

16 CASE STUDIES: PORT OPERATOR - MATURE CYBER LEADERSHIP –INADEQUATE MANAGEMENT INFORMATION

Case study narrative:

- Client is operating near to Network Information Systems Regulation 2018 standards which has been a process of over 3 years to achieve – following a planned and articulate strategy.
- UK port operator uses 'top-end' capability to monitor events on their network
- The monitoring product cost GBP 500,000 pa and has been in place 18 months
- Port has yet to realise any benefit from investment
- Too many false positives, too much data, few if any viable management options

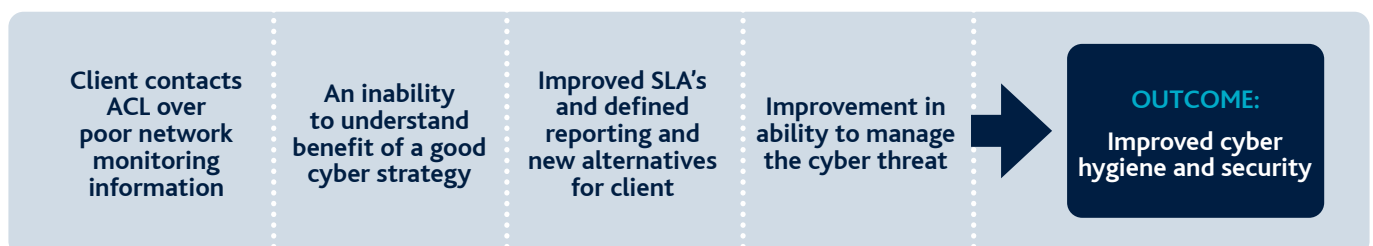
Investigation identified

- Security Information and Event Management (SIEM) provides huge amounts of data which is cognitively inaccessible and managerially impossible to interpret
- The board and management need clear information to help them manage and evidence management of the cyber risk
- Product configuration to deliver desired outcomes has not been achieved
- Defined board risk appetite; evidence of implementation of strategy; detailed evidence of process and measuring outcomes, evidence of continuing improvement across people process and technology

Initial Review

- Review the implementation of network monitoring
- Reconfigure the management information escalation to board
- Continued inadequate management information returned to the board to evidence monitoring of network and therefore not able to evidence state of the art processes benefiting the company
- Review SLA with service provider – specific advice offered
- Explore alternatives and tender for services

SUMMARY



Astaara London Limited is an appointed representative of Ambant Underwriting Services Limited, a company authorised and regulated by the Financial Conduct Authority under firm reference number 597301 to carry on insurance distribution activities. Astaara London Limited is registered in England and Wales company number 12570450. Registered office at 7th Floor, 1 Minster Court, Mincing Lane, London, EC3R 7AA.