Chicago Bank

Cyber Security Policy

Adeola Fayemi, Aliuddin Uddin, Daniel Stanecki, Elizabeth Herrera, Khushboo Garg, Tony Acosta Hernandez

May 4, 2021

Table of Contents

Cyber Security Policy Introduction

Banks and other financial institutions are subject to a great deal of cyber threats. These looming threats are becoming rapidly worse in terms of frequency and repercussions. With the implementation of this Enterprise Cybersecurity Policy, we will make the Chicago Bank one of the most robust and fundamentally sound banks in Chicago, guaranteeing the highest regulatory ratings in the business and establishing the bank as a role model institution within the community. In addition, we will ensure utmost stability to all of the bank's stakeholders and guarantee the bank customer service that exceeds expectations.

Scope

This policy applies to all of the Chicago Bank's permanent and part-time employees, contractors, partners, remote workers, interns, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware at both locations. Third party service providers providing hosting services or dealing with data outside of the Chicago Bank shall also comply with this policy.

Objectives

The objective of this Cybersecurity Policy is to create a plan for a Chicago-Based Bank that will allow them to keep information secure, comply with all expectations of the FFIEC Information Technology Examination Handbook, and meet the requirements of the New York State Department of Financial Services 23 NYCRR 500 Cybersecurity Requirements for Financial Services Companies. The plan will start by addressing the FFIEC expectations then continue

with 23 NYCRR 500 requirements. Finally, there will be an appendix which lists additional policies that this Bank should meet.

Policies Procedures & Guidelines

Policies from the FFIEC Information Technology Examination Handbook

Risk Measurement II.B

Risk measurement is used to determine the amount of risk of an investment and volatility involved either by accepting the risk or mitigating it. The establishment should have a comprehensive risk measurement process that will be used to determine the associated risks and measure the threats level to apply the appropriate solution to the problem. Risk measurement provides information on specific risk exposure or the accumulated risk exposure and the possibility of loss of said risk.

Risk Measurement should be carried out to calculate the probability of a loss. It can be measured using statistical methods used to predict the risk and volatility of investments of customers at the Chicago bank using Standard deviation, Sharpe Ratio and other risk measurement tools.

Risk Mitigation II.C

Risk mitigation is the action taken to reduce the effects of risk exposure, control and minimize the impact of known risks. There are four types of risk mitigation. They are; risk acceptance, risk avoidance, risk limitation and risk transfer.

Risk Acceptance: Some risks are more expensive to use other risk management options to mitigate it. The cost to avoid or limit the risk may outweigh the risk itself, so it is better to accept it.

Risk Avoidance: Risk should be avoided if it has a high probability of failure and huge financial loss. Chicago bank should avoid risk investments that have a high probability of failure that could affect the bank's ability to serve the community.

Risk limitation: Risk limitation is the most common risk mitigation strategy. It involves limiting a company's exposure risk by taking some actions which could either be accepting or avoiding risk. Chicago bank could limit the number of high risk investments to reduce the possibility of failure and financial loss.

Risk Transfer: Risk transfer is the handling of risk to a third party. The risk may have low probability, but the cost may behave. It can be used so that a company may focus more on its core service and competency. Chicago bank should transfer some of their IT workload to a trustworthy third party IT company to manage because of the number of IT staff they have.

Policies, Standards, and Procedures II.C.1

The Chicago Bank will need to define the institution's control environment using information security policies, standards, and procedures. Policies, standards, and procedures make clear the tasks assigned to employees and provide guidance in the overall functioning of information systems. A successful implementation of this policy involves effective behavior guidance, clear distribution of work, flexibility, and annual board review and approval.

Technology Design II.C.2

The Chicago Bank technology design will incorporate informational, functional, and network requirements while planning for the design. The design of the governing policies and technology must be used effectively against unidentified threats. The technology designers need to be aware of new threats, be ready to change design when needed and use preventative controls. Application control standards will be applied, they include policies and procedures related to user activities, and providing security and reliability to automated systems. The controls will be preventative, detective and corrective and will consist of input, processing and output controls.

Input controls will be automated to ensure accurate input information and will include the following automated controls:

- Duplication Checks: confirm that input is not duplicated
- Limit checks: confirm that predefined limits are not exceeded
- Validity checks: confirm that values fit input criteria

Processing Controls will be automated to ensure systems are processing record information correctly.

- Batch controls: are confirmed against multiple items like total dollars or documents processed
- Error Reporting: identify batches or elements with errors from processing

Output controls will be automated to accurately distribute processed information.

- Batch logs: will verify output against processed batch log totals
- Destruction controls: ensure that stored information is destroyed properly

Management has the responsibility to understand the benefits and limits of the Bank's technology and implement controls needed to counteract limitations. They should continually assess the technology design against the Bank's policies to maintain a proper level of information

security based on the two locations, 14,000 customers and 133 million dollar asset. Standards will be included in procedures to make sure management approves controls and ensure that appropriate personnel like network administrators, and security personnel are involved with the design.

Control Types II.C.3

The Chicago Bank will need several types of controls to reduce risk. Controls will be categorized by timing, nature and be in a layered controlled system that will deploy different controls at various points of the business process and IT systems to increase control strength and catch any weak or failed controls. The controls by timing are Preventative- these controls will be applied to applications and systems that prevent unauthorized users from conducting transactions. Detective controls are designed to alert management when incidents occur and will be implemented by creating reports from systems that show suspicious activity. Corrective controls will be in the Business continuity plans to remediate impact made to the Bank when incidents happen.

The nature controls are administrative, technical and physical. Administrative controls need to be added in policies and procedures throughout the information security program. The controls must also align with the boards approved risk appetite and employee expectations. Technical controls must be in place to prevent unauthorized activity and should be added to firewalls as well as other software or hardware that will be preventing unauthorized activity. Physical controls must be in place to protect the information security at the Bank by ensuring the facility itself has controlled access as well as any devices. The facility should require personnel to use approved access cards or keys to be able to enter the facility as well as any rooms that hold

secure information. Both locations should have a security guard team on surveillance and assets including cash should be stored behind safes and or a heavily protected area with locks.

Management should make sure correct controls are in place and being monitored as well as ensuring roles and responsibilities are assigned to different control type needs.

Control Implementation II.C.4

Controls that align with the Chicago Bank's security and strategic direction must be implemented. From the Bank’s risk assessment, the controls should at minimum, include end-point security, patch management, logging and monitoring, configuration management, scanning and penetration testing, and software development security controls. The control levels for the Chicago Bank should be decided based on the 14,000 customer size, and risk profile. The bank will use the following technology frameworks and industry standards for controls, guidance and implementation: NIST 800 series of publications, International Organization for Standardization (ISO) 27000 series, and Control Objectives for Information and Related Technology (COBIT).

The information security management team or individual must ensure the personnel needs for the controls are available, including proper training and security testing tools. Management should also implement risk based controls for handling security vulnerabilities and threats. They are also responsible for updating the security controls as the environment, technologies and business processes change.

User Security Controls II.C.7

The Chicago Bank's systems should grant access to users based on their role and responsibilities. Controls based on security policies and role-based controls will give user access rights to the Bank's physical and logical environments including:

- Identifying user role-based access that organizes information system and network privileges into roles
- Establishing conditions for roles assigned
- Authorizing and monitoring the use of guest/anonymous and temporary accounts
- Requiring an approved access card for entering facilities
- Requiring appropriate approvals for access request
- Deactivating accounts that are no longer required

Authorized users with elevated privileges pose potential risks to systems. The Bank's personnel can exploit their computer access for authorized reasons or increase risk of damage or loss of information. The following are types of risks vulnerabilities from internal users:

- Alteration of data.
- Deletion of production and backup data.
- Misdirected data.
- Disruption of systems.
- Destruction of systems.
- Misuse of systems for personal gain or to damage the institution.
- Appropriation of strategic or customer data for espionage or fraud schemes.
- Extortion for stolen data.
- Misuse of data following the termination or change in job responsibility of an employee.

It is IT management's responsibility to mitigate risk presented by users. They need to understand the risks to the Bank's information systems and institute appropriate controls to mitigate them and other potential risks. It is also the users responsibility to understand their role in preserving a proper security environment both physically and logically.

Physical Security II.C.8

The physical security of Chicago bank is as important as the cybersecurity of it. The physical security is prone to threats and disaster that could occur anytime. It could be manmade or natural. Management should implement appropriate preventive, detective, and corrective controls for physical (FFIEC). The local area the bank is located will determine the type of physical security that needs to be in place to prevent threats from humans, animals or environmental disaster. Since the bank is in the city, there is no need to have preventive measures for animals like coyotes, deer and other similar animals that are spotted in the suburbs. There should be a response for pest control as they are common in Chicago, and if they get into the bank, they could cause tremendous damage. Fences should be installed around the bank if necessary, to deter unwarranted perimeter breach. Anti glare/screen privacy filters should be added to the bank computers to protect customers information from being seen by unwanted visitors.

- Chicago bank should have policies governing the responsibilities and duties of security guards and authorized personnel who access secured areas where sensitive data are stored.
- Chicago bank should have bullet resistant glass partitions at teller stations.
- Access should be restricted to rooms that stored sensitive electronic devices that Chicago bank uses for its financial services.

Network Control II.C.9

The Chicago Bank needs network controls in order to develop a secure network. This means defining trusted and untrusted zones based on risk profile, layering the institution's trusted network and implementing controls, and using devices to control unauthorized traffic. Sensitive information should be protected by using Voice Over Internet Protocol and network management. Wireless access points, often a weak link in network control, need to be regulated and network monitoring systems need to be updated to be able to detect unauthorized wireless access points.

Logical Security II.C.15

The Chicago Bank needs logical security to mitigate risk. Users need only the minimum amount of access to complete their work, as any more increases risk to the institution. The bank will need to enroll new users, modify user permissions, and continually monitor access rights including conducting a periodic review and validation of access rights. The amount of access rights is to be determined by a manager and the owners responsible for each accessed resource. There should be documented approval from all parties involved. Privileged access, the ability to override controls, should be only given to those who absolutely need it, and they should complete appropriate training to hold that responsibility. In addition, privileged accounts should never be shared and they should be independently monitored.

Policies from the New York State Department Of Financial Services 23 NYCRR 500

Cybersecurity Policy Section 500.03

Throughout its lifecycle, all Chicago Bank's Data and any Information System that stores, processes, or transmits Bank's Data, including outsourced services shall be protected in a manner that is considered reasonable and appropriate, as defined and written in documentation approved and maintained by the Senior Officer, given the level of sensitivity, value, and criticality that data has to the Bank. In the application of cybersecurity policy, the Chicago Bank will also address the following areas which are in consistent with the given policy:

a) Data Governance and classification: Chicago Bank has designed a data classification scheme, to make sure the confidentiality, integrity, and availability of information is maintained. The level of security to be provided to the information will depend directly on the classification of the data.

b) Asset inventory and Device management: Chicago bank uses different types of information assets. Chicago bank will constantly maintain an inventory which will include the following details about the assets belonging to, or utilized by the bank:

    i) Asset name and its features
    ii) Owner's Information
    iii) The custodian of the information.
    iv) The sensitivity of the asset, due to regulations, laws, customer expectations or other requirements.

c) Access Control and Identity Management: Access to information and security systems of the bank is based on least privilege and need to know basis. There is a fragile balance between protecting the information and allowing access to the individuals who need to

utilize the information for approved purposes. This balance ought to be perceived. Chicago Bank addresses this need with this policy by user registrations, periodic reviews of user access rights, privilege management and inactive user accounts will be disabled after 90 days.

d) Business continuity and Disaster recovery planning and resources: Chicago Bank maintains a business continuity policy under which there is a detailed plan of disaster recovery. The Disaster Recovery Plan determines a specific method for making duplicates of information from which to reproduce original if there is a situation of disaster. Proper and detailed documentation has been done by the bank to ensure the efficient execution of the plans. On a periodic basis these plans are tested.

e) Network Security: From unauthorized access, the bank's network infrastructure needs to be protected. Only approved users will be allowed to make changes related to logical and physical network security. Appropriate controls have been established by the bank to secure data in private and public networks.

f) Physical Security and environmental controls: Access to work areas, offices and every area of the bank which contains sensitive information is physically restricted to only those people who need to know. All the IT facilities' entry is controlled with electronic access control. Bank's critical server rooms are located in that part of the bank where there is less chance of natural disasters or can be controlled promptly.

g) Vendor and Third Party Service Provider management: The Chicago Bank Information security policy characterizes prerequisites for completing an IT action with an outsourcer, including Cloud Computing. The bank has prepared the risk assessment and will perform appropriate activities to ensure itself about the third party's stability and competency.

There will be a written contract between the bank and third party which will clearly specify the services provided and the risk associated with the services. Also, this contract will include all the terms, conditions, responsibilities and liabilities. All the information used, maintained by the vendor will be under control by the bank.

h) Incidence Response: Chicago Bank has established a predictable and powerful interaction to address any actual or suspected security incidents identifying with data frameworks and information. Bank's incident management have a procedure which has the detail framework for early detection, reporting and responding to security incidents. All security incidents, whether actual or suspected, will be escalated as quickly as time permits.

Requirements or Controls:

1. While sending sensitive files externally, the files have to be password protected and should be under the knowledge of system administrator.
2. If new hardware is required by the bank then it has to be purchased from the vendor who is approved by the system administrator and only approved software configurations will be applied to it.
3. Lost or stolen hardware should be reported immediately to the system administrator.
4. System administrator will approve access to all the users and this will be subject to periodic review.
5. Only approved users can make changes to the network.
6. Third party users are not allowed to connect their devices to the wired or wireless network of the bank, unless authorized and approved by the sysadmin.
7. All the IT facilities' entry point is controlled and monitored by the electronic access and control system. Visitors' access will be controlled.
8. A limit of six consecutive login failures will result in account lockout until a system administrator unlocks it.

9. Only authorised users are allowed to deploy software changes and these changes will be documented and signed by the system administrator.

Roles and Responsibilities:

1. To determine the level of access needed to be given to the individuals.
2. System administrator will do the periodic test of disaster recovery plan.
3. To make sure that staff have sufficient training for the system they use in the bank.
4. System administrator will decide access criteria and back-up necessities for the data resources/ applications they own.
5. To manage its assets as per the bank's approved policies and procedures.

Chief Information Security Officer (Section 500.4)

The Chief Information Security Officer is responsible for:

1. Managing, implementing, checking, investigating, keeping up, and improving the cybersecurity program and enforcing the policy, all the related policies, standards, and guidelines.
2. The Chicago Bank's chief information security officer will confirm compliance to this policy through different techniques, including however not restricted to, occasional walk-thru, video observing, business device reports, internal and external audits, and feedback to the system administrator.
3. Security systems will limit access to credentials for the least advantage important to perform work duties and such access depends on job classification, role, and function.
4. Access control records for frameworks segments will be set to deny all except if privilege to a specific function is specifically permitted.

5. Specific procedures will be followed by the chief information security officer in context to removing IT and/or physical access to facilities, collection of premise keys, cards, and other mechanisms for secure facility access.
6. The chief information security officer ensures that staff of the bank know about their obligations and responsibility for data security.
7. Conducting and will work with risk assessments of Data Resources utilized and suggest mitigation controls.
8. The chief information security officer will monitor and respond to potential and/or actual IT security breaches. Also, he/she will provide advice on IT security issues.

Penetration Testing and Vulnerability Assessments (500.5)

The Chicago bank will, at least bi-annually, conduct penetration testing and vulnerability assessment exercises for all the critical systems, especially those facing the internet. These exercises will also be carried out when there are changes made to critical infrastructure, software, hardware, and policies. Penetration testing of the public facing systems and critical applications in the Chicago Bank are to be conducted only by the qualified cybersecurity personnel hired through a third party vendor by the Chicago Bank. Any vulnerabilities detected are to be resolved promptly so as to avoid exploitation of these vulnerabilities. These findings are to be monitored and recorded by the IT auditors as well as management at the Chicago Bank. The following types of penetration testing are to be conducted:

- Targeted testing - performed with Chicago Bank's IT team and the third party vendor's penetration testing team.
- External testing - targeting Chicago Bank's externally visible servers and devices.

- Internal testing - mimicking an attack from within the Chicago Bank by an authorized user with standard access privileges.
- Blind testing - simulating an attack by an actual hacker by giving pen testers very little information.
- Double-blind testing - similar to blind test, except only the CISO and security managers know of the attack. This is meant to test the Chicago Bank's security monitoring, incident identification and response plan.

Access Privileges (500.7)

The Chicago Bank will provide access privileges to employees based on the following criteria:

- Need to know - users or resources will be granted access to systems that are necessary to fulfill their roles and responsibilities.
- Least privilege - users or resources will be provided with the minimum privileges necessary to fulfill their roles and responsibilities.

Any requests for user's accounts and access privileges must be formally documented and approved when appropriate. Any requests for changes in access privileges must similarly be documented and approved when appropriate. When the changes in access privileges are no longer necessary, they are to be disabled or removed. Similarly, access privileges will be disabled or removed when a user is terminated or no longer has a legitimate reason to access the Chicago Bank's systems. The Chicago Bank must provide secure VPN access to the bank's assets/services from within and outside the bank's network. Existing access privileges will be reviewed at least annually to detect dormant accounts and/or accounts with excessive privileges.

Cybersecurity Personnel and Intelligence (500.10)

The Chicago Bank is responsible for hiring qualified cybersecurity personnel to manage, perform, and oversee the core cybersecurity functions specified in this cybersecurity policy. The following are the roles and responsibilities of the cybersecurity personnel that are to be hired by the Chicago Bank:

- Security Managers are responsible for:
    - Ensuring the enactment of the cybersecurity policies in this document are carried out daily.
    - Controlling budgets for security operations and monitoring expenditures.
    - Recruiting, training, and supervising security personnel.
    - Accomplish any further objectives set by the CISO.
- Security Administrators are responsible for:
    - Installing, administering, and troubleshooting network security solutions.
    - Monitoring network traffic for suspicious activity.
    - Creating network policies and authorization roles and defending against unauthorized access.
    - Configuring and supporting security tools.
    - Documenting any and all changes made to policies, software, and hardware.
- Security Technicians are responsible for:
    - Coordinating with systems and network administrators to ensure security technology is properly implemented.
    - Configuring firewalls, intrusion detection and prevention systems, implementing security software, and diagnosing and troubleshooting problems.
    - Documenting any and all changes to the information systems of the Chicago Bank.
- Help Desk is responsible for:
    - Responsible for identifying and diagnosing traditional technical problems and threats to the cybersecurity policies.

    - Alerting higher management of potential threats after diagnosing and documenting the problem.
    - Documenting any and all issues received by employees of the Chicago Bank.

Multi-Factor Authentication (500.12)

Effective Layered Controls

- fraud detection and monitoring systems that incorporate customer behavior into their algorithms and enable institutions to respond promptly and effectively to potential fraud activities.
- the use of techniques such as positive pay and debit block protection, and other measures that are designed to limit the amount of transactional activity on an account.
- A high-level framework for controlling account activities must be established, which includes transaction value thresholds, allowed recipients of payments, and permitted payment windows (e.g. days and times).
- IP (Internet Protocol) reputation-based tools are designed to prevent banking servers from accepting connection requests from IP addresses suspected of engaging in fraudulent activities.
- The establishment of policies and practices addressing the potential compromise of customers' devices and the detection of customers who may facilitate fraud.
- enhanced customer education so as to raise awareness of fraud risk and provide the customer with useful strategies to minimize the risk. [7]

Establishing Effective Layered Controls

- Effective authentication should provide customer acceptance, reliable performance, ease of use (with formal developed policies and procedures), scalability to handle growth, and compatibility with existing systems and plans for the future.
- The Effective Layered control must have the quality substance, not just the shape of an impact.
- Utilization of sophisticated “out-of-wallet” questions alongside “red herring” questions is taken into account effectively.

- It is generally accepted that access to simple device identification and the ability to locate a device are often circumvented by copying cookie files and using proxies.
- Using “one-time” cookies and making use of more complex digital fingerprints are considered to be effective safeguards

Internal Risk Assessments

- Institutions or industries that have experienced actual security breaches, identity theft, or fraud
- Using voice verification through call-back, email verification/approval, or cell phone identification as an option.
- Opening accounts online, especially when adding customers requires that customer verification procedures be followed.
- Analyzing banking transactions to spot suspicious patterns.
- Setting a dollar limit on how much can be spent at a checkpoint where manual intervention is required if the limit exceeds the preset value. [4]

Training and Monitoring (500.14)

Training Users:

- Adopt policies governing the acceptable and secure use of computer systems.
- Ensure that each employee is conversant in his or her cybersecurity responsibilities.
- Any user should be instructed not to open anything suspicious, regardless of the source, or click on links that look suspicious.
- Users should not be permitted to connect devices to the network on their own unless they have a legitimate business need or are using pre-approved devices.
- Users need to be instructed to use a strong password.
- It is important that users should understand the risks associated with external drives and CDs, as well as safe methods to use these devices.
- It is critical for users not to download and install unauthorized applications since they may contain malicious software.

- Users should be aware that sanctions will be taken against any personnel who offend cybersecurity awareness principles or security policies.
- The use of videos or webinars as an option for continuing education for executive management could help educate users and impart knowledge.

Security Awareness Training:

- Define compliance or auditing standards that your organization must comply with.
- Identify the safety and security awareness requirements for those particular standards.
- Identify the organization's objectives, risks, and security policies.
- Create a security awareness baseline for the company.
- Build a project charter to help define the scope of a security awareness training program.
- Setting up a steering committee to support planning, implementing and maintaining awareness programs.
- Determine who you wish to target – different roles require different or additional training (employees, IT staff, developers, managers).
- Determine what you would like to teach the different groups (the goal is as short a training as possible which will have the maximum impact).
- Consider how you will communicate this information - three categories of training: new, yearly and ongoing.
- Develop and/or purchase training material that meets the requirements of the program when it was first being created.
- Define the metrics you'll be using to evaluate program success.
- Design safety awareness training based on the identification of the various communication methods developed during programming.
- Implement a tracking mechanism that records when someone has completed training.
- Determine when your security awareness program needs to be reviewed every year.
- Identify and update new or changed threats or compliance standards; in an annual update.
- Perform regular assessment of organizational security awareness, comparing it to baselines.
- Conduct surveys to get feedback from employees on usability, efficiency, comprehensiveness, ease of implementation, recommended changes, and accessibility.

- Manage management's commitment to supporting, endorsement, and promotion of the program. [2]

Awareness Training Metrics

Metric	Training Effectiveness Indicator
Operational Metrics	
Reduced system downtime and network or application outages	Consistent, approved change-management processes; fewer malware outbreaks; better controls
Reduction in malware outbreaks and PC performance issues related to malware	Fewer opened malicious e-mails; increased reports from personnel of malicious e-mails
Increase in reports of attempted e-mail or phone scams	Better recognition by personnel of phishing and other social-engineering attempts
Increase in reporting of security concerns and unusual access	Increased understanding by personnel of risks
Increase in the number of queries from personnel on how to implement secure procedures	Better awareness by personnel of potential threats
DLP scanning and network traces are active but not detecting cardholder data outside the CDE	Better understanding by personnel of potential threats
Vulnerability scans are active and detect high or critical vulnerabilities	Decrease in time between detection and remediation
Vulnerabilities are addressed or mitigated in a timely manner	Better understanding by personnel of potential threats and risks to sensitive information
Training Program Metrics	
Increase in number personnel completing training	Attendance tracking and performance evaluations
Increase in number of employees with privileged access who have received required training	Attendance tracking and performance evaluations
Increase in personnel comprehension of training material	Feedback from personnel; quizzes and training assessments

Table No 1

Monitoring

Establishing Policies and Procedures:

- Identify behavior that may indicate suspicious internal activity if it occurs more frequently than a network baseline

- List indicators that could lead investigators to suspicious behavior.
- Create social media policies that define acceptable use of social media and information that shouldn’t be discussed online.
- Create a profile of behaviors and traits that might indicate an individual is an internal threat.
- Develop a model that demonstrates appropriate access to assets and the behavior associated with those assets for each type of employee.
- Create a comprehensive list of system and user behavior attributes that can be monitored to identify normal and abnormal patterns that enable the detection of anomalies and abuse.
- Conduct inspections of employees who have access to company’s funds or confidential information.
- The company should encourage each employee to document and report any suspicious behavior and to investigate and report anomalous behavior that does not appear to be in line with company standards.
- Monitor employees with upcoming or current personnel issues.
- Check audit logs regularly for activities that fall outside of the employee's normal scope of work.
- Identify data sources that have raw behavior data that may be useful in extracting behavior patterns.
- Establish strict policies and procedures for managing log files. Monitor the SIEM system on a regular basis.

Network and Application Monitoring Tool:

- Monitor the network over a period of time to determine a baseline for "normal" network activity.
- Develop tools to scan and analyze system and network monitoring logs effectively to detect abnormal system and internal activity.
- Disable any remote access for employees who have left the organization.
- Conduct investigation of personnel if any suspicious behavior is recorded.
- Limit the details of inquiries to relevant employees/staff.

- Determine when is an appropriate time to involve outside experts and law enforcement agencies in investigations
- Perform a forensic analysis of an incident
- Consider attending the information depositories as if the Congress develops it
- Establish relationships with state and local law enforcement agencies and monitor data sources since consolidated reports are currently limited
- In order to establish fair disciplinary processes, the organization must establish appropriate process procedures.
- Establish mechanisms by which customers can report fraudulent transactions or other suspicious activity on their accounts (such as unauthorized access attempts).
- Ensure that existing programs are linked to internal threat analysis activities.
- Use existing data collection platforms and direct the collected information for analysis

Access Control:

- Establish controls to prevent user privileges from becoming unauthorized and lateral movement between network resources.
- Provide minimum standards for technical safeguards for contractors using information systems by contract and audit compliance with such standards on a regular basis.
- Consider conducting periodic reviews of your accounts to avoid escalating privileges.
- Employees must have sufficient access rights to carry out daily tasks and nothing more.
- Renew access rights immediately if the employee changes roles.
- Periodically review the baseline configuration of the actual production system.
- Ensure that changes are approved after verification of business needs.
- Implement processes and policies to limit access rights / credentials to all users, especially privileged users, and to ensure that only the minimum required number is provided.
- Establish procedures for verifying the safety of personnel based on the level of access to individual information systems.
- Define a highly secured password requirement and train users to create strong passwords.
- Establish audits of the creation of accounts and password changes by system administrators.

- Make sure all shared accounts are absolutely necessary and that they are addressed in the risk management process.
- Make sure user permissions are properly audited.
- Removal of any permissions that are no longer required
- Adopt policies and procedures for account management that will limit administrative privileges to the absolute minimum necessary. [8]

Incident Response Plan (500.16)

Cybersecurity Events and internal processes for responding to those events;

- Detection and Analysis
    - Determine if there has been an accident.
    - Analyze predecessors and indicators
    - Find related information
    - Conduct research (i.e. search engines, knowledge databases)
    - Once the manager believes an incident has occurred, begin documenting the investigation and gathering evidence
    - Ensure that incident handling is prioritized according to relevant factors (functional impact, information impact, recovery effort, etc.).
    - Inform the relevant internal personnel and external organizations of the incident.
- Containment, Eradication, and Recovery
    - Gather, preserve, secure, document, and store evidence.
    - Keep the incident contained
    - Eliminate or eradicate the incident
    - Recognize and address all vulnerabilities that were exploited
    - Remove malicious software, inappropriate content, and other components.
    - Recovery from the incident is crucial
    - Bring the affected system back into operation at ready state
    - Ensure that the affected system is functioning normally

    - If necessary, carry out additional monitoring to look for future activity
- Post-Incident Activity
    - Prepare follow-up reports
    - Hold an additional lesson-learned session, mandatory if you've had a major incident.

1. Goals of the incident response plan;

- Identification of suspected cybersecurity incidents (i.e. monitoring for indications of unusual events and evaluation of one or more trigger points)
- Set a goal for each investigation and cleanup
- Analyze all available information about potential cybersecurity incidents
- Identify what really happened (i.e. DDOS, malware, system hackers, session hijacking, data corruption, etc.)
- Identification of compromised systems, networks and information (assets)
- Find out what information has been disclosed to unauthorized persons, stolen, deleted or tampered with.
- Identify who committed the act and why (e.g. financial gain, hacktivism, espionage, revenge, challenge, or simply fun)
- Develop an identification process explaining how it happened (i.e. how the attacker gained access to the system).
- Identify the potential business impact of a cybersecurity incident
- Undertake adequate investigations (i.e. using deep forensic diving skills) to identify (and possibly pursue) the perpetrators.

2. Delineate clear roles, responsibilities and the levels of authority for decision-making.

Chief Information Security Officer (CISO)

- Manage information security incidents by coordinating efforts.
- Ensure prompt investigations of any security incident.
- Determine which bank data was potentially exposed
- Keeping compromise systems secure to prevent further damage
- Provide guidance to stakeholders in the institution

Privacy Officer

- Coordinate efforts to meet regulatory requirements and notifications.
- With support from the General Counsel, reviewing the applicable state and federal laws and developing appropriate steps to comply with these laws in the event that any data exposure occurs.
- Assuring that all aspects of a data exposure management plan have been completed.

Incident Response Coordinator

- Administering efforts to gather the appropriate information
- Offering expertise in the procedures related to gathering information and documentation of procedures.
- Update the CISO and other leaders as necessary

Incident Response Handler

- Collecting data from systems
- Offering expertise in the technology and data sectors
- Providing information on procedures, as well as collecting the appropriate data, for Incident Management. [5]

3. Information sharing and internal and external communications are essential;

- It is critical to establish pre-defined lines of communication, both internally and externally, in response to an incident.
- A response team at your financial institution should also be communicating with proper auxiliary teams.
- Senior management must inform the board of directors as well of the incident so that the directors may help formulate a response strategy as required.
- The response team should also be able to obtain additional assistance from third parties, including legal counsel or forensics experts, as needed.
- A response team should immediately contact legal counsel and the institution's insurance provider if it determines that a potentially compromised incident has potentially compromised personally identifiable information or other legally protected information (unless instructed otherwise by legal counsel). [1]

4. Determination of requirements to eliminate all identified weaknesses in the information system and related controls;
    - Regular vulnerability assessments by leading information security companies identify many security holes in the organization. The resulting vulnerability reports should be prioritized according to risk and elimination planned accordingly.
    - Careful monitoring and documentation is essential to ensure that all deletion tasks are completed on time.
    - It is recommended that the information security company retest all results from the original report after the remediation is complete.
    - Management needs to be informed of the most important security risks during the vulnerability assessment.
    - Plan information security incident prevention activities and ensure you understand the basics are well covered. [6]
5. Documentation and reporting of incident response activities and Cyber Security events;
    - Clearly specify the classification policies so that incidents can be classified by severity in a timely manner and the appropriate response and response team can be used based on the nature and severity of the incident.
    - The severity of an attack should be reflected in the escalation, response, and report process.
    - Escalation policies should explain how different personnel inside the organization will be contacted within an incident and the responsibilities they will have in the incident analysis and response.
    - The escalation policy should address when to ask or obtain external assistance such as assistance from third parties or the federal government.
    - Policies for reporting should address coordination with third parties and external reporting, as well as internal and external reporting to external organizations.
6. Revision of an incident response plan as necessary following a cyber security event
    - Maintain operating system patches and application updates.

- Monitor and assess new vulnerabilities as they are reported by vendors and security companies by subscribing to an email notification service. [3]

Appendix A

List of subordinate policies

This appendix consists of additional cyber security policies needed to fulfill requirements of the FFIEC Information Security publication.

I. II.C.6 Mitigating Interconnectivity Risk

II. II.C.7(a) Security Screening in Hiring Practices

III. II.C.10 Change Management Within the IT Environment

IV. II.C.11 End-Of-Life Management

V. II.C.11 Malware Mitigation

VI. II.C.13 Control Of Information

VII. II.C.14 Supply Chain

VIII. II.C.16 Customer Remote Access to Financial Services

IX. II.C.17 Application Security

X. II.C.19 sEncryption

XI. II.C.18 Database Security

XII. II.C.22 Log management

XIII. III Security Operations

XIV. III.A Threat Identification and Assessment

XV. III.B Threat Monitoring

XVI. II.D Incident Response

Appendix B

List of subordinate policies

This appendix consists of additional cyber security policies needed to fulfill requirements of the 23 NYCRR 500.

I. Application Security (500.8)

II. Risk Assessment (500.9)

III. Third Party Service Provider Security Policy (500.11)

IV. Limitations on Data Retention (500.13)

V. Encryption of Nonpublic Information (500.15)

References

FFIEC, *Information Technology Examination Handbook (IT Handbook)*1–98 (2016).

New York State Department of Financial Services, *23 NYCRR 500*1–14 (2017).

Carnegie Mellon University. (2021). *Information Security - University Policies - Carnegie Mellon University*. https://www.cmu.edu/policies/information-technology/information-security-policy.html

Chirileanu, R. C., Kelly, D. K., & Clarke, J. C. (2018, July 17). *Temenos*. Temenos. https://www.temenos.com/wp-content/uploads/2019/07/governance-policy-information-systems-security-2019-jul-03.pdf

Jana Small Finance Bank. (n.d.). *Information Security Policy*. Jana Bank. https://www.janabank.com/images/policies/info-security-policy.pdf

[1]CONNECTICUT, U. O. (n.d.). Incident Response Plan. INFORMATION TECHNOLOGY IT SERVICES. Retrieved from https://security.uconn.edu/incident-response-plan/#

[2]Council, S. A. (2014, October). Best Practices for Implementing a Security Awareness Program. Security Standards Council.

[3]EXAMINATION, F. I. (n.d.). Incident Identification and Assessment. INFORMATION SECURITY. Retrieved from https://ithandbook.ffiec.gov/it-booklets/information-security/iii-security-operations/iiic-incident-identification-and-assessment.aspx

[4]Guidance, F. C. (n.d.). Account Authentication & Banking. FINANCIAL EDUCATION CORPORATION. Retrieved from https://www.myunionbankonline.com/customereducation/BS_AuthenticationConsumer_live.html

[5]Jason Creasey, J. (2013). Cyber Security Incident Response Guide. CREST. Retrieved from https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

[6]Michael Dailey, K. H. (2018, july 2). How Financial Institutions Should Prepare For and Respond to a Cybersecurity Incident. Retrieved from https://www.bankdirector.com/issues/how-financial-institutions-should-prepare-and-respond-cybersecurity-incident/

[7]Richard David Harris, R. M. (2011, July 19). Updated Regulatory Guidance for Authentication in an Internet Banking Environment: A New Standard of Care? Martindale Legal Library. Retrieved from https://www.martindale.com/legal-news/article_day-pitney-llp_1315246.htm

[8]SIFMA. (2018, February). INSIDER THREAT BEST PRACTICES GUIDE 2nd EDITION. Cyber Security. Retrieved from WWW.SIFMA.ORG

Rosencrance, L., & Mehta, P. (2018, October 31). *pen test (penetration testing)*. SearchSecurity. https://searchsecurity.techtarget.com/definition/penetration-testing