SOUTHGATE TERMINAL

Port Operations Security Documentation

ADDITION TO: Breach Disclosure Checklist.docx

INSERT LOCATION: Add as new section at the beginning, before existing checklist items

SECTION TITLE: Breach Classification Decision Tree

Breach Classification Decision Tree

Purpose

This decision tree provides systematic classification of security incidents to determine appropriate legal responses, notification requirements, and regulatory obligations. Use this before proceeding with any breach disclosure process.

Classification Categories

CATEGORY 1: Technical Anomaly (No breach classification)

- System glitches or configuration errors
- No evidence of unauthorised access
- No data exposure or system compromise
- Standard operational procedures sufficient

CATEGORY 2: Security Incident (Internal review required)

- Suspicious activity detected but contained
- Potential unauthorised access attempts
- System integrity questions but no confirmed compromise
- Enhanced monitoring and investigation needed

CATEGORY 3: Confirmed Breach (Regulatory review required)

- Confirmed unauthorised access to systems
- Evidence of data exposure or system manipulation
- Operational impact from security compromise
- Formal breach protocols and notifications required

CATEGORY 4: Persistent Unauthorised Access (Immediate escalation)

- Evidence of ongoing unauthorised system access

- Installation of unauthorised scripts or programs
- Lateral movement between systems
- Advanced persistent threat characteristics

Decision Tree Process

Step 1: Initial Evidence Assessment (5 minutes) **Question 1:** Is there evidence of unauthorised access to systems? - **NO** - Proceed to Technical Anomaly Assessment - **YES** - Proceed to Step 2

Question 2: Is there evidence of data exposure or system modification? - **NO** - Classify as Security Incident (Category 2) - **YES** - Proceed to Step 3

Question 3: Is there evidence of persistent or ongoing unauthorised access? - **NO** - Classify as Confirmed Breach (Category 3) - **YES** - Classify as Persistent Access (Category 4)

Step 2: Technical Anomaly Assessment **Indicators suggesting Category 1:** - [ ] System logs show configuration errors - [ ] Network issues correlate with maintenance activities - [ ] No authentication failures or unauthorised commands - [ ] Vendor systems involved with known issues

If ANY of these are present, escalate to Category 2: - [ ] Unusual timing of technical issues - [ ] Multiple systems affected simultaneously - [ ] External connections or traffic patterns - [ ] Administrative access during non-business hours

Step 3: Persistent Access Evaluation **Indicators of Category 4 (Persistent Access):** - [ ] Unauthorised cron jobs or scheduled tasks detected - [ ] Evidence of lateral movement between systems - [ ] Creation of unauthorised user accounts or privileges - [ ] Installation of unauthorised software or scripts - [ ] Log deletion or tampering evidence - [ ] Command execution outside normal parameters

Legal Classification Criteria

Category 1: Technical Anomaly **Legal Obligations:** - Internal documentation only - No external notifications required - Standard incident response procedures

Regulatory Requirements: - None (unless pattern develops)

Category 2: Security Incident **Legal Obligations:** - Internal legal review required - Consider preliminary insurance notification - Enhanced documentation requirements

Regulatory Requirements: - Monitor for escalation to reportable event - Prepare for potential future notifications

Category 3: Confirmed Breach Legal Obligations: - Formal legal assessment required - Insurance notification mandatory - Board/executive notification required - Consider external legal counsel

Regulatory Requirements: - Assess notification obligations under Cybersecurity Act - Consider Maritime Security Authority notification - Evaluate customer/partner notification requirements

Category 4: Persistent Unauthorised Access Legal Obligations: - Immediate executive escalation - External legal counsel engagement - Law enforcement consideration - Full insurance claim preparation

Regulatory Requirements: - Mandatory Cybersecurity Act notification (24-72 hours) - Maritime Security Authority immediate notification - Consider national security implications

Notification Timeline Requirements

Category 1: Technical Anomaly

- **Internal:** Document in incident log
- **Legal:** No specific timeline
- **Regulatory:** None required

Category 2: Security Incident

- **Internal:** Notify legal team within 4 hours
- **Legal:** Preliminary insurance contact within 24 hours
- **Regulatory:** Monitor for 72 hours for escalation

Category 3: Confirmed Breach

- **Internal:** Executive notification within 2 hours
- **Legal:** Full legal assessment within 8 hours
- **Insurance:** Formal notification within 24 hours
- **Regulatory:** Assessment complete within 24 hours, notifications within 72 hours

Category 4: Persistent Unauthorised Access

- **Internal:** Immediate executive notification
- **Legal:** External counsel within 4 hours
- **Insurance:** Immediate notification
- **Regulatory:** Notification within 24 hours (Cybersecurity Act)
- **Law Enforcement:** Consider immediate contact

Evidence Preservation Requirements

For All Categories 2-4:

- ☐ Preserve all system logs immediately
- ☐ Document timeline of events
- ☐ Secure affected systems from further access
- ☐ Photograph or screenshot evidence
- ☐ Maintain chain of custody for digital evidence

Additional for Categories 3-4:

- ☐ Engage forensic specialists if available
- ☐ Create bit-for-bit copies of affected systems
- ☐ Document all investigative actions
- ☐ Prepare for potential law enforcement involvement

Cross-Reference with Specific Incidents

Unauthorised Cron Jobs (INJ016A, INJ017A)

- **Initial Classification:** Category 2 (Security Incident)
- **Escalate to Category 4 if:** Evidence of system manipulation or ongoing access
- **Key Evidence:** Purpose of script, authorisation for installation, system impact

Log Deletion (INJ016B)

- **Initial Classification:** Category 3 (Confirmed Breach)
- **Escalate to Category 4 if:** Systematic deletion or ongoing tampering
- **Key Evidence:** What logs deleted, timing, method of deletion

Authentication Failures (INJ008A)

- **Initial Classification:** Category 2 (Security Incident)
- **Escalate to Category 3 if:** Successful unauthorised access confirmed
- **Key Evidence:** Number of attempts, source, success rate

System Configuration Changes (INJ006A)

- **Initial Classification:** Category 2 (Security Incident)
- **Escalate to Category 3 if:** Unauthorised modifications confirmed
- **Key Evidence:** Nature of changes, authorisation, operational impact

Decision Documentation Template

INCIDENT ID: [Unique identifier] **DATE/TIME:** [Classification decision time] **DECISION MAKER:** [Name and role] **CLASSIFICATION:** [Category

1-4]

EVIDENCE SUMMARY: - Primary indicators: [List key evidence] - Supporting factors: [Additional considerations] - Exclusionary factors: [Evidence against higher classification]

RATIONALE: [Brief explanation of classification decision]

REQUIRED ACTIONS: - [ ] Legal notifications: [Timeline and recipients] - [ ] Regulatory requirements: [Specific obligations] - [ ] Evidence preservation: [Specific requirements] - [ ] Escalation triggers: [Conditions for reclassification]

REVIEW TIMELINE: [When to reassess classification]

Success Criteria

- Accurate classification based on available evidence
- Appropriate legal and regulatory responses initiated
- Proper evidence preservation protocols followed
- Clear documentation for future reference and audit

Related Procedures

- Use with: Insurance Communications Template (for Categories 3-4)
- Coordinate with: Legal Risk Escalation Flowchart
- Reference: Post-Breach Reform Guidance (for Category 4)
- Escalate to: Crisis Decision Authority Matrix (for executive decisions)