A Guide for Incident Response

January 14, 2021

A Guide for Incident Response

Introduction

The following ICBA incident response guide has been created not to replace your incident response plan (IRP), but to provide you and your team necessary steps and other suggestions to assist in your incident response. [1]

Activation of Incident Response Plan

Evaluate if the incident warrants the need to activate your incident response plan (IRP).

- Many IRPs indicate that the plan may be activated if certain conditions are met, including but not limited to the unauthorized access to or loss of customer personally identifiable information (PII).
- If the incident fits the conditions within your IRP, then:
    - Declare that you are formally activating your IRP.
    - Assemble your incident response team.
    - Fill out any associated incident tracking documents. You may need these documents for your next IT audit or exam as well as possible future reports to the board, insurance claims, or legal proceedings.
- Distribute and review the IRP to all appropriate staff.
    - Review the IRP for the steps your bank has agreed it would perform.
    - Identify any steps that have not already been assigned to a designated individual and assign those steps appropriately.
    - Designate a staff member to keep notes on the areas of the IRP, that may need to be updated after the incident is resolved.

Organize the Incident Response

Evaluate the amount of time necessary to address the incident and setup meetings with appropriate stakeholders.

- Create a cadence for the incident response team's workgroup and technical meetings.
- Create a cadence for senior leadership to receive updates on the incident.

Contact Partners

The IRP should detail contacting all or most of the following organizations and agencies to either work toward an incident response and resolution, to notify them of the incident, or to look for additional resources that might be helpful in your incident response.

[1] The information provided in this guide does not, and is not, intended to provide nor constitute legal advice; instead, all information and content are for general informational purposes only. Community banks are advised to consult with appropriate and knowledgeable counsel about cyber incident requirements, responses, or actions.

- Third-party service provider(s) where the incident might have originated, has taken place, or has been affected.
    - Set up meetings to discuss the incident or potential incident. Be firm on the need for recurring and frequent meetings, even if it is only with your account representative and not their incident response team.
    - Request regular updates in timeframes that meet the bank's needs.
    - Document your correspondence with your third-party service provider, including but not limited to:
        - Requests and inquires to your third-party service provider(s).
        - Whether or not you received responses to your requests and inquiries.
        - The time it took to receive a response to requests and inquiries.
    - Create a timeline of all events, including your staff's responses, related to the incident.
- Third-party incident response vendor retained by the bank to assist during the incident.
    - Meet with your incident response vendor to discuss the incident (or potential incident) and to confirm how their service can assist your bank during the incident.
        - Not all incident response vendors are equipped or staffed to assist with all types of incidents, so evaluate their capabilities as it applies to the incident.
- Cybersecurity insurance company
    - Contact your cybersecurity insurance company early in the process. They will provide instructions as to what incident information should be collected and will most likely suggest an incident response company, for you to work with.
- Law enforcement
    - Contact law enforcement (Federal Bureau of Investigation, United States Secret Service, or Department of Justice) to notify them of the incident, and to seek assistance if applicable.
    - Law enforcement contact information can be found at www.icba.org.
- Regulators/FinCEN
    - Contact your regulatory agency (Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Federal Reserve Board, and State Department of Financial Institutions) to notify them of the incident as appropriate and in accordance with regulations and guidance.
    - File Suspicious Activity Reports, and other reports or records, with FinCEN as required by the Bank Secrecy Act and its implementing regulations if applicable.
- Incident information sharing
    - The bank may opt to provide FS-ISAC, or another information sharing organization, with information on the incident. FS-ISAC will then provide that information anonymously to the rest of the financial sector to help the financial sector's overall incident response.

    - The bank may also collect intelligence from FS-ISAC, or another information sharing organization, if something similar has happened elsewhere in the financial sector that might benefit your incident response.

Communication Plans

The IRP should detail a communication plan with communication streams directed at different stakeholders. Incident details may differ so collect the incident details from vendors and staff needed for your incident response communication plan. There should be communications for:

- Bank staff
    - Provide a statement on the incident for bank staff to use during conversations with customers.
    - Provide a document with answers to frequently asked questions about the incident or the impact of the incident.
- Customers
    - Create a formal customer notification on the incident. ICBA has sample customer communications at www.icba.org.
- Board members
    - Develop materials and documents to provide to the Board.
- News outlets
    - If questioned by news media, have a designated individual at the bank who is authorized to have those conversations.

Call Center Tips

Depending on the size and significance of the incident, consider staffing a specialized response call center with its own phone number, or direct calls from the general bank number(s) to the new call center.

- Questions are best answered by those dedicated to the incident, not those also engaged in other day-to-day operations.
- If call volume is an issue, consider reaching out to vendors to see if they can augment your staff by directing overflow to outsourced call centers.
    - Core providers often have overflow call centers for services like core and online banking conversions, so they might offer a service for incidents.

Stress

Incidents can be stressful times for all bank staff. Provide a list of resources to help staff who may need additional support during this time. Involve your senior leadership team and HR Department to monitor stress and to look for additional resources that can be provided throughout the incident response.

Resources

- ICBA Cyber & Data Security Resource Page
- CISA Incident Management Guide
- CISA Incident Response Training
- CISA Cyber Essentials
- Ready.gov Incident Management
- Ready.Gov IT Disaster Recovery Plan
- NIST Computer Security Incident Handling Guide
- NIST Cybersecurity Framework

About:
The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. With more than 50,000 locations nationwide, community banks constitute 99 percent of all banks, employ nearly 750,000 Americans and are the only physical banking presence in one in three U.S. counties. Holding more than $5 trillion in assets, more than $4 trillion in deposits, and more than $3.4 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation, and fueling their customers' dreams in communities throughout America.

ICBA is dedicated *exclusively* to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education, and high-quality products and services.

For more information, visit ICBA's website at www.icba.org.

Continue the Conversation:
Joel Williquette
Senior Vice President, Operational Risk Policy
Independent Community Bankers of America
Joel.Williquette@icba.org

Press Inquiries:
Nicole Swann
Vice President, Communications
Independent Community Bankers of America
Nicole.Swann@icba.org
202-821-4458