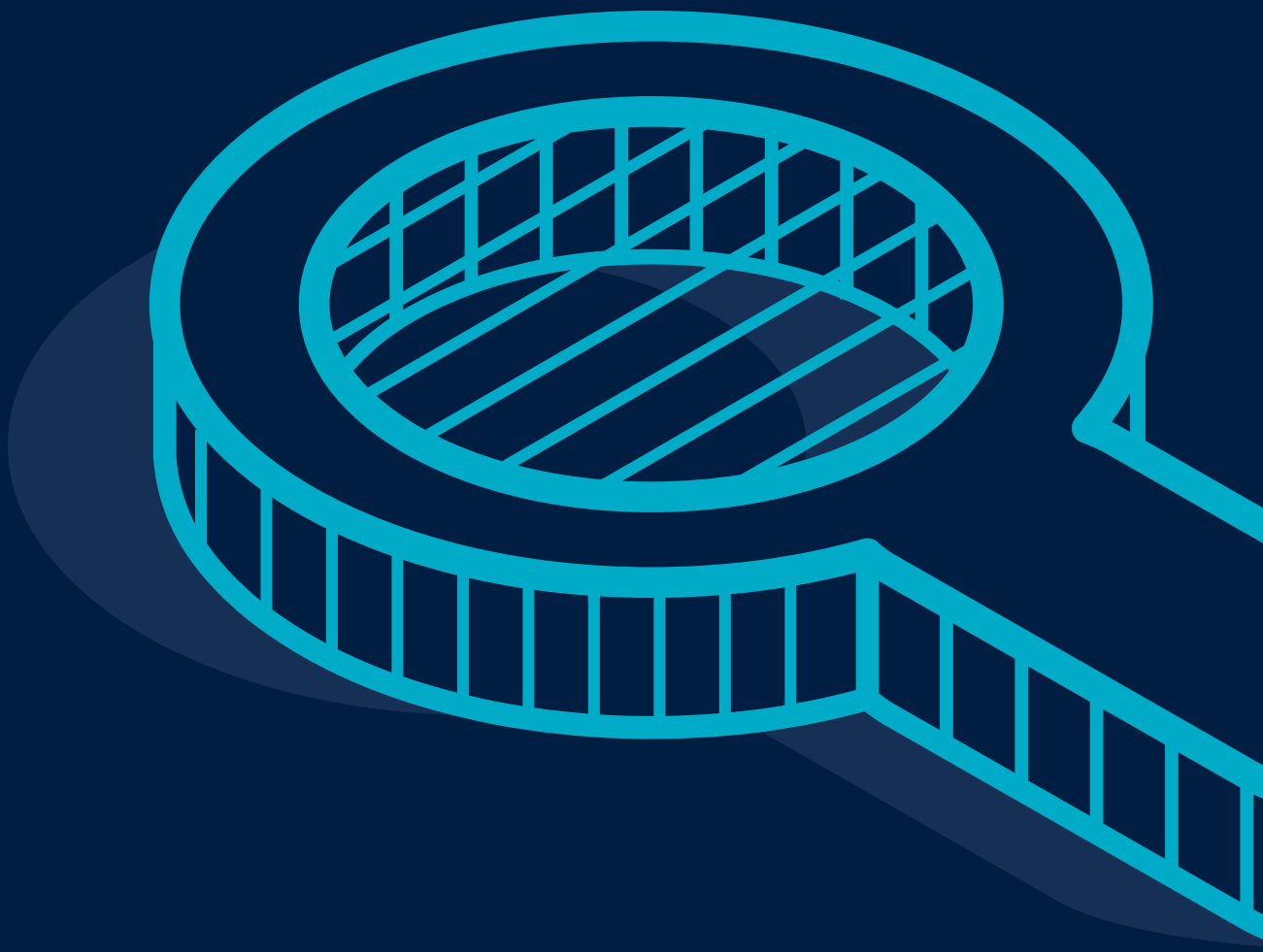
ASTAARA
COMPANY LIMITED

The AstaaraCyber Review Process

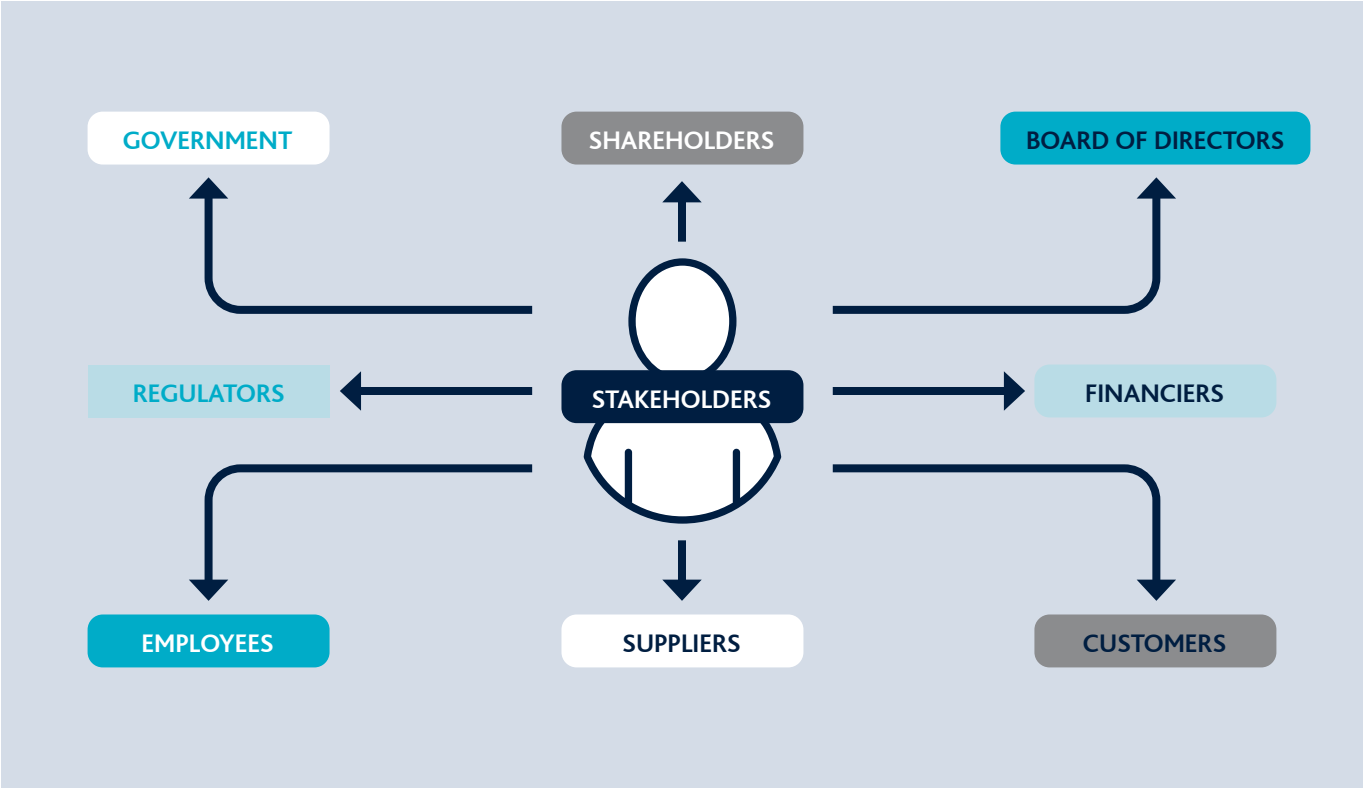


#ResilienceandRecovery

#ResilienceandRecovery

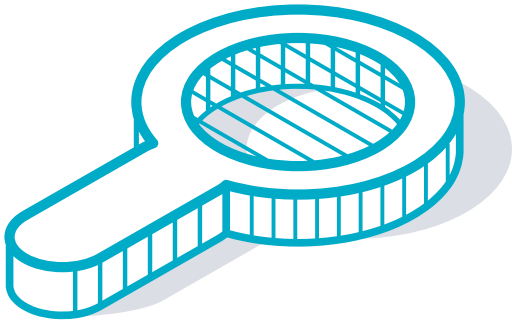
CONTENTS

1 ALL STAKEHOLDERS POTENTIALLY BENEFIT FROM ASTAARACYBER POLICY OF INSURANCE



Benefits of AstaaraCyber

- Increase confidence across all your stakeholders
- demonstrable leadership managing your ability to withstand and recover from cyber incidents
- differentiate your service with your customers
- evidence to your D&O underwriters you are managing the risk – help reduce the cost



2 AN OVERVIEW OF THE ASTAARACYBER CONSULTING PROCESS

- We operate a five stage process from evaluation to improvement
- This process provides a clear pathway and evidence of proactive actions taken to improve your cyber security posture
- There is an obligation on you to commit the necessary resources to gain the most out of our work
- We charge transparently for each stage of the process and establish clear outputs
  - » We scope the estimated work required for each stage of the process in conjunction with yourselves
  - » The basis of charging is per diem for the agreed piece of work. This price is agreed in advance.
  - » Only if there is a material change of scope will adjustments be made – any scope change will be agreed with you in advance

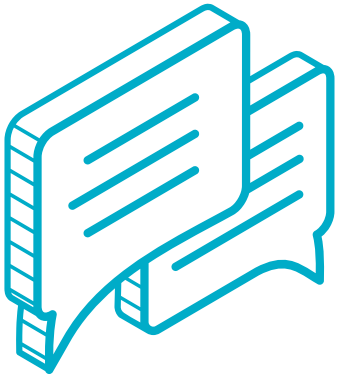
3 ASTAARACYBER: IMPROVING RESILIENCE TO AND RECOVERY FROM A CYBER ATTACK

Resilience

- Be more difficult to breach
- Compliance to recognised cyber security standards

Recovery

- BCP to minimise operational disruption
- Insurance for:
  - Defence & remediation
  - Physical loss
  - Liabilities
  - Loss of Revenue / BI

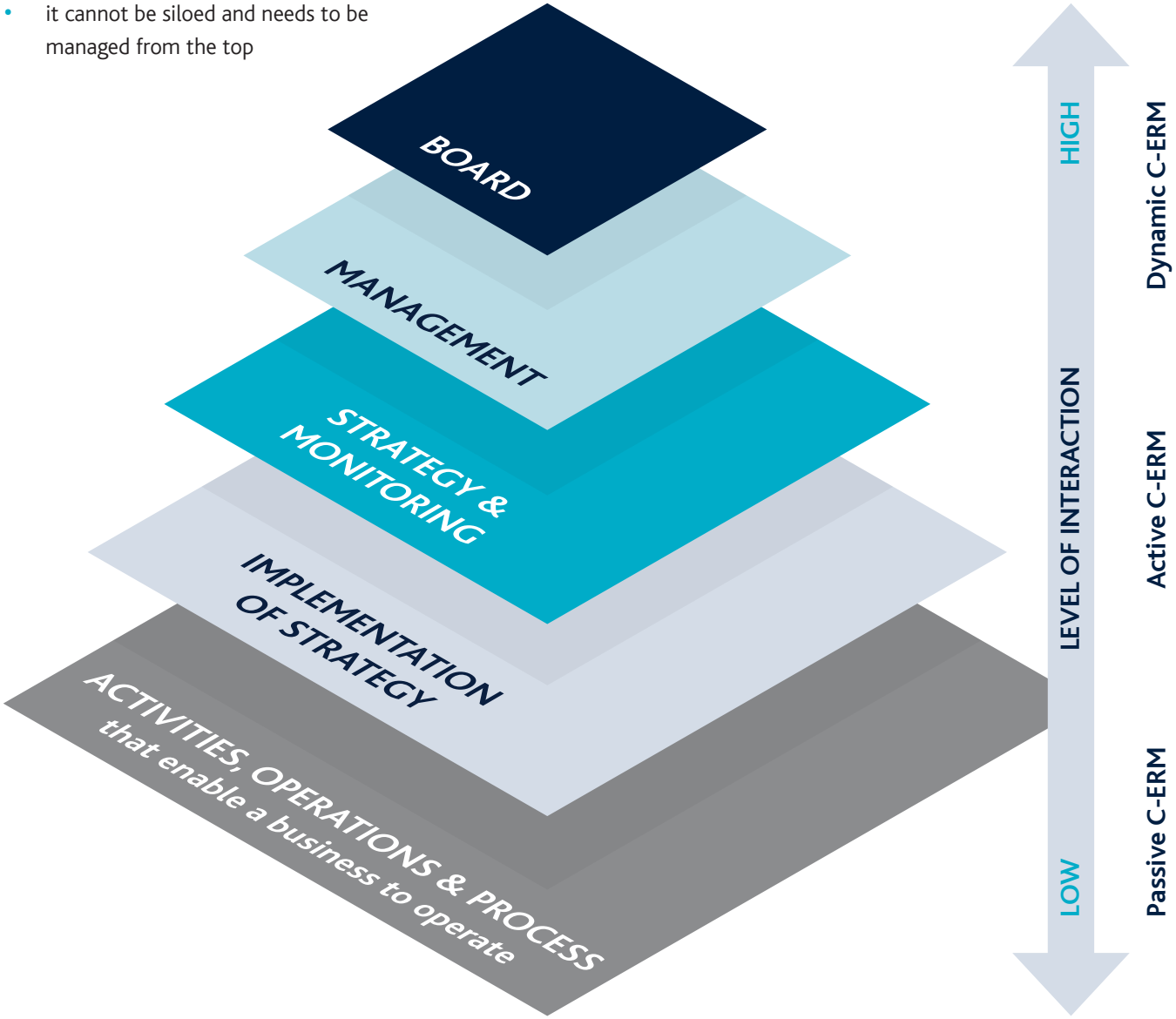


4 CONTROLLING THE CYBER RISK IS ABOUT ENTERPRISE RISK MANAGEMENT AND LEADERSHIP FROM THE TOP

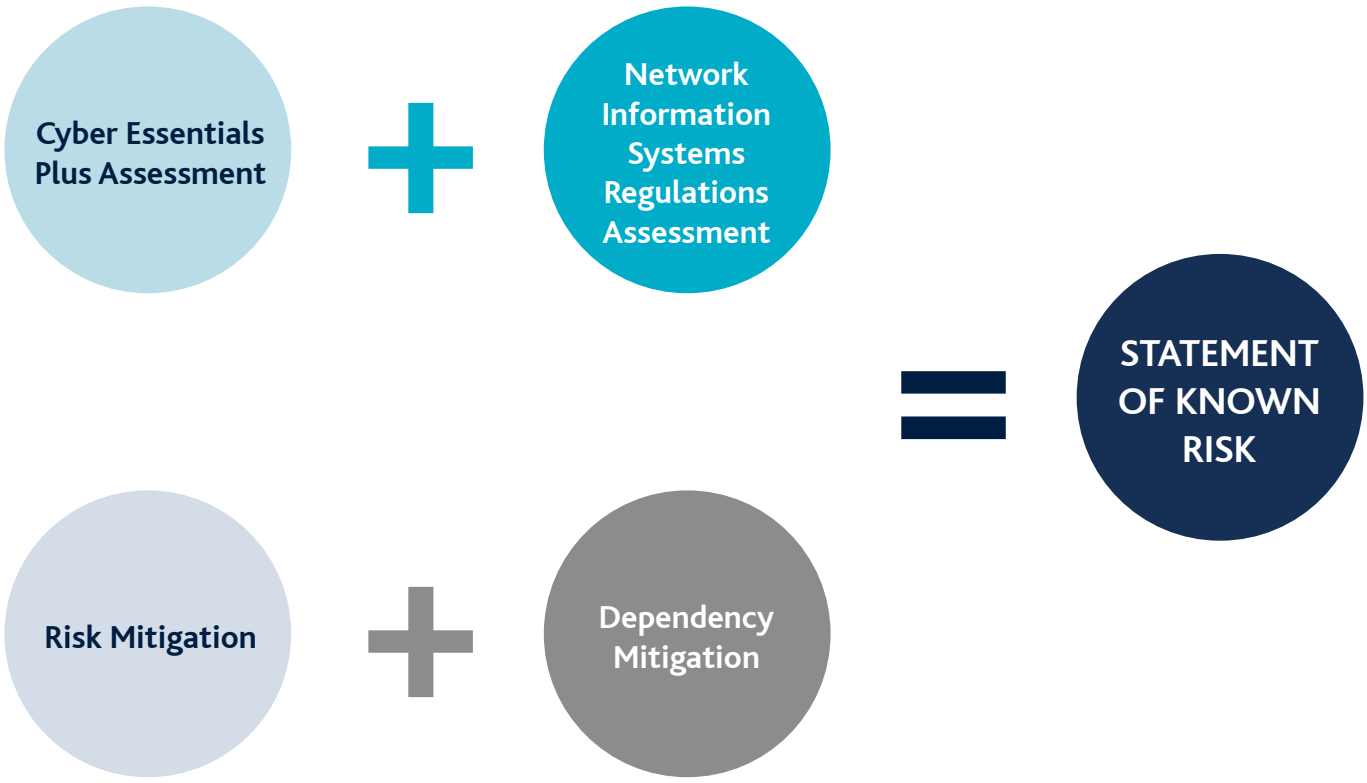
LEAP - Leadership, Evidence, Activity, Processes

Cyber affects all aspects of a business.

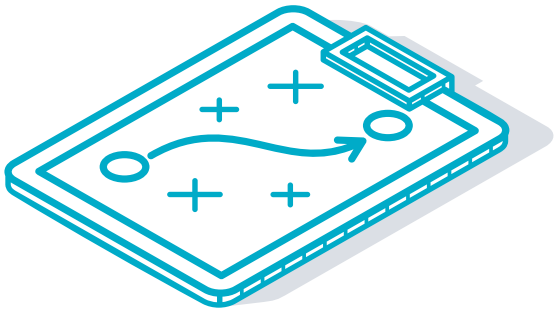
- it cannot be siloed and needs to be managed from the top



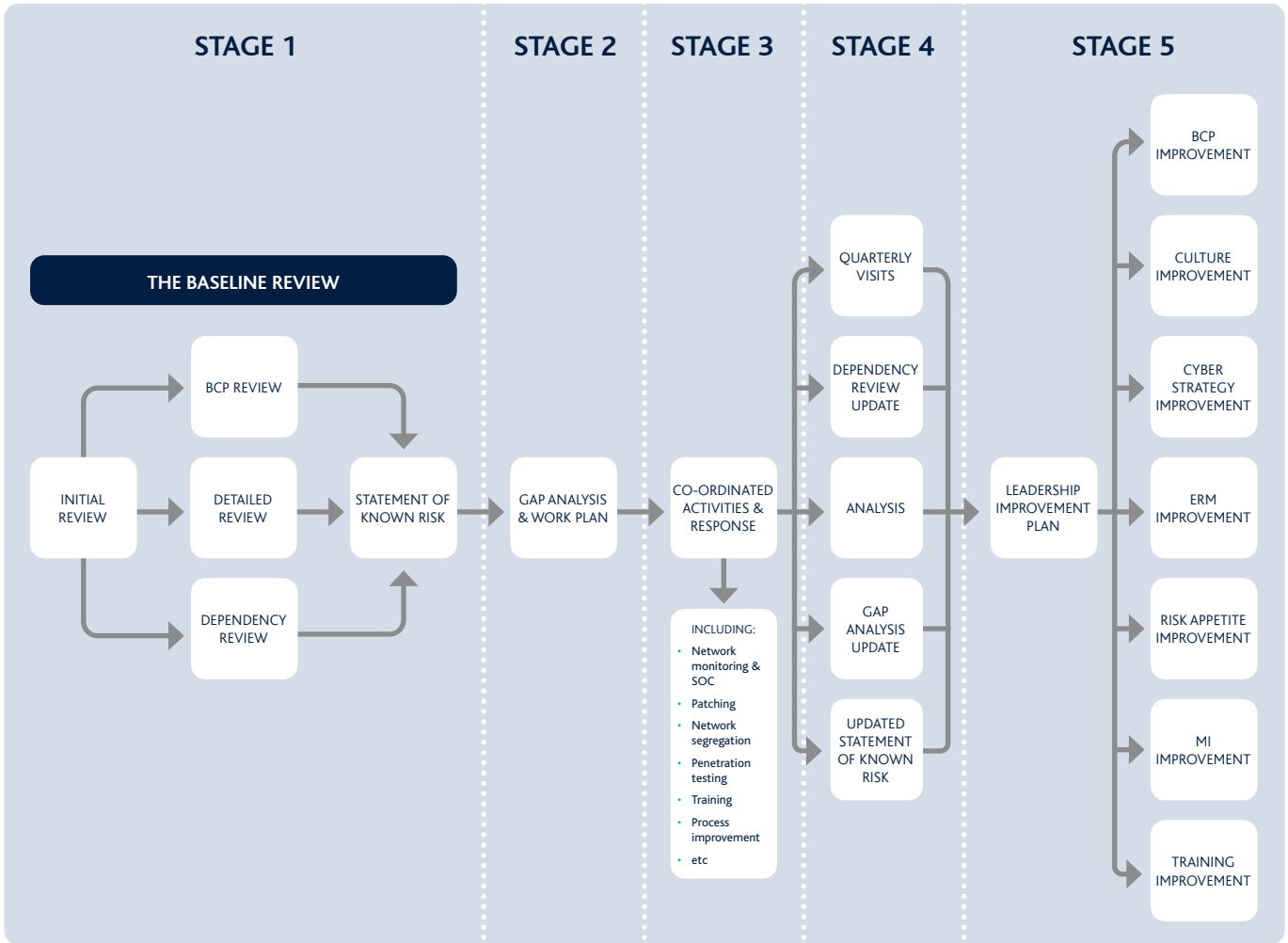
5 THE BASELINE REVIEW ASSESSES THE CURRENT CYBER POSTURE OF THE CLIENT AND PRODUCES THE STATEMENT OF KNOWN RISK

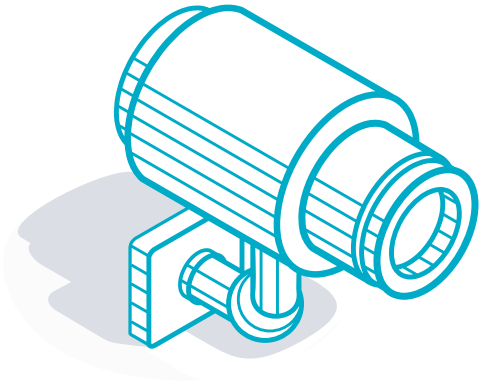


Cyber Essentials Plus, the UK's basic cyber security regime: https://www.ncsc.gov.uk/cyberessentials/overview
Network Information System Regulations, the UK's cyber regime for essential services https://www.ncsc.gov.uk/collection/caf/nis-introduction



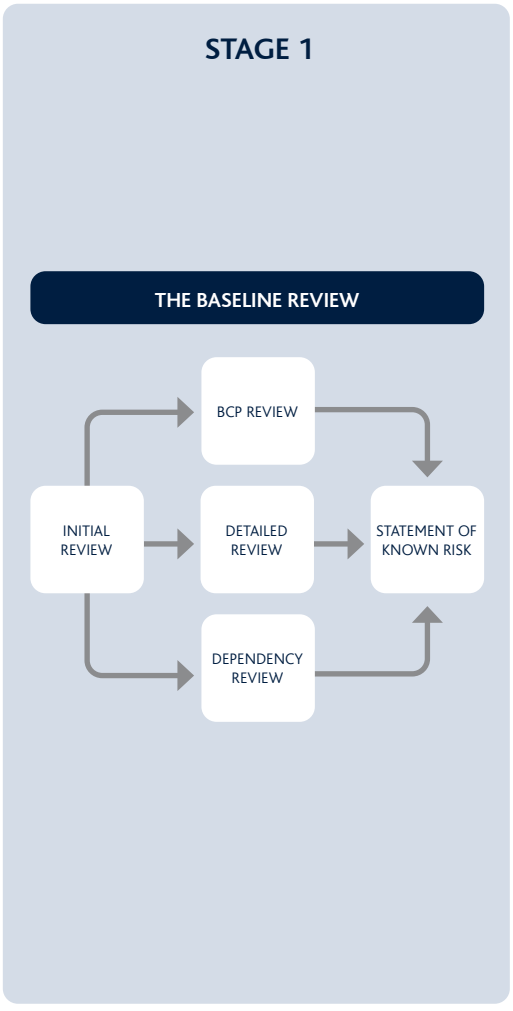
6 HOW DO WE DELIVER STRATEGIC OUTCOMES TO OWNERS



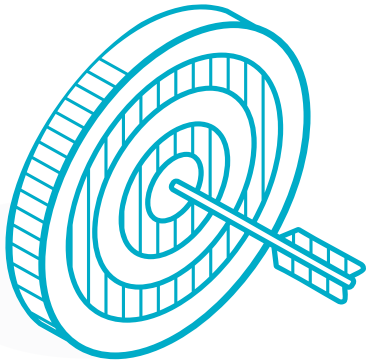


7 STAGE 1: THE BASELINE REVIEW FROM INITIAL REVIEW TO STATEMENT OF KNOWN RISK

- The Baseline review assesses the current cyber security posture of the client
- It is a critical determinant of the current insurability of a client
- This phase comprises of three elements



This stage allows us to identify the scope of future work and determines the next steps we agree with you in stage 2



8 STAGE I: FROM INITIAL ASSESSMENT TO STATEMENT OF KNOWN RISK FURTHER DETAIL ...

1 SCOPING AND INITIAL ASSESSMENT

- Web-based initial review questionnaire identifies main areas of cyber activity undertaken by the client.
- As part of the scoping element we will provide you access to our online portal
- The initial assessment will provide you with an initial output and determine the breadth and focus of the core reviews

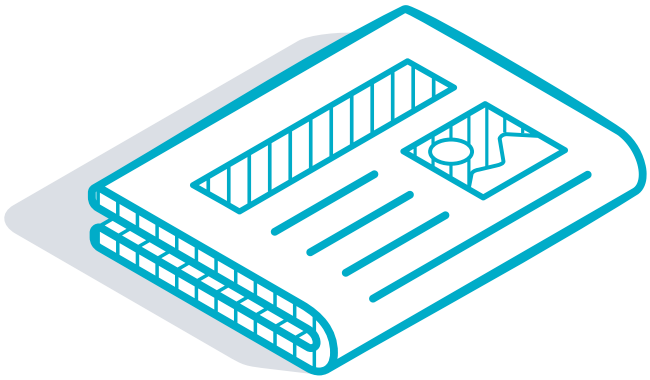
2 CORE REVIEWS

- In-depth process to identify risks, vulnerabilities and opportunities in the client's infrastructure.
  - » **BCP review:** business continuity plans need to be thorough, regularly tested and continually improved.
  - » **Detailed review:** seeks a much wider field of knowledge about a potential insured's ecosystem. Detailed look at processes, people, training and technology. Includes interviews and ship visits.
  - » **Dependency review:** considers which organisations are most critical to your success and whose services are critical to your operation. Covers terms and conditions under which you have acquired the services, and how the contract deals with outages and liability.

3 OUTPUT

A Statement of Known Risk

- an agreed set of risks, associated with people, processes or technology which need aggressive management to protect you from the worst consequences of a cyber breach
- Known risks form the basis of decisions on pricing and remediation
- We will specify the actions that will need to be taken by you to mitigate risk further, whether by us, through your suppliers or by your own teams



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

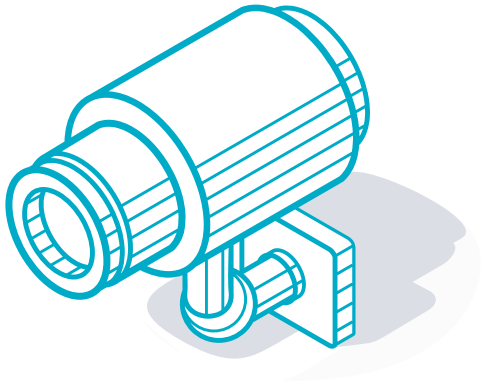
Client contacts ACL after a navigational incident

Poor network security allowed vessel to be vulnerable

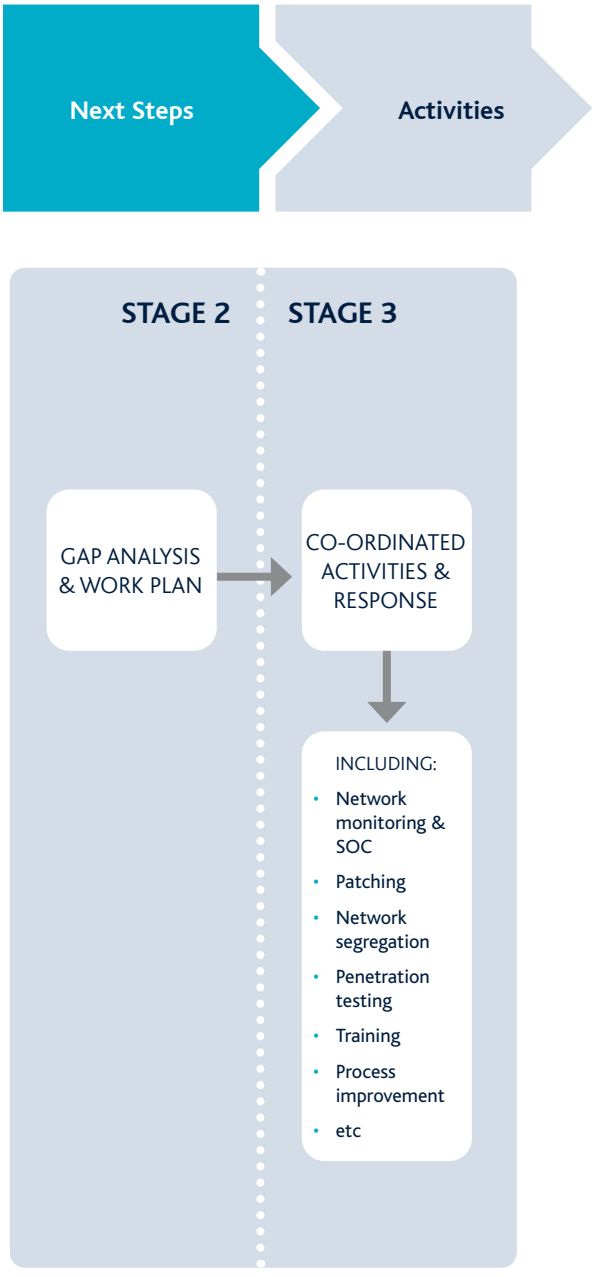
Investigation identified that a programme of co-ordinated activities is required

Improvement in cyber security posture of client

OUTCOME:
Improved cyber hygiene and security



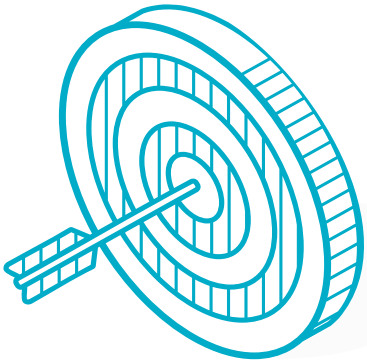
10 STAGES 2 AND 3: ASSESSING THE GAP, PLANNING REMEDIATION AND DELIVERING



- We identify the gaps in your approach to cyber security
- We measure where you are against CE+* and NISR^ and where you are
- We establish what activities need to be put in place
- Performing the co-ordinated activities well assists you in being at least CE+*

These stages allows us to develop a work plan and help you set up the coordinated activities to improve your cyber security posture

* CE+ = Cyber Essentials Plus, the UK's basic cyber security regime
^ NISR = Network Information System Regulations, the UK's cyber regime for essential services



11 STAGES 2 AND 3: ASSESSING THE GAP, PLANNING REMEDIATION AND DELIVERING

1 GAP ANALYSIS

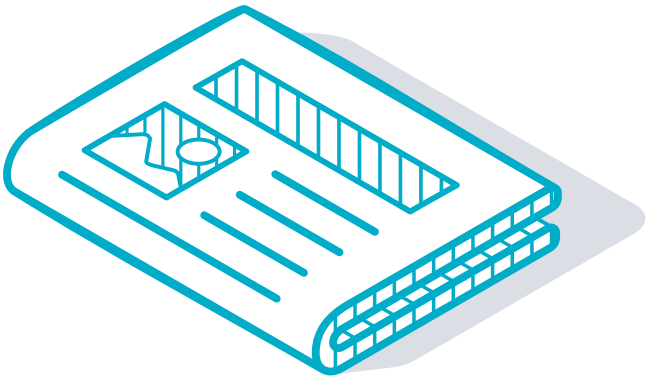
- The assessment will be done by qualified and accredited professionals
- It is based on the knowledge gained during the Baseline Review (Stage 1)
- This details the scale of the challenge, and what needs to be done

2 WORK PLAN

- In developing the Work Plan we consider within the context of your business in terms of:
  - What people need to do and stop doing
  - What process changes there need to be
  - What new processes there needs to be and
- We will work with you to evolve the underpinning technological changes required to remove any long standing vulnerabilities:
  - Most will be relatively straightforward e.g. technology purchasing;
  - Some might however take more time (e.g. cultural change)

3 CO-ORDINATED ACTIVITIES

- These are a range of activities to improve the levels of cyber hygiene
- These need to be dealt with programmatically
- These need to be switched into business as usual as quickly as possible to maintain the momentum of change.
- Activities need to be coordinated so that they do not conflict with each other and can operate alongside your core operational processes



12 CASE STUDY 2: POORLY PROTECTED ON-BOARD NETWORKS - LACK OF NETWORK SEGREGATION - CORRUPTION OF ECDIS SYSTEM

Case study narrative:

- Shipowner has satellite communications capability installed on their fleet and ships broadcast an IP address.
- Hackers accessed on-board networks using this IP address
- Hackers hop from external to internal networks to access chart and navigation systems, as well as accessing essential telemetry systems for e.g. engine management, ballast control etc.
- Hackers Altered ECDIS software to render inaccurate position
- Ship veered off course, wasting fuel and time
- Bridge management team had to resort to dead reckoning and non-GPS navigation techniques (a paper chart)

Investigation identified

- A lack of segregation (physical and logical) between on-board OT network, internal email network and satellite feed
- A lack of proper configuration of firewalls between these networks to permit only known types of traffic
- Access control systems inadequate

Recommendations & Remediation

- Gap analysis identified material shortcoming in vessel cyber security and related vessel safety management
- An agreed work programme would:
  - » Improve network segregation to improve operational resilience
  - » Improve network monitoring and security to improve vessel safety management
  - » Improve core defences by implementing a structured patching programme
  - » Improve access control and password management

SUMMARY

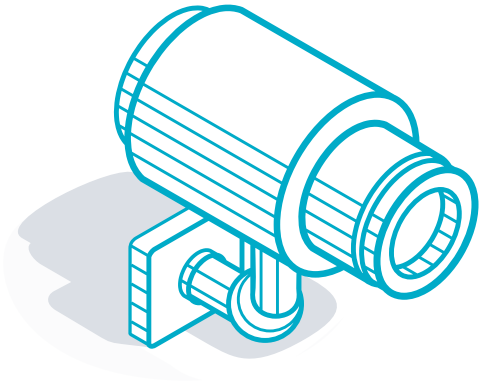
Client contacts ACL after a navigational incident

Poor network security allowed vessel to be vulnerable

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

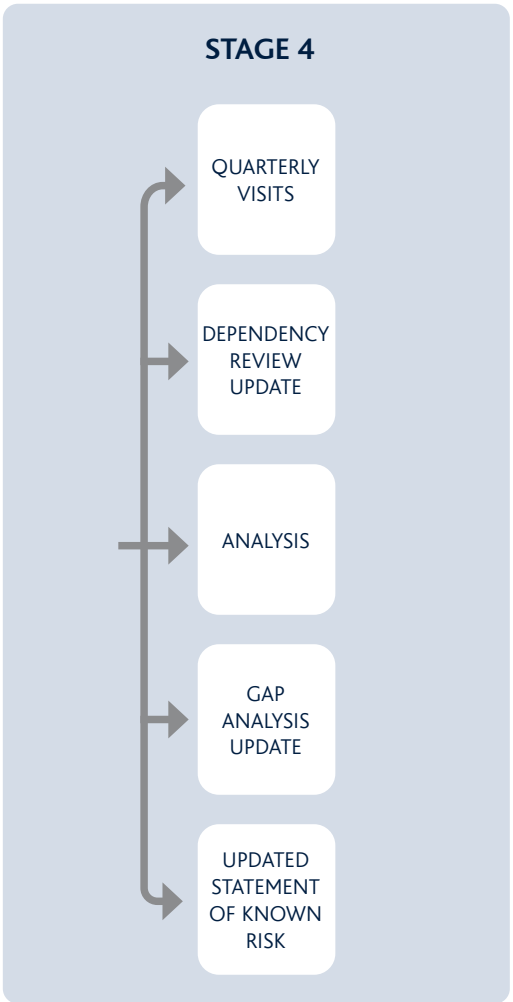
Improvement in cyber security posture of client

OUTCOME:
Improved cyber hygiene and security



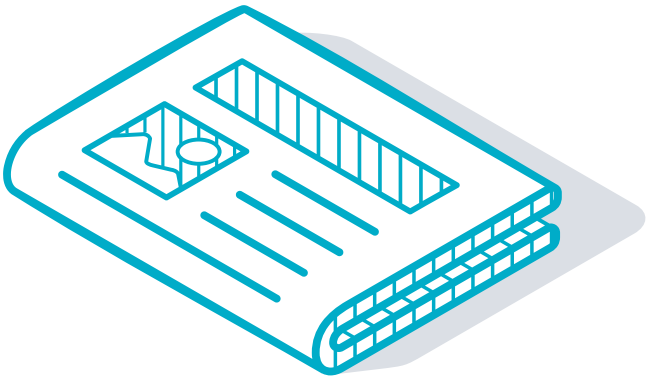
13 STAGE 4: KNOWING WHAT IS HAPPENING TO MAINTAIN THE ADVANTAGE

Evidence & Monitoring



- We help you gather the evidence of the activities that are being undertaken
- We review and verify the evidence: no surprises – accept some of this takes time
- We help provide regular monitoring of progress and reporting to the board
- We assess progress against the agreed Work Plan by using the output from the co-ordinated activities

This stage ensures the right things are done and provides transparency of the cyber risk and accountability of ownership



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

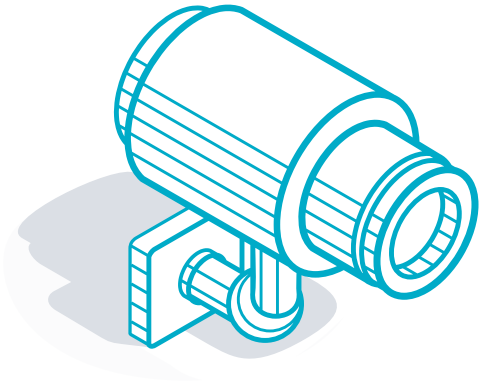
- Dependency on a single data centre with no operational back-ups
- Poor understanding of the importance of a critical shoreside supplier and potential impact on shipping operations
- Poorly worded contract prevented more pressure to be exerted on supplier
- No evidence of business continuity plan having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

Recommendations & Remediation

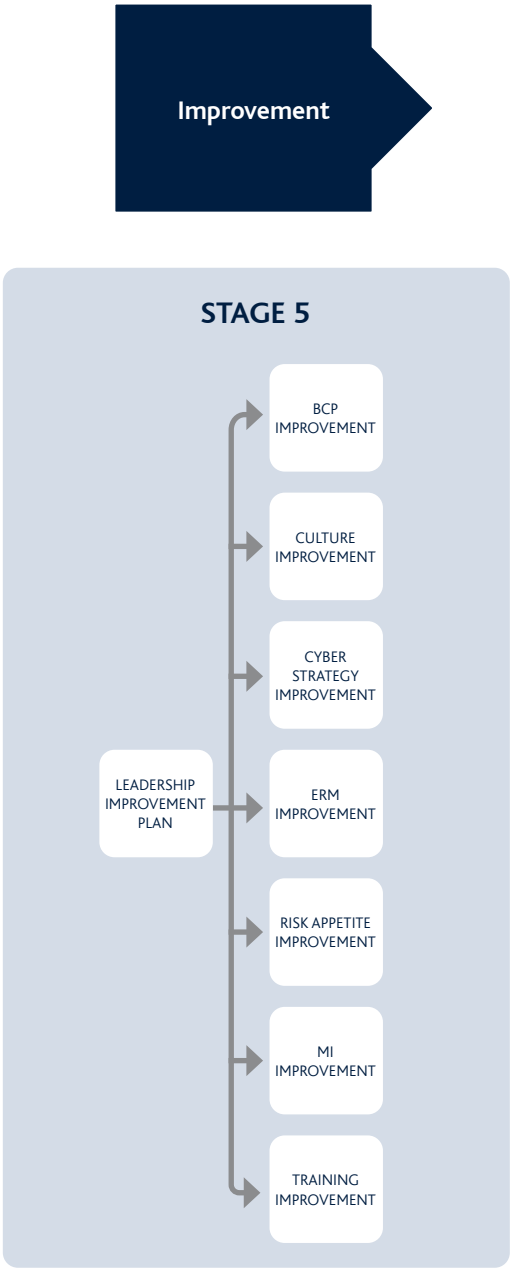
- Improved focus and understanding of critical suppliers and levels of dependency
- Improved contracting policy with suppliers that reflected the importance of the supplier services
- Revised data centre architecture with operational back-ups created and regularly tested
- Improved Business Continuity 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**

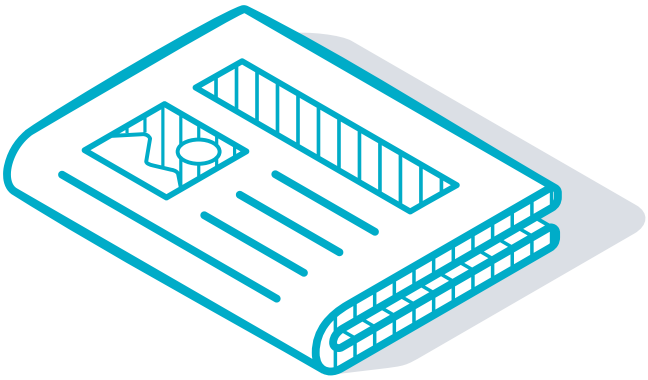


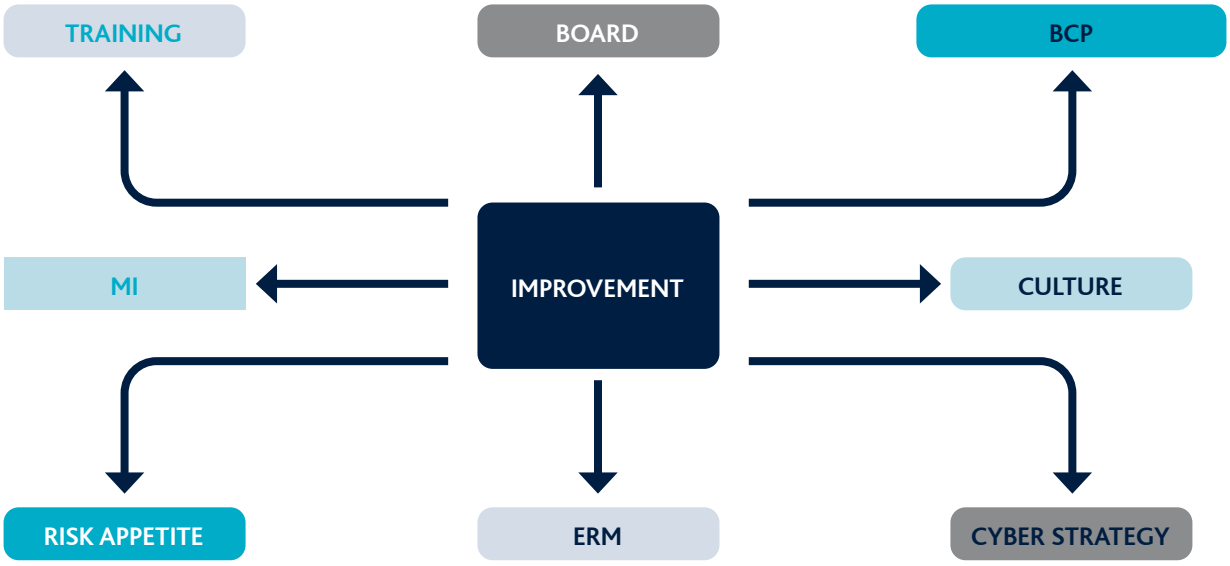
15 STAGE 5: CONTINUOUS IMPROVEMENT IS ENTERPRISE WIDE



- We recognise that the cyber threat is dynamic and constantly changing
- Standing still is not an option – it is a continuous process. As the threat evolves your response will get more detailed
- Processes that are only followed in emergency rapidly become unviable due to lack of practice and their expense

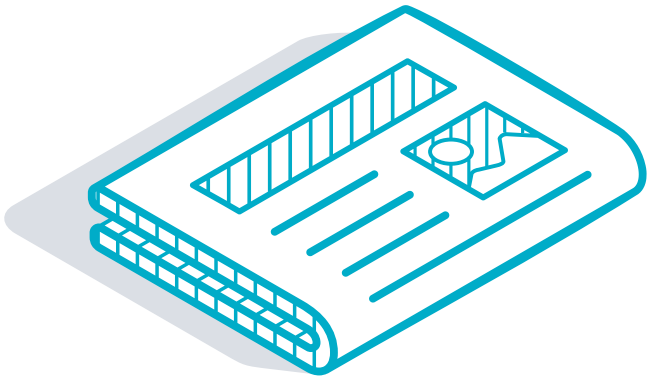
This stage ensures there is a drive to improve the resiliency to the cyber threat and improve the ability to recover





- This process allows insureds to improve their enterprise risk management policies processes and procedures and to have that improvement recognised
- It starts from the top: the board needs to own the cyber risk as it affects the whole enterprise
- BCPs must be regularly tested and lessons learnt and processes updated
- The culture of the organisation needs to be constantly evolving to respond to new digitisation, new technologies and new threats
- Critical to all of this is good management information, and appropriately trained staff who will need to use it and present it to management in a digestible and clear form for appropriate decision-making

OUR OBJECTIVE IS TO ENABLE YOU TO RETURN TO PROFITABILITY AFTER ATTACK AS SOON AS POSSIBLE – AND THE IMPROVEMENT OF THAT RECOVERY TIME IS A KEY SUCCESS CRITERIA FOR BOTH YOU AND US.



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

Client contacts ACL over poor network monitoring information

An inability to understand benefit of a good cyber strategy

Improved SLA's and defined reporting and new alternatives for client

Improvement in ability to manage the cyber threat

OUTCOME:
Improved cyber hygiene and security

ASTAARA
COMPANY LIMITED

www.astaara.co.uk

robert.dorey@astaara.co.uk william.egerton@astaara.co.uk james.cooper@astaara.co.uk