Ransomware Incident Response Runbook

Financial Services Enterprise Edition

Document Classification:	CONFIDENTIAL - Internal Use Only
Version:	2.1
Last Updated:	February 2026
Owner:	Information Security Team
Review Cycle:	Quarterly

Executive Summary

This runbook provides detailed procedures for responding to ransomware incidents affecting the organization's IT infrastructure. It is designed for security specialists, incident responders, and IT operations teams within a financial services environment.

Scope

- Detection and initial triage
- Containment strategies
- Eradication procedures
- Recovery operations
- Post-incident analysis and improvement

Critical Success Factors

- **Speed:** Initial response within 15 minutes of confirmed detection
- **Communication:** Stakeholder notification within 30 minutes
- **Containment:** Lateral movement stopped within 1 hour
- **Documentation:** All actions logged in ServiceNow with timestamps

Severity Classification

Level	Description	Response Time	Escalation
P1-Critical	Active encryption in production; customer data at risk	Immediate	CISO, CTO, CEO
P2-High	Ransomware detected but contained; limited spread	15 minutes	CISO, IT Director
P3-Medium	Ransomware artifacts detected; no active encryption	30 minutes	Security Manager
P4-Low	Suspicious activity; potential ransomware indicators	1 hour	Security Team Lead

Phase 1: Detection & Analysis

Objective: Identify ransomware activity quickly and accurately using multiple detection mechanisms.

1.1 CrowdStrike Falcon Detection

Primary Indicators:

- Real-time alerts for RansomwareDetection, SuspiciousProcess, MassFileEncryption
- Behavioral IOAs: Rapid file modifications, shadow copy deletion, VSSADMIN abuse
- Custom IOAs: Specific ransomware families (LockBit, BlackCat, Royal, ALPHV)

Investigation Steps:

1. Access Falcon Console → Investigate → Detections
2. Filter by Severity: Critical/High, Tactic: Impact (TA0040)
3. Review detection details: Process tree, file hashes (SHA256), network connections
4. Check 'Contain Host' status on affected endpoints
5. Export detection data for documentation

Key CrowdStrike Queries:

```
# Find potential ransomware processes
event_simpleName=ProcessRollup2
| search FileName IN ("*.exe","*.dll")
| where CommandLine LIKE "%shadow%" OR CommandLine LIKE "%vssadmin%"

# Detect mass file encryption
event_simpleName=FileWritten
| stats count by aid, FileName
| where count > 100 AND FileName LIKE "*.encrypted"

# Identify lateral movement
event_simpleName=NetworkConnectIP4
| search RemotePort IN (445,135,139,3389)
| stats dc(RemoteAddressIP4) by aid
```

1.2 Splunk SIEM Correlation

```
# Mass file modification detection
index=windows sourcetype=WinEventLog:Security EventCode=4663
| stats count by ComputerName, SubjectUserName
| where count > 500

# Suspicious PowerShell execution
index=windows EventCode=4104
| search ScriptBlockText IN ("*Invoke-WebRequest*", "*-enc*")
```

```
# VSS shadow copy deletion
index=windows sourcetype=WinEventLog:System EventCode=8222
| search Message="*shadow*delete*"

# Abnormal outbound connections
index=firewall action=allowed
| stats sum(bytes_out) as total_out by src_ip, dest_ip
| where total_out > 10000000
```

1.3 Initial Triage & Assessment (0-15 minutes)

- **Create ServiceNow Incident:** Category: Security Incident, Subcategory: Ransomware, Priority: Based on severity
- **Gather Initial Intelligence:** Affected systems count, user accounts, first detection timestamp, ransomware variant
- **Activate Incident Response Bridge:** Conference line, Slack/Teams channel, all team members join within 10 minutes
- **Initial Containment:** If single endpoint - contain in CrowdStrike immediately

Phase 2: Containment

Objective: Stop lateral movement and prevent further encryption while preserving evidence.

2.1 Network Isolation - Fortinet FortiGate

Create deny firewall policies to isolate affected subnets:

```
# FortiGate CLI Isolation Procedure
config firewall address
    edit "INFECTED_SUBNET_FINANCE"
        set subnet 10.20.30.0 255.255.255.0
        set comment "Ransomware quarantine - [Incident #]"
    next
end

config firewall policy
    edit 0  # Creates new policy at top
        set name "RANSOMWARE_QUARANTINE_[INCIDENT#]"
        set srcintf "port3"
        set dstintf "port1" "port2"
        set srcaddr "INFECTED_SUBNET_FINANCE"
        set dstaddr "all"
        set action deny
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

2.2 Endpoint Isolation - CrowdStrike

1. Falcon Console → Host Management → Hosts
2. Search for affected hostname or IP
3. Select host(s) → Actions → Contain Host
4. Confirm containment
5. **Note:** Contained hosts maintain CrowdStrike Cloud connection for RTR but cannot communicate with network

2.3 Active Directory Response

```
# Disable Affected User Accounts
$affectedUsers = @("jsmith", "mjones", "alee")

foreach ($user in $affectedUsers) {
    Disable-ADAccount -Identity $user
    Write-Host "[$(Get-Date)] Disabled account: $user"
}
```

```
# Force Kerberos ticket revocation
Invoke-Command -ComputerName DC01 -ScriptBlock {
    klist purge -li 0x3e7
}
```

2.4 Okta IAM Actions

1. Okta Admin Console → Directory → People
2. Search for affected users
3. Click user → More Actions → Suspend User
4. Sessions tab → Clear all sessions
5. Security Methods → Reset MFA
6. Create Okta group: RANSOMWARE_QUARANTINE_[DATE] and add users
7. Create policy to deny all access for this group

2.5 Backup System Protection

CRITICAL: Isolate backup infrastructure to prevent encryption spread.

```
# FortiGate - Protect Backup Servers
config firewall policy
    edit 0
        set name "PROTECT_BACKUP_SERVERS"
        set srcintf "port3"
        set dstintf "port4"  # Backup VLAN
        set srcaddr "INFECTED_SUBNET_FINANCE"
        set dstaddr "BACKUP_SERVERS"
        set action deny
        set service "ALL"
    next
end
```

Verify latest backups are clean (pre-infection):

```
# Veeam - Check backup integrity
Get-VBRBackup | Where-Object {$_.Name -like "*Finance*"} |
    Get-VBRRestorePoint |
    Sort-Object CreationTime -Descending |
    Select-Object -First 10 VmName, CreationTime
```

Phase 3: Eradication

Objective: Understand attack vector, timeline, and ensure complete removal of attacker access.

3.1 Forensic Analysis

Build complete attack timeline and identify root cause:

```
# Splunk - Build attack timeline
index=* (INFECTED_USERNAMES OR INFECTED_IPS)
| transaction maxspan=72h user, src_ip
| table _time, user, src_ip, action, object, result
| sort _time
```

3.2 Credential Reset Strategy

```
# Phase 1: Service Accounts
$serviceAccounts = @("svc_backup", "svc_monitoring", "svc_sql")

foreach ($account in $serviceAccounts) {
    $newPassword = -join ((33..126) | Get-Random -Count 32 |
        ForEach-Object {[char]$_})
    Set-ADAccountPassword -Identity $account -NewPassword
        (ConvertTo-SecureString $newPassword -AsPlainText -Force) -Reset
    Store-InCyberArk -Account $account -Password $newPassword
}

# Phase 2: User Accounts - Force password reset
$affectedUsers = Get-ADUser -Filter {Department -eq "Finance"}
foreach ($user in $affectedUsers) {
    Set-ADUser -Identity $user -ChangePasswordAtLogon $true
}
```

3.3 Persistence Removal

- **Scheduled Tasks:** Review and remove malicious tasks using Get-ScheduledTask
- **Registry Keys:** Check Run keys in HKLM and HKCU for malicious entries
- **Services:** Review non-Microsoft services for suspicious items
- **WMI Event Subscriptions:** Check WMI persistence mechanisms

3.4 Malware Removal

- **Option 1: System Rebuild (Recommended)** - Wipe and rebuild from trusted gold image for servers and highly compromised workstations

• **Option 2: In-place Remediation** - For workstations with minimal compromise: Delete malicious files, remove persistence, restore Defender, full scan

Phase 4: Recovery

Objective: Restore systems and data from clean backups in a controlled, phased manner.

4.1 Backup Restoration Strategy

Pre-Restoration Checklist:

- ■ Confirm threat actor access is removed
- ■ Verify backup integrity and cleanliness
- ■ Test restore to isolated environment first
- ■ Ensure systems are patched before restoration
- ■ CrowdStrike sensors active and monitoring
- ■ Network segmentation still in place for gradual release

Phased Restoration Approach:

- **Phase 1 (Hours 4-8):** Critical Infrastructure - Domain Controllers, DNS, DHCP, Email, File servers (read-only)
- **Phase 2 (Hours 8-16):** Business Critical Applications - SQL databases, application servers, UAT before production
- **Phase 3 (Hours 16-48):** User Data & Workstations - Prioritize by business criticality, clean rebuild preferred

SQL Server Database Restoration Example:

```
RESTORE DATABASE [FinancialDB]
FROM DISK = 'E:\Backups\FinancialDB_FULL_20260207.bak'
WITH NORECOVERY, REPLACE;

RESTORE LOG [FinancialDB]
FROM DISK = 'E:\Backups\FinancialDB_LOG_20260208.trn'
WITH RECOVERY,
STOPAT = '2026-02-08 13:00:00';  # Before encryption

DBCC CHECKDB ([FinancialDB]) WITH NO_INFOMSGS;
```

4.2 System Validation

Pre-Production Checklist (per system):

- ■ Operating system fully patched
- ■ All applications updated

■ CrowdStrike sensor installed and healthy

■ Windows Defender / AV enabled

■ Local admin password rotated

■ No malware detected (full scan)

■ No persistence mechanisms found

■ Logs forwarding to Splunk verified

■ Backup job configured and tested

4.3 Gradual Network Reintroduction

- **Hour 0-24:** Isolation with monitoring - Systems on isolated VLAN, enhanced monitoring, UAT
- **Hour 24-48:** Limited production access - Specific outbound only, full UTM inspection
- **Hour 48-72:** Full production (if clean) - Remove restrictions, return to normal policies
- **First 30 Days:** Continuous monitoring - Daily CrowdStrike hunts, weekly vulnerability scans

Phase 5: Post-Incident Activities

Objective: Learn from the incident and implement improvements to prevent recurrence.

5.1 Lessons Learned Session

Timing: Within 7 days of incident closure

Attendees: Incident response team, executive leadership, business unit leaders, external partners

Agenda:

- Incident Overview (15 min) - Timeline, attack vector, impact, financial cost
- What Went Well (20 min) - Detection mechanisms, effective actions, team collaboration
- What Didn't Go Well (30 min) - Detection gaps, delayed responses, communication breakdowns
- Root Causes (20 min) - Technical vulnerabilities, process weaknesses, training gaps
- Action Items (30 min) - Immediate, short-term, and long-term improvements with owners and dates

5.2 Process Improvements

Immediate (0-30 Days):

- Deploy advanced email security (Proofpoint TAP) - $50K
- Expand CrowdStrike to 100% coverage - $40K
- Implement immutable backups - $25K
- Update playbooks based on lessons learned - $0

Short-Term (1-3 Months):

- Deploy PAM solution (CyberArk) - $200K
- Implement network micro-segmentation - $150K
- Refresh security awareness training - $30K
- Enhance SIEM with UEBA - $40K

Long-Term (3-12 Months):

- Zero Trust Architecture implementation - $500K
- Enhance SOC maturity (+2 FTE, 24/7 coverage) - $300K/year
- Full DR site with real-time replication - $400K

• Cyber insurance review - Premium increase $50K

Success Metrics

Metric	Current	6 Month Target	12 Month Target
Mean Time to Detect	30 min	10 min	5 min
Mean Time to Respond	2 hours	1 hour	30 min
Phishing Click Rate	12%	5%	<3%
EDR Coverage	85%	100%	100%
Backup Success Rate	95%	99%	99.9%
MFA on Privileged Accounts	60%	100%	100%

Communication Protocols

Internal Communication

Initial Notification (Within 30 minutes):

TO: Incident Response Team | METHOD: ServiceNow + Email + SMS + Phone

```
Subject: URGENT - Security Incident Declared - Ransomware

INCIDENT ALERT
Severity: P1 - Critical
Type: Ransomware
Status: Active Response

Join Incident Response Bridge:
Phone: [BRIDGE NUMBER] PIN: [PIN]
Zoom: [LINK]
Slack: #incident-response-[date]

Initial Details:
- Detection Time: [TIME]
- Affected Systems: [SYSTEMS]
- Current Status: Containment in progress
- Incident Commander: [NAME]

Required Actions:
- Join bridge immediately
- Review triage in ServiceNow
- Stand by for assignments
```

Executive Notification (Within 30 minutes):

- TO: CISO, CTO, CEO, General Counsel
- Executive summary: Detection, scope, customer impact, containment status
- Immediate actions being taken
- Executive actions required: Approve expenditures, prepare for board notification
- Confidentiality reminder

Staff Communication (Affected Departments):

```
Subject: IT Service Interruption - [Department]

Dear Team,

We are experiencing a technical issue affecting [systems].
Our IT team is working to resolve this as quickly as possible.

What to do:
- Save work locally or to OneDrive
```

- Report unusual computer behavior to IT Security: [NUMBER]

What NOT to do:
- Do not shut down your computer if working normally
- Do not click suspicious emails or links
- Do not discuss on social media

Updates every 2 hours. Next update at [TIME].

Regulatory & Legal Considerations

Legal Hold

When to Implement: All ransomware incidents with potential litigation or regulatory investigation

Scope of Preservation:

- Emails (sent, received, drafts, deleted)
- Documents (Word, Excel, PDF)
- Instant messages (Slack, Teams)
- System logs and database records
- Handwritten notes, text messages

Cyber Insurance Claims

Step 1: Initial notification within 24 hours - Policy #, date of loss, type of incident

Step 2: Detailed claim submission within 30-60 days - Claim forms, forensics report, financial impact

Coverage Typically Includes: Incident response costs, forensics, legal fees, business interruption

Deductible: $25,000 (per occurrence typical)

Documentation Required: Forensics invoice, legal counsel invoice, business interruption worksheet

Law Enforcement Coordination

FBI IC3: File complaint at https://www.ic3.gov - Include incident details, financial loss, suspect information

Local FBI Field Office: Contact cyber squad for investigation assistance

Cooperation: Provide technical evidence, logs, malware samples, timeline

Important: Do NOT pay ransom without FBI consultation

Regulatory Requirements (Financial Services)

APRA CPS 234 Compliance (Australia):

- Materiality Assessment: Evaluate impact on services, customer data, data integrity, availability
- Notification: Within 72 hours for material incidents (voluntary notification recommended even if borderline)
- Detailed Report: Within 10 business days

- Final Update: Once fully remediated

Appendices

Appendix A: 24/7 Contact Lists

Maintain up-to-date contact information for:

- Incident Response Team (Commander, Security Analyst Lead, Network Engineer, Systems Admin, IAM Specialist)
- Executive Leadership (CISO, CTO, CEO, General Counsel)
- External Vendors (Forensics firm, breach counsel, cyber insurance, CrowdStrike, Fortinet)

Appendix B: Tool Access Quick Reference

CrowdStrike Falcon: https://falcon.crowdstrike.com - Okta SSO (MFA required)

Splunk: https://splunk.company.com - Okta SSO

Fortinet FortiGate: Management IP - Admin accounts in CyberArk

ServiceNow: Security incident category, Security IR assignment group

Okta Admin Console: Super admin accounts, API tokens

Appendix C: Common Ransomware TTPs (MITRE ATT&CK;)

Tactic	Technique	ID	Detection
Initial Access	Phishing	T1566	Email gateway alerts
Execution	Malicious File	T1204	EDR process monitoring
Persistence	Registry Run Keys	T1547	Registry monitoring
Defense Evasion	Disable AV	T1562	EDR prevention alerts
Credential Access	LSASS Memory	T1003	EDR memory protection
Lateral Movement	Remote Services	T1021	Unusual RDP logins
Impact	Data Encryption	T1486	Mass file modifications

Appendix D: Key Takeaways

Detection is Critical: Use CrowdStrike EDR and Splunk SIEM for multi-source detection within 15 minutes

Containment Speed: Isolate network with FortiGate policies and contain endpoints with CrowdStrike within 1 hour

Protect Backups: Isolate backup infrastructure immediately - it's your recovery lifeline

Reset All Credentials: Service accounts, user accounts, local admin - assume all are compromised

Document Everything: ServiceNow incident tracking with timestamps for compliance and lessons learned

Don't Pay Ransom: Company policy - no payment under any circumstances (requires Board approval for exceptions)

Validate Before Production: Full security validation before returning systems to production

Learn and Improve: Lessons learned within 7 days, implement improvements to prevent recurrence

Document Control

Author:	Information Security Team
Classification:	CONFIDENTIAL - Internal Use Only
Distribution:	Incident Response Team, Executive Leadership
Review Frequency:	Quarterly or after each incident
Next Review Date:	[To be scheduled]
Version History:	v2.1 - February 2026 - Created enterprise runbook
Contact:	security@company.com