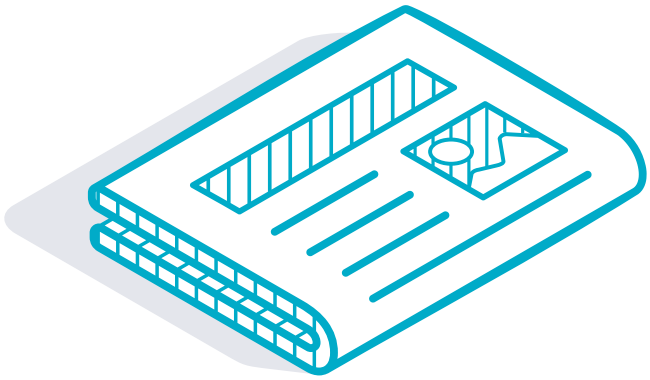

9 CASE STUDY 1: PHISHING - PROCESS FAILURE – LOSS OF FUNDS

Case study narrative:

- A shipping company needed to pay bunkering charges.
- A clerk in the accounts payable received an e-mail from the bunkering company informing them of a change of bank account.
- Because the document looked genuine, the clerk amended the details on the finance system and made the payment (USD 600,000).
- On arrival at the port in question, the ship requested bunkering and was met with a statement to the effect that they had not paid.
- Payment had been made before fraud was discovered.
- During investigation email found to be similar but not exactly the same as the genuine bunkering organisation; the attachment was a reasonably sophisticated forgery.

Scope of review:

Identify the cause of the loss and recommend improvements and next steps

Baseline review

- Identified the shipowner as immature in respect of cyber risk posture
- No board stated risk appetite for cyber loss
- No strategy or management leadership of cyber risk
- Minimum network security employed with anti-virus employed and updates met minimum maintenance requirements
- No regular or planned process for updating software
- Invoice payment process and in particular change of beneficiary approval oversight and approval was absent
- Primary e payments and procedures were satisfactory – but no oversight or second pair of eyes

Recommendations & Remediation

- Multi-factor authentication of e-payments be introduced
- Internal payment procedures enhanced
- Create and implement recovery plan with remitting bank for identifying suspicious payments
- Increase firewall security
- Define a cyber risk appetite

SUMMARY

Client contacts ACL after a navigational incident

Poor network security allowed vessel to be vulnerable

Investigation identified that a programme of co-ordinated activities is required

Improvement in cyber security posture of client

OUTCOME:
Improved cyber hygiene and security