Playbook

# Building an Incident Response Plan for Financial Services

CADO//

## How to Create an Incident Response Plan for Financial Services

In today's digital-first financial landscape, the threat of cyberattacks looms larger than ever. Banks, credit unions, insurance companies, and other financial institutions are prime targets for cybercriminals due to the vast amounts of sensitive data they handle and the potential for significant financial gain. As such, having a robust, well-structured incident response plan is not just a good practice—it's an absolute necessity.

This comprehensive guide will walk you through the process of creating a tailored incident response plan for financial services organizations, drawing on industry best practices, regulatory requirements, and real-world experiences. We'll go into each phase of the incident response lifecycle, providing detailed strategies, checklists, and considerations specific to the financial sector.

## 1. Understanding the Unique Challenges for Financial Services

Before diving into the specifics of creating an incident response plan, it's crucial to understand the unique challenges faced by financial institutions:

- **High-Value Target:** Financial organizations are prime targets for cybercriminals due to the potential for direct financial gain and the value of the data they hold.
- **Complex Systems:** Many financial institutions rely on a mix of legacy systems and cutting-edge technology, creating a complex IT environment that can be challenging to secure and monitor.
- **Regulatory Scrutiny:** The financial sector is heavily regulated, with strict requirements for data protection, incident reporting, and customer notification.
- **Interconnectedness:** Financial institutions are often interconnected through various networks and systems, meaning a breach in one organization can have far-reaching consequences.
- **Customer Trust:** In an industry built on trust, a mishandled security incident can have severe and long-lasting impacts on customer relationships and brand reputation.
- **Sophisticated Threats:** Financial institutions face a wide range of threats, from advanced organized crime to insider threats and supply chain attacks.
- **24/7 Operations:** Many financial services operate around the clock, making it challenging to implement security updates or take systems offline for investigation without disrupting critical services.

## 2. Regulatory Landscape and Compliance Requirements

Financial institutions must navigate a complex web of regulations and compliance requirements when it comes to cybersecurity and incident response. Key regulations include:

- **Gramm-Leach-Bliley Act (GLBA)**: Requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data.
- **Payment Card Industry Data Security Standard (PCI DSS)**: Applies to all organizations that handle credit card information.
- **Sarbanes-Oxley Act (SOX)**: While primarily focused on financial reporting, it has implications for IT controls and cybersecurity.
- **European Union's General Data Protection Regulation (GDPR):** Applies to financial institutions handling data of EU residents.
- **SEC's cybersecurity disclosure rules:** Relatively new rules around disclosing incidents.
- **DORA (the EU Digital Operational Resilience Act):** Is focused on resilience, but also includes requirements around managing and disclosing incidents.

When creating your incident response plan, ensure that it addresses the specific requirements of these regulations, including:

- Incident classification and reporting thresholds
- Timeframes for reporting incidents to regulators
- Requirements for customer notification
- Documentation and evidence preservation standards
- Post-incident reporting and remediation expectations

### How Cado Can Help

**"The fact that we no longer have to manually request access to a potentially compromised system via our cloud team is a game changer." Incident Response Lead, Large Financial Institution**

**Ready to hear more about how Cado can help you be prepared for beaches? Try the Cado platform free trial.**

## Case Studies: Learning from Real-World Incidents

The financial services sector has faced numerous cybersecurity incidents over the years, providing valuable lessons for incident response planning. By examining these real-world cases, we can gain insights into effective strategies and potential pitfalls. Let's explore some notable incidents and the key takeaways for financial institutions:

### Capital One Data Breach (2019)

- **Incident:** A former Amazon Web Services employee exploited a misconfigured firewall to access Capital One's cloud-based data, affecting approximately 100 million customers in the US and Canada.

**Key Lessons:**

- Cloud security configuration is critical: Financial institutions must regularly audit and secure their cloud environments.
- Insider threats are real: Robust access controls and monitoring systems are essential, even for former employees or contractors.
- Swift response matters: Capital One's quick detection and disclosure of the breach helped mitigate potential damages and maintain customer trust.

### Equifax Data Breach (2017)

- **Incident:** Hackers exploited a known vulnerability in Apache Struts software, compromising sensitive data of millions of consumers.

**Key Lessons:**

- Timely patching is crucial: Financial institutions must have processes in place to quickly identify and patch known vulnerabilities.
- Segmentation is important: Proper network segmentation could have limited the attackers' ability to move laterally within Equifax's systems.
- Incident response readiness is essential: Equifax's delayed and poorly coordinated response highlighted the need for well-prepared incident response teams and communication plans.

### Bangladesh Bank Heist (2016)

- **Incident:** Cybercriminals used SWIFT credentials to transfer nearly $1 billion from Bangladesh Bank's account at the Federal Reserve Bank of New York, successfully stealing $81 million.

**Key Lessons:**

- Multi-factor authentication is critical: Implement strong authentication measures for all critical financial systems and transactions.
- Anomaly detection is vital: Implementing advanced fraud detection systems could have

flagged the unusual transaction patterns.
- International cooperation is necessary: The incident highlighted the need for better collaboration between financial institutions, regulators, and law enforcement agencies across borders.

These case studies highlight several critical aspects that financial institutions should incorporate into their incident response plans.

## The Six Phases of Incident Response for Financial Institutions

Now, let's go into each phase of the incident response lifecycle, tailoring our approach to the specific needs of financial institutions.

### Preparation

The preparation phase is critical for laying the groundwork for an effective incident response. For financial institutions, this phase should be particularly comprehensive:

#### Establish a Dedicated Incident Response Team

Form a cross-functional team including representatives from:

- Incident classification and reporting thresholds
- IT Security
- Legal/Compliance
- Operations
- Risk Management
- Public Relations/Communications
- Human Resources
- Customer Service
- Senior Management
- Board of Directors (for escalation and oversight)

As you bring the team together:

- Define clear roles and responsibilities for each team member
- Establish an on-call rotation to ensure 24/7 coverage
- Consider creating specialized sub-teams for different types of incidents (e.g., fraud, data breaches, DDoS attacks)

### Develop Comprehensive Security Policies and Procedures

Create detailed policies addressing:

- Data classification and handling
- Access controls and authentication (including multi-factor authentication)
- Network segmentation and firewall configuration
- Encryption standards for data at rest and in transit
- Mobile device and remote access security
- Third-party vendor risk management
- Employee security awareness training
- Social engineering and phishing prevention
- Incident reporting and escalation procedures
- Business continuity and disaster recovery

Ensure policies align with relevant regulatory requirements and industry standards (see above).

### Conduct a Thorough Risk Assessment

Identify and categorize critical assets:

- Core banking systems
- Customer databases
- Trading platforms
- Payment processing systems
- ATM networks
- Online and mobile banking platforms

Assess potential threats and vulnerabilities:

- External threats (e.g., cybercriminals)
- Internal threats (e.g., disgruntled employees, accidental data leaks)
- Third-party risks (e.g., vendors, partners, service providers)

Evaluate the potential impact of various incident types:

- Data breaches
- Ransomware attacks
- Distributed Denial of Service (DDoS) attacks
- Account takeovers

- Wire fraud
- ATM skimming

Prioritize risks based on likelihood and potential impact

### Create Detailed Response Strategies and Playbooks

Develop specific playbooks for different types of incidents, including:

- Unauthorized access to customer accounts
- Malware infections on critical systems
- Insider data theft
- Payment card breaches
- DDoS attacks on online banking platforms
- Ransomware attacks on core systems
- Business Email Compromise (BEC) attempts
- Mobile banking app compromises

Each playbook should include:

- Step-by-step response procedures
- Roles and responsibilities
- Communication templates
- Escalation criteria
- Regulatory reporting requirements
- Evidence preservation guidelines

### Establish Communication Protocols

Define clear communication channels and procedures for:

- Internal stakeholders (employees, executives, board members)
- Customers
- Regulators (e.g., OCC, FDIC, SEC, FCA)
- Law enforcement agencies
- Media and public relations

Prepare template messages for various incident scenarios, including:

- Initial customer notifications

- Public statements
- Regulatory disclosures
- Internal employee communications

Establish a secure, out-of-band communication method for the incident response team (e.g., encrypted messaging app).

### Implement and Test Incident Response Tools

Deploy essential incident response tools, including:

- Security Information and Event Management (SIEM) systems
- Endpoint Detection and Response (EDR) solutions
- Network forensics tools
- Data loss prevention (DLP) software
- Automated incident response platforms
- Digital forensics tools

Regularly test and update these tools to ensure they're functioning correctly and are capable of handling the latest threats

### Conduct Regular Training and Simulations

Organize frequent tabletop exercises and simulations to:

- Familiarize team members with the incident response plan
- Test the effectiveness of response strategies
- Identify areas for improvement
- Practice communication and decision-making under pressure

Include scenarios specific to the financial sector, such as:

- Large-scale data breaches affecting millions of customer records
- Ransomware attacks on core banking systems
- Insider trading facilitated by compromised employee accounts
- ATM cash-out schemes
- Sophisticated fraud campaigns targeting high-net-worth clients

Involve senior management and board members in select exercises to ensure top-level buy-in and understanding of incident response processes

### Establish Relationships with External Partners

Identify and establish relationships with:

- Law enforcement agencies
- Regulatory bodies
- External forensics firms
- Legal counsel specializing in cybersecurity
- Public relations firms with crisis management experience
- Threat intelligence sharing organizations (e.g., FS-ISAC)

Pre-negotiate contracts with key service providers to ensure rapid response capabilities.

## Identification

The identification phase focuses on detecting and confirming security incidents. For financial institutions, this phase should emphasize:

### Implement Robust Monitoring Systems

Deploy advanced monitoring solutions to detect anomalies across:

- Network traffic (both internal and external)
- User behavior and access patterns
- Financial transactions
- Access to sensitive data and systems
- Cloud services and third-party integrations
- Mobile banking apps and ATM networks

Implement detection systems to identify subtle patterns indicative of sophisticated attacks

### Establish Clear Incident Classification Criteria

Define specific thresholds for classifying incidents based on:

- Type of affected systems (e.g., core banking, trading platforms, customer-facing applications)
- Potential financial impact
- Number of affected customers
- Regulatory implications
- Reputational risk

Create a tiered incident severity scale (e.g., Low, Medium, High, Critical) with clear definitions and response requirements for each level.

### Create a Comprehensive Incident Reporting System

Implement a streamlined process for employees, customers, and partners to report suspicious activities or potential incidents

- Establish a 24/7 incident reporting hotline
- Develop an internal ticketing system to track and manage reported incidents
- Create an anonymous reporting channel for potential insider threats

### Leverage Threat Intelligence

- Utilize financial sector-specific threat intelligence feeds to stay informed about emerging threats and attack patterns
- Participate in information sharing organizations like FS-ISAC
- Implement automated threat intelligence platforms to correlate external threat data with internal security events

### Conduct Regular Security Assessments

Perform frequent vulnerability scans and penetration tests, including:

- Network infrastructure
- Web applications and APIs
- Mobile banking apps
- ATM systems
- Third-party integrations

Conduct regular security audits of critical systems and processes, and consider implementing a bug bounty program to leverage external security researchers.

### Monitor Social Media and Stolen Credential Forums

- Implement social media monitoring tools to detect potential phishing campaigns or brand impersonation attempts
- Conduct regular forum monitoring to identify stolen credentials or leaked data related to your institution

### Establish Baseline Behavior

- Create baseline profiles for normal system and user behavior to more easily identify deviations that could indicate a security incident

## Containment

Once an incident is confirmed, swift containment is crucial to minimize damage. For financial institutions, containment strategies should include:

### Implement Immediate Containment Measures

Depending on the type of incident, take immediate actions such as:

- Isolating affected systems from the network
- Freezing compromised user accounts
- Blocking suspicious IP addresses or geographic regions
- Temporarily disabling affected services (e.g., online banking portal)
- Implementing additional authentication measures for high-risk transactions
- Activating fraud detection and prevention mechanisms

### Preserve Evidence

Ensure that all containment actions are documented in detail:

- Create forensic images of affected systems before making any changes
- Preserve log files, network traffic captures, and other relevant data
- Maintain a chain of custody for all collected evidence

### Assess the Scope of the Incident

Rapidly determine the extent of the breach or attack:

- Identify all affected systems and data
- Determine the number of impacted customers
- Assess potential financial losses and regulatory implications
- Analyze the attack vector and methodology used

### Implement Access Controls

Review and adjust access controls to prevent further unauthorized access:

- Reset passwords for affected accounts and systems

- Implement additional authentication measures (e.g., step-up authentication for sensitive operations)
- Revoke compromised credentials and certificates
- Review and restrict privileged access

### Notify Relevant Authorities

- Inform appropriate regulatory bodies as required by law and industry regulations
- Contact law enforcement agencies if criminal activity is suspected
- Engage legal counsel to guide the notification process and ensure compliance

### Activate Crisis Communication Plan

Implement the pre-defined communication plan to inform:

- Internal stakeholders (employees, executives, board members)
- Affected customers
- Partners and vendors
- Media (if necessary)

Use pre-prepared communication templates, adapting them to the specific incident.

### Monitor for Ongoing Activity

- Implement enhanced monitoring of affected systems and related infrastructure
- Watch for signs of lateral movement or persistence mechanisms

### Assess Business Impact

- Evaluate the impact on critical business functions and customer-facing services
- Implement business continuity measures as needed to maintain essential operations

## Eradication

The eradication phase focuses on eliminating the root cause of the incident and strengthening defenses. For financial institutions, this should involve:

### Remove Malicious Components

Thoroughly remove any malware, backdoors, or unauthorized access points from affected systems. Conduct a comprehensive sweep of all potentially affected systems, including:

- Servers and workstations

- Network devices
- Mobile devices
- Cloud services and applications

### Patch Vulnerabilities

Address any vulnerabilities that were exploited during the incident:

- Apply security patches to all affected systems
- Update software and firmware to the latest secure versions
- Reconfigure systems and applications to eliminate security weaknesses
- Implement virtual patching where immediate updates are not possible

### Enhance Security Controls

Implement additional security measures to prevent similar incidents:

- Strengthen access controls and authentication mechanisms
- Improve network segmentation to isolate critical systems
- Enhance encryption practices for data at rest and in transit
- Implement or improve data loss prevention (DLP) solutions
- Enhance endpoint protection and EDR capabilities
- Strengthen email and web filtering

### Conduct a Thorough Investigation

Perform a detailed forensic analysis to:

- Determine the root cause of the incident
- Identify the full attack timeline and methodology
- Assess the full extent of the damage and data exposure
- Identify any potential insider involvement
- Determine if the attack is part of a larger campaign targeting the financial sector

### Update Security Policies and Procedures

- Revise existing security policies and procedures based on lessons learned from the incident
- Update incident response playbooks to reflect new knowledge and best practices
- Enhance employee training programs to address any identified gaps

### Conduct a Post-Eradication Sweep

- Perform a comprehensive security assessment of all systems to ensure complete eradication
- Conduct penetration testing to verify the effectiveness of new security measures

### Rebuild Affected Systems

- If necessary, completely rebuild affected systems from known clean sources
- Restore data from verified clean backups
- Implement additional security hardening measures during the rebuild process

### Review and Enhance Monitoring Capabilities

- Update detection rules and monitoring systems based on the incident characteristics
- Implement any new monitoring tools or capabilities identified as necessary during the incident

## Recovery

The recovery phase focuses on restoring normal operations safely and efficiently. For financial institutions, this should include:

### Develop a Phased Recovery Plan

- Prioritize the restoration of critical systems and services
- Create a timeline for bringing systems back online in a controlled manner

### Restore from Clean Backups

- Use verified, clean backups to restore affected systems and data
- Ensure restoration process doesn't reintroduce vulnerabilities or malware

### Implement Additional Monitoring

- Deploy enhanced monitoring solutions to detect any persistent threats or abnormal activities
- Implement real-time alerts for suspicious behavior on restored systems

### Gradually Restore Services

Carefully bring systems and services back online, prioritizing critical operations:

- Core banking systems
- Online and mobile banking platforms
- ATM networks
- Payment processing systems
- Trading and investment platforms

- Customer service systems

### Conduct Thorough Testing

- Perform comprehensive testing of restored systems to ensure they are functioning correctly and securely
- Conduct security scans and penetration tests on restored systems
- Test all integrations and data flows between systems

### Monitor for Anomalies

- Closely monitor restored systems for any signs of persistent threats or abnormal behavior
- Implement extended monitoring periods for critical systems

### Lessons Learned

The Lessons Learned phase is a critical component of the incident response lifecycle for financial institutions. It provides an opportunity to reflect on the incident, evaluate the response efforts, and identify areas for improvement. This phase should be conducted no more than two weeks following a cyber event to ensure that details are still fresh in the minds of the response team.

For financial services organizations, the Lessons Learned phase is particularly important due to the sensitive nature of financial data and the potential for significant reputational and financial damage from cyber incidents. Here are key steps to maximize the value of this phase:

- **Complete Incident Documentation:** Throughout the incident response process, team members should have been documenting their actions in an Incident Handlers Journal. During the Lessons Learned phase, this documentation should be finalized and compiled into a comprehensive report that outlines the entire incident response sequence. This report should be clear and easily understood by stakeholders outside of the incident response team, including senior management and potentially regulators.

- **Conduct a Post-Incident Review Meeting:** Organize a meeting with all relevant stakeholders, including the incident response team, affected business units, and senior management. This meeting should follow a structured evaluation framework to ensure all aspects of the incident and response are covered. Key questions to address include:
    - When was the cyber incident first detected, and by whom?
    - How was the incident reported and to whom?
    - What were the containment and eradication strategies employed?
    - How effective were the recovery processes?
    - What areas did the response team excel in?
    - Where can improvements be made for future incidents?

- **Analyze Regulatory Compliance:** For financial institutions, it's crucial to review whether all regulatory requirements were met during the incident response. This includes assessing if breach notifications were made within required timeframes and if the proper authorities were notified.

- **Evaluate Financial Impact:** Assess the financial impact of the incident, including direct costs (e.g., system repairs, customer notifications) and indirect costs (e.g., reputational damage, loss of business). This information can be valuable for justifying future cybersecurity investments.

- **Update Incident Response Plan:** Based on the insights gained from the review, update the incident response plan to address any gaps or inefficiencies identified. This might include refining communication protocols, adjusting escalation procedures, or updating containment strategies.

- **Enhance Training and Awareness:** Use the lessons learned to improve cybersecurity training programs for employees. Real-world examples from the incident can be particularly effective in illustrating the importance of security practices.

- **Review Third-Party Relationships:** If the incident involved or impacted any third-party vendors, review these relationships and consider whether additional security measures or contractual changes are needed.

- **Document Lessons Learned:** Create a formal "Lessons Learned" document that can be shared with relevant stakeholders and used to inform future incident response efforts. This document should include:
    - A summary of the incident
    - What went well in the response
    - Areas for improvement
    - Action items for enhancing future incident response capabilities

- **Conduct Follow-Up Assessments:** Schedule follow-up assessments to ensure that identified improvements are being implemented and are effective.

- **Share Information:** Consider sharing anonymized information about the incident with industry peers through information sharing organizations like FS-ISAC (Financial Services Information Sharing and Analysis Center). This collaborative approach can help strengthen the overall cybersecurity posture of the financial services sector.

By thoroughly executing the Lessons Learned phase, financial institutions can continuously improve their incident response capabilities, adapt to evolving threats, and demonstrate to regulators and customers their commitment to robust cybersecurity practices.

## Future Trends in Financial Services Incident Response

As the financial services sector continues to evolve, so too must incident response strategies. Looking ahead, several trends are likely to shape the future of incident response in the industry:

### Regulatory Evolution

As cyber threats evolve, so will the regulatory landscape:

- Real-Time Reporting: Regulators may require near real-time reporting of significant security incidents, necessitating more automated incident response processes.
- Cross-Border Coordination: International financial institutions will need to navigate an increasingly complex web of global cybersecurity regulations.
- Privacy Considerations: Incident response procedures will need to balance security requirements with evolving data privacy regulations.

Financial institutions should stay abreast of regulatory changes and ensure their incident response plans remain compliant.

### Cloud-Native Security and Incident Response

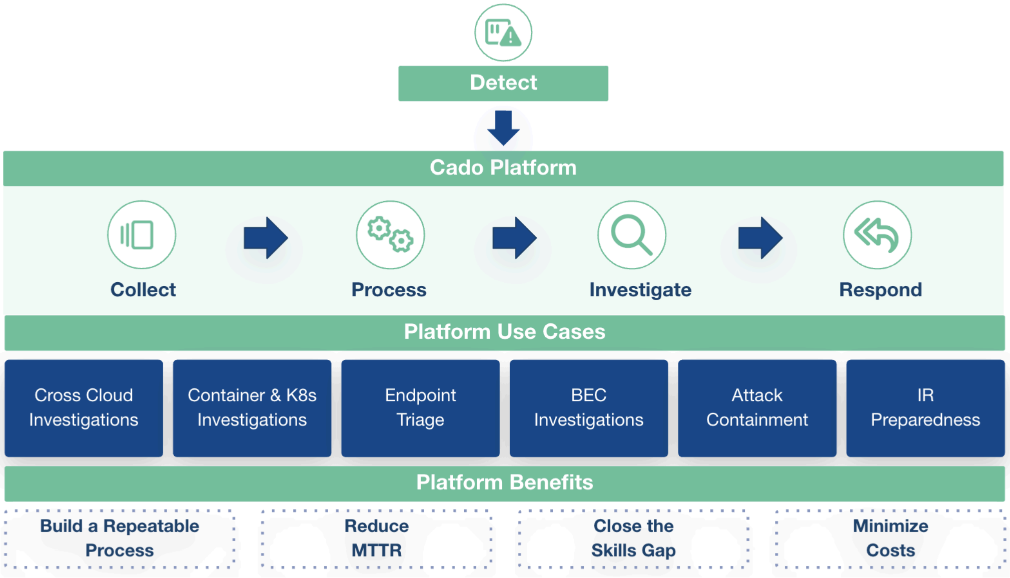
As financial institutions continue to migrate to cloud environments, incident response strategies will need to adapt:

- Cloud-Specific Tools: Incident response teams will need to become proficient with cloud-native security tools and services provided by major cloud platforms.
- Multi-Cloud Environments: Response plans must account for incidents that span multiple cloud providers and on-premises infrastructure.
- Serverless and Container Security: New approaches will be needed to detect and respond to incidents in serverless computing environments and container-based applications.

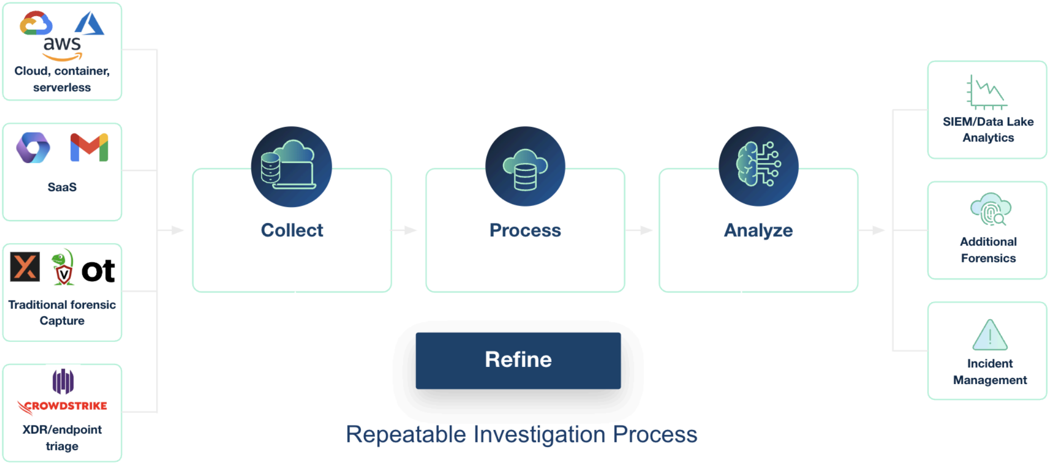
Financial institutions should ensure their incident response capabilities evolve alongside their cloud adoption strategies.

## How Cado Fits In

The Cado platform enables you to prepare for, respond to, and remediate incidents:



The Cado platform does this through enabling a repeatable investigation process during incidents:



## Ready to hear more about how Cado can help you be prepared for beaches? Try the Cado platform free trial.

**Start Your Free Trial**