Cybersecurity Incident Response TTX Pre-Reading

Dr Diarmuid Ó Briain

DEPARTMENT OF ELECTRONIC ENGINEERING & COMMUNICATIONS
SOUTH EAST TECHNOLOGICAL UNIVERSITY

1. Executive Summary

As a critical institutional intermediary driving the regional energy transition across Carlow, Kilkenny, Wexford, and Waterford, the South East Energy Agency (SEEA) manages sensitive energy performance metrics, coordinates multi-million euro retrofitting programmes, and maintains shared digital pathways with all four partner Local Authorities.

Because the agency sits at the intersection of public funding, local authority infrastructure, and private contracting supply chains, any compromise to SEEA's digital integrity poses an immediate systemic risk to the wider public sector network and regional climate targets.

This document outlines the legal, financial, and governance realities the Board must master ahead of the TableTop eXercise (TTX) on the 2nd July 2026.

2. The EU Cybersecurity Framework

The European Union (EU) has developed a comprehensive suite of regulations and directives designed to harmonise digital resilience, protect personal data, and secure critical infrastructure networks across Ireland and the wider Union.

3. The Regulatory Landscape

NIS2 Directive & The National Cyber Security Bill 2026

The National Cyber Security Bill 2026 transposes the EU's revised Directive (EU) 2022/2555 Network Information Security v2 (NIS2) into Irish law, putting the National Cyber Security Centre (NCSC) on a statutory footing. This directive mandates strict, harmonised cybersecurity Risk-Management Measures (RMM), establishes rigorous incident reporting timelines, and enforces direct accountability on senior management and corporate boards for their organisation's resilience against complex digital threats.

- **Classification**: Public administration and energy sectors are considered highly critical. Under NIS2, SEEA acts as an essential or important intermediary.
- **Supply Chain Mandate**: NIS2 explicitly requires entities to manage cybersecurity risks within their supply chains, meaning SEEA is legally responsible for the security posture of its connections to Local Authorities and private contractors.

GDPR & The Irish Data Protection Act 2018

Regulation (EU) 2016/679 General Data Protection Regulation (GDPR): This regulation governs the lawful processing and protection of personal data belonging to grant applicants, residential upgrade pipelines, and community group records within the Irish energy sector, and is enforced nationally by the Data Protection Commission (DPC).

Entities and Cyber Resilience

- **Directive (EU) 2022/2557 Critical Entities Resilience Directive (CER)**: Establishes an all-hazards legal framework requiring Irish public and private operators in vital sectors, including energy and transport, to anticipate, withstand, and recover from non-cyber operational disruptions, physical threats, and climate risks. This is managed in Ireland by Office of Emergency Planning (OEP) within the Department of Defence (DoD).

- **Regulation (EU) 2024/2847 Cyber Resilience Act (CRA)**: Introduces mandatory, uniform EU-wide cybersecurity requirements for hardware and software products placed on the Irish market, enforcing a secure-by-design and secure-by-default methodology and strict lifecycle vulnerability tracking for manufacturers and suppliers. Ireland utilises existing market-monitoring regulators, such as the Communications Regulator (ComReg) for digital products and electronic communications, to ensure hardware and software manufacturers comply with secure-by-design and secure-by-default requirements before placing goods on the market.

AI Act, SoA and the Regulation of Artificial Intelligence Bill 2026

- **Regulation (EU) 2024/1689 Artificial Intelligence Act**: Establishes a harmonised, risk-based legal framework that prohibits unacceptable AI practices and enforces strict safety, transparency, and data governance mandates on high-risk systems to safeguard fundamental rights across public and private sectors. A new AI Office of Ireland (AIOI), will be established under the Regulation of Artificial Intelligence Bill 2026, and will be the centralised coordinator and the default authority for cases crossing multiple sectors.
- **Regulation (EU) 2025/38 Cyber Solidarity Act (SoA)**: Establishes a coordinated EU-wide framework to detect, prepare for, and respond to large-scale cybersecurity threats by integrating Irish national capabilities with a shared European Cyber Shield and emergency response mechanisms to safeguard critical infrastructure; under this framework, the National Cyber Security Centre (NCSC) serves as Ireland’s designated National Cyber Hub, directly linking the state into the European network.

4. Strict Incident Reporting Timelines

When a significant incident or personal data breach occurs, multiple regulatory clocks start ticking simultaneously.

Regulatory / Governance Framework	Reporting Milestone	Requirement & Content
NIS2 (NCSC Portal)	24 Hours	**Early Warning**: Inform the NCSC whether the incident is suspected to be caused by unlawful or malicious acts, and if it has cross-border impact.
NIS2 (NCSC Portal)	72 Hours	**Incident Notification**: Provide an initial assessment, including severity, impact, and indicators of compromise.
GDPR (DPC Portal)	72 Hours	**Data Breach Notification**: Mandatory submission to the DPC detailing the nature of the breach, types of personal data compromised, and immediate mitigation steps.
NIS2 (NCSC Portal)	On Request (Intermediate)	**Status Update**: Submit an intermediate status update to the NCSC if requested during active incident handling.
NIS2 (NCSC Portal)	1 Month	**Final Progress Report**: Detailed root-cause analysis, mitigation applied, and final business impact. Includes an updated estimate of the financial impact.
Public Sector Governance	Immediate (Within 0–2 Hours)	**Sectoral & Shareholder Notification**: Internal protocol dictates notifying the parent Department of the Environment, Climate and Communications (DECC) and partner Local Authority Chief Executives to isolate networks and prevent municipal contagion.

5. Enforcement & Penalties

Non-compliance is no longer just an IT or operational failure; it carries severe statutory and financial consequences.

Regulatory Framework	Entity Category	Max €€€ Penalty	Turnover Based Alternative	Additional Statutory Powers
NIS2 Directive	Essential Entities	€10m	2% of total worldwide annual turnover (higher of the two)	Regulatory bodies can mandate public disclosure of non-compliance, including identifying the specific individuals responsible.
NIS2 Directive	Important Entities	€7m	1.4% of total worldwide annual turnover (higher of the two)	
GDPR Regulation	All Applicable Entities	€20m	4% of global annual turnover (higher of the two)	

6. Corporate Governance & Executive Responsibilities

The National Cyber Security Bill 2026 shifts the burden of cyber accountability directly onto the Executive Board. Cybersecurity is recognised as a fiduciary and corporate governance duty, not an IT issue.

Direct Board Accountability: Senior management must directly approve and oversee the implementation of the organisation's cybersecurity RMMs.

Personal Liability: Under NIS2, management can be held personally liable for a failure to ensure compliance or implement risk frameworks.

Mandatory Training: Board members and senior executives are legally required to undergo regular cybersecurity training to understand risk identification and management.

7. Pre-TTX Reflection Questions

To get the most out of the upcoming simulation, consider your specific role (Chairperson, Council Rep, Audit Chair, or Communications Lead) against these three core questions:

- *At what exact point does an operational IT malfunction legally transition into a mandatory Board-level data breach notification?*
- *If capital pipelines are frozen mid-transaction due to a cyber containment hold, what emergency financial frameworks can the Board legally deploy to preserve local contractor cash flows?*
- *How do we protect our regional **Trusted Intermediary** status when balancing the legal obligation for transparency with the need to prevent network panic across our partner Local Authorities?*

For a deeper dive into how boards must adapt to these shifting liabilities, watch this ***Unpacking the National Cyber Security Bill webinar*** which breaks down the specific compliance obligations and governance overhauls coming into effect.

https://tinyurl.com/cs-bill26

Notes: