Finger Lakes Community Bank

Incident Response Plan

Jeremy Willett

Table of Contents

[Executive Summary 2](#_Toc137730007)

[Operational Plan and Analysis 8](#_Toc137730008)

[Incident Response Process with Key Roles and Responsibilities Assignments 8](#_Toc137730009)

[Courses of Action Table 16](#_Toc137730010)

[Countermeasures Analysis 22](#_Toc137730011)

[Organizational Systems 23](#_Toc137730012)

[Organizational Operations 25](#_Toc137730013)

[Personnel 26](#_Toc137730014)

[References 28](#_Toc137730015)

Executive Summary:

On May 25th, Finger Lakes Community Bank (FLCB) was hacked, and an international funds transfer was made under the guise of being legitimate. Due to several pitfalls and shortcomings in FLCB’s security protocols, regulatory compliance, and undertrained staff, an attack was made that allowed a group of hackers to approve a funds transfer by acting as the clerk and CFO, who were needed to complete the transfer. While this incident was not prevented when it occurred, future incidents can be. With cybersecurity being a new focus for the leadership of FLCB, the goal is to bring FLCB in line with industry and regulatory standards for security, incident detection and response, and data protection. By doing so, the impacts of future incidents can be mitigated to reduce the impact they have on the organization, its operations, and its personnel. The development of a defined, written incident response process combined with the use and implementation of security countermeasures will ensure that FLCB meets the compliance requirements of several State and Federal laws and regulations, as well as serve to protect FLCB in the future as new incidents occur. By meeting these standards, it will greatly enhance the security posture of FLCB by implementing key measures to address compliance gaps and improve incident response. FLCB will establish and update policies and procedures to align with legal, regulatory, and policy requirements. These policies will provide clear guidelines on information security, incident response, acceptable use, and employee training. By having these policies in place, employees will be better equipped to understand their roles and responsibilities in maintaining a secure environment.

To initiate this approach and effectively communicate it to stakeholders, the security team will focus on two key aspects: education and collaboration. First, the team will conduct training sessions and awareness programs to educate executives on the importance of compliance and its impact on the organization's security posture. This will involve explaining the legal and regulatory requirements, emphasizing the potential consequences of non-compliance, and highlighting the benefits of a proactive security approach. Second, the team will foster collaboration by establishing regular communication channels with executive stakeholders. This will involve providing regular security updates, sharing incident reports, and engaging in discussions to address any concerns or questions. The team will ensure that these communications are presented in a consumable and non-technical manner, using language that resonates with the stakeholders' business perspectives. By fostering collaboration and providing clear, understandable information, the security team can gain the support and commitment of executive stakeholders to prioritize security initiatives and allocate necessary resources.

By following this approach, the organization will enhance its security posture by aligning with legal, regulatory, and policy requirements. Employees will be better educated and aware of their responsibilities, reducing the likelihood of falling victim to phishing or other social engineering attacks. The implementation of robust network security measures and incident response procedures will minimize the impact of security incidents and enable swift and effective response. Ultimately, this approach will create a more resilient and secure environment, safeguarding the organization's sensitive data and financial transactions. To do this, it is recommended that the following steps be taken:

1. Conduct a Compliance Gap Analysis: Assess the organization's current practices, policies, and procedures against relevant legal and regulatory requirements. Identify areas where the organization falls short of compliance and prioritize the necessary improvements.
2. Develop and Update Policies: Based on the compliance gap analysis, develop or update policies and procedures to ensure compliance with applicable regulations. Ensure these policies are communicated to employees and regularly reviewed and updated as necessary.
3. Develop an Employee Training and Awareness Program: The organization should conduct regular training and awareness programs to educate employees about cybersecurity threats, safe computing practices, and the organization's policies and procedures. This training can help employees recognize and report suspicious emails or activities, reducing the risk of successful attacks.
4. Establish a Written Incident Response Plan and Process: This report provides an incident response process with defined roles and responsibilities as well as a clearly defined course of action table. Thes resources should be implemented into the company for use during any future incidents to minimize any impact security threats have on the bank.

Legal, regulatory, and policy compliance issues play a significant role in shaping an organization's approach to detection and response in cybersecurity incidents. Finger Lakes Community Bank’s recent incident has several relevant regulatory considerations that impact the importance of complying with these regulatory requirements:

* Data Protection Regulations: The organization needs to comply with data protection regulations, such as the Gramm-Leach-Bliley Act (GLBA) in the United States. These regulations require the protection of personal data and impose notification requirements in the event of a data breach. As FLCB operates in New York, it must comply with 23 NYCRR 500 – Cybersecurity Requirements for Financial Services Companies. This New York Law requires: “Introducing a cybersecurity program, including data protection policies, Appointing a Chief Information Security Officer, Conducting regular penetration testing and bi-annual risk assessments, Maintaining an audit trail of data, and Developing a written incident response plan” (BreachRX, 2023). Regarding this incident, if any personal data was compromised or accessed, the organization would need to assess the extent of the breach and take appropriate actions, including notifying affected individuals and regulatory authorities, if necessary.
* Financial Regulations: As a bank, Finger Lakes Community Bank is subject to financial regulations, such as the Bank Secrecy Act (BSA) and the Payment Card Industry Data Security Standard (PCI DSS). These regulations aim to safeguard financial transactions, prevent money laundering, and protect sensitive financial data. During this incident, an attempted unauthorized wire transfer highlights the potential violation of financial regulations. The organization would need to investigate the incident, report it to relevant financial authorities, and implement measures to prevent such incidents in the future. As part of the Bank Secrecy Act, FLCB has other compliance requirements they are missing. This act requires financial institutions to establish anti-money laundering (AML) programs. To amend the BSA, the Anti-Money Laundering Act of 2020 (AMLA) introduced further penalties and requirements. “The newest version of the Bank Secrecy Act identifies five key compliance pillars: The designation of a compliance officer, development of internal policies, creation of a training program for employees, integration of independent testing and auditing, and development of risk-based processes for ongoing customer due diligence (CDD)” (Bonderud, 2023).
* Incident Response and Reporting Requirements: As part of FLCB’s requirement to comply with 23 NYCRR 500, a written incident response plan is needed to be compliant. This plan is required to include:
  + 1. “The Process for responding to a cybersecurity event.
    2. Defined Goals of the incident response plan.
    3. Definitions for roles, responsibilities, and decision-making authority for anyone involved in incident response measures.
    4. Guidelines for external and internal communications regarding the incident
    5. Requirements for how to remediate weaknesses identified in information systems or controls.
    6. Guidelines for how to document cybersecurity events and incident response efforts.
    7. Process for evaluating and revising the incident response plan after a cybersecurity event” (BreachRX, 2023).
* Employee Awareness and Training: Legal and regulatory compliance often involves ensuring that employees are aware of their responsibilities and trained in relevant security practices. During this incident, the funds transfer clerk fell victim to a phishing email, leading to the potential compromise of sensitive financial information. The organization should have policies and training programs in place to educate employees about phishing attacks, social engineering techniques, and safe email practices. Further, training is required under 23 NYCRR 500 and recommended as an ongoing tool by most regulatory bodies.

To address the legal, regulatory, and policy compliance issues, FLCB should have established policies and procedures in place. Some relevant policies and measures include:

* Information Security Policy: This policy defines the organization's commitment to safeguarding information assets, outlines roles and responsibilities, and establishes security controls to protect against unauthorized access, data breaches, and other security incidents.
* Incident Response Plan: The incident response plan outlines the steps to be followed in the event of a cybersecurity incident, including the roles and responsibilities of various stakeholders, communication protocols, evidence preservation procedures, and reporting requirements.
* Acceptable Use Policy: This policy governs the appropriate use of the organization's information systems and resources, including guidelines for handling emails, visiting websites, and downloading files. It can include rules for email usage, password management, and restrictions on accessing potentially risky websites.
* Employee Training and Awareness Program: The organization should conduct regular training and awareness programs to educate employees about cybersecurity threats, safe computing practices, and the organization's policies and procedures. This training can help employees recognize and report suspicious emails or activities, reducing the risk of successful attacks.

The lack of compliance with legal, regulatory, and policy requirements can significantly increase the vulnerability of a bank to the type of attack that occurred to FLCB. Compliance frameworks and regulations are designed to establish security measures and best practices to protect sensitive data and financial transactions. When an organization fails to adhere to these requirements, it creates gaps and weaknesses in its security posture. During this incident, the bank's lack of compliance is evident in multiple areas. First, the bank's perimeter firewall and server logs indicated that there were repeated connections from a suspicious IP address associated with a known hosting company involved in cybercrime activities. This indicates a failure to implement robust network security measures that could have prevented or detected unauthorized access attempts.

Second, the bank's email messaging server connected frequently with the suspicious IP address. This highlights a potential lack of email security controls and protocols, such as spam filters, email authentication mechanisms, or user awareness training. These weaknesses allowed the phishing email containing a remote access Trojan to bypass the bank's defenses and reach the funds transfer clerk, who unknowingly clicked on a malicious link. Additionally, the absence of multi-factor authentication or strict authorization processes for financial transactions was evident in the scenario. The director of finance relied on email communication for an urgent funds transfer request, despite standard procedures that require hand-signed approvals. This lack of stringent authentication and approval mechanisms increases the risk of unauthorized transactions and makes it easier for attackers to exploit vulnerabilities within the organization. Furthermore, the scenario reveals that the organization's incident response and reporting procedures may not have been fully aligned with legal and regulatory requirements. There is no mention of immediate reporting to regulatory authorities or law enforcement agencies, which is mandated by 23 NYCRR 500 as well as the Computer-Security Incident Notification requirement set forth by the FDCI, OCC, and Federal Reserve on May 1st, 2021.

Overall, the lack of compliance with legal, regulatory, and policy requirements exposes the bank to heightened cybersecurity risks. It creates opportunities for attackers to exploit vulnerabilities, gain unauthorized access, and compromise sensitive data or financial transactions. Compliance with these requirements ensures that appropriate security controls, protocols, and incident response mechanisms are in place, significantly reducing the likelihood of successful attacks and minimizing the impact of security incidents. To resolve these gaps in compliance and security, it is necessary to identify all the gaps that exist and address them to protect FLCB from future security incidents and threats.

Operational Plan and Analysis:

Incident Response Process with Key Roles and Responsibilities Assignments:

| *Identify individual steps and list them in logical sequence below:* | *Identify the role and who performs it below, ensuring it corresponds to the step in the first column in the table:* | *Identify your rationale behind the assignment, ensuring you address implementation concerns related to the step and the role/responsibility in the first two columns in the table:* |
| --- | --- | --- |
| Detection | | |
| Step | Role/Responsibility | Rationale Behind Assignment |
| 1. Monitor | IT staff members will primarily be responsible for monitoring company systems and networks for unusual activity. This includes reviewing logs, network traffic, and system alerts for the presence of IOCs. Any potential alerts will be escalated to the security analyst for further analysis. | The IT team, as a whole, is small at Finger Lakes Community Bank (FLCB). It would not be reasonable to have the security analyst responsible for the monitoring of systems and networks to look for IOCs because they are a single person. The IT staff can work as a team to monitor the networks and systems and then escalate potential IOCs to the security analyst who can determine whether to move them to the next step. |
| 1. Investigate | The security analyst will be responsible for receiving escalated alerts from the IT staff and investigating as necessary to determine if they are a security event or not. | The security analyst is best positioned to leverage their knowledge and skillset to dig into escalated alerts further and determine if they need to be escalated further to a full-fledged incident. After this stage, the event will trigger full incident response and proceed to being addressed and resolved. |
| 1. Classify | The security analyst will classify the severity of the event (Insignificant< Low<Medium<High<Extreme) and the criteria that it fits into. | This step is based on the results of the investigation performed in the previous step. As a result, the security analyst is best positioned to classify the event as he prepares the notifications necessary. |
| 1. Notify | The security analyst will notify all stakeholders involved of the event and the need to resolve it. This should be reported to all members of the incident response team including the CEO, President, CIO, CFO, IT staff, Legal counsel, and the Firewall vendor Cyberstop. | Notification needs to be performed by someone well informed and capable of speaking about the incident and the threats it poses. The security analyst is best positioned to do this as this falls directly into their expertise and they can properly relay the urgency this needs to be dealt with. The CIO will take on the roll of Incident Response Team lead from this point forward fur the limited staff of FLCB. |
| 1. Document | The CIO is responsible for ensuring documentation is completed by everyone on the Incident Response Team. This step is an ongoing step that will be performed throughout the process. Everyone involved is responsible for documenting all findings, actions, and resources. | This was included as a step at the beginning because it is vital to the entire process. As IOCs are escalated, it is vital that all actions, processes, and findings are documented to be able to learn from and explain why each event was classified as an event or not. |
| Response | | |
| Step: | Role/Responsibility | Rationale Behind Assignment |
| 1. Containment | The security analyst will work closely with the IT staff during the response stage to handle the incident. This team will have the best available skillset to contain the incident. The CIO will oversee the response process but allow the team to utilize their skillsets to contain the threat. | Combining the security analyst with the IT staff to create a response team allows all employees with the technical knowledge necessary to contain the incident on a technical level. FLCB has a small number of staff and combining these employees into one team leverages their skillets and knowledge to contain the threat. |
| 1. Analysis | The security analyst will be responsible for analysis of the event to determine the root cause of the event and the extent of the damage. The security analyst will work with close oversight from the CIO. | Analysis requires specific knowledge. The security analyst is best positioned to analyze the threat after it has been contained. While the analyst will be performing this step, because of the size of the staff at FLCB, the CIO will act the supervisor/team lead throughout the incident response process. |
| 1. Eradication | The combined team of the security analyst and the IT staff will be responsible. The team should remove any malware, backdoors, or other malicious software from the affected system(s). | Back to a technical step that needs to encompass all those involved with the networks and systems. The combined team is the best option the company has at its disposal to eliminate the threat from the systems/networks. |
| 1. Recovery | The combined security analyst/IT staff team will work together to restore the system/network to their normal operations. | This step immediately follows eradication, and the team should move directly to it once the threat has been eliminated. To perform this step effectively and securely, those with technical skills should be responsible. |
| Communication and Reporting | | |
| Step: | Role/Responsibility | Rationale Behind Assignment |
| 1. Establish Communication Channels | The CIO will establish communication channels with other stakeholders with the combined security analyst/IT staff team responds to the incident. The step will run parallel with the response phase. | The CIO is acting as Incident Response Team lead. It is his responsibility to establish communication channels to ensure that information is shared quickly and accurately. This can include phone trees, email distribution lists, and messaging platforms. |
| 1. Notify Key Stakeholders | Once lines of communication are established, the CIO will inform stakeholders of the incident and keep them up to date as the process unfolds. | As the technical team is responding to the event, the CIO will be acting as supervisor over the situation. This provides him with the necessary information to inform key stakeholders such as other executives and the legal team. This helps ensure that everyone is aware of the situation and can take appropriate action. |
| 1. Prepare Incident Reports | The CIO will work with the security analyst/IT staff team to prepare incident reports that document the details of the incident, including what happened, when it happened, and how it was resolved. These reports should also include any remediation efforts that were undertaken, and any lessons learned from the incident. | The step will fall at the end of the response phase coinciding with the lessons learned step. While the entire time will work to develop these reports, the CIO is primarily responsible for their development and presentation to other stakeholders. |
| 1. Communicate with external parties | If the incident involves sensitive or confidential data, the CIO should work with the CEO, CFO, President, and legal team to communicate with external parties, such as customers or regulatory bodies, to keep them informed about the situation. | This step will be necessary once the extent of the damage of the incident has been discovered. In the event that sensitive or confidential information has been stolen, compliance with regulatory and legal standards is crucial to continued operation of FLCB. |
| 1. Provide regular updates | The CIO, with communication lines still open, will provide regular updates to the stakeholders so they may continue to properly do their jobs. This step is an extension of the notifying key stakeholders steps. | As an extension of step 2, the CIO will continue to update the other stakeholders to ensure they are properly informed and up to date on the incident status, including what actions have been taken and what the next steps are. |
| 1. Conduct a post-incident review | After the incident has been resolved, the incident response team should conduct a post-incident review to assess the incident response process's effectiveness and identify areas for improvement. This may include all stakeholders involved depending on the severity of the incident. | This is the culmination of the entire process. Depending on the severity of the incident, it may be necessary to have all stakeholders present to provide post incident updates from the various fields each team member works in. |
| 1. Lessons Learned | The CIO, once the system is back to normal, should meet with the combined security analyst/IT staff team to conduct a post-incident review to identify any improvements that can be made to the incident response plan or the organization's security posture. | This is the culmination of the entire technical team to review and address shortcomings in the process. The entire technical staff should report their results to the CIO and the CIO should combine the recommendations from the staff to improve the security posture of FLCB and improve the incident response process. |
| Prevention | | |
| Step: | Role/Responsibility | Rationale Behind Assignment |
| 1. Establish Indicators of Compromise (IOCs) | Security Analyst is responsible with support from the CIO and IT staff. The security analyst is expected to be knowledgeable in common forms of attack and signs to look out for. | It is important to establish a baseline for reference when trying to determine if the system is being or has been compromised. By defining IOCs to be looked for, and providing them as a resource material to staff, this can prove to be beneficial in detecting an attack in a timely manner. |
| 1. Update policies and procedures | Based on the post-incident review and Lessons Learned, the incident response team should update policies and procedures to prevent similar incidents in the future. This could include updating security controls, training employees, or implementing new technologies. | This step is an entire process that includes everyone involved. It is important for the C-suite executives to listen to feedback from the security analyst and IT staff to properly implement necessary changes to current policies and procedures as necessary to prevent the incident from reoccurring in the future. The CIO should work to ensure the feedback is received and acted upon. |
| 1. Implement security controls | The security analyst/IT staff should implement new security controls or update existing ones to prevent similar incidents from occurring. This could include implementing new firewalls, intrusion detection systems, or access controls. | With the incident resolved and a plan of action in place to resolve shortcomings and update necessary systems and networks to prevent the incident from recurring, the technical staff should work to implement the new changes to put them into effect. |
| 1. Train employees | The security analyst/IT staff should train employees on the updated policies and procedures and any new security controls that have been implemented. This will help ensure that employees understand their roles and responsibilities in preventing incidents. | With support from the CIO and other c-suite executives, the security analyst and IT staff can work to train employees on new policies and security controls so they can understand what is happening, why it happened, what to look for in the future, and how to prevent it. |
| 1. Conduct regular security assessments | The incident response team should conduct regular security assessments to identify potential vulnerabilities in the organization's infrastructure and systems. The entire team should take part to ensure security audits become a regular process and external security audits should be conducted annually. | The entire team is necessary here as it is the C-suite executives who will ultimately make the decision to conduct audits that cost money. It is important to have them in the loop and part of the process so they can see the importance these audits can have as their results can highlight important weaknesses in the company’s security. |
| 1. Test incident response plan | The CIO should prioritize testing the incident response plan with the rest of the incident response team throughout the year. The incident response team should test the incident response plan to ensure that it is effective and up to date. This could include tabletop exercises, simulations, or penetration testing. | The CIO’s main responsibility is the security of FLCB’s information and data assets. By ensuring that regular testing of the incident response process is conducted, he ensures the process is up to date and viable in the event an incident happens again. |
| 1. Continuous monitoring | The IT staff goes back to its original role of monitoring of the systems and networks for IOCs. | At this point, the entire process starts over, and the continued monitoring of the company systems and networks continues. This defers back to the step of the detection phase. |

Courses of Action Table:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *Course of Action: Unauthorized Activities* | | | | | | |
| Objective: | | | To provide reference material to identify, isolate, and eliminate threats to the company and its assets. Provides guidance on the steps an attacker will take to gain unauthorized access into the company systems and networks, common indicators of compromise by an attacker, where to look for these indicators and the methods that should be taken to respond and defend attacks made against the company system and network. | | | |
| Attack Methods & Features | | | Detection Location and Methods | | Response Method | Response Objective |
| ATTACK PHASE | Step | ATTACK ACTION(S) | INDICATOR(S) OF COMPROMISE | DETECTION POINT | DEFENSIVE COUNTERMEASURE(S) | DEFENSIVE PHASE |
| Targeting | 1 | Identify insecure public-facing target system | Spike(s) in network traffic from unusual IP address(es) | Public-facing web server logs(s)  Perimeter firewall log(s) | Catalog suspicious IP address(es) for further analysis  Conduct targeted research into IP address registration and DNS data | Preparation |
| Reconnaissance | 2 | Gather information through research to identify vulnerabilities leading to possible vectors of attack.  Discover internet-facing servers (Lockheed Martin, 2015).  Compile Email addresses, employee names, contact information, IP address ranges, Active Machines, Open ports and services, OS and application Versions (PSOL, 2017).  Physical inspection of network and security measures if possible. | Suspicious network traffic from unidentified sources.  Alerts from SIEM or IDRP.  Increase in social engineering attempts made against employees (phishing emails/phone calls, fraud).  Reports or manual analysis of log files. | Log files from various sources (SIEM/IDRP, Firewall, Server, Network, Email).  Employee reports of increased/persistent phishing attempts.  Alerts from SIEM or IDRP. | Ensure SIEM/IDRP is kept up to date.  Review access control policies to ensure maintenance of least privilege.  Employee training to recognize and report suspicious behavior or suspected social engineering attempts.  Clear and available method for employees to report security concerns.  Manual review of alerts from SIEM/IDRP.  Regular review of various log files (SIEM/IDRP, Firewall, Server, Network, Email).  Prioritize defenses around technologies or people based on recon activity (Lockheed Martin, 2015).  Document changes made to the system and any analysis of security incidents. | Detection / Identification |
| Weaponization | 3 | (1) use advanced knowledge of coding to generate custom malware and exploit code from scratch or (2) download a handy tool to create a payload and weaponize something like a PDF or Microsoft Word/Excel file based on a pre-written template and pre-written exploit (PSOL, 2017).  Select backdoor implant and appropriate command and control infrastructure for operation. (Lockheed Martin, 2015) | Issues relating to system/network performance reported by users on their devices or multiple devices.  Malware detection notifications.  Network traffic to unauthorized / unidentified IP addresses. | Employee reports on performance issues of devices.  Log files from various sources (SIEM/IDRP, Firewall, Server, Network, Email).  Alerts from SIEM or IDRP. | Proactive due diligence and risk management (PSOL, 2017).  Awareness of how threat actors work to compromise organizations (PSOL, 2017).  Keep Antimalware, SIEM/IDRP, and OS software up to date.  Conduct full malware analysis – not just what payload it drops, but how it was made (Lockheed Martin, 2015).  Collect files and metadata for future analysis (Lockheed Martin, 2015).  Document all findings related to current trends regarding vulnerabilities, threats, and attack trends.  Document changes made to the system and any analysis of security incidents. | Detection / Identification |
| Exploitation | 4 | Once developed and delivered on the target system, the exploit activates the attack to compromise the target system/network via the identified vulnerability.  Software, hardware, or human vulnerability.  Acquire or develop zero-day exploit.  Adversary triggered exploits for server-based vulnerabilities.  Victim triggered exploits:   * Opening attachment of malicious email. * Clicking malicious link (Lockheed Martin, 2015). | “Unusual Outbound Network Traffic.  Anomalies in Privileged User Account Activity.  Geographical Irregularities.  Swells in Database Read Volume.  HTML Response Sizes.  Large Numbers of Requests for the Same File.  Mismatched Port-application Traffic.  Suspicious Registry or System File Changes.  DNS Request Anomalies.” (Fortinet, 2023) | SIEM/IDRP log files indicating malicious connections to unidentified IP addresses.  Antimalware software alerts/ Log files.  Firewall Log files  Windows Event Log files.  Network Log files. | “User awareness training and email testing for employees.  Secure coding training for web developers.  Regular vulnerability scanning and penetration testing.  Endpoint hardening measures:   * Restrict Admin privileges. * Custom endpoint rules to block shellcode execution.   Endpoint process auditing to forensically determine exploit origins” (Lockheed Martin, 2015).  Document changes made to the system and any analysis of security incidents. | Detection / Identification |
| Installation | 5 | Install a persistent backdoor or implant in the victim environment to maintain access for an extended period of time (Lockheed Martin, 2015). | New/unknown programs or processes running on the system.  Suspicious activity in log files.  Performance issues such as large memory usage or increased CPU usage on endpoint devices.  Accounts being used in suspicious manner / normal system interaction changes. | SIEM/IDRP log files indicating malicious connections to unidentified IP addresses.  Antimalware software alerts/ Log files.  Firewall Log files  Windows Event Log files.  Network Log files.  Privilege escalation occurring on unauthorized accounts. | Endpoint instrumentation to detect and log installation activity. Analyze installation phase during malware analysis to create new endpoint mitigations (Lockheed Martin, 2015).  Network hardening to ensure no unnecessary ports are open.  Utilize inbound/outbound traffic filters on firewalls to prevent the use of unapproved applications.  Document changes made to the system and any analysis of security incidents. | Containment |
| Command & Control | 6 | Malware establishes a two-way communication channel that allows the remote manipulation of the target system.  “Most common command and control channels are over web, DNS, and email protocols. Command and control infrastructure may be adversary owned or another victim network itself” (Lockheed Martin, 2015). | New/unknown programs or processes running on the system.  Suspicious activity in log files.  Performance issues such as large memory usage or increased CPU usage on endpoint devices.  Accounts being used in suspicious manner / normal system interaction changes. | SIEM/IDRP log files indicating malicious connections to unidentified IP addresses.  Antimalware software alerts/ Log files.  Firewall Log files  Windows Event Log files.  Network Log files.  Privilege escalation occurring on unauthorized accounts. | Discover command and control infrastructure through malware analysis (Lockheed Martin, 2015).  Network hardening to ensure no unnecessary ports are open.  Require proxies for all types of traffic (HTTP, DNS) (Lockheed Martin, 2015).  Utilize inbound/outbound traffic filters on firewalls to prevent the use of unapproved applications.  Document changes made to the system and any analysis of security incidents. | Containment |
| Actions on Objectives | 7 | Utilize established system control to execute the primary objective of the attack (data exfiltration, ransomware, etc.).  Collect user credentials.  Privilege escalation  Internal reconnaissance.  Lateral movement through environment.  Collect and exfiltrate data.  Destroy systems.  Overwrite or corrupt data.  Surreptitiously modify data. (Lockheed Martin, 2015)  Obfuscation: conceal presence and mask activity to avoid detection and thwart the inevitable investigation (Buckbee, 2023). | New unrecognized/unauthorized account being created on the system. Specifically, accounts granted administrator privileges.  Unauthorized access, copying, or deletion of files in databases.  Corrupted or encrypted files in databases or on local machines.  Performance issues such as large memory usage or increased CPU usage on endpoint devices.  Denial of service or access to digital resources/assets.  Accounts being used in suspicious manner / normal system interaction changes. | SIEM/IDRP log files indicating malicious connections to unidentified IP addresses.  Antimalware software alerts/ Log files.  Firewall Log files  Windows Event Log files.  Network Log files.  Privilege escalation occurring on unauthorized accounts. | “Establish incident response playbook, including executive engagement and communications plan.  Detect data exfiltration, lateral movement, unauthorized credential usage.  Immediate analyst response to all CKC7 alerts.  Forensic agents pre-deployed to endpoints for rapid triage.  Network packet capture to recreate activity.  Conduct damage assessment with subject matter experts” (Lockheed Martin, 2015).  Document changes made to the system and any analysis of security incidents for reporting as per the communication plan. | Eradication |
| Analysis | 8 | “Conduct a lessons-learned analysis to review the effectiveness and efficiency of incident handling. Capture lessons learned, initial root cause, problems executing courses of action, and any missing policies and procedures. The primary objectives for the analysis include:   * Ensuring root-cause has been eliminated or mitigated. * Identifying infrastructure problems to address. * Identifying organizational policy and procedural problems to address. * Reviewing and updating roles, responsibilities, interfaces, and authority to ensure clarity. * Identifying technical or operational training needs. * Improving tools required to perform protection, detection, analysis, or response actions” (CISA, 2021).   **Communications Plan**: A comprehensive communication plan is vital when an incident occurs. Communications should be made to all affected parties, including employees, customers, investors, business partners, and other stakeholders. This communication should detail the events of the security incident without withholding key details that allow consumers to protect themselves and their information. As part of these communications regarding the incident, legal requirements should be considered as “all states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. In addition, depending on the types of information involved in the breach, there may be other laws or regulations that apply to your situation” (FTC, 2021).  Beyond the consumer, internal communications will be necessary to notify various departments of what has occurred as well as the remediations that need to take place. The results of the lessons-learned analysis should be shared with each department affected so they can rectify any leftover issues or vulnerabilities as fast as possible. As this communication is vital to the recovery of the incident postmortem, thorough documentation throughout the incident ensures all stakeholders are informed of the event and can effectively and efficiently resolve any remaining issues for the company to return to normal operations as quickly as possible. | | | | |

Table \*Rasp,T. (2019, January 21). SNHU ISE-620 Incident Detection and Response. Module 6 Rubric Milestone Number 2. Retrieved on October 19, 2020 from <https://learn.snhu.edu/d2l/lor/viewer/view.d2l?ou=6606&loIdentId=22795>

Countermeasures Analysis:

Security countermeasures are essential to protect organizational systems, operations, and personnel from the negative impacts of various attack methods. These countermeasures, when properly implemented, can significantly mitigate the risks, and reduce the potential harm caused by attacks. Each of these areas has security countermeasures that serve to primarily protect each area, however, all the countermeasures overlap and work together to create a comprehensive defense-in-depth strategy to defend against as many vectors of attack as possible.

Organizational Systems:

* + Intrusion Detection and Prevention Systems (IDPS): IDPS can detect and prevent unauthorized access attempts, malware infections, and other malicious activities targeting organizational systems. By identifying and blocking potential threats, IDPS reduces the chances of successful attacks and protects critical systems and data.
  + Firewalls: Firewalls act as a barrier between internal networks and external entities. They monitor and control network traffic, filtering out potentially harmful data packets and blocking unauthorized access attempts. By enforcing access control policies, firewalls limit the impact of attacks on organizational systems.
  + Encryption and Data Protection: Encrypting sensitive data both at rest and in transit is a fundamental security measure. By implementing encryption algorithms and secure protocols, organizations can protect data from being intercepted or manipulated by attackers. Even if attackers manage to access encrypted data, they will face significant challenges in decrypting it, reducing the impact of a breach. Implementing encryption mechanisms safeguards sensitive data from unauthorized access.
  + Regular Patching and Updates: Keeping software and systems up to date with the latest security patches and updates closes known vulnerabilities. By reducing the attack surface, organizations can minimize the risk of exploitation and subsequent impacts on their systems.

One more countermeasure to note here is the implementation and use of a Security Information and Event Management System (SIEM). SIEM is a comprehensive approach that combines security information management (SIM) and security event management (SEM) to provide real-time monitoring, threat detection, and incident response capabilities. "The underlying principles of any SIEM system are to aggregate data, identify deviations from the norm, and suggest appropriate actions. For example, when a network security issue is detected, a SIEM solution might log event data, generate an alert, and instruct other security devices to mitigate the issue. SIEM technology plays an important part in any data security strategy without it, IT staff lack a place to view all logs and events, which can cause people to miss issues" (Tunggal, 2023). A SIEM benefits and contributes to reducing the negative impacts on organizational systems by:

* Real-time Monitoring: SIEM collects and analyzes logs and security events from various sources within the organizational systems, such as network devices, servers, and applications. It provides real-time visibility into system activities, allowing security teams to detect and respond promptly to any suspicious or malicious behavior.
* Threat Detection: SIEM uses advanced analytics, correlation rules, and threat intelligence to identify potential security incidents and attack patterns. It can detect anomalies, such as unusual login activities, data exfiltration attempts, or unauthorized access attempts. By detecting threats early, SIEM enables proactive measures to prevent attacks from escalating and causing severe damage.
* Incident Response: SIEM plays a crucial role in incident response by providing security teams with centralized and contextualized information about security events. It helps in prioritizing and investigating incidents efficiently, facilitating a faster and more effective response. SIEM can automate response actions, such as isolating affected systems or blocking malicious IPs, to contain the impact of attacks and minimize their consequences.
* Compliance and Auditing: SIEM solutions often include compliance management features, helping organizations meet regulatory requirements. They provide reports, logs, and audit trails that can be used for compliance audits, incident investigations, and forensic analysis. By maintaining compliance, organizations reduce the potential negative impacts of non-compliance penalties and reputational damage.
* Threat Intelligence Integration: SIEM can integrate with external threat intelligence feeds, enabling organizations to stay updated on the latest threat trends, indicators of compromise (IOCs), and known malicious entities. This integration enhances the detection capabilities of the SIEM solution, enabling proactive defense against emerging threats and reducing the risk of successful attacks.

By incorporating SIEM into the organizational systems' security countermeasures, organizations gain improved visibility, proactive threat detection, and effective incident response capabilities. SIEM enhances the overall security posture, reducing the negative impacts of attack methods on organizational systems by enabling faster detection, response, and mitigation of security incidents.

Organizational Operations:

* + Access Control Mechanisms: Implementing robust access controls limits user privileges and ensures that only authorized individuals can access sensitive information and perform critical operations. By enforcing the principle of least privilege, organizations reduce the potential damage that can be caused by attackers who gain unauthorized access.
  + Incident Response Plans: Having well-defined incident response plans enables organizations to respond swiftly and effectively to security incidents. These plans outline the necessary steps to mitigate and recover from an attack, minimizing the disruption to ongoing operations and reducing the overall impact on the organization. When an attack occurs, effective security countermeasures enable organizations to respond swiftly and mitigate the impact. Incident response plans, including incident handling procedures, communication protocols, and designated response teams, can help coordinate actions to contain and recover from an attack. Organizations can isolate compromised systems, patch vulnerabilities, restore backups, and take other necessary steps to limit the damage and restore normal operations.
  + Employee Awareness and Training: Regular security awareness programs educate employees about potential threats and best practices for mitigating them. By training personnel to identify and respond to social engineering attacks, phishing attempts, or other common attack vectors, organizations can prevent successful attacks and safeguard their operations.

Special consideration and care need to be taken to meeting regulatory requirements that affect bank operations. Auditing and regulatory requirements play a crucial role in reducing negative impacts on a bank's operations.

* Auditing: Finger Lakes Community Bank implements regular internal and external audits to assess the effectiveness of its security measures, processes, and controls. Audits help identify vulnerabilities, gaps in security, and areas for improvement. By conducting comprehensive audits, the bank can proactively address any issues before they are exploited by attackers, reducing the potential negative impacts on its operations.
* Regulatory Compliance: As a financial institution, Finger Lakes Community Bank must adhere to various regulatory requirements, such as those imposed by banking regulatory bodies (e.g., the Office of the Comptroller of the Currency, the Federal Reserve, and the FDIC in the US) and data protection regulations (e.g., the General Data Protection Regulation (GDPR) in the EU or the Gramm-Leach-Bliley Act (GLBA) in the U.S.). Compliance with these regulations ensures that the bank follows industry best practices and security standards, reducing the risk of regulatory penalties and reputational damage.
* Data Protection: Banks deal with sensitive customer information, such as personal and financial data. Regulatory requirements such as the GDPR, GLBA and PCI-DSS often mandate the implementation of robust data protection measures, including encryption, access controls, and secure transmission protocols. By complying with these requirements, Finger Lakes Community Bank protects customer data from unauthorized access, reducing the negative impacts of data breaches on its operations and maintaining customer trust.
* Incident Response Planning: Regulatory frameworks often require financial institutions to have robust incident response plans in place. By having well-defined incident response procedures, Finger Lakes Community Bank can limit the disruption caused by incidents, mitigate potential financial losses, and safeguard its operations.
* Vendor Management: Regulatory requirements also extend to the bank's relationships with third-party vendors. Finger Lakes Community Bank needs to ensure that its vendors meet specific security and compliance standards. Implementing a comprehensive vendor management program, including due diligence assessments, contractual agreements, and regular monitoring, reduces the risk of a vendor-related incident impacting the bank's operations.

Personnel:

* + Multi-factor Authentication (MFA): Security countermeasures often include robust access control mechanisms to ensure that only authorized individuals can access sensitive information or critical systems. By implementing strong authentication methods such as multi-factor authentication, biometrics, or smart cards, organizations can reduce the risk of unauthorized access. This helps protect against attacks like password theft, social engineering, or unauthorized account usage. Implementing MFA requires users to provide multiple forms of identification before accessing systems or data. By adding an extra layer of security, MFA reduces the likelihood of unauthorized access even if credentials are compromised.
  + Security Policies and Procedures: Establishing clear security policies and procedures ensures that employees understand their responsibilities and adhere to the best security practices. By defining guidelines for password management, data handling, and incident reporting, organizations minimize the risk of human error leading to successful attacks.
  + Regular Training and Education: Continuous security training and education help personnel stay updated on emerging threats and effective defense strategies. By empowering employees with knowledge and skills, organizations can create a security-conscious culture, reducing the likelihood of falling victim to attacks. Security countermeasures are not solely technical solutions; they also involve educating employees about potential risks and best practices. Regular security awareness programs and training sessions can help employees recognize and respond to social engineering attacks, phishing attempts, or other malicious activities. By promoting a security-conscious culture, organizations can minimize the success rate of attacks and ensure that employees are an active line of defense.

By implementing a combination of technical and organizational security countermeasures, organizations can significantly reduce the negative impacts of attack methods on their systems, operations, and personnel. Further, these countermeasures work to ensure compliance with regulations imposed on the banking industry. These countermeasures work together to create multiple layers of defense, making it harder for attackers to succeed and mitigating the potential damage caused by successful attacks. It is important to regularly assess and update security measures to stay ahead of evolving threats and maintain a robust security posture.

# References

Bonderud, D. (2023). *How to implement the five pillars of AML compliance*. Retrieved from Persona: https://withpersona.com/blog/five-pillars-aml-compliance#:~:text=The%20newest%20version%20of%20the,processes%20for%20ongoing%20customer%20due

BreachRX. (2023). *23 NYCRR 500 Incident Response Guidelines*. Retrieved from BreachRX: https://www.breachrx.com/global-regulations-data-privacy-laws/new-york-dfs-23nycrr500/

Buckbee, M. (2023, March 23). *What is The Cyber Kill Chain and How to Use it Effectively*. Retrieved from Varonis: https://www.varonis.com/blog/cyber-kill-chain

CISA. (2021, November). *Cybersecurity Incident & Vulnerability Response Playbooks*. Retrieved from Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/sites/default/files/publications/Federal\_Government\_Cybersecurity\_Incident\_and\_Vulnerability\_Response\_Playbooks\_508C.pdf

Fortinet. (2023). *Indicators of Compromise (IOCs)*. Retrieved from Fortinet: https://www.fortinet.com/resources/cyberglossary/indicators-of-compromise

FTC. (2021, February). *Data Breach Response: A Guide for Business*. Retrieved from Federal Trade Commission: https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business

Lockheed Martin. (2015). *Gaining the Advantage: Applying the Cyber Kill Chain Methodlogy to Network Defense*. Retrieved from Lockheed Martin: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining\_the\_Advantage\_Cyber\_Kill\_Chain.pdf

PSOL. (2017). *Cyber Kill Chain 1: Reconnaissance*. Retrieved from PSOL: https://www.psoltech.com/cyber-kill-chain-1-reconnaissance/

PSOL. (2017). *Cyber Kill Chain II: Weaponization*. Retrieved from PSOL: https://www.psoltech.com/cyber-kill-chain-ii-weaponization/

Tunggal, A. T. (2023, April 6). *SIEM vs. IDS: What is the Difference?* Retrieved from UpGuard: https://www.upguard.com/blog/siem-vs-ids