Cybersecurity Incident Response TTX

Kilkenny Chamber Event | Hotel Kilkenny | Wednesday, 23 September 2026

Company Name: _____

Table #: _____

Assigned Role:
- ☐ MD/Owner
- ☐ IT/Ops
- ☐ Finance
- ☐ Comms/Client

Note Table Role Assignments:

- ***Managing Director / Owner***: Focuses on executive liability, legal duties, and enforcing the 'Single Voice Rule.'
- ***Operations & IT Lead***: Focuses on operational containment, system isolation, and technical vendor triage.
- ***Finance & Supply Chain Lead***: Focuses on cash flow preservation, manual workarounds, and client audit requirements.
- ***Communications & Client Lead***: Focuses on customer containment, press office management, and statutory regulator updates.

Table Roles & Rules of Engagement (7 Minutes)

Rules of Engagement:

1. ***Accept the Premise***: (scenario constraints are facts; do not fight technical details),
2. ***Embrace the Fog of War***: (dynamic injects), and
3. ***No Solo Decisions***: (integrate cross-functional perspectives).

INJECT 1: Ransomware Lockout & Cloud ERP Vendor Disruption (15 Mins)

SCENARIO INJECT 1: At 08:30 hrs, a major cloud Enterprise Resource Planning (ERP) and invoicing provider used by local SMEs experiences a catastrophic ransomware attack. Your company loses access to customer billing and order fulfillment databases. The threat actor claims to possess client financial records and threatens public leakage.

Regulatory Clocks & Notifications Triggered (Check applicable):

☐ Mandatory NCSC NIS2 Early Warning (24 Hrs)
☐ DPC GDPR Personal Data Breach Notice (72 Hrs)
☐ Corporate Client / Key Supplier Contractual Notice

Action 1.1: Immediate 24-Hour Containment Priority
What top 2 actions must your company take immediately?

1. _____

_____

2. _____

_____

Customer Transparency:
How do you respond when key corporate clients demand immediate written confirmation regarding data integrity?

_____

_____

_____

INJECT 2: Supply Chain Pressure, Payment Freezes & Media Rumours (13 Mins)

SCENARIO INJECT 2: Day 2 of the outage. A tier-1 corporate client freezes all pending contract payments (€150k+ pipeline) until your firm passes a comprehensive cyber audit.

Concurrently, rumors circulate on local social media alleging client data leaks, and local press request an official statement.

Action 2.1: Manual 'Paper Bridge' Workaround

How will you maintain billing & order fulfillment offline?

_____

_____

_____

Action 2.2: Director Governance & Comms Control

Who is authorised to speak?

_____

What message is off-limits?

_____

_____

WRAP-UP: Business Action Commitments & CyFun Alignment (10 Mins)

Target Cyber Baseline: Ireland's NCSC Cyber Fundamentals (CyFun) Basic 28 Controls

Top 3 Post-Exercise Action Commitments for My Business:

1. **Governance & Training**:

   _____

   _____

2. **Technical Hygiene** (MFA/Backups/Patching):

   _____

   _____

3. **Supply Chain & Vendor Audit Readiness**:

   _____

   _____

CyFun 2025