# Cybersecurity Risk Register: Farmers and Miners Bank

Noah Sturgill, Colby Farmer, & Kaylee Scarce

MIS 3120 01

Dr. Karen Carter

December 4, 2024

**Abstract**

The Risk Register for Farmers and Miners Bank serves as a comprehensive tool for identifying, assessing, and managing risks across all facets of the institution. The risk register categorizes assets into logical and physical categories. For each asset, threats and attack vectors are evaluated; afterward, a Likert scale value of one to five is assigned based on the likelihood and impact of the threats. Using the Likert scale evaluation, a risk matrix was created for each group of assets; the risk matrix is stacked based on the likelihood and impact of each risk. Using the risk matrix, a Cybersecurity Incident Response Plan (CIRP) was created. The CIRP is in alignment with regulatory compliance and industry standards such as the NIST Cybersecurity Framework and ISO 27001. The register is created such that the institution can expand the register with more threats as needed.

## Table of Contents

## Introduction and Background

The purpose of this assessment is to create an in-depth risk assessment for Farmers and Miners Bank. Farmers and Miners Bank, established on July 2, 1979, in Pennington Gap, Virginia, initially operated under the name Farmers and Miners Bank of Lee County. On December 27, 1988, it adopted its current name. The bank's main office is located at 41526 West Morgan Avenue, Pennington Gap, VA 24277. Over the years, Farmers and Miners Bank has expanded its presence, operating six branches across Virginia, including locations in Clintwood, Ewing, Rose Hill, Weber City, and Wise. The bank states that it is dedicated to providing value, convenience, and personalized service to its customers, aiming to be a reliable financial partner for both individuals and businesses in the communities it serves (Farmers and Miners Bank).

## Scope Statement

This cybersecurity risk analysis will create a Risk Register to identify assets, compliance, and mitigation strategies for Farmers and Miners Bank relating to cybersecurity.

### Identify

This section outlines the various requirements and stakeholders relevant to Farmers and Miners Bank. The cybersecurity requirements include compliance with federal, state, and local laws and standards pursuant to banking practices.

### Requirements

#### *Federal*

- Gramm-Leach-Bliley Act (GLBA), Public Law 106-102: Requires financial institutions to explain their information-sharing practices to customers and to safeguard sensitive data.
    - Financial institutions must provide an annual written notice to their customers explaining their information-sharing practices. Compliance is monitored through audits by federal agencies such as the Federal Trade Commission (FTC) and financial regulators.

- Federal Financial Institutions Examination Council (FFIEC), Public Law 95-360: FFIEC provides guidelines and standards on how financial institutions should address cybersecurity risks. Additionally, the FDIC (Federal Deposit Insurance Corporation) refers to FFIEC for standards in cybersecurity.
    - The FFIEC issues guidelines that are reviewed annually, and institutions are expected to continually adhere to these standards. This is enforced through regular audits through regulatory agencies.
- Sarbanes-Oxley Act (SOX), Public Law 107-204: SOX requires establishing internal controls and procedures for financial reporting, including safeguarding data and its integrity.
    - Institutions must implement internal controls and submit written reports on their financial data security annually. Auditors verify compliance with SOX standards, and failure to comply can result in fines or legal penalties.
- Cybersecurity Information Sharing Act (CISA), Public Law 114-113: CISA encourages sharing cybersecurity threats between financial entities and the federal government.
    - While participation is voluntary, financial institutions can share cybersecurity threats with the federal government via written reports or through online systems like the Department of Homeland Security's Automated Indicator Sharing (AIS) platform.
- Federal Trade Commission (FTC) Safeguards Rule, 16 CFR Part 314: The Safeguards Rule is an expansion of GLBA that outlines security measures for financial institutions to protect customer information. It mandates banks to develop, implement, and maintain a comprehensive security program.
    - Financial institutions are required to develop and maintain written security plans. These plans must be reviewed regularly, often yearly, and updated as needed.
- Bank Secrecy Act (BSA), Public Law 91-508: The BSA focuses on detecting financial crimes; these regulations require banks to adopt technologies that secure transaction data, identify verification, and data reporting.

- Financial institutions must regularly update their technologies to ensure the security of transaction data and must submit reports to federal agencies.

***Standards***

- ➢ International Organization for Standards (ISO): ISO 27001 lays the foundation for policy development in information systems. ISO 27110 outlines the guidelines for creating and maintaining Internet security policies.
  - Financial institutions may adopt ISO standards to align with international best practices; meet compliance requirements in global operations; and enhance trust among stakeholders by certifying adherence to rigorous information security protocols.
- ➢ National Institute of Standards and Technology (NIST): The NIST standards for risk management outline techniques for managing and reducing cybersecurity risks.
  - Financial institutions can voluntarily adopt NIST standards, such as the NIST Cybersecurity Framework (CSF), to guide their risk management processes. Compliance with NIST is generally ongoing, with institutions reviewing and updating their cybersecurity policies in alignment with new guidelines. See Public Laws 113-283, 800-63B.

***State***

- ➢ Virginia Consumer Data Protection Act (VCDPA): VCDPA mandates banks ensure strong data protection policies, especially regarding the collection, use, and storage of customer information. Virginia Codes §§ 59.1-575—59.1-585
- ➢ Virginia Information Technologies Agency (VITA): VITA outlines several standards that guide the creation of cybersecurity policy.

### *Industry*

- PCI Security Standards: PCI outlines several security standards relating to business transactions. Maintaining compliance with these standards protects customer information.
- Office of the Comptroller of the Currency (OCC): Banking institutions must comply with cybersecurity standards set by the OCC and Federal Reserve; the primary focus of the regulatory authorities is operational resilience, business continuity, and data integrity.
- Financial Industry Regulatory Authority (FINRA): FINRA provides cybersecurity guidance for financial institutions; additionally, FINRA recommends policies for safeguarding information and protecting against cybersecurity threats.

### *Stakeholders*

The stakeholder groups for Farmers and Miners Bank include customers, employees, and shareholders. The interests of each stakeholder group need to be understood when calculating acceptable risk thresholds. Customers are interested in secure banking services, data security, and transparent fees. Employees desire workplace safety, good working conditions, and job security. Shareholders prioritize profitability, corporate governance, and risk management.

## Protect

This section takes the established scope surrounding Farmers and Miners Bank, including the federal, state, industry, and stakeholder expectations, and further evaluates them through the lens of cybersecurity. The Protect section is being approached using a preventative methodology.

### *Security Measures*

- Authentication Methods
  - Two-factor authentication (2FA) can add a layer of security to digital assets; 2FA requires at least two forms of identification for access.

- Security Tokens generate time-based codes that could be used on smart cards to add an extra layer of protection for physical assets.

➢ Software Measures

- Firewalls act as gatekeepers, controlling the flow from the bank's internal network traffic and external networks; additionally, they provide traffic monitoring and logging, potentially preventing denial of service attacks.
- Antivirus software protects endpoint devices; furthermore, the software encrypts system files, mitigating the risk of a ransomware attack.

➢ Personnel Measures

- Cybersecurity awareness training educates employees on common cyber threats such as phishing, social engineering, and ransomware. Regular mandatory training sessions could mitigate the risks of an employee breach.
- Password management policies would reduce the risk of unauthorized access to banking systems. Requiring a minimal length and complexity increases the difficulty of many common password-based attacks.
- Incident response training ensures employees know how to react when a cybersecurity incident occurs. Well-prepared personnel can minimize damage by responding quickly and appropriately.

➢ Segmentation Measures

- Network segmentation would divide the bank's network into smaller isolated zones. Implementation of Virtual Local Area Networks (VLANs) would separate customer-facing systems from internal systems.
- Role-based segmentation using the principle of least privilege would ensure individuals can only access information and systems necessary for their jobs.

## Assets, Threats, and Vulnerabilities

### Assets

***Physical Assets***

- Hardware
  - Servers: Centralized computer systems for hosting applications, storing customer data, and processing transactions.
  - Workstations: Devices used by employees for day-to-day operations.
  - Networking Equipment: Routers, switches, and other devices that manage network traffic.
  - Point-of-Sale (PoS) Systems: Machines used to process customer payments and transactions at branch locations.
  - Automated Teller Machines (ATMs): Machines for customer transactions and cash withdrawals.
  - Backup Devices: Physical hard drives, tape drives, or cloud storage devices used for data backup.
  - Printers, Scanners, and Copiers: Peripherals that are used for document processing.
  - Physical Security Systems: Security cameras, badge readers, and alarms.
- Facilities
  - Branch Locations: Physical buildings where banking operations occur.
  - Data Centers: Dedicated facilities housing servers and critical infrastructure.
  - Offsite Backup Locations: Facilities that store redundant data and house backup systems.
- Vaults and Safes: Secure storage for physical assets.
- People
  - Shareholders**:** Individuals who have a vested interest in the financial success of the business. They provide the bank with the financial resources necessary for the bank's operation.

- IT Systems Administrator: Manages and maintains the bank's IT infrastructure.
- Tellers: Handle the day-to-day banking transactions and account management for customers.
- Bank Manager: Oversees day-to-day operations, manages staff, and oversees policy and procedure compliance.

***Logical Assets***

- Software and Applications
  - Core Banking System: Software handling deposits, withdrawals, loan processing, and other financial operations.
  - Customer Relationship Management (CRM) Software: Tools used to manage customer information and interactions.
  - Payment Processing Software: Systems for managing debit, credit, and other electronic transactions.
  - Mobile and Online Banking Applications: Platforms that customers use for remote banking services.
  - Loan Origination Software: Systems to manage loan applications and approvals.
  - Enterprise Resource Planning (ERP) Software: Tools used for managing internal operations.
  - Document Management Systems: Software for storing, retrieving, and managing electronic documents.
  - Fraud Detection Systems: Automated tools used in the identification of fraudulent activities.
  - Antivirus Software: Programs used to protect endpoints from malicious software.
- Databases
  - Customer Data: Personal identification information (PII) and other sensitive information may be contained in institution databases.

- Financial Records: Systems that store financial statements, transactions, and logs.
- Loan Databases: Information related to loan processing.
- Backup Databases: Redundant copies of critical data stored for disaster recovery purposes.

➢ Network Infrastructure

- Virtual Private Networks (VPNs): Secure channels for remote employees to access internal systems.
- Domain Name System (DNS): Services managing domain names and IP addresses.
- Email Systems: Internal and external email services for communications.
- Firewall and Intrusion Detection Systems (IDS): Security systems for monitoring and blocking malicious traffic.

Figure 1 showcases the flow of data for Farmers and Miners Bank. All operations revolve around the core banking system. The external entities in the system are customers, ATMs, regulators, and employees. Processes of the core banking system include login system management, ATM operations, and report handling. The data stores of the system are the customer database, the transaction database, and the loan database.

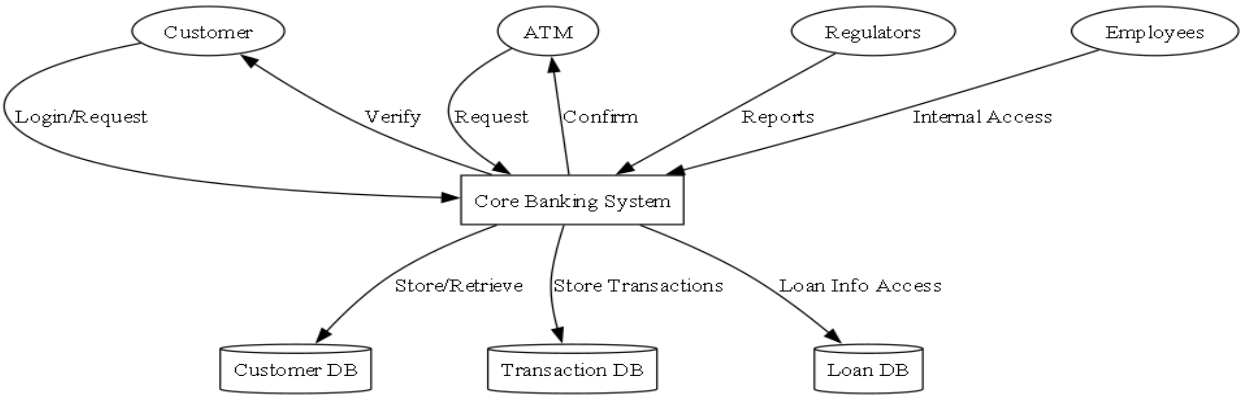


Figure 1. *Data Flow Diagram*

## Threats and Vulnerabilities

Potential attackers to consider for Farmers and Miners Bank include disgruntled employees, competitors, nation-state hackers, and untrained employees. Both categories of employees are of the highest importance in mitigating the risk of an attack.

### *Threats to Physical Assets*

- Servers
  - Unauthorized Access: attackers could gain physical access to servers, leading to data theft, tampering, or installation of malicious software. Attack vectors include insider threats, social engineering, or physical break-ins.
    - Likelihood: Rare (1). Physical security measures, including locked doors, cameras, and alarm systems reduce risk (Dulaney & Eastom, 2023).
    - Severity: Major (4). A breach could lead to severe data loss or compromise, especially given the sensitivity of banking data.
- Workstations
  - Device Theft/Loss: Stolen or lost devices can expose sensitive customer data. Attack vectors include theft by insiders or misplaced devices.
    - Likelihood: Possible (2). The office environment is secured with monitored access (Dulaney & Eastom, 2023).
    - Severity: Moderate (3). May expose customer data if lost but mitigated by in-house software and limited mobility of devices.
  - Malware Infections: Workstations may become compromised by malware, leading to data theft or unauthorized access to the banking system. Attack vectors include phishing attacks, malicious downloads, or using infected external devices.
    - Likelihood: Possible (2). Weekly phishing testing, quarterly training, and Cynet monitoring mitigate risks (Dulaney & Eastom, 2023).

        - Severity: Major (4). Malware could compromise sensitive customer data or lead to unauthorized access.

- Point-of-Sale Systems
    - Ransomware Attacks: PoS systems can be infected with malware designed to capture payment card data or lock down systems until a ransom is paid. Attack vectors include exploiting unpatched software or installing malware onto the system via phishing emails.
        - Likelihood: Possible (2). Measures of monitoring, training, and patching mitigate the chances of an attack occurring.
        - Severity: Severe (5). Disruption to PoS systems could directly impact revenue and operations.
    - Data Skimming: Attackers can install software skimming tools or hardware to capture cardholder data during transactions. Attack vectors include physical tampering or exploiting vulnerabilities to install skimming software.
        - Likelihood: Possible (2). Constant monitoring and standard operating procedures reduce skimming risks (Dulaney & Eastom, 2023).
        - Severity: Major (4). Compromise of payment data could significantly impact customer trust and lead to financial loss.
- Networking Equipment
    - Network Intrusion: Attackers could exploit vulnerabilities in routers or firewalls to access internal networks. Attack vectors include exploitation of unpatched firmware, brute-force attacks, or man-in-the-middle (MITM) attacks (MITRE 2024).
        - Likelihood: Possible (2). Firewall, IPS, and constant monitoring reduce risks (Dulaney & Eastom, 2023).
        - Severity: Major (4). Intrusion could provide access to sensitive internal systems and data.

- Denial of Service (DoS): Attackers could launch a DoS attack to overwhelm the network, causing downtime for systems and services. Attack vectors may leverage botnets or volumetric attacks.
  - Likelihood: Possible (2). Backup ISP and segmented networks mitigate these risks.
  - Severity: Moderate (3). It may cause service delays, but redundancy measures limit downtime impact.

➢ Automated Teller Machines (ATMs)

- Physical Tampering: attackers could tamper with ATMs to install skimmers or malware to steal customer card data. Attack vectors include skimming devices, external malware installation, or insider manipulation.
  - Likelihood: Possible (2). Monitoring and regular checks help detect tampering.
  - Severity: Major (4). Could compromise customer card data if successful or lead to large financial losses from currency stored in the machine.
- ATM Software Exploitation: Attackers could gain remote access to an ATM, allowing the attacker to manipulate the ATM's function. Attack vectors include insider threats and unpatched software.
  - Likelihood: Rare (1). Segmented from the network and regular testing performed.
  - Severity: Moderate (3). This could cause a temporary loss of ATM availability.

➢ Physical Security Systems

- Attackers could bypass physical security systems, allowing them access to restricted areas. Attack vectors could include inside threats, social engineering, or technical manipulation.
  - Likelihood: Rare (1). The complexity of the physical security system mitigates the chances of a physical breach.
  - Severity: Major (4). Would allow unauthorized access to sensitive areas, potentially leading to data theft.

***Threats to Logical Assets***

- Core Banking System
  - Data Breach: The attacker could gain access to the core banking system, leading to the theft of customer data or the disruption of banking operations. Attack vectors include credential theft, unpatched software vulnerabilities, SQL injections, or privilege escalation attacks (MITRE 2024).
    - Likelihood: Possible (2). The regular penetration testing, upkeep of firewall(s), and overall inclusion of awareness in their standards of operation make the chance of a breach low, but not impossible.
    - Severity: Major (4). The breaching of the core banking system would be devastating for the business and its patrons.
  - Insider Abuse: Employees with privileged access could abuse their rights to access or manipulate customer data or financial records. Attack vectors include disgruntled employees and insufficient access control policies.
    - Likelihood: Possible (2). Multi-factor authentication, privilege management, and regular vulnerability management mitigate risks.
    - Severity: Major (4). Insider abuse could lead to unauthorized data manipulation or exposure.
- Payment Processing System
  - Transaction Fraud: Fraudulent transactions could be processed through the system, leading to a financial loss for the bank or its customers. Attack vectors include phishing, card cloning, or unauthorized access to payment systems.
    - Likelihood: Possible (2). Routine employee training, Cynet monitoring, and phishing tests increase employee awareness to mitigate attack vectors (Verizon, 2024).
    - Severity: Major (4). Fraudulent transactions could lead to financial loss and reputational damage.
  - System Downtime: A disruption in the payment processing system could lead to delays or failures in processing customer transactions. Attack

vectors include software bugs, distributed denial-of-service (DDoS) attacks, or third-party service failure.

- Likelihood: Possible (2). Backup ISPs and resilience measures support uptime, though bugs remain possible (Dulaney & Eastom, 2023).
- Severity: Moderate (3). Downtime could disrupt customer transactions, affecting customer service.

- Mobile and Online Banking System
  - Account Takeover: Attackers could compromise customer accounts and gain control of online or mobile banking access. Attack vectors include phishing attacks, weak authentication mechanisms, or the exploitation of mobile application vulnerabilities (MITRE 2024).
    - Likelihood: Possible (2). Weekly phishing training, two-factor authentication, and monitoring mitigate the risk of an account takeover (Dulaney & Eastom, 2023).
    - Severity: Severe (5). Exploited vulnerabilities could expose customer data or compromise access.
  - Application Vulnerabilities: Bugs or vulnerabilities in the mobile/online banking applications could expose customer data or provide unauthorized access to accounts. Attack vectors include exploitation of unpatched software, insecure APIs, or session hijacking (MITRE, 2023).
    - Likelihood: Possible (2). Cynet testing, external testing, and patch management reduce the risk of application vulnerabilities.
    - Severity: Major (4). Exploited vulnerabilities could expose customer data or compromise access.
- Databases
  - Data Breach: Sensitive data stored in databases could be exposed or stolen. Attack vectors include SQL injection, credential theft, or unpatched database software.

        - Likelihood: Possible (2). AES 256 encryption, firewalls, and secure protocols provide strong data protection (Dulaney & Eastom, 2023).
        - Severity: Severe (5). A breach could expose extensive sensitive information leading to lengthy damage controls.
    - Unauthorized Data Modification: Attackers could alter or delete customer data, affecting the accuracy of financial records. Attack vectors include insufficient access control, unmonitored database access, or SQL injections (MITRE, 2023).
        - Likelihood: Possible (2). Privilege management and monitoring help detect unauthorized access attempts (Verizon).
        - Severity: Moderate (3). Data modification could impact financial record accuracy and customer trust. However, backups and rollbacks could mitigate the time to recovery.
- Backup Systems
    - Ransomware Attacks: Ransomware could infect critical systems, leading to the encryption of files and rendering backup and recovery ineffective. Attack vectors include phishing, malicious downloads, or unpatched software.
        - Likelihood: Possible (2). Daily backups, off-site replication, and phishing training efforts reduce risks (Dulaney & Eastom, 2023).
        - Severity: Severe (5). A ransomware infection could significantly impact recovery efforts and disrupt operations.
- Virtual Private Networks (VPNs)
    - Credential Theft: Attackers could steal VPN login credentials, allowing unauthorized access to the internal network. Attack vectors include phishing attacks, brute-force attacks, and exploiting weak authentication mechanisms.
        - Likelihood: Rare (1). Given the very limited to nonexistent remote access available, remote access credential theft is rare.

        - Severity: Major (4). Compromised credentials with successful access could lead to unauthorized access to sensitive information.
    - VPN Misconfiguration: Improperly configured VPN settings could expose the internal network to external threats. Attack vectors include misconfigured encryption settings and misconfigured routing settings.
        - Likelihood: Rare (1). The controlled IT environment with professional staff and limited access mitigates the risk of a VPN misconfiguration.
        - Severity: Moderate (3). A misconfiguration could expose internal systems, but mitigations like firewalls further mitigate risk.
- Domain Name System (DNS)
    - DNS Spoofing: Attackers could manipulate DNS entries to redirect legitimate traffic to malicious websites. Attack vectors include cache poisoning, malicious DNS resolvers, or DNS hijacking.
        - Likelihood: Rare (1). Secure DNS configurations, monitoring, and limited access mitigate the risks of an attack occurring (Verizon, 2024).
        - Severity: Moderate (3). While the attack could lead to a redirection, the overall risk to customer data remains limited.
    - DNS Hijacking: Attackers take control of the bank's DNS servers, redirecting traffic to malicious sites and disrupting access to banking services. Attack vectors include credential theft, misconfiguration, or vulnerability exploitation in DNS management.
        - Likelihood: Rare (1). Controlled access to DNS configurations and credential management reduces risk (Dulaney & Eastom, 2023).
        - Severity: Major (4). A highjacking could disrupt access to banking services and redirect users to malicious sites.
- Email Systems
    - Phishing Attacks: Phishing emails may be sent to bank employees or customers to steal credentials, install malware, or facilitate financial fraud.

Attack vectors include email messages that appear to be legitimate but are malicious.

- Likelihood: Possible (2). Email filtering, regular phishing tests, and quarterly training mitigate the risk of a successful phishing attack (Dulaney & Eastom, 2023).
- Severity: Moderate (3). A successful phishing attempt could lead to malware installation or credential theft.

- Email Account Compromise: Attackers may compromise employee email accounts to launch internal attacks. Attack vectors include credential theft, brute-force attacks, or exploiting weak email authentication protocols.
  - Likelihood: Rare (1). Multi-factor authentication, IP tracking, and regular phishing training mitigate the risk of an account compromise (Dulaney & Eastom, 2023).
  - Severity: Major (4). A compromised account could allow attackers to initiate internal attacks.

➢ Firewall and Intrusion Detection System (IDS)

- Firewall Misconfiguration: Improperly configured firewalls may allow unauthorized traffic to pass into the network. Attack vectors include weak rules, misconfigured policies, or outdated firmware.
  - Likelihood: Rare (1). Constant monitoring, Cynet oversight, and professional IT staff reduce this risk (Dulaney & Eastom, 2023).
  - Severity: Major (4). Misconfiguration could allow unauthorized access, impacting the entire network (Verizon, 2024).
- Overloading Firewall/IDS: Distributed Denial of Service (DDoS) attacks could target Firewalls and IDS systems, overwhelming them and rendering them ineffective. Attack vectors include high-volume traffic attacks aimed at consuming firewall/IDS resources.
  - Likelihood: Rare (1). Backup ISP and IDS/IPS mitigate the risk of a denial of service attack.
  - Severity: Moderate (3). While an attack could temporarily overwhelm systems, resiliency measures would limit the impact.

## 5x5 Risk Matrices

### Physical Assets

Table 1**:** Vulnerability Risk Assessment Matrix for Farmers and Minors Bank, illustrates the relationship between severity and likelihood of identified vulnerabilities. This matrix compares 15 physical assets against potential threats, utilizing a color-coded risk scale: Green (Low: Likelihood 1-2, Severity 1-2), Yellow (Moderate: Likelihood 2-3, Severity 2-3), Orange (High: Likelihood 3-4, Severity 3-4) and Red (Critical: Likelihood 4-5, Severity 4-5). This visualization facilitates prioritized risk across the bank's critical systems

**Table 1**.

*Physical Assets Risk Matrix*

| | 1<br>Insignificant | 2<br>Minor | 3<br>Moderate | 4<br>Major | 5<br>Severe |
|---|---|---|---|---|---|
| 5<br>Frequent | | | | | |
| 4<br>Often | | | | | |
| 3<br>Likely | | | | | |
| 2<br>Possible | | | -Workstation Loss or Damage<br>-Denial of Service | -Malware Infections<br>-Data Skimming<br>-Network Intrusion<br>-Physical Tampering | -Ransomware Attacks (PoS) |
| 1<br>Rare | | | -Software Exploitation | -Server Attack<br>-Physical Bypass | |

**Logical assets**

Table 2: Vulnerability Risk Assessment Matrix for Farmers and Minors Bank, illustrates the relationship between severity and likelihood of identified vulnerabilities. This matrix compares 9 logical assets against potential threats,

utilizing a color-coded risk scale: Green (Low: Likelihood 1-2, Severity 1-2), Yellow (Moderate: Likelihood 2-3, Severity 2-3), Orange (High: Likelihood 3-4, Severity 3-4) and Red (Critical: Likelihood 4-5, Severity 4-5). This visualization facilitates prioritized risk across the bank's critical systems.

**Table 2.**
*Logical Assets Risk Matrix*

| | 1 Insignificant | 2 Minor | 3 Moderate | 4 Major | 5 Severe |
|---|---|---|---|---|---|
| 5 Frequent | | | | | |
| 4 Often | | | | | |
| 3 Likely | | | | | |
| 2 Possible | | | -System Downtime<br>-Unauthorized Data Modification<br>- Phishing Attacks | -Data Breach<br>-Insider Abuse<br>-Transaction Fraud<br>-Application Vulnerabilities | -Account Takeover<br>-Data Breach<br>-Ransomware Attacks (Stored Data) |
| 1 Rare | | | -VPN Misconfiguration<br>-DNS Spoofing<br>-Overloading Firewall/IDS | -Credential Theft<br>-DNS Hijacking<br>-Email Account Compromise<br>-Firewall Misconfiguration | |

# Mitigation and Continuity Plan

## Purpose

The purpose of this Cybersecurity Incident Response Plan (CIRP) is to establish or further assist the already existing establishment of a structured and efficient approach to handling cybersecurity incidents. Executing this plan will minimize the impact of incidents, safeguard sensitive information, and ensure the continuity of critical operations at Farmers and Miners Bank. Once an incident occurs, the CIRP will remain in place until operations are restored to their normal state. In doing so, Farmers and Miners will mitigate potential damage to systems, assets, and integrity.

## Scope

This CIRP covers all assets, systems, and operations of Farmers and Miners Bank, including physical, logical, and third-party assets. It applies to all employees, third-party vendors, and stakeholders engaged in activities that could impact the security posture of the bank. With the inevitability of an attack, this plan outlines a structured approach for handling incidents, from detection to reconstitution, while addressing the previously identified threats. During an incident, critical operations will occur throughout the institution’s six branches and one data center. These are home to Farmers and Miners' critical systems including their core banking system, customer relationship management software, payment processing software, mobile and online banking applications, loan origination software, enterprise resource planning software, document management systems, fraud detection systems, and antivirus software. On top of this, the databases and network infrastructure are as equally critical as their systems to operations. Given the nature of this business, all employees from top to bottom have a role to play in the scope of this incident response plan.

**Assumptions and Planning Principles**

- Realistic Risk Acknowledgment
    - Cyberattacks and disruptions are inevitable. Underestimating this risk leads to inadequate preparation, while at the same time, overestimating can lead to inefficient use of resources. Finding the balance in estimation will ensure preparedness while maintaining mindfulness of resources.
- Duration of CIRP
    - The CIRP is designed to maintain critical operations under the Continuity Plan (CP) for a specific, realistic duration before full restoration is online, and the business is back to normal operation outside the plan.
- Proactive Decision-Making
    - Preparedness involves anticipating disruptions and having well-documented steps to follow to minimize damage.
- Personnel Structure
    - With Farmers and Miners' personnel structure, certain roles were communicated and confirmed. However, assumptions were made regarding already existing roles. Specifically, it is assumed that Farmers and Miners Bank includes roles typically seen within a business and bank in the circumstance it wasn't communicated and confirmed.
- Disruption
    - The CIRP assumes that any attack or disruption worthy of activating the CIRP has the potential to affect any assets within all of the company's branches and/or the data center.

**System Description and Architecture**

Farmers and Miners Bank maintains critical systems, architecture, and inter-facility communication, ensuring the bank's branches and data center can continue operating during a cybersecurity incident. This section details how these systems are interconnected, emphasizing backup measures to ensure continued operation.

### *Overview and Critical Functions (CFs)*

The Continuity Plan (CP) highlights essential Critical Functions (CFs) that must remain operational during a disruption:

- ➢ Transaction Processing
  - ○ Handles ongoing deposits, withdrawals, wires, loans, and related financial transactions.
- ➢ Data Access and Integrity
  - ○ Ensures uninterrupted access to secure and accurate data for customers and personnel.
- ➢ Communication Systems
  - ○ Maintains secure communication channels within and between the company's locations.

### *Systems Descriptions and Documentation*

The bank's infrastructure implies well-documented, detailed critical systems. Their functions and supporting architecture include the following:

- ➢ Servers
  - ○ Primarily Dell servers running Windows Server 2016 and 2022. These are managed daily to ensure optimal performance. (personal communication, October 23, 2024).
- ➢ Workstations
  - ○ Windows 10 (pending upgrades to Windows 11) PCs. These are updated regularly to maintain compliance and security (personal communication, October 23, 2024).
- ➢ Networking Equipment
  - ○ The main routers are Ubiquiti, which are used in tandem with Lightspeed switches to connect internal networks (personal communication, October 23, 2024).

- ISP(s)
  - The primary internet service provider is Point Broadband with a backup ISP by Scott County Telecom to ensure uninterrupted connectivity (personal communication, October 23, 2024).

### *Functional Description*

The functional description builds on the overview, providing detailed insight into the interactions between systems.

- WAN and Data Center Communication
  - A wide-area network (WAN) link connects database servers to each branch, remotely. If the WAN fails, communication shifts to backup modems, which, albeit slow, will support critical operations during disruptions (personal communication, October 23, 2024).
- Data Center Security
  - Servers are housed in a secondary, secured location. It is accessible only to authorized personnel, with environmental controls and separate camera monitoring (personal communication, October 23, 2024).
- Inter-System Communication
  - Core banking, loan processing (through CSI Nupoint), and hosted banking software (LetcherPro) interact seamlessly, with multifactor authentication and encryption securing data exchanges (personal communication, October 23, 2024).

### *Highly Sensitive Information*

Farmers and Miners Bank gathers, analyzes, and stores highly sensitive information. As an FDIC-insured financial institution, the organization houses bank data, customer data, Personally Identifiable Information (PII), and financial records. This information is encrypted using AES 256 (personal communication, October 23, 2024). An Incident Response Team (IRT) is trained to be capable of locating and protecting this highly

sensitive information once the CIRP is activated. This team can be comprised of already existing employees who will switch gears when the CIRP is activated or a dedicated team whose primary responsibility is as a member of the IRT.

***Physical and Environmental Controls***

- Branch Security
  - Physical access to branch locations is restricted with key locks, alarm systems, and camera surveillance (personal communication, October 23, 2024).
- Data Center Protection
  - Includes temperature and moisture monitoring/controls, as well as strict access control, with only two authorized, designated personnel permitted for entry (personal communication, October 23, 2024).

***Backup and Recovery Systems***

- Daily Backups
  - Full server backups are executed nightly, with data replicated to off-site servers to ensure real-time availability (personal communication, October 23, 2024).
- ISP Communication
  - In case of primary ISP failure, the data center will automatically switch to the backup ISP, maintaining essential connectivity.

***Responsibilities***

In the event of a cyberattack or a disruption, having assigned responsibilities makes situations clearer to everyone concerned. This section will address what typically assigned responsibilities during a CIRP should be, while also detailing the already existing roles in the company which will continue to operate during an incident and their responsibilities. Regardless of what primary responsibilities an employee's role may have, they all must simultaneously assume the responsibility

of being proactive in the protection of the business' information both during and outside the activation of the CIRP.

***CIRP and Continuity Plan (CP): Roles and Responsibilities***

- CP Program Manager
  - Ensures that each of the CP roles is on track.
- CP Coordinator
  - Develops, completes, and activates the Business Continuity Plan (BCP) and has direct authority to declare when action is to begin.
- CP Teams
  - Emergency Management Team (EMT)
    - Senior managers with authority.
  - Damage Assessment Team (DAT)
    - Assesses the damages and determines their respective severities.
  - Technical Recovery Team (TRT)
    - Recovers critical IT resources and specializes in resource recovery.

***Existing Roles and Responsibilities***

- IT Department
  - Data Backup and Recovery
    - Ensure the daily backups are completed and validated.
    - Oversee the restoration process when data losses occur.
  - Threat Monitoring and Response
    - Use Cynet to monitor for inside threats while responding to suspicious activities (personal communication, October 23, 2024).
  - Incident Escalation
    - Move incidents to management and external partners such as law enforcement or insurance providers as needed.
  - Access Control Management
    - Execute privilege de-escalation immediately upon employee termination.

        - Manage privileges between new hires, trusted employees, and ascending roles.

- Compliance Officer
    - Regulatory Communications
        - Ensure compliance with all reporting requirements, such as notifying regulators within 24 hours of a significant incident (personal communication, October 23, 2024).
    - Policy Enforcement
        - Verify that cybersecurity measures align with regulatory standards.
        - Oversee annual and quarterly cybersecurity training.
- HR Department
    - Onboarding and Offboarding
        - Oversee secure onboarding by coordinating with the IT department to provide appropriate access controls and cybersecurity training.
        - Notify IT immediately of employee terminations for prompt access revocation.
    - Employee Training
        - Collaborate with the Compliance Officer(s) to schedule and track mandatory cybersecurity awareness training process.
- Bank Manager and Branch Manager(s)
    - Incident Oversight
        - Manage overall responses to significant incidents, ensuring critical functions remain operational.
    - Stakeholder Communication
        - Act as a primary point of contact for stakeholders, keeping them up-to-date on the incident(s) and resolutions.
- Employees
    - Cybersecurity Awareness
        - Complete regular cybersecurity awareness training.
        - Remain vigilant for potential threats.

- Verified through regularly issued, fake phishing emails (personal communication, October 23, 2024).

- Incident Reporting
  - Report any suspicious activities to the IT Department or designated authorities immediately.
- Policy Adherence
  - Follow all cybersecurity and data protection policies. This includes all password and multifactor authentication protocols.
- Ethical Practices
  - While ethics can be considered subjective, it is important to complete daily tasks with cyber-ethics in mind.

**Notification and Activation Phase**

This phase ensures timely and effective response to cybersecurity incidents at Farmers and Minors Bank.

➢ Notification Procedures

1. Incident Detection: Monitor systems, networks, and applications for anomalies.
2. Initial Assessment: Determine incident severity and impact.
3. Notification: Inform CIRP stakeholders, including management, IT, compliance, and external parties (regulators, law enforcement).
4. Activation: Declare incident response activation.

➢ Activation Steps

1. Alert Incident Response Team
2. Notify management and stakeholders
3. Engage external exports if necessary
4. Start incident containment

**Recovery Phase**

The Recovery Phase aims to restore Farmers and Miners Bank's critical operations efficiently and securely after a cybersecurity incident. Following these

steps and maintaining a timeline for each part of the process will offer stability in the steadfast restoration of assets.

- ➢ Recovery Steps
    1. Assess damage and prioritize recovery tasks.
    2. Activate backup systems and data.
    3. Identify and address root causes.
    4. Implement temporary fixes, followed by permanent solutions.
    5. Validate system and data integrity.
    6. Notify stakeholders of recovery progress.
    7. Conduct post-recovery review and analysis.
- ➢ Timeline
    - ○ Immediate (0-2 hours): Assess damage and activate backup systems.
    - ○ Short-term (2-24 hours): Restore critical functions.
    - ○ Medium-term (24-72 hours): Rebuild systems, networks and applications.
    - ○ Long-term (beyond 72 hours): Conduct post-recovery review and implement permanent restoration measures.

**Reconstitution Phase**

Once the CIRP has run its course, the reconstitution phase begins. This comes after the attack has been addressed, and affected systems are back online. First and foremost, the involved teams must have an allocated amount of stand-down time to review the incident. From there, the business can return to normal by following these steps:

- ➢ Reconstitution Steps
    1. System Validation and Testing
        a. Conduct thorough testing to ensure all systems are functioning correctly and securely. This includes verifying data integrity, network stability, and system performance.
        b. Run security checks, such as vulnerability scans and penetration tests, to confirm that no residual threats or vulnerabilities remain.
    2. Documentation and Reporting

   a. Compile a detailed Incident Response Report which includes:
      i. A timeline of the incident.
      ii. Actions that were taken to mitigate the threat and restore operations.
      iii. An assessment of the effectiveness of the response strategies.
   b. Use IRP to identify areas for improvement in future scenarios.
3. Team Review and Lessons Learned
   a. Conduct a post-incident review meeting with the entire security team. Discuss what worked well, what needs improvement, and how to implement those changes going forward.
4. Stakeholder and Employee Communication
   a. Meet with stakeholders, employees, customers, and regulatory authorities to brief each party.
   b. Explain that normal operations have resumed.
   c. Share varying levels of sensitive information as it pertains to the information access of each role.
5. Plan Refinement and Training
   a. Take the lessons learned from the Incident Response Report and update the CIRP.
   b. Schedule training as needed to better plan for the next incident.

**Plan Training, Testing, and Exercises**

To ensure readiness, Farmers and Miners Bank will implement regular training, testing, and exercises focused on the CIRP to validate effectiveness and improve team response capabilities. These activities include:

- Regular Training: Conduct annual CIRP training for all employees, with tailored training for roles in the Incident Response Team (IRT).
- Scenario-Based Exercises: Execute tabletop exercises quarterly, simulating realistic cybersecurity incidents (for example, ransomware, phishing, and data breaches).

- ➢ Live Drills: Perform semi-annual live drills to test system recovery processes, including backups, failovers, and system restoration.
- ➢ Post-exercise Review: After each exercise or drill, conduct a detailed debrief to analyze performance. Document lessons learned and update the CIRP accordingly.

**Plan Maintenance**

The objective of plan maintenance is to ensure the CIRP remains current, effective, and aligned with Farmers and Miners Bank's evolving needs.

- ➢ Key Actions:
    1. Regular Reviews: Review and update the CIRP annually or after significant organizational or technological changes. Include employee, stakeholder, and regulatory body feedback in updates.
    2. Incident Analysis Feedback: After each cybersecurity incident, incorporate findings from post-incident reviews into the CIRP.
    3. Policy Alignment: Align the CIRP with updates to regulations and industry best practices.
    4. Documentation Management: Maintain a centralized secure repository for CIRP documentation; ensure all employees have access to the latest version of the plan.
    5. Technological Adaptations: Update the CIRP to reflect new hardware, software, or operational practices.
    6. Continuous Improvement: Use feedback from training, testing, and incident responses to continuously refine and enhance the CIRP.

**Mitigation Table**

Table 3 outlines the top ten threats by risk for Farmers and Minors Bank's assets. Aligning with industry frameworks (NIST Cybersecurity Framework, MITRE ATT&CK), this assessment outlines the risk, existing security, mitigation strategy, and residual risk for these ten threats. Corresponding mitigation

strategies encompass best practices, technological enhancements, and procedural improvements.

**Table 3**

*Risk Register Table*

**(see next page)**

| **Threat** | **Existing Security Controls** | **Current Risk Level** | **Mitigation Strategy** | **Residual Risk** |
|---|---|---|---|---|
| Data Breach | Regular penetration testing, firewalls. | Possible | Maintain multi-factor authentication, intrusion detection | Low |
| Data Skimming | Constant Monitoring, and standard operating procedures. | Possible | Enhance log monitoring with automated anomaly detection if not currently used. | Low |
| Network intrusion | Firewall, IPS, constant monitoring. | Possible | Continue regular vulnerability scans, and ensure timely firmware updates. | Low |
| Physical Tampering | Monitoring and regular checks. Surveillance coverage | Possible | Maintain monitoring, access controls, and surveillance. | Low |
| Threat | Existing Security Controls | Current Risk Level | Mitigation Strategy | Residual Risk |
| Ransomware Attacks (PoS) | Daily backups, off-site replication, patch management. | Possible | Maintain patch management and backup integrity | Low |
| Malware Infections | Weekly phishing testing, quarterly training | Possible | Maintain antivirus software with automatic updates | Low |
| Insider Abuse | Privilege management, vulnerability management | Possible | Continue least privilege access and periodic access reviews. | Low |
| Transaction Fraud | Quarterly training, Cynet monitoring. | Possible | Maintain real-time monitoring and anomaly detection. | Low |

(*Table cont.*)

| Threat | Existing Security Controls | Current Risk Level | Mitigation Strategy | Residual Risk |
|---|---|---|---|---|
| Application Vulnerabilities | Cynet testing, external testing, patch management. | Possible | Maintain vulnerability scanning and secure coding practices. | Low |
| Account Takeover | Weekly phishing training, multi-factor authentication, and real-time monitoring. | Possible | Maintain multi-factor authentication and enhanced login monitoring. | Low |

**Continuity Plan**

Given Farmers and Miners Bank's extensive existing controls, all identified risks are within tolerable levels. The institution needs to continue its vigilant philosophy concerning the identification and management of risks. The risk register should be regularly reviewed and updated as new risks are identified.

In the event of an incident, expected costs are as follows: Operating on research from downtime costs for small businesses, the expected loss of downtime per minute falls between $137 to $427 per minute. Therefore, assuming $300 is lost per minute, the institution would lose approximately $18,000 for each hour of downtime (Pingdom Team).

**Residual Risk**

All residual risks identified through this assessment are considered low; however, security controls need to be maintained, monitored, and updated as necessary to maintain this status. Additionally, this assessment provides a black-box overview without an assessment of individual system components or configurations; additional risks may exist at a system level that are outside the scope of this assessment.

**Risk Owner**

The stakeholders and IT personnel for Farmers and Miners Bank are responsible for ensuring the residual risks remain within the tolerance level. Failure to maintain risks within the tolerance level may increase the risk of a breach and financial loss.

## References

Dulaney, E., & Eastom, C. (2023). *CompTIA Security+ Study Guide* (7th ed.). McGraw Hill.

Farmers and Miners Bank. (n.d.). *About us*. Retrieved December 2, 2024, from https://www.farmersandminersbank.com/about

MITRE. (2024). *ATT&CK®: Adversarial Tactics, Techniques, and Common Knowledge*.

Pingdom Team. (2023). *Average cost of downtime per industry*. Pingdom. Retrieved from https://www.pingdom.com/outages/average-cost-of-downtime-per-industry/

Verizon. (2024). *2024 Data Breach Investigations Report*.