Northgate Engineering Ltd

IR-PLAY-001

Classification

Internal Use

Document Owner

Rachel Okafor

Approved By

David Whitfield

Effective Date

March 1, 2026

Northgate Engineering Ltd

Core Incident Response Playbooks

Cyber Incident Response Toolkit

Six attack-specific operational guides for the most common cybersecurity incident types.

Table of Contents

Introduction

This document contains six attack-specific playbooks that supplement the general Incident Response Procedure (IR-PROC-001). Each playbook addresses a high-frequency, high-impact attack type and provides responders with pre-defined detection indicators, containment decision trees, eradication steps, recovery validation criteria, and communication requirements specific to that attack type.

These playbooks are designed to be used during active incidents by the Incident Response Team (IRT) and Crisis Management Team (CMT). They assume the general response lifecycle defined in IR-PROC-001 is being followed and provide attack-specific guidance at each phase. Responders should have the relevant playbook available (printed or digital) alongside the role-specific checklists from IR-CHECK-001 during active response.

Playbook Index

#	Playbook	Typical Severity	Key Differentiator
1	Ransomware / Encryption Attack	P1–P2	Assume double extortion. Isolate before investigate. Insurance engagement critical within 1 hour.
2	Business Email Compromise (BEC)	P1–P3	Time-critical financial recovery. Wire recall window is 24–72 hours. Legal and bank engagement immediate.
3	Data Breach / Exfiltration	P2–P3	Regulatory notification clock starts at awareness. Evidence preservation for legal proceedings paramount.
4	Insider Threat	P2–P3	HR and Legal coordination from outset. Covert investigation may precede overt containment.
5	Distributed Denial of Service (DDoS)	P2–P3	May be smokescreen for concurrent attack. Engage ISP/CDN provider immediately.
6	Supply Chain Compromise	P1–P2	Scope expands rapidly. Vendor coordination essential. May affect multiple organisations simultaneously.

How to Use These Playbooks

When an incident is classified in IR-CLASS-001 and matched to one of the six playbook types, the Incident Commander should direct the IRT to follow the relevant playbook in conjunction with IR-PROC-001. The playbook does not replace the general procedure; it provides attack-specific detail within the same five-phase lifecycle. Where the playbook specifies an action that differs from the general procedure, the playbook takes precedence for that incident type. Each playbook follows a consistent structure: Threat Profile (understand the attack), Detection Indicators (recognise it), Immediate Actions (first 60 minutes), Containment Decision Tree (stop it), Eradication Steps (remove it), Recovery Validation (verify it’s gone), Communication Requirements (notify stakeholders), and Lessons Learned Focus Areas (improve from it).

Playbook 1: Ransomware / Encryption Attack

This playbook covers ransomware incidents including single-extortion (encryption only), double-extortion (encryption plus data theft), and triple-extortion (encryption, data theft, plus DDoS or customer harassment). The modern ransomware threat landscape is dominated by ransomware-as-a-service (RaaS) groups that typically gain access days or weeks before deploying encryption, exfiltrating data during the pre-encryption dwell period.

1.1 Threat Profile

Attribute	Detail
Attack objective	Encrypt victim data to extort payment. Increasingly combined with data theft for double leverage. Some groups additionally threaten DDoS or direct contact with customers/partners.
Typical initial access	Phishing email with malicious attachment or link, exploitation of internet-facing vulnerabilities (VPN appliances, RDP, web applications), compromised credentials purchased from initial access brokers, or abuse of legitimate remote access tools.
Dwell time before encryption	Median 5–14 days (varies by group). Attackers use this time to: escalate privileges, move laterally, identify and disable backups, exfiltrate data, and stage encryption tools across maximum endpoints.
Common MITRE ATT&CK techniques	T1566 (Phishing), T1190 (Exploit Public-Facing App), T1078 (Valid Accounts), T1021 (Remote Services for lateral movement), T1486 (Data Encrypted for Impact), T1490 (Inhibit System Recovery), T1048 (Exfiltration Over Alternative Protocol)
Business impact	Complete operational shutdown possible. Recovery timeline ranges from days (well-prepared, current backups) to weeks or months (poor backup posture, complex environment). Financial impact includes response costs, business interruption, potential ransom payment (not recommended), regulatory fines, and reputational damage.
Insurance considerations	Most cyber insurance policies require immediate notification (within hours, not days). Insurer will typically assign their own IR vendor and legal counsel. Payment of ransom requires insurer approval and sanctions screening. Failure to notify promptly may void coverage.

1.2 Detection Indicators

The following indicators may signal ransomware activity at various stages of the attack lifecycle. Early detection during the pre-encryption phase dramatically reduces impact.

Stage	Indicator	Detection Source
Initial access	Phishing email delivered and attachment opened or link clicked. Exploitation of known vulnerability on internet-facing asset. Anomalous VPN or RDP login from unusual geography or at unusual time.	Email security logs, EDR alerts, VPN/authentication logs, vulnerability scanner
Privilege escalation	Use of credential dumping tools (Mimikatz, LaZagne, comsvcs.dll). Creation of new	EDR process telemetry, Active Directory audit logs, SIEM correlation

	administrator accounts. Modification of Group Policy Objects. DCSync or DCShadow activity against domain controllers.	
Lateral movement	Multiple RDP connections between internal systems. PsExec or WMI remote execution. SMB connections to administrative shares (C$, ADMIN$). Anomalous use of IT management tools (remote desktop, deployment tools).	Network traffic analysis, EDR lateral movement alerts, authentication logs
Backup destruction	Volume Shadow Copy deletion (vssadmin delete shadows). Backup agent stopped or uninstalled. Backup repository permissions modified. Backup server targeted for encryption or deletion.	Backup monitoring alerts, EDR process monitoring, Windows event logs (Event ID 524)
Data exfiltration	Large outbound data transfers to cloud storage (Mega, Dropbox, anonymised endpoints). Use of archive tools (7-Zip, WinRAR) on large file collections. DNS tunnelling or encrypted channel to unknown endpoints. Unusual after-hours data access patterns.	DLP alerts, proxy/firewall logs, network traffic analysis, cloud access security broker
Encryption deployment	Ransom note files appearing (README.txt, DECRYPT_FILES.html, etc.). File extensions changed to unknown types (.encrypted, .locked, custom extensions). Rapid sequential file modification across multiple directories. CPU and disk I/O spike across multiple systems simultaneously.	EDR alerts, file integrity monitoring, user reports, system performance monitoring

1.3 Immediate Actions — First 60 Minutes

These actions shall be executed in sequence upon confirmation of ransomware activity. Speed is critical: every minute of delay allows further encryption and data loss.

Step	Action	Owner	Target Time
1	ISOLATE affected systems from the network immediately. Use EDR network quarantine, disable switch ports, or physically disconnect. Do NOT power off systems — volatile memory contains encryption keys and process evidence.	IT/Security Lead	0–10 min
2	CLASSIFY the incident in IR-CLASS-001. Ransomware is typically P1 Critical (if business-critical systems affected) or P2 High. When in doubt, classify as P1.	Incident Commander	5–15 min
3	ACTIVATE full CMT for P1, partial for P2. Distribute role-specific checklists from IR-CHECK-001.	Incident Commander	10–20 min
4	NOTIFY insurance broker immediately (P1: within 1 hour). Provide: date/time of discovery, initial scope, whether data exfiltration is suspected. Insurer will assign IR vendor and legal counsel.	Executive Sponsor	Within 60 min

5	ASSESS backup status. Determine: Are backups accessible? Are they known to be uncompromised? What is the most recent clean backup date? Are offline/immutable backups available? Do NOT attempt restoration yet.	IT Operations	15–45 min
6	PRESERVE evidence. Capture memory dumps from affected systems (before any remediation). Begin evidence log per IR-EVID-001. Preserve email gateway logs, VPN logs, and authentication logs from the past 30 days.	IT/Security Lead	15–60 min
7	IDENTIFY ransomware variant if possible. Check ransom note for group identification. Upload encrypted file sample to ID Ransomware (id-ransomware.malwarehunterteam.com) or No More Ransom (nomoreransom.org). Known variant identification may reveal available decryptors.	IT/Security Lead	30–60 min
8	DETERMINE scope. How many systems are affected? Is encryption still active/spreading? Are domain controllers compromised? Has Active Directory integrity been verified?	IT/Security Lead	30–60 min
9	ESTABLISH out-of-band communication. Do NOT use corporate email if Exchange/M365 may be compromised. Use personal mobile phones, non-corporate messaging, or a pre-established emergency communication channel.	Communications Lead	0–15 min
10	ASSESS data exfiltration indicators. Review proxy/firewall logs for large outbound transfers in the days preceding encryption. Assume double extortion until evidence indicates otherwise.	IT/Security Lead	30–60 min

1.4 Containment Decision Tree

The Incident Commander shall work through the following decision points in sequence to determine the appropriate containment strategy:

Decision Point	If YES	If NO
Is encryption still actively spreading?	IMMEDIATE: Isolate all network segments where encryption is active. If segment boundaries are unclear, isolate the entire environment from the internet and implement internal segment isolation. Speed over precision.	Proceed to next decision point. Encryption may have completed or been triggered on a timer.
Are domain controllers compromised?	CRITICAL ESCALATION: AD compromise means the attacker has full environment control. Isolate DCs immediately. Plan for full AD rebuild or restoration from known-good backup. Engage specialist AD recovery vendor (insurer will typically provide). All credentials must be considered compromised.	Verify DC integrity with forensic analysis before relying on AD for recovery operations.
Is data exfiltration confirmed	Block identified exfiltration channels	Continue monitoring for exfiltration

or suspected?	(IPs, domains, cloud storage endpoints). Preserve network logs showing exfiltration evidence. Notify Legal/Compliance Lead immediately — regulatory notification clock may have started. Notify insurance broker of data exposure.	indicators. Do not assume no exfiltration has occurred; confirm through log analysis.
Are backups intact and usable?	Protect backups immediately: disconnect backup infrastructure from network, verify backup integrity, identify most recent clean restore point. Backups are the primary recovery path.	Engage insurer-assigned IR vendor to assess decryption options. Do NOT contact the threat actor directly without legal counsel and insurance approval. Evaluate feasibility of rebuild from installation media.
Is the initial access vector identified?	Close the access vector immediately (patch vulnerability, disable compromised VPN, block phishing infrastructure). If not closed, the attacker may re-enter during recovery.	Prioritise identification. Common vectors: internet-facing VPN/RDP vulnerability, phishing email, compromised credentials. Review logs for initial compromise indicators.

1.5 Eradication Steps

Step	Action	Verification
1	Identify and close the initial access vector. Patch exploited vulnerability, disable compromised accounts, block attacker infrastructure at firewall.	Access vector confirmed closed. No active inbound connections from attacker infrastructure.
2	Remove all ransomware binaries, scripts, and tools from affected systems. Check startup items, scheduled tasks, services, Group Policy, WMI subscriptions, and registry run keys.	EDR scan confirms no malicious artifacts. Manual verification of persistence locations on all affected hosts.
3	Eliminate all attacker persistence mechanisms. Remove backdoor accounts, revoke implanted certificates, delete web shells, remove malicious GPOs, revoke OAuth tokens.	Full persistence audit completed. No unauthorised accounts, certificates, or scheduled tasks remain.
4	Reset ALL domain credentials if AD compromise confirmed. Execute KRBTGT reset (twice, 12 hours apart). Reset all service account passwords. Invalidate all Kerberos tickets and NTLM hashes.	Credential rotation completed and verified. Golden ticket and silver ticket attacks mitigated by KRBTGT reset.
5	Rebuild or restore affected systems from known-good backups or clean media. Do NOT attempt to decrypt-in-place and continue using compromised systems for P1/P2 incidents.	Systems rebuilt/restored. Post-restoration integrity scan clean.
6	Verify network segmentation and monitoring. Ensure enhanced detection is in place for indicators associated with this specific ransomware group/variant.	Detection rules deployed. Network segmentation verified. Monitoring confirmed operational.

1.6 Recovery Validation

Validation Check	Criteria	Owner
System integrity	All recovered systems scanned with current EDR signatures. No indicators of compromise. No unexpected network connections, processes, or services.	IT/Security Lead
Data integrity	Restored data verified against known-good checksums or business logic validation. Random sampling of restored files confirms they are uncorrupted and complete.	IT Operations + Business Owner
Credential security	All compromised credentials rotated. MFA re-enrolled for affected users. Service account passwords changed. Break-glass credentials rotated.	IT/Security Lead
Backup integrity	Backup infrastructure reconnected with enhanced protection (immutable backups, offline copies, separate credentials). Next scheduled backup completes successfully.	IT Operations
Detection enhancement	Specific IOCs from this incident added to detection rules. Enhanced monitoring in place for ransomware-associated TTPs. Alert thresholds reviewed.	IT/Security Lead
Business validation	All business-critical applications functional. Customer-facing services operational. Business owners confirm acceptable performance and data accuracy.	Business Owners

1.7 Communication Requirements

Audience	Timing	Key Messages
Insurance broker	Within 1 hour of discovery (P1). Do not delay for full scope.	Date/time discovered, initial scope, systems affected, suspected data exfiltration, whether ransom demand received, need for IR vendor and legal counsel assignment.
Executive leadership	Within 30 minutes (P1). Every 2–4 hours thereafter.	Business impact, estimated recovery timeline, whether customer data at risk, financial exposure estimate, insurance engagement status, any ransom demand (amount and response recommendation).
All staff	Within 4 hours if staff-facing systems affected.	What systems are unavailable, expected duration, what staff should and should not do (do not attempt to access affected systems, do not open suspicious emails, report anything unusual), alternative work arrangements if applicable.
Customers	Only after legal counsel approval. Timing depends on regulatory obligations and confirmed data exposure.	What happened (high-level), whether their data is affected, what protective steps they should take, how to contact Northgate Engineering Ltd with concerns. Do NOT speculate about scope before confirmation.
Regulators	Per regulatory deadlines tracked in IR-CLASS-001. GDPR: 72 hours. Others per jurisdiction.	Nature of breach, categories/numbers of data subjects, likely consequences, measures taken. Use templates from IR-COMMS-001.

Law enforcement	Consider engagement for: known criminal group, financial loss >$50,000, nation-state attribution, if recommended by insurer or legal counsel.	Incident summary, timeline, indicators of compromise, estimated financial impact. Coordinate through Legal/Compliance Lead.

1.8 Ransom Payment Considerations

RidgeLine Cyber Defence does not recommend paying ransoms. Payment funds criminal operations, does not guarantee data recovery or deletion of stolen data, and may expose the organisation to sanctions risk. However, the decision to pay or not pay is ultimately a business decision that must be made by the organisation's leadership with legal counsel and insurance broker involvement. If payment is being considered, the following must be confirmed before any payment: legal counsel has confirmed there are no sanctions prohibitions on payment to the identified threat actor; the insurance broker has been consulted and payment is covered under the policy terms; senior leadership has formally approved the decision in writing; and a qualified third-party negotiator (typically assigned by the insurer) is engaged to manage communications with the threat actor. Direct communication with the threat actor without legal counsel and negotiator involvement is strongly discouraged.

1.9 Lessons Learned Focus Areas

The post-incident review for ransomware incidents should specifically address: how long was the attacker in the environment before detection (dwell time), and what detection capabilities could have identified the intrusion earlier; were backups adequate (frequency, integrity testing, offline/immutable copies, separation from production credentials); was the initial access vector preventable with existing controls, and what additional controls would mitigate it; was network segmentation sufficient to limit lateral movement; and how effective was the organisation's communication and decision-making under the pressure of a P1 incident.

Playbook 2: Business Email Compromise (BEC)

This playbook covers BEC incidents including CEO/CFO impersonation fraud, vendor invoice manipulation, payroll diversion, gift card scams, and account takeover leading to internal BEC. BEC is the highest-financial-loss cybercrime category globally, with losses frequently exceeding the cost of ransomware incidents. The critical differentiator is the time-sensitive nature of financial recovery: wire transfers can often be recalled within 24–72 hours, but success rates drop sharply after that window.

2.1 Threat Profile

Attribute	Detail
Attack objective	Trick employees into transferring funds, redirecting payments, or disclosing sensitive information by impersonating trusted parties (executives, vendors, legal counsel, HR).
Typical attack methods	Email spoofing (display name or domain lookalike), compromised legitimate email accounts (credential phishing or password spray), man-in-the-middle interception of email threads, phone call social engineering reinforcing email requests.
Common scenarios	CEO urgency fraud ('wire £250K to this account for a confidential acquisition'), vendor invoice modification (altered bank details on legitimate-looking invoices), payroll diversion (employee requests HR change direct deposit to new account), real estate wire fraud (intercepted property transactions).
Financial exposure	Median BEC loss ranges from £25,000 to £500,000+ per incident. Some incidents exceed £10 million. Losses are frequently unrecoverable after the 72-hour wire recall window.
Detection difficulty	BEC emails often contain no malware, no malicious links, and no attachments — they evade traditional email security controls entirely. Detection relies on behavioural analysis, employee awareness, and financial controls (dual authorisation for wire transfers).

2.2 Detection Indicators

Category	Indicator	Detection Source
Email spoofing	Display name matches executive but sender domain differs (e.g., ceo@company-corp.com vs ceo@company.com). Reply-to address differs from sender. DMARC failure on inbound email. Lookalike domain registered recently (domain age <30 days).	Email gateway DMARC reports, email header analysis, domain monitoring services
Account compromise	Impossible travel alerts (login from two distant locations within impossible timeframe). Inbox rules created to forward or delete emails (attackers hide their activity). Mail sent from compromised account to external addresses with attachments. Password reset followed by unfamiliar login.	Azure AD / Entra ID sign-in logs, mailbox audit logs, impossible travel alerts, inbox rule audit
Financial request anomalies	Urgent wire transfer request bypassing normal approval process. Request to change vendor bank details. Request sent outside normal business hours or during executive absence. Request references 'confidential' or 'do not discuss with others'. New payee account in a different country than expected.	Employee reports, financial process controls, email content inspection
Thread hijacking	Reply to an existing email thread but from a different (spoofed) sender address. Subtle changes to email thread content (modified bank	Email header analysis (compare Message-ID, References headers), employee awareness

	details, altered instructions). Email thread appears to continue naturally but with new requests not previously discussed.	

2.3 Immediate Actions — First 60 Minutes

Step	Action	Owner	Target
1	STOP any pending financial transactions. Contact the finance team immediately to halt any wire transfers, ACH payments, or other financial transactions related to the BEC. If a wire transfer has been initiated, proceed immediately to Step 2.	Incident Commander	0–5 min
2	INITIATE wire recall. Contact the originating bank's fraud department immediately. Provide: transaction reference, amount, recipient bank details, date/time of transfer. Request an urgent recall. For international wires, request a SWIFT recall message. For domestic wires, request Fedwire/CHAPS reversal. Every minute counts — recall success rates decrease rapidly after 24 hours.	Finance Lead + Legal	0–30 min
3	REPORT to law enforcement. File a report with Action Fraud (UK), IC3 (US FBI), or equivalent authority. For wires exceeding £50,000, consider direct contact with the relevant financial crime unit. Law enforcement may be able to initiate a Financial Fraud Kill Chain to freeze funds.	Legal/Compliance	Within 60 min
4	CLASSIFY in IR-CLASS-001. BEC with successful wire transfer is typically P1 (>£100K) or P2. BEC attempt without financial loss is typically P3. Account takeover enabling BEC is minimum P2.	Incident Commander	5–15 min
5	DETERMINE if email account is compromised. If the BEC originated from an internal account: immediately reset the account password, revoke all active sessions, disable the account if investigation requires, search for inbox rules (forwarding, deletion), and review sent items for additional fraudulent emails.	IT/Security Lead	15–45 min
6	IDENTIFY scope. Were multiple employees targeted? Were multiple transactions requested? Has the same vendor/executive been impersonated before? Review email logs for similar patterns across the organisation.	IT/Security Lead	30–60 min
7	PRESERVE evidence. Export the BEC email(s) with full headers. Preserve mailbox audit logs for any compromised accounts. Screenshot any financial transaction confirmations. Document the complete communication chain.	IT/Security Lead	15–60 min
8	NOTIFY insurance broker if financial loss confirmed or if account compromise is confirmed.	Executive Sponsor	Within 60 min

2.4 Containment Decision Tree

Decision Point	If YES	If NO
Was a wire transfer or payment executed?	PRIORITY 1: Initiate wire recall immediately (Step 2 above). Every hour of delay reduces recovery probability. Simultaneously proceed with investigation.	Focus on investigation and preventing future attempts. Lower urgency but still requires incident documentation.
Is an internal email account compromised?	Reset password. Revoke sessions. Audit inbox rules. Review sent items for additional BEC. Search for forwarding rules to external addresses. Check for OAuth app consents granted by the compromised user. Enable enhanced logging on the account.	Attack was external spoofing. Focus on email security controls (DMARC enforcement, lookalike domain blocking). No immediate account containment required.
Were multiple employees targeted?	Organisation-wide alert: notify all employees of the specific BEC pattern. Alert finance team to hold all wire transfers pending verification. Review all pending payments for similar patterns.	Targeted attack on individual. Brief the targeted individual and their team. Review similar transaction requests in the past 90 days.
Is the attacker still active in the compromised account?	Immediate account lockout (not just password reset — disable the account). Preserve current session data for forensics. Monitor for the attacker switching to other compromised accounts.	Account secured. Proceed with investigation at normal pace.
Is this a vendor impersonation (invoice modification)?	Contact the real vendor through a known-good channel (not email) to verify bank details. Review all payments to this vendor in the past 6 months. Alert AP/procurement team to verify all pending vendor payments.	Proceed with standard BEC investigation.

2.5 Eradication and Recovery

BEC eradication focuses on securing compromised accounts, strengthening financial controls, and closing the attack vector:

Action	Detail	Verification
Secure compromised accounts	Reset passwords with strong, unique credentials. Re-enrol MFA. Remove all suspicious inbox rules, delegates, and forwarding. Revoke OAuth application consents. Review recent sign-in activity for other compromised sessions.	Account audit shows no suspicious rules, forwards, or consents. Sign-in logs show only legitimate access.
Enforce DMARC	Implement DMARC at p=reject for the organisation's domains. Monitor for lookalike domains (typosquatting). Configure email gateway to flag external emails impersonating internal display names.	DMARC aggregate reports confirm enforcement. External impersonation warnings active.

Strengthen financial controls	Implement or verify dual authorisation for all wire transfers above £$50,000. Require out-of-band verification (phone call to known number) for any change to vendor bank details. Implement cooling-off period for new payee additions.	Financial controls documented, tested, and confirmed by Finance Lead.
Recover funds	Continue working with bank fraud department and law enforcement on fund recovery. Engage the insurer's recovery specialist if applicable. Document all recovery efforts for insurance claim.	Recovery status documented. Unrecoverable amount quantified for insurance claim.
Employee awareness	Issue targeted awareness communication about the specific BEC technique used. Include concrete examples (sanitised) from this incident. Reinforce verification procedures for financial requests.	Awareness communication sent. Finance and executive teams briefed.

2.6 Communication Requirements

Audience	Timing	Key Messages
Originating bank	Immediately upon discovery of fraudulent transfer	Transaction details, fraud report, recall request, law enforcement report reference
Law enforcement	Within 1 hour of confirmed financial loss	Incident report, transaction details, email evidence, any attribution information
Insurance broker	Within policy-mandated timeframe (typically same day)	Financial loss amount, circumstances, recovery efforts, law enforcement engagement
Executive leadership	P1: within 30 min. P2: within 2 hours.	Financial exposure, recovery prospects, root cause (spoofing vs account compromise), control improvement recommendations
Affected employees	After investigation determines scope	What happened (appropriate level of detail), what they should do differently, reinforcement of verification procedures
Vendor (if impersonated)	Once vendor impersonation is confirmed	Alert the vendor that their identity is being used for fraud. Request they notify other customers. Verify their systems are not compromised.

2.7 Lessons Learned Focus Areas

Post-incident review should address: were financial controls (dual authorisation, out-of-band verification) in place and followed; was the BEC email detectable by email security controls or did it bypass them entirely; is DMARC at enforcement level for all organisational domains; were employees trained to recognise BEC indicators; and how quickly was the wire recall initiated relative to the transfer execution.

Playbook 3: Data Breach / Exfiltration

This playbook covers incidents involving confirmed or suspected unauthorised access to and/or exfiltration of sensitive data including personal data, financial records, intellectual property, and trade secrets. The critical differentiator is the regulatory notification dimension: the clock for notification obligations typically starts when the organisation becomes aware of the breach, making rapid legal assessment essential.

3.1 Threat Profile

Attribute	Detail
Attack objective	Access, copy, and exfiltrate sensitive data for financial gain (sale on dark web, extortion), competitive advantage (IP theft), espionage (nation-state), or ideological motivation (hacktivism).
Common exfiltration methods	Cloud storage upload (Mega, Google Drive, Dropbox, AWS S3), email to external account, DNS tunnelling, encrypted channels to attacker-controlled infrastructure, physical media (USB), or abuse of legitimate synchronisation tools.
Data types at highest risk	Personal data (names, addresses, ID numbers, financial information), payment card data (PCI DSS scope), health records (HIPAA scope), authentication credentials, intellectual property and trade secrets, customer databases, M&A or financial information.
Regulatory implications	GDPR: 72-hour notification for personal data breaches. NIS2: 24-hour early warning. US: varies by state (30–90 days). HIPAA: 60 days. PCI DSS: immediate. SEC: 4 business days for material incidents. Multiple jurisdictions may apply simultaneously.

3.2 Detection Indicators

Stage	Indicator	Detection Source
Reconnaissance	Unusual database queries (SELECT * from large tables, enumeration of schemas). Abnormal file share access patterns (user accessing folders outside their normal scope). Bulk download of documents from SharePoint/OneDrive/Google Drive.	Database audit logs, file access logs, CASB alerts, DLP alerts
Staging	Creation of compressed archives (ZIP, RAR, 7z) from sensitive data locations. Data moved to a staging directory or temporary location. Large files created in unusual locations.	EDR file creation alerts, DLP alerts, file integrity monitoring
Exfiltration	Large outbound data transfers (>100MB to external destinations outside normal business patterns). Connections to known file-sharing services from servers that should not access them. DNS queries to unusual domains with high query volume (DNS tunnelling). Encrypted connections to new external IP addresses.	Firewall/proxy logs, DLP alerts, DNS logs, network traffic analysis, CASB

Post-exfiltration	Data appearing on dark web marketplaces or paste sites. Extortion communication from threat actor claiming data possession. Customer or partner reports of receiving fraudulent communications using stolen data.	Dark web monitoring, threat intelligence feeds, customer/partner reports

3.3 Immediate Actions — First 60 Minutes

Step	Action	Owner	Target
1	BLOCK active exfiltration channels if identified. Block destination IPs/domains at firewall. Disable compromised accounts. Sever network connections from staging servers to external destinations.	IT/Security Lead	0–15 min
2	CLASSIFY in IR-CLASS-001. Score the Regulatory dimension based on data types involved. Personal data breach is minimum score 4 (Significant). Confirmed exfiltration of personal data is typically P2 or P1.	Incident Commander	5–15 min
3	ENGAGE Legal/Compliance Lead immediately. The regulatory notification clock starts at ‘awareness’ of the breach, which may be this moment. Legal must assess notification obligations within hours, not days.	Incident Commander	0–15 min
4	PRESERVE evidence. Network traffic captures showing exfiltration. Database audit logs. File access logs. Email logs if exfiltration was via email. Do NOT delete or modify any logs.	IT/Security Lead	15–60 min
5	DETERMINE what data was accessed/exfiltrated. Identify the specific databases, file shares, or systems accessed. Determine data classification of affected records. Estimate the number of records/individuals affected.	IT/Security Lead	30–60 min
6	INITIATE regulatory notification tracker in IR-CLASS-001. Enter all applicable regulations, discovery timestamp, and deadline hours. The Regulatory Tracker auto-calculates deadline dates.	Legal/Compliance	Within 60 min
7	NOTIFY insurance broker if personal data breach confirmed or if incident is P1/P2.	Executive Sponsor	Within 60 min

3.4 Containment Decision Tree

Decision Point	If YES	If NO
Is exfiltration still active?	Block immediately. Sever all identified exfiltration channels. Accept that blocking may alert the attacker to detection. Stopping data loss takes priority over covert investigation.	Exfiltration has stopped or was a single event. Focus on scope determination and evidence preservation.

Is the attacker still present in the environment?	Contain attacker access (account lockout, network isolation of compromised systems). Assess whether to contain overtly (risk: attacker destroys evidence, activates destructive payload) or covertly (risk: continued data access during monitoring period). Decision requires Incident Commander + Legal + IT/Security Lead.	Attacker has departed or access has been revoked. Focus on determining full scope and closing access vector.
Is personal data confirmed as exfiltrated?	Regulatory notification preparation begins immediately. Legal assesses jurisdiction-specific obligations. Communications Lead prepares breach notification drafts using IR-COMMS-001 templates. Notification deadlines tracked in IR-CLASS-001.	Monitor for confirmation. Preserve evidence that may later confirm or rule out personal data exposure. Do not assume no personal data exposure until investigation confirms.
Is the exfiltrated data encrypted at rest?	Encrypted data reduces (but may not eliminate) notification obligations depending on jurisdiction. Legal to assess. Document encryption status as it affects risk assessment for regulators.	Unencrypted data exfiltration. Full notification obligations likely apply. Prepare for worst-case notification scope.
Can the volume of exfiltrated data be quantified?	Document confirmed volume and record types. This directly determines notification scope (number of affected individuals), regulatory reporting requirements, and potential financial exposure.	Use network traffic analysis and access logs to estimate. Provide Legal with best-case and worst-case estimates for notification planning.

3.5 Eradication, Recovery, and Communication

Eradication follows the same pattern as the general procedure (IR-PROC-001 Section 5.4): close access vector, remove persistence, rotate credentials, verify clean. Recovery adds a critical step: enhanced data monitoring. Deploy DLP rules specifically targeting the data types that were exfiltrated. Increase monitoring sensitivity on affected systems for a minimum of 90 days. Communication for data breach incidents is defined by regulatory obligations and must be coordinated through Legal/Compliance Lead using the templates in IR-COMMS-001. Key communication audiences include: regulators (within mandated timeframes), affected individuals (content requirements vary by jurisdiction), insurance broker (ongoing updates), and potentially media (reactive statements only unless proactive disclosure is legally required or strategically appropriate).

3.6 Lessons Learned Focus Areas

Post-incident review should address: were DLP controls in place and would they have detected the exfiltration earlier; was data classified correctly and were access controls proportionate to classification; was the volume of data accessible to the compromised account appropriate (least privilege); could network monitoring have detected the exfiltration pattern; and was the regulatory notification process executed within mandated timeframes.

Playbook 4: Insider Threat

This playbook covers incidents involving current or former employees, contractors, or trusted third parties who misuse authorised access to cause harm. Insider threats include malicious insiders (intentional harm), negligent insiders (accidental exposure through carelessness), and compromised insiders (legitimate users whose credentials have been stolen). This playbook focuses on malicious and negligent scenarios; compromised insider scenarios are addressed through the relevant attack-type playbook (BEC, credential theft, etc.).

4.1 Threat Profile

Attribute	Detail
Attack objective	Data theft (IP, customer data, trade secrets for competitive advantage or sale), sabotage (destruction of data or systems), fraud (financial manipulation), or espionage (state-sponsored recruitment of insiders).
Typical indicators	Behavioural: disgruntlement, disciplinary issues, resignation notice, financial difficulties. Technical: access to data outside job requirements, bulk downloads, use of personal storage devices, after-hours access, attempts to bypass security controls, access to systems after role change or termination notice.
Key differentiator	The insider has legitimate credentials and authorised access. Traditional perimeter security controls are ineffective. Detection depends on behavioural analytics, access monitoring, and DLP controls.
Legal complexity	Insider investigations involve employment law, privacy law (monitoring of employee activity), potential criminal prosecution, and possible civil litigation. HR and Legal must be involved from the outset. Evidence collection must be legally defensible.

4.2 Detection Indicators

Category	Indicator	Detection Source
Data access anomalies	Accessing files, databases, or systems outside normal job function. Bulk download of sensitive documents. Copying data to personal cloud storage or USB devices. Accessing data after submitting resignation or during notice period.	CASB, DLP, UEBA, file access audit logs, USB device logs
Account behaviour	After-hours access (outside normal working pattern). Access from unusual locations. Shared account usage. Attempts to escalate privileges. Accessing systems targeted for decommission or data migration.	Authentication logs, UEBA, VPN logs, privilege access management
Communication anomalies	Emails with attachments to personal email addresses. Use of unauthorised communication channels. Contact with competitors (where monitored and legally permitted). Encrypted personal messaging on corporate devices.	Email DLP, endpoint monitoring, CASB

Evasion behaviour	Disabling security tools on endpoint. Using privacy tools (VPN, Tor) on corporate network. Renaming files to evade DLP rules. Splitting large files into smaller transfers. Accessing data through less-monitored channels.	EDR tamper alerts, proxy logs, DLP evasion detection
Pre-departure indicators	Bulk data access in the weeks before resignation. Accessing archival or historical data not needed for current role. Downloading customer lists, pricing data, or strategic documents. Connecting personal devices to corporate network.	UEBA trend analysis, HR resignation data correlation, DLP

4.3 Immediate Actions and Containment

Insider threat response differs fundamentally from external attack response. The decision between covert investigation and overt containment must be made early and involves balancing evidence collection against ongoing risk:

Decision Point	Covert Approach	Overt Approach
When to use	Suspicion but not confirmed harm. Need to determine scope before alerting the insider. Legal/HR advise that evidence collection requires continued monitoring. Potential criminal prosecution where premature alerting could compromise the case.	Active data exfiltration confirmed and ongoing. Sabotage in progress. Risk of continued access outweighs investigative value of monitoring. Individual has already been alerted (e.g., through access denial).
Account action	Do NOT reset password or disable account. Increase monitoring verbosity. Deploy enhanced logging on all systems the insider accesses. Implement DLP rules to block or alert on exfiltration without notifying the user.	Disable account. Revoke all access. Disable badge/physical access. Collect corporate devices. Disable VPN and remote access.
HR involvement	HR briefed confidentially. HR provides employment context (performance issues, disciplinary history, notice period). HR advises on legal constraints for monitoring.	HR activates suspension or termination process. HR manages the face-to-face conversation with the individual (with Legal present if disciplinary/criminal).
Legal involvement	Legal assesses monitoring legality under applicable employment and privacy law. Legal advises on evidence admissibility for potential disciplinary, civil, or criminal proceedings.	Legal present for suspension/termination conversation. Legal advises on litigation hold and evidence preservation.
Evidence handling	All monitoring evidence must be collected in a legally defensible manner. Chain of custody maintained from the outset. Forensic imaging may need to be covert (after-hours, during planned maintenance).	Forensic imaging of all corporate devices immediately upon collection. Mailbox export and preservation. Access log extraction and preservation.

4.4 Eradication and Recovery

Once the investigation phase is complete and the decision to proceed with overt action has been made: revoke all access (logical and physical) simultaneously to prevent the insider from destroying evidence or escalating activity; collect all corporate devices, access cards, and credentials; forensically image all corporate devices before re-provisioning; review all systems the insider had access to for unauthorised modifications, backdoors, or time-delayed destructive actions (logic bombs); rotate any shared credentials or service accounts the insider had access to; and review the insider's access to third-party systems and notify affected third parties. Recovery focuses on verifying data integrity on all systems the insider accessed, restoring any deleted or modified data from backup, and implementing additional access controls to prevent similar insider actions.

4.5 Communication Requirements

Internal communication must be tightly controlled to protect the investigation, the individual's rights (especially in jurisdictions with strong employment protections), and the organisation's legal position. Only the Incident Commander, HR Lead, Legal/Compliance Lead, and Executive Sponsor should be aware of an active insider threat investigation. If the insider threat results in a data breach affecting personal data, regulatory notification obligations apply as per Playbook 3. Customers, partners, or other external parties should only be notified after legal counsel has assessed the obligation and appropriate messaging.

4.6 Lessons Learned Focus Areas

Post-incident review should address: were user activity monitoring and DLP controls adequate to detect the insider's actions; was the principle of least privilege enforced (did the insider have access beyond their job requirements); were pre-departure controls in place (enhanced monitoring during notice period, exit checklist); was the HR-to-IT offboarding process timely and complete; and does the organisation need to implement or enhance insider threat program capabilities.

Playbook 5: Distributed Denial of Service (DDoS)

This playbook covers DDoS attacks including volumetric (bandwidth exhaustion), protocol (TCP/UDP state table exhaustion), and application-layer (HTTP flood, API abuse) attacks. The critical differentiator is that DDoS is frequently used as a smokescreen for concurrent attacks (data exfiltration, account takeover) and as an extortion mechanism (pay or the attack continues). Always investigate for concurrent threats during a DDoS incident.

5.1 Threat Profile

Attribute	Detail
Attack types	Volumetric: UDP flood, DNS amplification, NTP amplification, memcached amplification (overwhelm bandwidth). Protocol: SYN flood, fragmented packet attack (exhaust firewall/load balancer state tables). Application-layer: HTTP flood, slowloris, API abuse (exhaust web server/application resources).
Attack objective	Service disruption (reputational damage, customer impact), extortion (RDDoS — pay to stop), smokescreen for concurrent attack (distract defenders while exfiltrating data or compromising systems), hacktivism (political or ideological motivation), competitive sabotage.
Typical duration	Minutes to days. Sophisticated attackers modulate attack vectors to evade mitigation. Multi-vector attacks combine volumetric, protocol, and application-layer simultaneously.
Business impact	Customer-facing services unavailable. Revenue loss during downtime. SLA breaches with customers. Reputational damage. Operational disruption if internal services share the same internet connectivity.

5.2 Detection Indicators

Type	Indicator	Detection Source
Volumetric	Bandwidth utilisation exceeds 80% of available capacity. Traffic from many source IPs with similar patterns. Traffic concentrated on specific protocols (UDP 53, UDP 123, UDP 11211). Geographic distribution of traffic inconsistent with normal customer base.	ISP/CDN monitoring, firewall traffic logs, network monitoring tools
Protocol	TCP half-open connections exceed normal thresholds. Firewall/load balancer state table approaching capacity. Connection timeout errors increasing. SYN-to-ACK ratio anomalous.	Firewall session logs, load balancer health, network device CPU/memory
Application-layer	HTTP request rate exceeds normal baselines. Requests targeting specific resource-intensive endpoints (search, login, API). User agent strings uniform or anomalous. Requests from IP ranges with no legitimate user association. Server response times degrading progressively.	Web application firewall (WAF) logs, web server access logs, application performance monitoring
Extortion precursor	Email threatening DDoS attack unless payment is made. Small ‘demonstration’ attack followed by extortion demand. Ransom demand referencing a known DDoS group.	Email reports, correlation with observed attack

5.3 Immediate Actions — First 60 Minutes

Step	Action	Owner	Target
1	CONFIRM DDoS (distinguish from legitimate traffic spike, infrastructure failure, or misconfiguration). Check: is the traffic pattern anomalous? Are multiple services affected? Does the pattern match known DDoS signatures?	IT/Security Lead	0–10 min
2	ACTIVATE upstream mitigation. Contact ISP/CDN/DDoS mitigation provider to enable scrubbing or activate always-on mitigation if not already enabled. Most ISPs have emergency DDoS response procedures; know the contact number in advance.	IT/Security Lead	0–20 min
3	CLASSIFY in IR-CLASS-001. DDoS affecting customer-facing revenue services is typically P2. DDoS with concurrent data breach indicators is P1. DDoS against non-critical internal services may be P3.	Incident Commander	5–15 min
4	INVESTIGATE FOR CONCURRENT ATTACKS. This is critical. DDoS is frequently a distraction. While the DDoS is absorbing attention, check for: unusual authentication activity, data exfiltration indicators, new admin accounts created, configuration changes, malware alerts.	IT/Security Lead	15–60 min
5	IMPLEMENT local mitigation. Enable rate limiting on affected endpoints. Block traffic from identified malicious IP ranges (if identifiable and not spoofed). Enable geo-blocking if attack traffic originates primarily from non-customer regions. Activate WAF rules for application-layer attacks.	IT Operations	15–45 min
6	COMMUNICATE outage to affected stakeholders. Update status page. Notify customer support team. Prepare holding statement for social media/media enquiries.	Communications Lead	15–60 min
7	PRESERVE evidence. Capture traffic samples for forensic analysis. Preserve firewall and WAF logs. Document attack vectors and timeline. If extortion demand received, preserve the communication.	IT/Security Lead	30–60 min

5.4 Containment and Recovery

DDoS containment is primarily an upstream activity: the ISP, CDN provider, or dedicated DDoS mitigation service absorbs and scrubs the malicious traffic before it reaches the organisation's infrastructure. The organisation's role is to activate this protection, provide information about legitimate traffic patterns to improve scrubbing accuracy, and implement local mitigations for any traffic that bypasses upstream filtering.

Recovery involves verifying that all services have returned to normal performance once the attack subsides or is mitigated, reviewing whether any data integrity issues occurred during the attack (particularly for application-layer attacks that may have interacted with backend databases), and confirming that concurrent attack investigation found no evidence of compromise. If a concurrent

attack is detected, escalate to the appropriate playbook (Playbook 1 for ransomware, Playbook 3 for data breach, etc.) and reclassify the incident accordingly.

5.5 Ransom DDoS (RDDoS) Considerations

If a ransom demand accompanies the DDoS attack, do not pay. Paying RDDoS demands funds criminal operations and marks the organisation as a paying target for future attacks. Instead: preserve the extortion communication as evidence; report to law enforcement; ensure DDoS mitigation is activated and maintained; and prepare for sustained or repeated attacks as the attacker tests resolve. Most RDDoS campaigns move on to other targets if initial payment is not forthcoming and mitigation is effective.

5.6 Lessons Learned Focus Areas

Post-incident review should address: was DDoS mitigation in place and how quickly was it activated; did the organisation check for concurrent attacks and was the investigation thorough; was the mitigation provider effective and were SLA commitments met; are customer-facing services architected to absorb or degrade gracefully under load; and does the organisation's incident response plan need updating to better integrate DDoS-specific procedures.

Playbook 6: Supply Chain Compromise

This playbook covers incidents where the organisation is compromised through a trusted third party: a software vendor (malicious update or compromised build pipeline), a managed service provider (attacker pivots from MSP to customer environments), a hardware supplier (tampered equipment), or a SaaS provider (breach of shared platform affecting customer data). Supply chain compromises are among the most difficult incidents to detect, scope, and remediate because the trust relationship between the organisation and the vendor is the attack vector.

6.1 Threat Profile

Attribute	Detail
Attack vectors	Compromised software update (SolarWinds-style): attacker inserts malware into a legitimate software update distributed to all customers. Compromised MSP: attacker gains access to the MSP's management tools and pivots to customer environments. SaaS platform breach: shared infrastructure compromise exposes multiple tenants' data. Hardware supply chain: tampered devices shipped to target organisations.
Detection difficulty	Extremely high. The malicious activity comes from a trusted source (signed software update, authorised MSP access, legitimate SaaS platform). Traditional security controls are designed to trust these sources. Detection typically relies on anomalous behaviour after the trusted source has been compromised.
Scope uncertainty	The initial scope is unknown and potentially very large. If a software vendor is compromised, every customer running that software may be affected. Scoping requires understanding exactly which vendor components are deployed, what access those components have, and what activity has occurred through those components.

Multi-party coordination	Response requires coordination with the compromised vendor, potentially other affected organisations, industry ISACs, and government cybersecurity agencies. Information sharing is essential but may be constrained by NDAs, legal considerations, and vendor cooperation.

6.2 Detection Indicators

Scenario	Indicator	Detection Source
Software supply chain	Anomalous network connections from recently updated software (connections to unknown external IPs, DNS resolution of suspicious domains). Software behaviour change after update (new processes spawned, new registry keys created, new scheduled tasks). Vendor advisory or industry alert about compromise of a product in use.	EDR process monitoring, network traffic analysis, vendor notifications, industry ISAC alerts, threat intelligence feeds
MSP compromise	Anomalous remote access sessions from MSP IP ranges (unusual hours, accessing systems outside normal MSP scope). New administrative accounts created through MSP management tools. Configuration changes not corresponding to approved change requests. MSP-originated lateral movement to systems outside their management scope.	Remote access logs, AD audit logs, change management correlation, PAM logs
SaaS platform breach	Vendor notification of security incident affecting the platform. Anomalous activity within the SaaS application (unauthorised access, data export, configuration changes). Third-party threat intelligence indicating SaaS platform compromise.	Vendor incident notifications, SaaS application audit logs, CASB alerts, threat intelligence
Hardware tampering	Device behaviour inconsistent with specifications. Unexpected network connections from new hardware. Firmware analysis reveals modifications from known-good baseline. Supply chain documentation gaps (unsealed packaging, unexpected routing, missing tamper-evident seals).	Network monitoring, firmware integrity validation, physical inspection, supply chain audit

6.3 Immediate Actions — First 60 Minutes

Step	Action	Owner	Target
1	CLASSIFY as P1 or P2 by default. Supply chain compromises affect trusted components with potentially broad access. Do not underestimate initial severity.	Incident Commander	0–10 min
2	IDENTIFY all instances of the compromised vendor's product/service in the environment. Software asset inventory,	IT Operations	15–60 min

	MSP access scope, SaaS integration points, hardware deployment records.		
3	ASSESS vendor access scope. What systems does the compromised vendor component have access to? What privilege level? What data can it reach? What network segments can it traverse?	IT/Security Lead	15–60 min
4	ISOLATE compromised vendor components if feasible without catastrophic business impact. Disable or block the software, revoke MSP access, disable SaaS integrations, or quarantine hardware. If isolation would cause business-critical outage, implement enhanced monitoring as interim measure and document the risk acceptance.	Incident Commander + IT/Security Lead	30–60 min
5	CONTACT the vendor through a verified out-of-band channel (not through potentially compromised vendor tools). Determine: is the vendor aware of the compromise? What is the vendor's response status? What indicators of compromise can the vendor provide? What mitigation guidance has the vendor issued?	Program Owner	Within 60 min
6	CHECK industry sources. Search vendor name on CERT/CSIRT advisories, industry ISACs, security news sites, and threat intelligence platforms. Other organisations may already be reporting the same compromise.	IT/Security Lead	15–60 min
7	PRESERVE evidence. Do not update or reinstall the compromised vendor product until forensic images have been captured. Preserve network logs showing all communication from vendor components. Preserve vendor access logs and audit trails.	IT/Security Lead	30–60 min
8	ASSESS downstream impact. Does Northgate Engineering Ltd provide services to other organisations that may be affected by this supply chain compromise? If so, assess whether the compromise could propagate downstream and notify affected parties.	Program Owner	30–60 min

6.4 Containment Decision Tree

Decision Point	If YES	If NO
Is the compromised component actively being exploited against your environment?	Isolate immediately. Revoke all vendor access. Disable the software/integration. Accept business impact. Active exploitation means attacker has access NOW.	Implement enhanced monitoring. Prepare for isolation if exploitation indicators emerge. Develop contingency plan for rapid isolation.
Does the vendor have administrative/privileged access to your systems?	HIGH RISK. Even without active exploitation, privileged vendor access means potential for full environment compromise. Strongly consider revoking access and managing business impact. Rotate all credentials the vendor has access to.	Lower immediate risk but assess data access scope. Vendor may have read access to sensitive data even without administrative privileges.

Has the vendor issued a patch or mitigation guidance?	Apply the vendor's mitigation immediately. Verify the mitigation is effective (the patch itself could be compromised in sophisticated scenarios — verify through independent analysis or trusted third-party validation).	Implement local mitigations: network-level blocking of known malicious indicators, application-level access restrictions, enhanced monitoring. Maintain regular contact with vendor for updated guidance.
Are other organisations reporting the same compromise?	Leverage shared intelligence. IOCs and TTPs from other affected organisations accelerate your investigation. Engage with industry ISAC for coordinated response. Consider whether joint disclosure or coordinated notification is appropriate.	Your organisation may be an early detector. Share IOCs with trusted partners and industry ISAC (after legal counsel approval) to assist others.
Does the compromise affect a component essential to business operations with no alternative?	Risk-based decision required. Document the risk acceptance. Implement maximum compensating controls (network segmentation, enhanced monitoring, reduced privilege). Set a deadline for the vendor to provide a resolution or plan migration to alternative.	Replace or decommission the compromised component. Use this incident as justification for reducing vendor concentration risk.

6.5 Eradication, Recovery, and Communication

Eradication in supply chain compromises often requires waiting for the vendor to issue a verified clean update or patch. Until then, compensating controls must bridge the gap. Recovery may require rebuilding systems that ran compromised vendor software from known-good pre-compromise images, rotating all credentials that were accessible to the compromised component, and verifying data integrity across all systems within the component's access scope.

Communication for supply chain incidents is complex because multiple stakeholders are involved: the compromised vendor, your organisation, potentially other affected organisations, regulators (if personal data is involved), and customers (if their data or services are affected). Coordinate with the vendor on disclosure timing where possible, but Northgate Engineering Ltd's regulatory notification obligations take precedence over vendor preferences. Do not delay regulatory notification because the vendor has requested confidentiality.

6.6 Lessons Learned Focus Areas

Post-incident review should address: was the organisation's software/vendor inventory accurate and complete; was vendor access appropriately scoped and monitored; were there detection capabilities specifically for trusted-source anomalies; does the vendor risk management program need strengthening (assessment frequency, access review, contractual security requirements); and should the organisation diversify away from the compromised vendor or require additional security assurances.

Framework Traceability

These playbooks implement attack-specific guidance within the response framework established by IR-PROC-001. The following framework controls are specifically addressed by the playbook content:

Framework	Control	Playbook Coverage
ISO 27001:2022	A.5.25 — Assessment and decision	All playbooks: detection indicators and classification guidance
ISO 27001:2022	A.5.26 — Response	All playbooks: containment decision trees, eradication steps, recovery validation
ISO 27001:2022	A.5.27 — Learning	All playbooks: lessons learned focus areas
ISO 27001:2022	A.5.28 — Evidence collection	All playbooks: evidence preservation in immediate actions
NIST CSF 2.0	RS.AN-03 — Analysis	All playbooks: threat profile, detection indicators, scope assessment
NIST CSF 2.0	RS.MI-01/02 — Containment/Eradication	All playbooks: containment decision trees, eradication steps
NIST CSF 2.0	RS.CO-02 — Communication	All playbooks: communication requirements
CIS Controls v8	17.4 — IR process	All playbooks: attack-specific response procedures
CIS Controls v8	17.8 — Post-incident reviews	All playbooks: lessons learned focus areas
NIST SP 800-61r3	Detection and Analysis	All playbooks: detection indicators, triage criteria
NIST SP 800-61r3	Containment/Eradication/ Recovery	All playbooks: containment decision trees, eradication steps, recovery validation

Disclaimer

This is a customisable template only. It is not legal advice. Organisations should seek qualified professional advice for their specific circumstances and jurisdiction. Incident response decisions should be informed by the specific context of each incident, legal counsel, and insurance broker guidance.