Incident Analysis:

After conducting an initial investigation, I have determined that the breach occurred through a phishing email campaign that targeted ABC SecureBank employees. The email, which appeared to be from a legitimate source, contained a malicious link that downloaded a Remote Access Tool (RAT) onto the employee's computer. The RAT allowed the attacker to gain unauthorized access to the system and move laterally within the network.

The point of entry was a workstation used by a customer service representative, who clicked on the malicious link on January 10, 2023. The breach occurred over a period of 14 days, from January 10 to January 24, 2023.

Forensic Analysis:

Digital forensics analysis of the affected systems revealed the presence of a custom-built RAT, which was used to exfiltrate sensitive customer data. The RAT was designed to evade detection by traditional security controls and was able to communicate with the attacker's command and control (C2) server.

Logs and evidence collected during the forensic analysis include:

- Network logs showing the initial infection and lateral movement within the network
- System logs showing the installation and execution of the RAT
- Memory dumps of the infected systems
- Network captures of the data exfiltration

Data Recovery:

Based on the forensic analysis, it appears that the attacker was able to access and exfiltrate sensitive customer data, including names, account numbers, and transaction history. The type and quantity of data exposed are as follows:

- 100,000 customer accounts were accessed
- 50,000 account numbers were exfiltrated
- 20,000 transaction histories were accessed

To contain the incident and prevent further data loss, I recommend implementing the following measures:

- Isolate the affected systems from the network
- Implement a network-wide password reset
- Enable two-factor authentication for all users
- Conduct a thorough review of access controls and permissions

Regulatory Compliance:

The data breach notification laws and regulations that apply to this incident include:

- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Gramm-Leach-Bliley Act (GLBA)

To ensure compliance with these regulations, I recommend the following:

- Notify affected customers within 72 hours of the breach discovery
- Provide written notification to regulatory bodies, including the Federal Trade Commission (FTC) and the Office of the Comptroller of the Currency (OCC)
- Conduct a thorough risk assessment and implement additional security controls to prevent future breaches

Communication and Notification:

The communication plan for notifying affected customers, stakeholders, and regulatory bodies should include the following:

- Clear and concise language explaining the breach and the actions being taken to contain and mitigate it
- Information on the type and quantity of data exposed
- Instructions on how to protect themselves from potential fraud and identity theft
- Contact information for customer support and incident response teams

Post-Incident Review:

After the breach has been contained and mitigated, I recommend conducting a thorough review to identify weaknesses in the security posture and provide recommendations for improving security. This review should include:

- A thorough analysis of the incident response plan and its effectiveness
- An assessment of the security controls in place at the time of the breach
- Identification of areas for improvement, including employee training and awareness programs
- Recommendations for implementing additional security controls, such as advanced threat detection and incident response tools.