TTXLAB

FULL REPORT

Ransomware Incident Response — Enterprise Payment Systems

Comprehensive board-grade report including operational performance, risk context, and remediation path.

62/100

MATURITY	CONFIDENCE	DURATION
Developing	moderate (2.2)	1h 30m

EXERCISE ID	SCENARIO TYPE	RISK GAPS	RECOMMENDATIONS
IR-20260312-A1B2C3	ir	5	4

STARTED	ENDED	DECISION CADENCE	PARTICIPATION
3/12/2026, 7:00:00 AM	3/12/2026, 8:30:00 AM	3.3/hr	80%

Executive Snapshot

Board scan in under 60 seconds

VALIDITY	OPEN CAP	BLOCKED CAP
moderate (68)	3	1

Top 3 Board Risks

1. Ransomware recovery timeline exceeds 72-hour RTO due to unverified backup integrity
2. PCI DSS breach notification deadline missed due to delayed regulatory coordination
3. Reputational damage from delayed or inconsistent customer communications

Top 3 Required Actions

1. Establish Ransomware-Specific Escalation Playbook (open)
2. Add Backup Integrity Verification to IR Checklist (open)
3. Implement Pre-Staged Breach Notification Templates (open)

Validity note: Scenario fidelity is moderate — the ransomware inject sequence was realistic but lacked lateral movement complexity.

BOARD ACTION FOCUS

The top remediation action is "Establish Ransomware-Specific Escalation Playbook".

DEVELOPING — INDEX 2

The organization operates at a Developing maturity level (index 2 of 4), indicating that core incident response capabilities exist but rely on ad hoc decision-making rather than documented, repeatable processes. Escalation criteria and regulatory notification workflows require formalization before the next scheduled exercise.

Export Tier: Full Report · Audience: Security, operations, and governance teams. Contents: Complete analysis, timelines, findings, roadmap, and appendices. When to use: Implementation planning and internal program reviews.

SECTION 1

Executive Summary

Decision-ready synthesis of performance, risk, and priority actions

SITUATION

The organization demonstrated competent initial detection and containment of a ransomware event targeting payment infrastructure, achieving network isolation within 15 minutes of the first alert — wel...

KEY RISK

Critical gaps in escalation policy, regulatory notification sequencing, and backup verification introduce material risk of extended recovery timelines and regulatory exposure in a live incident.

PRIORITY ACTION

The board should prioritize funding a ransomware-specific escalation playbook and pre-staged breach notification templates within 30 days to close the highest-impact gaps identified.

BOARD DECISION AGENDA — NEXT 90 DAYS

1. Establish Ransomware-Specific Escalation Playbook

Owner: CISO · Deadline: 30 days · Impact: High risk reduction

Rationale: The team lacked documented criteria for ransomware response decisions, including negotiation stance, law enforcement notification tr...

2. Add Backup Integrity Verification to IR Checklist

Owner: IT Operations Lead · Deadline: 30 days · Impact: High risk reduction

Rationale: Team assumed backup viability without verification. A mandatory backup validation step in the containment checklist would prevent re...

3. Implement Pre-Staged Breach Notification Templates

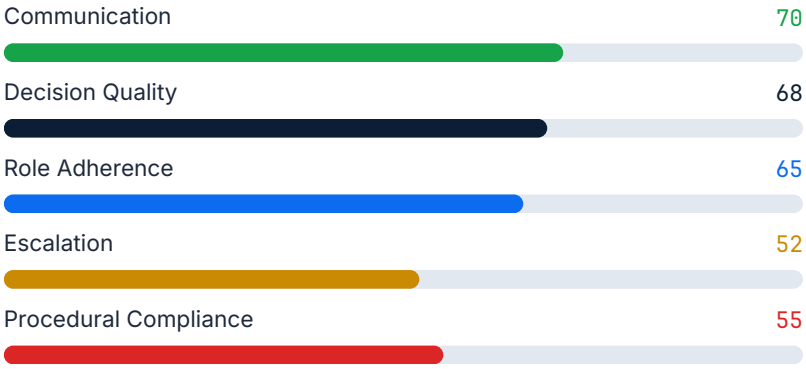
Owner: Communications Lead · Deadline: 60 days · Impact: High risk reduction

Rationale: Communications Lead spent significant time drafting notifications from scratch during the exercise. Pre-approved templates for commo...

SECTION 2

Readiness Scorecard

Dimension-level assessment and confidence calibration



Confidence	moderate (2.2)
Duration	1h 30m
Decision cadence	3.3/hr
Participation	80%

SECTION 3

Key Findings

Dimension-level strengths, gaps, and evidence anchors

escalation · 52/100

Escalation to Sev-1 was fast, but subsequent escalation steps — particularly regulatory notification and vendor access revocation — were delayed or omitted.

Evidence: evt-3, evt-8

procedural compliance · 55/100

The team followed general incident response procedures but lacked ransomware-specific checklists. Backup verification and vendor credential review were not included in containment steps.

Evidence: evt-4, evt-6

role adherence · 65/100

Most participants stayed within their assigned roles. Legal counsel remained passive throughout; proactive legal guidance on notification timelines would have strengthened the response.

Evidence: evt-3, evt-7

decision quality · 68/100

Key decisions were sound — the Sev-1 declaration was prompt and the no-negotiation stance aligned with industry best practices. Decision documentation could be improved for post-incident review.

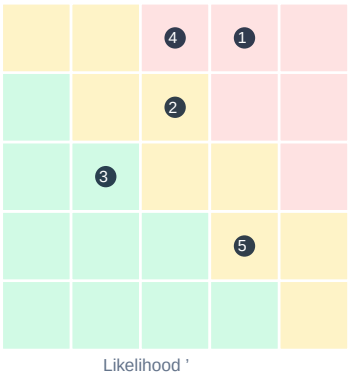
Evidence: evt-3, evt-6

SECTION 4

Risk Exposure

Likelihood–impact distribution of highest-priority gaps

Likelihood × Impact



1. No documented escalation criteria for ransomware-specific demands
2. Regulatory notification timeline not established until 32 minutes into the exercise
3. No pre-established communication templates for customer notification
4. Backup validation was not performed before confirming recovery capability
5. Vendor VPN access review was not part of the initial containment checklist

SECTION 4

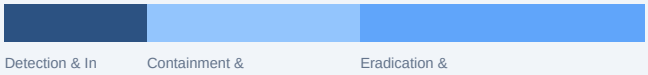
Critical Decision Timeline

What happened, when it happened, and who drove key moves

0m	Detection & Initial Triage	FACILITATOR	Exercise begins. Scenario: SOC detects unusual outbound traffic from payment processing server.
3m	Detection & Initial Triage	FACILITATOR	INJECT: 4.2 GB transferred to an unknown external IP in the last 90 minutes.
7m	Detection & Initial Triage	Incident Commander	Declaring this a Severity 1 incident. Immediate containment: isolate the payment server.
15m	Detection & Initial Triage	IT Operations Lead	Payment server isolated from production network. No lateral movement detected. Starting forensic image.
25m	Containment & Forensics	FACILITATOR	INJECT: Ransomware note discovered. Threat actor demands 50 BTC within 48 hours.
32m	Containment & Forensics	CISO	We do not negotiate. Focus on confirming exfil scope, activating CrowdStrike retainer, preparing PCI DSS notification.
50m	Eradication & Recovery Planning	Communications Lead	Draft holding statement prepared. Recommending we wait for legal clearance before issuing.

70m	Eradication & Recovery Planning	FACILITATOR	INJECT: CrowdStrike confirms exfiltration of ~12,000 payment card records via compromised vendor VPN credential.
80m	Eradication & Recovery Planning	Legal Counsel	PCI DSS requires notification within 24 hours of confirmed breach. We need to engage the card brands immediately.
85m	Eradication & Recovery Planning	Incident Commander	Closing exercise. Key follow-ups: finalize notification timeline, schedule backup integrity review, revoke vendor VPN credentials.

Phase Duration



SECTION 5

Recommendations & Roadmap

Prioritized actions with ownership, sequencing, and expected risk reduction

#	Recommendation	Priority	Owner	Deadline	Effort	Risk Red.
1	Establish Ransomware-Specific Escalation Playbook	critical	CISO	30d	M	high
2	Add Backup Integrity Verification to IR Checklist	high	IT Operations Lead	30d	S	high
3	Implement Pre-Staged Breach Notification Templates	high	Communications Lead	60d	S	medium
4	Conduct Quarterly Vendor Access Reviews	medium	IT Operations Lead	90d	M	medium

0–30 days

1. Establish Ransomware-Specific Escalation Playbook
2. Add Backup Integrity Verification to IR Checklist

31–60 days

1. Implement Pre-Staged Breach Notification Templates

61–90 days

1. Conduct Quarterly Vendor Access Reviews

SECTION 6

Comparative Trend

Performance movement versus prior exercises and closure trajectory

Baseline exercise — no prior data available for comparison.

Overall Score improving

Communication improving

Decision Quality improving

Escalation improving

Procedural Compliance improving

SECTION 7

Participant Accountability Register

Engagement levels and continuity across the exercise window

Name	Role	Joined	Dropped	Messages	Engagement
Sarah Mitchell	Incident Commander	3/12/2026, 6:55:00 AM	–	3	0.92
James Rivera	Communications Lead	3/12/2026, 6:56:00 AM	–	1	0.45
Karen Liu	Legal Counsel	3/12/2026, 6:58:00 AM	–	0	0.15
Daniel Park	IT Operations Lead	3/12/2026, 6:57:00 AM	–	1	0.58
Maria Chen	CISO	3/12/2026, 6:59:00 AM	–	1	0.72

SECTION 8

Scoring Methodology

How readiness was measured and normalized for comparability

Weighted score dimensions: communication=20%, decision_quality=25%, role_adherence=20%, escalation=15%, procedural_compliance=20%. Confidence and validity both combine evidence density, participation coverage, role diversity, hotwash completion, and planned-vs-actual duration.

Confidence thresholds: High (≥ 2.5), Moderate (1.8–2.49), Low (< 1.8).

SECTION 9

Regulatory Mapping

Framework alignment references for audit and governance workflows

NIST_CSF

Controls: DE.CM-01, RS.AN-03, RS.CO-02, RC.CO-01

Recommendations: rec-001, rec-002

ISO_22301

Controls: 8.4.3, 8.4.4, 8.5

Recommendations: rec-003

SOC2
Controls: CC7.3, CC7.4, CC7.5

Recommendations: rec-001, rec-004

SECTION 10

Source Traceability

Verified external references used to shape report framing and structure

Scoring methodology and readiness dimensions
Source: NIST Cybersecurity Framework 2.0 · https://www.nist.gov/cyberframework

Incident timeline interpretation and handling cadence
Source: NIST SP 800-61r2 · https://csrc.nist.gov/pubs/sp/800/61/r2/final

Preparedness and response control coverage framing
Source: CISA Resources · https://www.cisa.gov/resources-tools/resources

Board-level risk communication framing
Source: Deloitte Cyber Risk · https://www.deloitte.com/us/en/services/consulting/services/cyber-risk.html

Governance and accountability narrative structure
Source: EY Cybersecurity · https://www.ey.com/en_us/services/cybersecurity

Executive summary document formatting conventions
Source: Smartsheet Executive Summary Examples · https://www.smartsheet.com/content/executive-summary-examples

SECTION A

Appendix A — Full Annotated Timeline

Condensed event log for board and audit reference

Timeline entries are condensed in this PDF. See Transcript PDF for full message text.

Elapsed	Phase	Actor	Type	Content
0m	Detection & Initial Triage	AI Facilitator	system_notice	Exercise begins. Scenario: SOC detects unusual outbound traffic from payment processing server.
3m	Detection & Initial Triage	AI Facilitator	facilitator_inject	INJECT: 4.2 GB transferred to an unknown external IP in the last 90 minutes.
7m	Detection & Initial Triage	Sarah Mitchell	user_message	Declaring this a Severity 1 incident. Immediate containment: isolate the payment server.
15m	Detection & Initial Triage	Daniel Park	user_message	Payment server isolated from production network. No lateral movement detected. Starting forensic image.
25m	Containment & Forensics	AI Facilitator	facilitator_inject	INJECT: Ransomware note discovered. Threat actor demands 50 BTC within 48 hours.
32m	Containment & Forensics	Maria Chen	user_message	We do not negotiate. Focus on confirming exfil scope, activating CrowdStrike retainer, preparing PCI DSS notification.
50m	Eradication & Recovery Planning	James Rivera	user_message	Draft holding statement prepared. Recommending we wait for legal clearance before issuing.

70m	Eradication & Recovery Planning	AI Facilitator	facilitator_inject	INJECT: CrowdStrike confirms exfiltration of ~12,000 payment card records via compromised vendor VPN credential.
80m	Eradication & Recovery Planning	Karen Liu	user_message	PCI DSS requires notification within 24 hours of confirmed breach. We need to engage the card brands immediately.
85m	Eradication & Recovery Planning	Sarah Mitchell	user_message	Closing exercise. Key follow-ups: finalize notification timeline, schedule backup integrity review, revoke vendor VPN credentials.

SECTION D

Appendix D — Role Swim-Lane Timeline

Role-level pacing, sequencing, and escalation markers

SECTION E

Appendix E — Remediation Gantt

30/60/90/180 delivery horizon by recommendation priority