack. The bank's website is slow and, for the most part, inaccessible to customers. The call volume resulting from customers who can't access their online bank accounts is overwhelming the institution's ability to handle calls in a timely manner. The bank invokes its Incident Response Plan. After further analyzing the systems, the IT manager discovers that members of the incident response team were so focused on the DDoS attack, they didn't realize that some of the alerts indicated a second attack had successfully stolen data from the bank. The DDoS attack was merely a diversion.

5

CYBER CHALLENGE

FARMERS BANK OF
WESTBURG

FDIC

2. ASSESSMENT

What are possible financial, operational, and reputational impacts to your institution resulting from the DDoS attack?

Does the loss of data lead to other adverse outcomes?

QUESTION(S)

5

CYBER CHALLENGE

FARMERS BANK OF
WESTBURG

FDIC

3. INCIDENT MANAGEMENT

How does your institution's incident detection/incident response process identify and respond to a multi-pronged attack?

Does the Incident Response Plan include a structured damage assessment or a checklist to help the incident response team categorize and respond to suspected attacks?

QUESTION(S)

5

CYBER CHALLENGE

FARMERS BANK OF
WESTBURG

FDIC

4. MITIGATION

What kind of mitigation techniques, either within your organization or through service providers, has your institution implemented or considered for potential cyber attacks?

What computer devices and logs might contain useful forensic information to aid in the recovery from this incident?

QUESTION(S)

5

CYBER CHALLENGE

FARMERS BANK OF
WESTBURG

FDIC

5. MESSAGING

What measures in the Incident Response Plan address public messaging that reduces confusion for the customers or limits the effects of a disruption?

What type of template is included in the Incident Response Plan to help guide the development of messages (e.g., press release, customer notification) so they can be crafted quickly and are appropriate for the situation?

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

QUESTION(S)

5

CYBER CHALLENGE

FARMERS BANK OF
WESTBURG

FDIC

6. CROSS TRAINING

How many employees are qualified to discuss active cyber-attacks with your Internet Service Provider (ISP), outsourced security monitoring firms, and other service providers? Is this coverage sufficient?

What kind of training program is in place at your institution to ensure that IT and information security staff are able to properly and effectively use the institution's technology solutions? If formal training is not available, how does your staff stay abreast of changing technology?

5

CYBER CHALLENGE

FARMERS BANK OF
WESTBURG

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?

5

CYBER CHALLENGE

FARMERS BANK OF
WESTBURG

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 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?**

5

CYBER CHALLENGE

FARMERS BANK OF
WESTBURG

FDIC

9. REFERENCES

- FDIC FIL-11-2014: Distributed Denial of Service (DDoS) Attacks
  https://www.fdic.gov/news/news/financial/2014/fil14011.html

- FFIEC Joint Statement: Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources
  https://www.ffiec.gov/press/PDF/FFIEC%20DDoS%20Joint%20Statement.pdf

EXTERNAL REFERENCES

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

- DDoS Quick Guide
  National Cybersecurity and Communications Integration Center
  https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf

- Understanding Denial-of-Service Attacks
  United States Computer Emergency Readiness Team
  https://www.us-cert.gov/ncas/tips/ST04-015