DARKTRACE

Building an Incident Response Plan for Financial Services

darktrace.com

Introduction

In today's digital-first financial landscape, the threat of cyber-attacks 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 (IRP) is not just a good practice—it's an absolute necessity.

This comprehensive guide will walk you through the process of creating a tailored IRP 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.

Understanding the unique challenges for financial services

Before diving into the specifics of creating an IRP, 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.

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):** Focuses on resilience but also includes requirements around managing and disclosing incidents.

When creating your IRP, 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

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:

CASE STUDY

Capital One Data Breach (2019)[1]

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.

CASE STUDY

Equifax Data Breach (2017)[2]

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.

[1] Capital One, July 19, 2019, "Information on the Capital One Cyber Incident," Available at: https://www.capitalone.com/digital/facts2019/

[2] EPIC.org, September 2017, "Equifax Data Breach," Available at: https://archive.epic.org/privacy/data-breach/equifax/

CASE STUDY

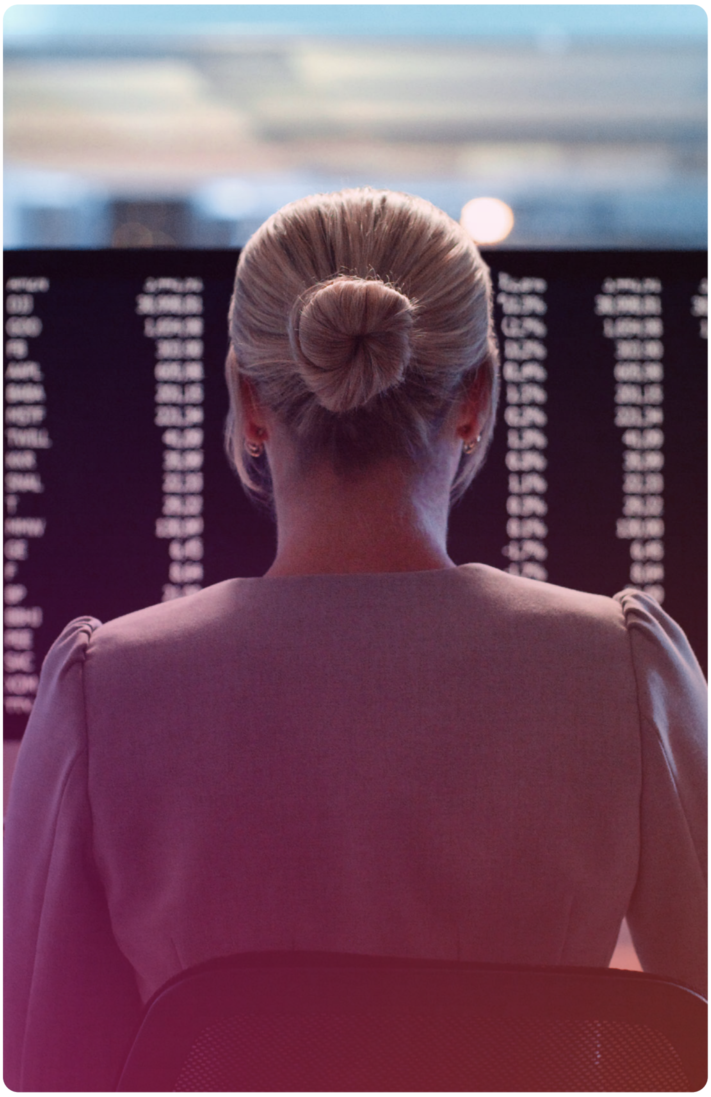
Bangladesh Bank Heist (2016)[3]

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 IRPs.

[3] Wikipedia, October 2023, "Bangladesh Bank robbery," Available at: https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery

Key components of an effective IRP

Developing a comprehensive IRP involves several critical steps and components, which can be broadly categorized as preparation, detection and analysis, containment, eradication, recovery, and post-incident activities.

1. Preparation

Preparation is the cornerstone of an effective IRP. It involves the identification and assessment of risks, as well as the establishment of policies, tools, and resources necessary for incident response.

Understanding potential threats and vulnerabilities is crucial for effective incident response planning.

Begin by identifying all critical assets, including hardware, software, networks, and data, and assess the risks associated with them. For financial institutions, this may include core banking systems, customer databases, trading platforms, payment processing systems, ATM networks, and online and mobile banking platforms. When looking for potential threats, make sure to check for internal, external, and third-party risks.

Create an incident response policy

Before diving into the specifics of an IRP, it's important to establish an overarching incident response policy. This policy should:

- Define what constitutes a security incident
- Outline roles and responsibilities for incident response
- Establish documentation and reporting requirements
- Provide a framework for classifying and prioritizing incidents

Start by drafting comprehensive policies that outline how to respond to various types of incidents. These documents should be clear, detailed, and accessible to all staff. Ensure that they cover all aspects of the incident response lifecycle, from detection to post-incident review, such as:

- 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

These policies and procedures will shape incident response playbooks, which include step-by-step response procedures, roles and responsibilities, communication templates, escalation criteria, regulatory reporting requirements, and evidence preservation guidelines.

Make sure to 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

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

Establish relationships with external partners and pre-negotiate contracts with key service providers to ensure rapid response capabilities:

- 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., Financial Services Information Sharing and Analysis Center (FS-ISAC))

Assemble an incident response team

Form a dedicated incident response team with clearly defined roles and responsibilities. This team should include individuals with the necessary skills and expertise to handle different types of incidents. Ensure 24/7 coverage and on-call procedures for the team.

For smaller organizations, this may be a central team. Larger financial services organizations may opt for a distributed model with multiple teams or a coordinating team that provides guidance. Consider creating specialized sub-teams for different types of incidents.

Key roles to consider include:

- 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)

Conduct training and testing

Regular training and testing are essential to ensure that the response team is prepared to handle real incidents.

Conduct tabletop exercises and simulated attacks to:

- Familiarize team members with the IRP
- 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.

02. Detection and analysis

The ability to detect and analyze threats swiftly is crucial. This phase involves the following components.

Monitoring systems: Implement robust monitoring tools and techniques to detect anomalies that may indicate a security incident. These systems should be capable of real-time alerts to enable rapid response.

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

Incident classification: Develop a framework for classifying incidents based on their severity and potential impact. This classification helps prioritize response efforts and allocate resources effectively. Create a tiered incident severity scale (e.g., Low, Medium, High, Critical) with clear definitions and response requirements for each level.

Incident reporting systems: Implement a streamlined process for employees, customers, and partners to report suspicious activities or potential incidents. This may include a 24/7 incident reporting hotline, an internal ticketing system, and an anonymous reporting channel for potential insider threats.

Threat intelligence: Use financial sector-specific threat intelligence feeds to stay informed about emerging threats and attack patterns, participate in information sharing organizations like FS-ISAC, and implement automated threat intelligence platforms to correlate external threat data with internal security events.

Regular security assessments: Perform frequent vulnerability scans and penetration tests, including network infrastructure, web applications and APIs, and third-party integrations.

Incident documentation: Maintain thorough records of all incidents, including time of occurrence, nature of the incident, and steps taken in response. This documentation is vital for post-incident analysis and compliance reporting.

03. Containment, eradication, and recovery

Once an incident is detected, the next steps involve containment, eradication, and recovery to prevent further damage and restore normal operations.

Containment strategies: Choose containment strategies based on the nature and severity of the incident. Immediate containment is crucial to prevent further damage. This can involve isolating affected systems, blocking malicious traffic, or disabling compromised accounts.

Assess the scope of the incident: Rapidly determine the extent of the breach or attack by identifying all affected systems and data, determining the number of impacted customers, assessing potential financial losses and regulatory implications, analyzing the attack vector and methodology used.

Short-term containment: Implement immediate actions to isolate affected systems and prevent the incident from spreading. This might include disconnecting systems from the network or blocking specific IP addresses.

Long-term containment: Develop a strategy for more sustainable containment, which may involve temporary fixes or workarounds that allow systems to operate securely while the issue is fully resolved.

Eradication: After containment, work on eliminating the root cause of the incident. This may involve removing malware, patching vulnerabilities, and addressing security weaknesses. Ensure that all affected systems are thoroughly cleaned and secured to prevent reinfection.

Recovery: Restore and validate system functionality.
This includes recovering data from backups, reinstalling compromised systems, and ensuring that all systems are fully operational and secure before they are brought back online.

04. Post-incident activities

Post-incident activities are essential for learning from the incident and improving future responses. These activities provide 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.

Incident review: Conduct a thorough review of the incident, including what happened, how it was handled, and what could be improved. This debriefing should involve all relevant stakeholders to gather diverse perspectives.

- **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 of improvement, and action items for enhancing future incident response capabilities.

Reporting and communication: Preserve evidence and document all containment actions in detail for internal review and external requirements. Communicate the incident and the response to all relevant parties, potentially including authorities and regulatory bodies, law enforcement, and legal counsel. This may also include media and customers if their data was compromised.

Analyze regulatory compliance: For financial institutions, it's critical 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.

Update policies and procedures: Based on the lessons learned, update your IRP and related policies to address any identified gaps or weaknesses. Continuous improvement is key to staying ahead of evolving threats.

Enhance training and awareness: In light of the recent incident, improve cybersecurity training programs for employees, especially because real-world examples from the incident can be particularly effective at 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.

Share information: Consider sharing anonymized information about the incident with industry peers through information sharing organizations like FS-ISAC. This collaborative approach can help strengthen the overall cybersecurity posture of the financial services sector.

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 IRPs 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 Darktrace can help

Darktrace delivers a multi-layered approach to cyber resilience in a single cybersecurity platform, helping teams stay proactive with their incident response planning, encompassing all phases: preparation, detection and analysis, containment, eradication, recovery, and post-incident activities.

For preparation, Darktrace understands your organization's unique risk profile, including an AI-based risk scoring system based on your specific technologies, firewall configurations, human communications patterns, CVEs, and MITRE adversary techniques, as well as your attack surface.

Darktrace / Proactive Exposure Management →

Darktrace / Attack Surface Management →

For detection, analysis, containment, and eradication, Darktrace brings unprecedented visibility, threat detection, investigation, and incident response to cloud, network, email systems, endpoints, identities, and Operational Technology (OT). Powered by multi-layered AI, Darktrace can identify known and unknown threats and autonomously respond at machine speed. Learn more:

Darktrace / CLOUD →

Darktrace / NETWORK →

Darktrace / EMAIL →

For recovery, Darktrace provides an AI-recovery and incident simulation engine that uplifts teams, optimizes incident response processes, and reduces the impact of active cyber-attacks using an understanding of your data. Learn more:

Darktrace / Incident Readiness & Recovery →

And forensics: Darktrace's offerings have been bolstered with the acquisition of Cado Security Ltd., which enables security teams to gain immediate access to forensic-level data in multi-cloud, container, serverless, SaaS, and on-premises environments. Learn more:

Darktrace / Forensic Acquisition & Investigation →

See Darktrace in action with a personalized meeting:

Request a demo →

■ About Darktrace

Darktrace is a global leader in AI for cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,400+ employees who protect nearly 10,000 customers globally. To learn more, visit http://www.darktrace.com.

North America: +1 (415) 229 9100 Europe: +44 (0) 1223 394 100 Asia-Pacific: +65 6804 5010 Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com