**NIST CSF 2.0 Cyber security Framework (CSF) for Banking Industry**

By

Solanke abayomi s.

fe/24/6766294920

to

tedprime (Alc) abeokuta

ogun state

**NIST Cyber security Framework (CSF) 2.0** to manage the 15 critical assets in a financial institution like GT Bank involves implementing specific actions across the five core functions: **Identify, Protect, Detect, Respond, and Recover**. Below are how the framework can be applied to each asset:

**1. Customer Account Data**

* **Identify**: Classify data as highly sensitive, considering it involves personal and financial information.
* **Protect**: Encrypt data at rest and in transit, enforce strict access controls, and use MFA.
* **Detect**: Implement real-time monitoring for unauthorized access or suspicious activities.
* **Respond**: Immediately isolate affected accounts, notify customers, and engage incident response teams.
* **Recover**: Restore data from secure backups, ensure integrity, and perform post-incident reviews.

**2. Online Banking Platform**

* **Identify**: Categorize the platform as critical for business operations and customer service.
* **Protect**: Use advanced firewalls, DDoS protection services, and secure coding practices.
* **Detect**: Monitor for unusual traffic patterns and unauthorized access attempts.
* **Respond**: Activate incident response protocols to mitigate attacks and communicate with customers.
* **Recover**: Quickly restore service availability using backups and load balancing, and conduct a root cause analysis.

**3. ATM Networks**

* **Identify**: Recognize ATMs as high-risk points for both physical and cyber-attacks.
* **Protect**: Implement physical security measures, encryption for transactions, and tamper detection software.
* **Detect**: Use surveillance and software to detect tampering or unauthorized access.
* **Respond**: Shut down compromised ATMs, notify authorities, and initiate forensic investigations.
* **Recover**: Replace compromised components and update security measures based on the incident analysis.

**4. Core Banking System**

* **Identify**: Classify as the backbone of banking operations, with the highest security priority.
* **Protect**: Apply strict access controls, regular patch management, and encryption of all transactions.
* **Detect**: Continuously monitor for anomalies or unauthorized access using IDS/IPS.
* **Respond**: Isolate affected systems, roll back unauthorized changes, and notify key stakeholders.
* **Recover**: Restore from the latest backups, verify data integrity, and review system configurations.

**5. Payment Processing System**

* **Identify**: Classify as a critical financial processing system with significant transactional data.
* **Protect**: Encrypt payment data, implement PCI DSS compliance, and use tokenization.
* **Detect**: Monitor for unusual transaction patterns and unauthorized access.
* **Respond**: Temporarily suspend payment processing if compromised, notify partners, and engage response teams.
* **Recover**: Resume operations using clean, secure backups and assess transaction logs for fraud.

**6. Financial Transaction Records**

* **Identify**: Recognize as essential records for regulatory compliance and financial accuracy.
* **Protect**: Encrypt records, use role-based access controls, and apply secure storage solutions.
* **Detect**: Implement logging and auditing of access to records.
* **Respond**: Freeze access to compromised records, assess the extent of the breach, and involve legal teams.
* **Recover**: Restore accurate records from backups, ensure compliance with regulatory requirements, and document the recovery process.

**7. Mobile Banking Applications**

* **Identify**: Classify as a critical customer-facing service with high security and privacy requirements.
* **Protect**: Use secure coding practices, encryption, and regular security testing (e.g., penetration testing).
* **Detect**: Monitor for unauthorized app modifications or breaches.
* **Respond**: Push emergency security updates, notify affected users, and revoke compromised sessions.
* **Recover**: Release a secure version of the app, restore user trust, and reinforce security measures.

**8. Corporate Email System**

* **Identify**: Classify as a critical communication tool with potential for phishing and data exfiltration risks.
* **Protect**: Implement email encryption, anti-phishing measures, and MFA.
* **Detect**: Monitor for phishing attempts, unauthorized access, and data leaks.
* **Respond**: Quarantine compromised accounts, inform employees, and enhance email filtering.
* **Recover**: Restore email services from secure backups, re-enable secure access, and retrain employees.

**9. Data Backup Systems**

* **Identify**: Classify as essential for disaster recovery and business continuity.
* **Protect**: Encrypt backup data, enforce access controls, and store backups in secure offsite locations.
* **Detect**: Monitor for unauthorized access or corruption of backups.
* **Respond**: Replace compromised backups with clean copies, notify relevant stakeholders, and secure backup infrastructure.
* **Recover**: Restore affected systems using secure backups, verify data integrity, and update backup protocols.

**10. Third-Party Vendor Systems**

* **Identify**: Classify as external systems with potential access to sensitive data.
* **Protect**: Enforce strict third-party security requirements, use secure APIs, and conduct regular vendor assessments.
* **Detect**: Monitor third-party access and communications for anomalies.
* **Respond**: Suspend vendor access if a breach occurs, conduct a security audit, and notify affected parties.
* **Recover**: Reestablish secure connections, review contracts, and reinforce vendor management policies.

**11. Regulatory Compliance Data**

* **Identify**: Classify as high-priority data for legal and regulatory purposes.
* **Protect**: Ensure encryption, regular audits, and strict access controls.
* **Detect**: Monitor for unauthorized access or tampering with compliance data.
* **Respond**: Report breaches to regulators, assess the impact, and secure the affected data.
* **Recover**: Restore data to a compliant state, ensure accuracy, and document corrective actions.

**12. Internal Financial Controls**

* **Identify**: Classify as crucial for preventing fraud and ensuring financial integrity.
* **Protect**: Implement access controls, regular audits, and fraud detection systems.
* **Detect**: Monitor financial transactions and control processes for irregularities.
* **Respond**: Investigate suspected fraud, adjust controls, and report findings to management.
* **Recover**: Strengthen controls, restore financial integrity, and reassess control systems.

**13. SWIFT Network**

* **Identify**: Classify as a high-security network for international financial transactions.
* **Protect**: Implement strong encryption, access controls, and multi-layered security.
* **Detect**: Monitor SWIFT traffic for anomalies or unauthorized transactions.
* **Respond**: Halt suspicious transactions, notify affected banks, and conduct a thorough investigation.
* **Recover**: Restore secure operations, verify transaction accuracy, and implement additional security measures.

**14. Physical Branch Security Systems**

* **Identify**: Classify as essential for safeguarding physical assets and sensitive areas.
* **Protect**: Use secure locks, surveillance cameras, and access control systems.
* **Detect**: Monitor for unauthorized access or tampering with security systems.
* **Respond**: Lock down compromised areas, alert security personnel, and repair security breaches.
* **Recover**: Re-secure the branch, restore physical controls, and assess potential losses.

**15. IT Infrastructure (Servers)**

* **Identify**: Classify as critical infrastructure for all banking operations.
* **Protect**: Implement strong access controls, encryption, and regular patching.
* **Detect**: Monitor server performance and access logs for anomalies.
* **Respond**: Isolate affected servers, restore from backups, and engage IT security teams.
* **Recover**: Rebuild and secure servers, restore data, and conduct a post-incident review.

**Summary**

This comprehensive approach, based on the NIST CSF 2.0 framework, ensures that each critical asset is thoroughly managed across its lifecycle, from identification to recovery. By applying these strategies, GT Bank can significantly reduce the likelihood and impact of cybersecurity incidents, ensuring the resilience and security of its operations.