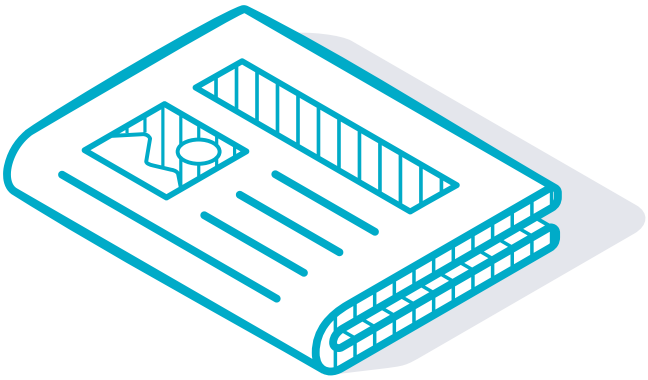

14 CASE STUDY 3: SHIPOWNER'S IT SERVICES SUPPLIER DATA CENTRE IN THIRD COUNTRY ATTACKED AND CONNECTIVITY LOST

Case study narrative:

- A container shipping operator loses connectivity to essential data due to the collapse of the data centre in a third country
- The loss of data impedes loading and unloading for 3 vessels in port at the time of the incident
- Disaster recovery invoked however it takes 4 days
- Owner incurs additional port charges
- Ship owner loses significant money owing to loss of availability data
- Poorly negotiated contract with data centre exacerbates loss to owner
- Data centre was vulnerable – arising from poor installation of backup and anti virus upgrade

Investigation identified

- Dependency on a single data centre with no operational back-ups
- Poor understanding of the importance of a critical shoreside supplier and potential impact on shipping operations
- Poorly worded contract prevented more pressure to be exerted on supplier
- No evidence of business continuity plan having been tested
- No senior management oversight between data management and shipping operations

Recommendations & Remediation

- Improved focus and understanding of critical suppliers and levels of dependency
- Improved contracting policy with suppliers that reflected the importance of the supplier services
- Revised data centre architecture with operational back-ups created and regularly tested
- Improved Business Continuity Plan and programme of regular testing involving testing across the different functions in the business

SUMMARY

Client contacts ACL after a loss of essential data → **Poor BCP means no available back-up systems** → **Poor understanding of critical dependencies and contractual indemnities** → **Improved contracting regime and BCP** → **OUTCOME: Improved cyber hygiene and security**