6

CYBER CHALLENGE

Farmers State Bank of Robertsburgh

FDIC

1. VIGNETTE DESCRIPTION

Some Automated Teller Machines (ATMs) at the bank have sent out "low cash alerts" to the remote monitoring system. The bank's staff works with its service provider for ATM processing and maintenance to determine the cause of the unexpected alerts. The service provider eventually identifies malware on the first ATM and suspects that a second ATM, displaying similar issues, is also infected with malware. The delivery mechanism and sources of attack are unknown at this time. The bank is surprised to learn that its service provider contract does not cover operating system or security patching.

6

CYBER CHALLENGE

Farmers State Bank of Robertsburgh

FDIC

2. ASSESSMENT

What are possible financial and operational impacts to your institution resulting from the incident?

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?

QUESTION(S)

6

CYBER CHALLENGE

Farmers State Bank of Robertsburgh

FDIC

3. PATCH MANAGEMENT

An operating system and some form of logical security (e.g., policies, procedures) are required to ensure the secure operations of any application used by the public, including ATMs. What is the institution's process for identifying such systems and timely patching them?

Software, like other assets, has a life expectancy. What is the institution's process for identifying and updating systems that are nearing end of life?

QUESTION(S)

6

CYBER CHALLENGE

Farmers State Bank of Robertsburgh

FDIC

4. VENDOR MANAGEMENT

Consider the range of maintenance, service, and administration functions for ATMs. How has your institution identified and assigned security responsibilities that remain with the institution?

Developing relationships and managing service providers are important to ensuring that all security-related roles and responsibilities are carried out consistently and appropriately. What measures are in place to identify and manage those roles and responsibilities?

QUESTION(S)

6

CYBER CHALLENGE

FDIC

5. IT AUDIT PROGRAM

The IT audit program should be part of the institution's risk assessment program. How are lower-risk systems, such as ATMs, included (frequency, depth) in the IT audit scope?

Which audit activities cover the wide range of maintenance responsibilities and information security risks to which ATMs are exposed?

To what extent do the IT audit program, the information security risk assessment, and the patch management program address other devices (i.e., HVAC, conferencing systems, and outdoor electric signs) that are connected to, or accessible from, the institution's network?

QUESTION(S)

6

CYBER CHALLENGE

FDIC

6. ATM SECURITY

How are ATM security and maintenance practices reviewed to ensure current threats are addressed and industry standards are met?

Are reviews limited to physical security measures, or do they include active cash management, daily balancing, and software patching?

QUESTION(S)

6

CYBER CHALLENGE

Farmers State Bank of Robertsburgh

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 expanded to account for new activities?

QUESTION(S)

6

CYBER CHALLENGE

Farmers State Bank of Robertsburgh

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?**

6

CYBER CHALLENGE

Farmers State Bank of Robertsburgh

FDIC

9. REFERENCES

- **FFIEC Joint Statement on Destructive Malware**
  http://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf
- **FFIEC Joint Statement: End of Microsoft Support for Windows XP Operating System**
  http://ithandbook.ffiec.gov/media/154161/final_ffiec_statement_on_windows_xp.pdf
- **FFIEC IT Examination Handbook, Outsourcing Technology Services**
  http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx
- **FIL-62-2004 Guidance on Developing an Effective Computer Virus Protection Program**
  https://www.fdic.gov/news/news/financial/2004/fil6204.html
- **FIL-43-2003 Guidance on Developing an Effective Software Patch Management Program**
  https://www.fdic.gov/news/news/financial/2003/fil0343.html