Incident Response Programs

Why are incident response programs important?

Financial institutions remain a prime target for cyber threat actors, primarily due to the wealth of personal and financial information they manage for their customers. The ability to quickly detect, contain, and recover from cyber-attacks can help to lessen operational impacts and minimize the erosion of consumer trust, financial losses, and the regulatory consequences that can accompany a successful cyber-attack. The institution's **incident response program** is the cornerstone that helps to ensure that these consequences are minimized to the greatest extent possible when a cyber-attack occurs. Moreover, it is the key pillar of an institution's overall **resilience strategy** because it drives the institution's initial reactions to withstand and recover from disruptions that will inevitably occur.

Incident response basics

According to the FFIEC, "The goal of incident response is to minimize damage to the institution and its customers. The institution's program should have defined protocols to declare and respond to an identified incident. More specifically, the incident response program should include, as appropriate:

- Containing the incident;
- Coordinating with law enforcement and third parties;
- Restoring systems, preserving data and evidence;
- Providing assistance to customers; and
- Otherwise facilitating operational resilience of the institution."

Incident response "involves a combination of people and technologies" and that the quality of incident response is attributable to "the institution's culture and its policies, procedures, and training." In addition, it is "a function of the relationships the institution formed before the incident with law enforcement, incident response consultants and attorneys, information-sharing entities (e.g., FS-ISAC), and others." And at the heart of the incident response program is the **incident response plan (IRP)**. The IRP is the quintessential, living document that addresses the "action steps, involved resources, and communication strategy upon identification of a threat or potential event."[1]

To further illustrate the incident response life cycle, NIST has developed a "high-level incident response life cycle model based on the six CSF 2.0 Functions, which organize cybersecurity outcomes at their highest level:

- **Govern (GV)**: The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- **Identify (ID)**: The organization's current cybersecurity risks are understood.
- **Protect (PR)**: Safeguards to manage the organization's cybersecurity risks are used.
- **Detect (DE)**: Possible cybersecurity attacks and compromises are found and analyzed.
- **Respond (RS)**: Actions regarding a detected cybersecurity incident are taken.

[1] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Information Security - III.D - Incident Response. September 2016.

Recover (RC): Assets and operations affected by a cybersecurity incident are restored."[2]

Components of incident response

There are many considerations for financial institutions in developing and implementing an incident response program and incident response plan. The FFIEC highlights a number of **primary considerations**, including:

- Defining **policies and procedures** to guide responses to incidents
- Selecting, installing, and understanding the **tools that will play a part in the response process**
- Balancing **concerns regarding confidentiality, integrity, and availability for devices and data** (i.e., containment and restoration strategies which account for systems that can be disconnected and systems that must remain operational)
- Defining **circumstances when incident response activities are to be initiated**
- Assigning **appropriate individuals or teams with responsibilities and authorities** to carry out incident response activities and **ensuring that appropriate personnel are notified and available when needed**
- Defining **circumstances and mechanisms for reaching out to external personnel and experts**, as needed
- Establishing **notification thresholds and protocols** for informing regulators, customers, and law enforcement and communications strategies that define the "how, when, what, and who" of communicating to outside parties
- Assigning **appropriate authorities to personnel or teams to handle containment of the incident and restoration activities**
- Documenting and maintaining **incident evidence**, as well as the **decisions made and the actions taken** during the response
- Developing **required thresholds** for returning compromised services, equipment, and software to the network
- Defining circumstances for filing a **Suspicious Activity Report**[3]

The CSBS Ransomware Self-Assessment Tool (R-SAT) provides additional, more granular recommendations for specific incident response procedures, including:

- Monitoring **social media, hyper-local social media, and other news sources** for public awareness
- Implementing **out-of-band communications** to mitigate threat actor use of single sign-on (SSO) to access containment and remediation efforts
- Implementing **alternative strategies for connecting to critical third-party vendors** in the event of an incident
- Establishing **escalation procedures for enacting the business continuity/disaster recovery plans** in the event of significant or long-term impacts to operations

The FFIEC notes that, "Management should align incident response procedures with other related processes (e.g., cybersecurity, network operations, and physical security), outsourced services (e.g.,

[2] National Institute of Standards and Technology. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. April 2025.
[3] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Information Security - III.D - Incident Response. September 2016.

contracted incident response obligations), and verify that the procedures are considered during planning and business continuity plan development."[4] Moreover, because of the wide variety of threats (ransomware, DDoS, business email compromise, etc.) potentially affecting the institution, the use of incident-specific response playbooks can more efficiently enable quicker response to the most likely or impactful types of attack and help to minimize disruption across the breadth of the institution.

The importance of testing and learning from real-world events

The incident response program and the incident response plan are not static by nature; they are living documents that require frequent updates. **Periodic testing of the incident response plan** is an essential exercise to ensure that the program and plan are accurate, up-to-date, and reliable when needed most. Testing also helps to ensure that individuals and teams charged with responsibilities in the IRP are familiar with their assignments. In the heat of an incident, well-trained personnel who are familiar with the IRP can reduce the likelihood that critical tasks are forgotten. IRP testing should address responses to a variety of incidents that the institution is most likely to experience and should involve all personnel with assigned responsibilities. In addition, testing events should ideally include senior management to ensure top-down awareness of response procedures, staff responsibilities, and general oversight needs in the event of an incident.

Experiences from real-world cyber events also provide the institution with perhaps the most beneficial opportunity to update the incident response program and incident response plan. Documentation of responses to an actual cyber incident (i.e., an after-action report) can cast a light on both strengths and weaknesses in the plan. Following an actual cyber incident, the institution should identify areas of the IRP that require adjustment (e.g., stale contact lists for vendors and response team members, duplication of duties and other response process issues, etc.).

Changes in vendors or staffing, the addition of new business units, or changes in the institution's technology environment are all events that necessitate a careful review of the incident response program. Cyber incidents can create near-instant chaos for the institution and discovering that the incident response program and plan are stale can mean the difference between an efficient, effective recovery and a disorganized response that can leave the institution floundering- especially when time is of the essence.

Any deficiencies identified from testing exercises, responses to real-world incidents, or changes in the institution's environment should be **tracked, prioritized and remediated appropriately**. Management should make any necessary changes to the incident response program and incident response plan with appropriate urgency to ensure that they are ready to deploy immediately in the event of an incident- even if these modifications are necessary between normal policy review and approval cycles.

[4] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Business Continuity Management - V.F.1 - Incident Response. November 2019.