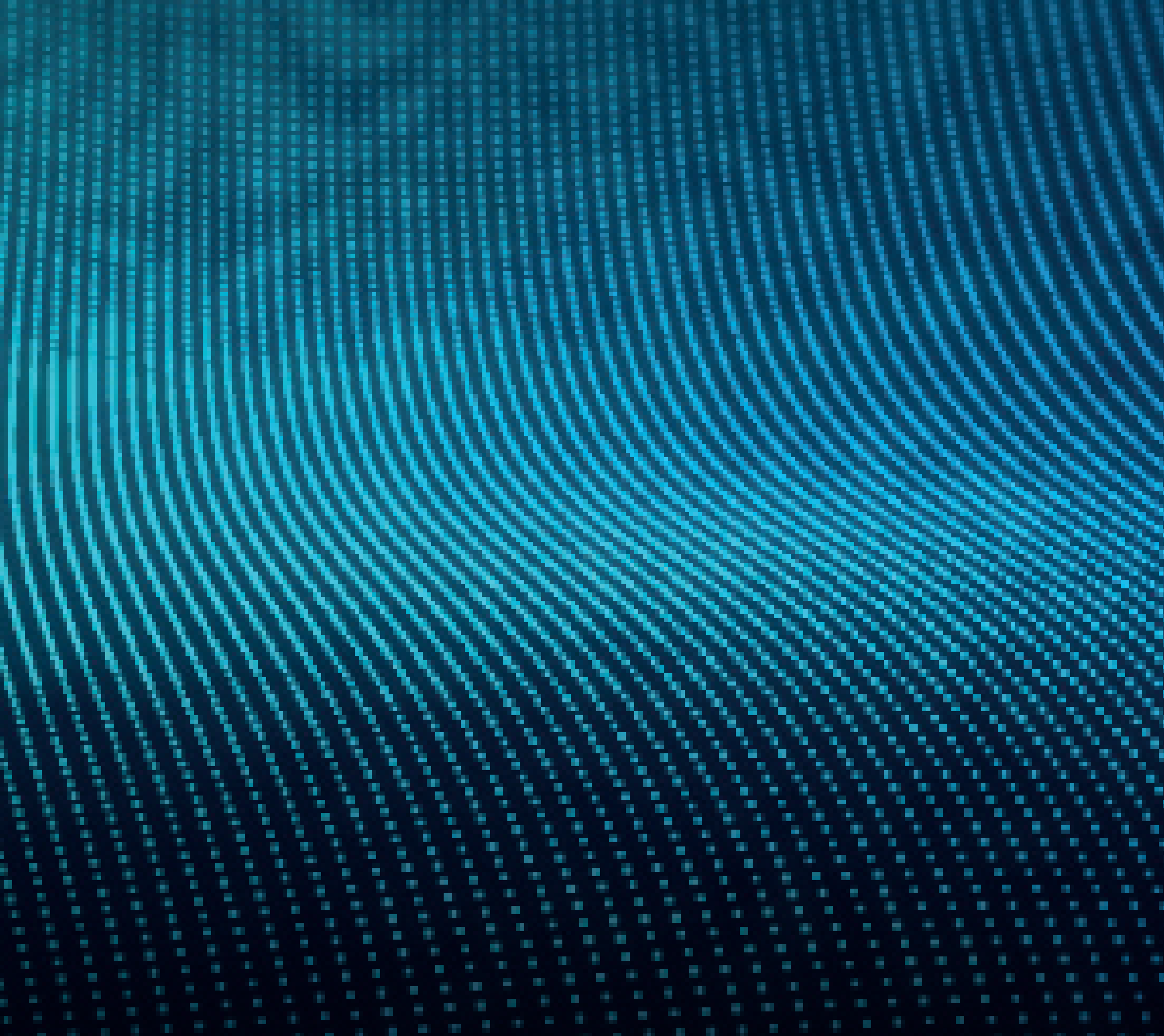

Case Study

Incident Response and Implementation

cybersecurity
associates

Case Study

Incident Response and Implementation

Many organisations treat any incident response with a reactive and unstructured approach. However, information security incidents need to be approached with a timely and well-coordinated response to maximise recovery when multiple stakeholders are involved.

CSA facilitated the design, development, implementation and testing of a full incident response capability for a large UK Nuclear client. Whilst our approach targeted multiple business units, the main priority was the maritime business sector due to its operationally-focused requirements.

The CSA team undertook a 2-day workshop to establish numerous different cyber incident scenarios and mapped a necessary course of action for each. This approach not only produced an operational incident response playbook but ensured all stakeholders were engaged to understand their roles and responsibilities within the incident response process.

On completion of the workshop and associated scenario-based planning sessions, CSA produced a bespoke and agreed incident response process, including playbooks, based on the NIST cyber security framework tailored to the Maritime business unit. Finally, once the process and playbooks were operational, CSA returned to undertake facilitated table-top training and exercises to ensure all deliverables were fit for purpose.

cybersecurity
associates

Security Operations Centre

Training

Monitoring, Detection and Protection

Response

Consulting

Cyber Assessments

Cyber Executives