IRON DICE
CYBER READINESS TABLETOP

Cyber Tabletop Exercise

After-Action Report

Prepared for: IronDice Casino

Sample After-Action Report

Fictional Exercise Data

Executive Summary

This after-action report summarizes the tabletop exercise conducted for IronDice Casino. The scenario simulated a ransomware incident affecting casino operations, leadership decision-making, communication effectiveness, and technical containment. The exercise was designed to evaluate how the organization responds under pressure when operational continuity, regulatory reporting, guest trust, and strategic judgment collide.

Incident Narrative Summary

The exercise began with unusual technical behavior that gradually evolved into a confirmed ransomware attack. Participants were required to distinguish fact from assumption while coordinating an increasingly complex response.

The team used available logs, alerts, and security telemetry to investigate the incident and improve its understanding of the attack's scope.

Containment measures were initiated to restrict unauthorized access and reduce the likelihood of further spread.

The response gained structure as the team activated the Incident Response Plan and assigned an Incident Commander, improving accountability, urgency, and decision ownership.

Leadership improved situational awareness by establishing an incident timeline, helping connect technical conditions with business consequences.

Communication extended across executive leadership and external stakeholders, supporting coordinated legal, insurance, regulatory, and business decisions.

The team began considering continuity and recovery measures, indicating movement from immediate response toward restoration of stable operations.

Overall, the exercise revealed meaningful readiness gaps that should be addressed through clearer escalation paths, stronger investigation practices, and continued cross-functional training.

Exercise Overview

Casino	IronDice Casino
Session	Sample Exercise Tabletop Session
Scenario	Ransomware Incident
Start	8/16/2026, 10:50:25 AM
End	8/16/2026, 11:13:57 AM

IRON DICE
CYBER READINESS TABLETOP

Participants

- Bob — IT Support
- Mary — Network Administrator
- George — System Admin
- Sheila — Security Admin
- Michael — IT Director
- Joe — Chief Information Officer
- Dawn — General Manager

Crisis Maturity Index (CMI) Results

The Crisis Maturity Index (CMI) measures how effectively the team performed across five dimensions of crisis leadership: detection, decision-making, communications, containment, and strategic judgment.

CMI Score Gauge: 68 / 150

Raw Score: 68 | Available Score: 150 | Participants: 7

Needs Improvement 0–79	Moderate 80–109	High Capability 110–150

Assessment: Needs Improvement

The normalized score indicates that crisis readiness needs improvement within the portions of the exercise that were demonstrated. The strongest observed areas were detection and analysis, technical containment, communication and escalation, decision-making, and strategic risk judgment. Areas not meaningfully demonstrated included none of the core CMI dimensions. This score is normalized to a 150-point scale based on 68 points earned out of 150 available points for the roles and scenario conditions active in this session.

NIST CSF 2.0 Alignment

NIST CSF 2.0 alignment summarizes earned exercise points across Govern, Identify, Protect, Detect, Respond, and Recover functions based on scored actions, communications, and facilitator adjustments.

Function	Score	Alignment
Govern	29 / 56	52%
Identify	Not Evaluated	N/A
Protect	14 / 21	67%
Detect	22 / 58	38%
Respond	44 / 56	79%
Recover	5 / 8	63%

IRON DICE
CYBER READINESS TABLETOP

NIST Category Detail

NIST Function	NIST Area	Capability	Score	Alignment
Detect	DE.AE	Adverse Event Analysis	21 / 44	48%
Detect	DE.CM	Continuous Monitoring	1 / 14	7%
Govern	GV.OV	Organizational Oversight	3 / 6	50%
Govern	GV.RM	Risk Management Strategy	0 / 3	0%
Govern	GV.RR	Roles & Responsibilities	26 / 47	55%
Protect	PR.AA	Identity & Access Control	12 / 12	100%
Protect	PR.DS	Data Security	0 / 3	0%
Protect	PR.PS	Platform Security	2 / 6	33%
Recover	RC.RP	Recovery Planning	5 / 8	63%
Respond	RS.CO	Incident Communications	36 / 48	75%
Respond	RS.MA	Incident Mitigation	1 / 1	100%
Respond	RS.RP	Response Planning	7 / 7	100%

NIST Functional Analysis

Govern, which reflects executive oversight, decision authority, risk ownership, and organizational accountability, showed moderate alignment during the exercise. The strongest related capability was Roles & Responsibilities (GV.RR) at 55%. The lowest related capability was Risk Management Strategy (GV.RM) at 0%.

Identify was not evaluated during this exercise. The NIST CSF Identify function measures organizational preparedness before an incident begins, including understanding critical assets, business dependencies, and organizational risk. Because this exercise focused on investigating an uncertain intrusion that developed into ransomware, meaningful opportunities to influence this function were limited. This does not indicate poor performance, but rather that these capabilities are established before an incident occurs.

Protect, which reflects access control, system safeguards, data protection, and preventive security measures, showed moderate alignment during the exercise. The strongest related capability was Identity & Access Control (PR.AA) at 100%. The lowest related capability was Data Security (PR.DS) at 0%.

Detect, which reflects recognizing abnormal activity, analyzing indicators, and maintaining visibility during the incident, showed limited alignment during the exercise. The strongest related capability was Adverse Event Analysis (DE.AE) at 48%. The lowest related capability was Continuous Monitoring (DE.CM) at 7%.

Respond, which reflects incident communications, response coordination, escalation, and execution of response procedures, showed strong alignment during the exercise. The strongest related capability was Response Planning (RS.RP) at 100%. The lowest related capability was Incident Communications (RS.CO) at 75%.

Recover, which reflects restoration planning, recovery coordination, and returning operations to a stable state, showed moderate alignment during the exercise. The strongest related capability was Recovery Planning (RC.RP) at 63%.

IRON DICE
CYBER READINESS TABLETOP

Performance Pattern Analysis

Across the exercise, team performance declined as pressure intensified. Average round performance was 11.3 points. The strongest recurring dimension was Decision Discipline, while the most persistent challenge area was Detection & Awareness. Score volatility was high, suggesting the team's response pattern was reactive and uneven across rounds.

Round	Detection & Awareness	Decision Discipline	Communication Control	Technical Containment	Strategic Risk Judgment	Bonus / Penalty	Round Score
1	3/5	4/5	3/5	5/5	0/5	0	15

Manual Score Contribution: 0
Auto Score Contribution: 21

Round	Detection & Awareness	Decision Discipline	Communication Control	Technical Containment	Strategic Risk Judgment	Bonus / Penalty	Round Score
2	5/5	5/5	5/5	4/5	0/5	-2	17

Manual Score Contribution: 0
Auto Score Contribution: 36

Round	Detection & Awareness	Decision Discipline	Communication Control	Technical Containment	Strategic Risk Judgment	Bonus / Penalty	Round Score
3	0/5	5/5	5/5	2/5	5/5	1	18

Manual Score Contribution: 0
Auto Score Contribution: 31

Round	Detection & Awareness	Decision Discipline	Communication Control	Technical Containment	Strategic Risk Judgment	Bonus / Penalty	Round Score
4	0/5	4/5	4/5	3/5	5/5	-2	14

Round	Detection & Awareness	Decision Discipline	Communication Control	Technical Containment	Strategic Risk Judgment	Bonus / Penalty	Round Score
5	0/5	1/5	1/5	1/5	0/5	0	3

Manual Score Contribution: 0
Auto Score Contribution: 3
Automatic Scoring Events:

Round	Detection & Awareness	Decision Discipline	Communication Control	Technical Containment	Strategic Risk Judgment	Bonus / Penalty	Round Score
6	0/5	0/5	0/5	0/5	1/5	0	1

Manual Score Contribution: 0
Auto Score Contribution: 1

IRON DICE
CYBER READINESS TABLETOP

Executive Action Items

The following priority actions were generated from improvement opportunities observed during this exercise.

- Review alerts carefully to distinguish legitimate threats from false positives while documenting findings.
- Define alert triage procedures and escalation thresholds.
- Perform organization-wide IOC hunting during significant incidents rather than limiting investigations to known affected devices.
- Document results and update containment decisions based on findings.

Property Follow-Up Checklist

During the exercise, your team selected the following actions in response to the scenario. These choices reflect expected real-world behavior under pressure. For each item below, confirm that the capability exists, is documented, and can be executed when needed.

- ☐ Do you know where to look for indicators of compromise (logs, SIEM, EDR)?
- ☐ Do you have endpoint visibility across critical systems?
- ☐ Is your SIEM actively monitored or just collecting data?
- ☐ Do you know how to identify a clean recovery point?
- ☐ Do you validate backups before restoration?
- ☐ Do you have an Incident Response Plan (IRP/IDR)?
- ☐ Do staff know when and how to invoke it?
- ☐ Is it tested regularly?
- ☐ Do you know your recovery point (RPO) and recovery time (RTO)?
- ☐ Are your backups immutable (locked for a defined period)?
- ☐ Do you know where backups are stored and who has access?
- ☐ Do you have pre-approved messaging templates for incidents?
- ☐ Do you have a public communication plan?
- ☐ Who is authorized to speak during an incident?
- ☐ Do you know your cyber insurance coverage and notification requirements?
- ☐ Do you understand breach notification requirements?
- ☐ Is legal integrated into your response plan?

IRON DICE
CYBER READINESS TABLETOP

Task Coordination Analysis

Task coordination evaluated the team's ability to delegate work, execute assigned responsibilities, and report completion back through the incident command structure. 13 tasks reached a final state during this exercise.

Task Results: 12 completed | 1 work completed but not reported | 0 incomplete | 0 expired without assignment.

Verify backup recovery points are uncompromised

Result: COMPLETED

Assigned By: General Manager

Assigned To: System Admin

Assigned Round: Round 2

Completed Task Actions: Isolate Backup Recovery Point

The assigned work was completed and the result was reported back through the task chain.

Task Score: 3 / 3

Contain a suspected compromised privileged account

Result: COMPLETED

Assigned By: IT Director

Assigned To: System Admin

Assigned Round: Round 1

Completed Task Actions: Disable Account, Revoke Sessions

The assigned work was completed and the result was reported back through the task chain.

Task Score: 3 / 3

Review security evidence to determine the scope of ransomware activity

Result: COMPLETED

Assigned By: IT Director

Assigned To: Security Admin

Assigned Round: Round 2

Completed Task Actions: Review EDR Logs, Review SIEM

The assigned work was completed and the result was reported back through the task chain.

Task Score: 3 / 3

Isolate affected endpoints to limit ransomware spread

Result: COMPLETED

Assigned By: Security Admin

Assigned To: Network Administrator

Assigned Round: Round 2

Completed Task Actions: Isolate Endpoint

The assigned work was completed and the result was reported back through the task chain.

Task Score: 3 / 3

Build an incident timeline for executive decision-making and external response

Result: COMPLETED

Assigned By: General Manager

Assigned To: Chief Information Officer

Assigned Round: Round 3

Completed Task Actions: Create Timeline

The assigned work was completed and the result was reported back through the task chain.

Task Score: 3 / 3

Trace suspicious network activity and identify affected network paths

Result: COMPLETED

Assigned By: Security Admin

Assigned To: Network Administrator

Assigned Round: Round 1

Completed Task Actions: Run Network Tracing, Review Logs

The assigned work was completed and the result was reported back through the task chain.

Task Score: 3 / 3

Prepare an executive incident summary after gathering operational and technical impact information

Result: COMPLETED

Assigned By: General Manager

Assigned To: Chief Information Officer

Assigned Round: Round 3

Completed Task Actions: Write Executive Summary

The assigned work was completed and the result was reported back through the task chain.

Task Score: 3 / 3

Run diagnostics and review logs after restoring a critical system

Result: COMPLETED

Assigned By: IT Director

Assigned To: System Admin

Assigned Round: Round 4

Completed Task Actions: Run Diagnostic Tools, Review Logs

The assigned work was completed and the result was reported back through the task chain.

Task Score: 3 / 3

Collect and review endpoint logs for signs of suspicious activity

Result: COMPLETED

Assigned By: IT Director

Assigned To: IT Support

Assigned Round: Round 2

Completed Task Actions: Collect Logs, Review Logs

The assigned work was completed and the result was reported back through the task chain.

Task Score: 3 / 3

Secure a user account suspected of being compromised

Result: COMPLETED

Assigned By: IT Director

Assigned To: IT Support

Assigned Round: Round 3

Completed Task Actions: Disable Account, Revoke Sessions

The assigned work was completed and the result was reported back through the task chain.

Task Score: 3 / 3

Take a suspected compromised workstation out of service

Result: COMPLETED

Assigned By: Chief Information Officer

Assigned To: IT Support

Assigned Round: Round 5

Completed Task Actions: Shutdown Computer, Remove Computer

The assigned work was completed and the result was reported back through the task chain.

Task Score: 3 / 3

Coordinate incident notification to the Tribal Gaming Agency and Tribal Council

Result: COMPLETED

Assigned By: General Manager

Assigned To: Chief Information Officer

Assigned Round: Round 4

The assigned work was completed and the result was reported back through the task chain.

Task Score: 3 / 3

Notify the cyber insurance carrier and confirm response requirements

Result: COMPLETED

Assigned By: IT Director

Assigned To: Chief Information Officer

Assigned Round: Round 3

Completed Task Actions: Talk With Insurance

The assigned work was completed and the result was reported back through the task chain.

Task Score: 3 / 3

Collect security logs for investigation, insurance, and legal review

Result: AWAITING REPORT

Assigned By: General Manager

Assigned To: Security Admin

Assigned Round: Round 2

Completed Task Actions: Collect Logs

Task Score: 2 / 3

Coordination Observation

The team successfully demonstrated the complete task coordination lifecycle by assigning work, executing required activities, and reporting completion back through the incident command structure.

Final Decision Analysis

Decision: Pay

Roll: 3

Additional payment demanded.

Knowledge Assessment

Strengths Demonstrated

Disable Account

Compromised account access was contained by promptly disabling affected user accounts, limiting opportunities for continued unauthorized access.

Facilitator Insight: Disabling an account is often faster and less disruptive than shutting down an entire system. Early credential containment can stop an attacker from moving further into the environment.

Revoke Sessions

Active user sessions were revoked, immediately reducing the attacker's ability to maintain unauthorized access.

Facilitator Insight: Password resets alone may not remove an attacker's access. Terminating active sessions forces reauthentication and immediately reduces ongoing risk.

IRON DICE
CYBER READINESS TABLETOP

Collect Logs

Log collection activities were completed, providing investigators with the evidence needed to understand the scope and timeline of the incident.

Facilitator Insight: Logs are one of the first things investigators need and one of the first things attackers often try to erase. Preserve them before making significant system changes.

Review Logs

Log analysis was performed to validate attacker activity, identify affected systems, and support informed containment decisions.

Facilitator Insight: Good responders do not guess. They verify. Reviewing logs frequently reveals how the attacker entered, what they touched, and whether they are still active.

Isolate Endpoint

Endpoint isolation procedures were effectively used to contain the incident while preserving valuable evidence for analysis.

Facilitator Insight: Isolation is often the safest first containment action. It stops communication without sacrificing valuable evidence.

Run Network Tracing

Network tracing provided valuable insight into communication paths and helped identify potentially affected systems.

Facilitator Insight: Following the network often reveals compromised systems you did not know existed. Think beyond the first infected machine.

Run Diagnostic Tools

Diagnostic tools were used to distinguish operational issues from security-related events, improving decision quality.

Facilitator Insight: Do not assume every outage is a cyberattack, and do not assume every cyberattack explains every outage. Diagnostics help separate symptoms from root cause.

Review EDR Logs

Endpoint Detection and Response telemetry was reviewed to improve visibility into attacker behavior and affected systems.

Facilitator Insight: Your EDR platform often knows more than any single administrator. Use it to understand attacker behavior instead of relying on assumptions.

Review SIEM

SIEM monitoring and event correlation were used to improve situational awareness across the environment.

Facilitator Insight: A SIEM connects the dots across the environment. Looking at a single system rarely tells the whole story.

Isolate Backup Recovery Point

Backup recovery points were protected, helping preserve reliable recovery options throughout the incident.

Facilitator Insight: Attackers increasingly target backups before deploying ransomware. Protect your recovery before you need your recovery.

Restore Backup

Backup restoration capabilities were successfully exercised, demonstrating confidence in organizational recovery procedures.

Facilitator Insight: Backups are not valuable because they exist. They are valuable because you have already proven they can be restored.

Incident Response Plan Activation

The Incident Response Plan was formally activated, providing structure, accountability, and coordinated response efforts.

Facilitator Insight: A plan sitting on a shelf is only paperwork with ambition. The important moment is when someone formally activates it and moves the organization into response mode.

Incident Commander

An Incident Commander was clearly established, providing centralized leadership and coordinated decision-making.

Facilitator Insight: The Incident Commander does not have to be the most technical person in the room. They need to keep the response organized, decisions moving, and communication clear.

Coordinate Team Efforts

Response teams coordinated effectively across technical and business functions, reducing duplication and improving response efficiency.

Facilitator Insight: The best technical response can still fail if teams are not working from the same priorities and timeline.

Incident Timeline

A detailed incident timeline was maintained, supporting accurate documentation, investigation, and executive reporting.

Facilitator Insight: The timeline becomes the organization's memory when the room gets noisy. Without it, everyone is forced to reconstruct the incident from fragments later.

Write Executive Summary

Executive leadership received timely status updates that supported informed business decisions during the exercise.

Facilitator Insight: Executives do not need a technical briefing. They need the current business impact, response progress, major risks, and decisions requiring leadership attention.

IRON DICE
CYBER READINESS TABLETOP

Ownership Notification

Ownership was notified appropriately, allowing executive leadership to provide strategic oversight throughout the incident.

Facilitator Insight: Ownership does not need every technical detail before being notified. They need timely awareness when business operations, financial exposure, reputation, or public trust may be affected.

Cyber Insurance Notification

Cyber insurance resources were engaged appropriately, ensuring access to policy benefits and specialized response support.

Facilitator Insight: Insurance notification is not just about filing a claim. It may unlock approved vendors, legal resources, and response guidance at the exact moment the organization needs help.

Work with Legal

Legal counsel participated appropriately, supporting regulatory compliance and informed decision-making.

Facilitator Insight: Legal should not be treated as a last step before public notification. They are part of the response structure when data exposure, regulatory obligations, or public statements may be involved.

Talk with Media

Media communications were managed through authorized channels, protecting organizational credibility.

Facilitator Insight: The media will often report what they know before you are ready. Having an approved spokesperson protects credibility.

Craft Public Message

Public messaging was carefully developed to balance transparency with operational security.

Facilitator Insight: The first public statement often shapes public perception. Prepare it carefully, but do not wait for every technical detail before communicating.

General Manager Notification

The General Manager remained informed throughout the exercise, enabling timely business decisions and organizational coordination.

Facilitator Insight: The General Manager doesn't need every technical detail. They need enough information to make informed business decisions and keep the organization aligned.

IT Director Notification

The IT Director maintained effective oversight of technical response activities and resource coordination.

Facilitator Insight: The IT Director should never discover a major incident secondhand. They should be one of the first leadership roles engaged.

Operations Leadership Notification

Operations leadership actively participated in recovery planning, helping align technical efforts with business priorities.

Facilitator Insight: Technology supports the casino. Operations runs it. Recovery decisions should always consider operational impact alongside technical recovery.

Security Team Notification

Security personnel maintained continuous communication throughout the investigation, improving threat visibility and containment.

Facilitator Insight: Security teams should never be playing catch-up during an incident. They should be helping drive the investigation from the beginning.

System Administration Notification

System Administrators remained engaged throughout the response, supporting infrastructure stability and recovery efforts.

Facilitator Insight: Recovery starts with infrastructure. The earlier System Administrators understand the situation, the sooner recovery planning can begin.

Network Administration Notification

Network Administrators provided valuable infrastructure visibility and containment support during the exercise.

Facilitator Insight: The network often tells the story of the attack. Early involvement helps identify additional affected systems before the attacker moves further.

Tribal Council Notification

Tribal Council received appropriate executive briefings, supporting governance and organizational oversight.

Facilitator Insight: Tribal leadership needs business awareness, not technical jargon. Focus on impact, risk, and executive decisions.

Tribal Gaming Agency Notification

Regulatory communications were appropriately considered, demonstrating awareness of gaming compliance responsibilities.

Facilitator Insight: Regulators dislike surprises more than bad news. Early, accurate communication builds trust and demonstrates sound governance.

Insurance Carrier Notification

The cyber insurance carrier was engaged appropriately, ensuring access to available response resources and policy support.

Facilitator Insight: Insurance notification isn't just about filing a claim. It may unlock experts who can significantly improve the response.

IRON DICE
CYBER READINESS TABLETOP

Legal Counsel Notification

Legal Counsel participated throughout the exercise, supporting compliance, risk management, and informed executive decision-making.

Facilitator Insight: Legal should be part of the response team, not simply the reviewers of the press release after decisions have already been made.

Opportunities for Improvement

Contact External SOC

Opportunity: External security resources were not engaged during the exercise.

Why it Matters: External security providers often have specialized expertise and additional visibility that internal teams may not possess.

Recommendations:

• Define escalation criteria for involving third-party incident response partners early in significant events.

• Maintain current contact information and engagement procedures for external security support.

Facilitator Insight: One of the best decisions an organization can make is recognizing when additional expertise is needed. Early escalation often shortens recovery time.

Analyze Alerts

Opportunity: Security alert analysis was not exercised during the exercise.

Why it Matters: Security alerts provide early indicators of malicious activity and help responders prioritize their efforts.

Recommendations:

• Review alerts carefully to distinguish legitimate threats from false positives while documenting findings.

• Define alert triage procedures and escalation thresholds.

Facilitator Insight: Every alert deserves context before action. Responding too slowly increases risk, while responding too quickly to false positives wastes valuable time.

Hunt IOC

Opportunity: Threat hunting for indicators of compromise was not exercised during the exercise.

Why it Matters: Searching for indicators of compromise helps determine whether attackers have spread beyond initially identified systems.

Recommendations:

• Perform organization-wide IOC hunting during significant incidents rather than limiting investigations to known affected devices.

• Document results and update containment decisions based on findings.

IRON DICE

CYBER READINESS TABLETOP

Facilitator Insight: Finding one infected system rarely means you have found the entire attack. Hunt for evidence that the compromise spread elsewhere.

Recommend Isolation

Opportunity: Containment recommendations were not provided during the exercise.

Why it Matters: Timely recommendations from security personnel help leadership make informed containment decisions before an incident expands.

Recommendations:

• Define clear authority for recommending containment actions during active incidents.

• Ensure security teams know when to escalate isolation recommendations to leadership.

Facilitator Insight: Security teams should clearly recommend containment actions, even if leadership ultimately makes the decision.

Recommend Insurance Notification

Opportunity: Cyber insurance notification recommendations were not discussed during the exercise.

Why it Matters: Many cyber insurance policies require prompt notification to preserve coverage and provide access to approved response resources.

Recommendations:

• Review policy notification requirements before an incident occurs.

• Include insurance notification recommendations in incident response procedures.

Facilitator Insight: Insurance notification is not simply paperwork. It can immediately expand the resources available to your organization.

Recommend Legal Notification

Opportunity: Legal notification recommendations were not discussed during the exercise.

Why it Matters: Legal counsel helps determine regulatory obligations, preserve privilege, and reduce organizational liability.

Recommendations:

• Engage legal counsel early whenever data exposure or regulatory reporting may be involved.

• Include legal escalation criteria in incident response playbooks.

Facilitator Insight: Security teams do not need to interpret regulations, but they should recognize when legal expertise is needed and recommend involving counsel early.

Declare Incident Severity

Opportunity: Incident severity was not formally established during the exercise.

Why it Matters: Classifying incident severity establishes response priorities and determines which resources should be engaged.

Recommendations:

• Use predefined severity criteria to ensure incidents are classified consistently.

• Tie severity levels to escalation, notification, and resource requirements.

Facilitator Insight: Severity drives response. Without an agreed classification, every department may respond at a different level of urgency.

Document Business Continuity Posture

Opportunity: Business continuity status was not documented during the exercise.

Why it Matters: Understanding operational readiness allows leadership to prioritize resources and maintain essential business functions.

Recommendations:

• Assess continuity capabilities throughout the incident.

• Document changing operational risks and recovery dependencies.

Facilitator Insight: Technical recovery and business recovery are not always the same thing. Leadership needs visibility into both.

Manage Communications

Opportunity: Centralized communication management was not exercised during the exercise.

Why it Matters: Centralized communications prevent conflicting messages and maintain organizational credibility.

Recommendations:

• Assign a single communications lead responsible for coordinating internal and external messaging.

• Use approved messaging channels and review processes during significant incidents.

Facilitator Insight: When everyone becomes the spokesperson, nobody controls the message. Centralized communications reduce confusion and misinformation.

Issue Public Statement

Opportunity: Public communication procedures were not exercised during the exercise.

Why it Matters: Timely public statements reduce speculation and reassure guests, employees, and stakeholders.

Recommendations:

• Issue public communications only after key facts have been confirmed and leadership approves the messaging.

• Coordinate public statements with legal counsel, executive leadership, and communications staff.

Facilitator Insight: Silence creates a vacuum that rumors quickly fill. Timely, accurate communication helps preserve confidence even during difficult events.

Finance Leadership Notification

Opportunity: The Director of Finance was not notified during the exercise.

Why it Matters: Cyber incidents often create financial risk through business interruption, fraud, insurance claims, vendor payments, and recovery costs. Finance leadership plays a critical role in managing these risks.

Recommendations:

• Notify Finance whenever financial exposure or payment processes may be affected.

• Coordinate financial impact assessments and insurance claim activities with Finance leadership.

Facilitator Insight: Finance is often focused on keeping money flowing while attackers are trying to redirect it. Early awareness helps prevent costly mistakes.

IT Support Notification

Opportunity: The IT Support Desk was not notified during the exercise.

Why it Matters: The IT Support Desk often receives the first reports from employees experiencing suspicious activity and becomes the primary communication point for end users.

Recommendations:

• Provide the Service Desk with approved messaging and escalation procedures.

• Ensure Help Desk staff understand current incident status and reporting expectations.

Facilitator Insight: Your Help Desk becomes your eyes and ears during an incident. Give them the information they need before the phones start ringing.

Exercise Summary

This tabletop exercise evaluated organizational decision-making, communication, and incident response capabilities based on the participating roles and the scenario presented. The observations and recommendations contained in this report should be used to strengthen operational readiness, refine incident response procedures, and guide future tabletop exercises.

Cyber resilience is not measured by the absence of incidents, but by an organization's ability to recognize, contain, communicate, and recover when they occur. Every exercise provides an opportunity to improve readiness before a real incident tests those capabilities.