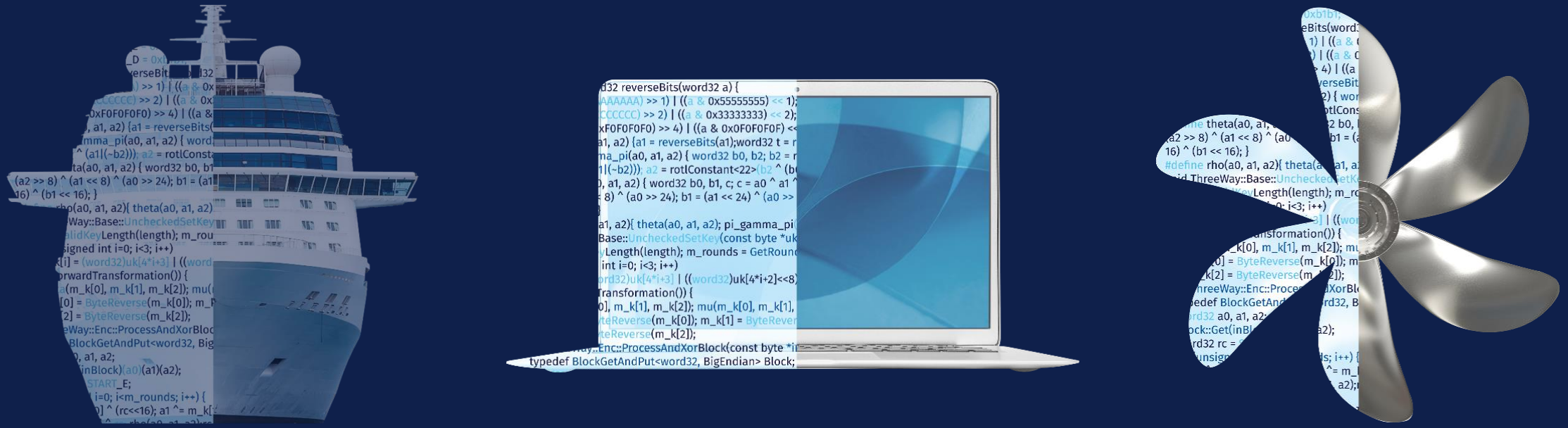
WHEN TRUST MATTERS

IMPROVING CYBER-RESILIENCE IN MARITIME INDUSTRY

Vijayan Manogara
Principal Consultant – Industrial Cybersecurity

14 Nov 2022

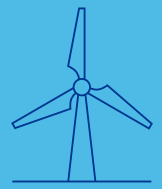


DNV is an independent assurance and risk management company

157	~12,000	100,000	100+	5% R&D
years	employees	customers	countries	of annual revenue

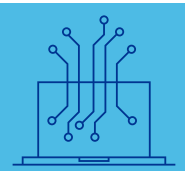
Ship and offshore classification and advisory

Energy advisory, certification, verification and monitoring



Management system certification, supply chain and product assurance

Software, platforms and digital solutions



Our purpose

To safeguard life, property, and the environment

Our vision

A trusted voice to tackle global transformations

Cyber Security is a key driver in DNV's Purpose and Vision

DNV's Cyber Security Services and Capabilities

Strategy & Programme
Develop effective cyber security strategies and programmes, even when you face tight deadlines

Testing & Verification
Test and verify the resilience of systems, networks and components, and access practical, unbiased advice to enable you to prioritize mitigation of vulnerabilities

Safety & security risk management
Ensure security and safety in the design of new and existing projects

Governance, risk & compliance
Implement robust governance, risk, and compliance strategies across projects and operations

Incident response & investigation
Understand what went wrong, what you need to do to recover effectively and establish robust procedures for handling cyber attacks

Insights & training
Ensure that you have the right insights and training in place to build awareness across the full life cycle of your operations

Applied Risk
a DNV company

ISASecure

DNV

DNV cyber security maritime/offshore references

World's biggest **passenger ships**

World's first **LNG powered ships**

World's largest **LNG carriers**

World's harshest conditions **drill-ships**

World-class **production assets**

World's most **complex** surveys

DNV

Main drivers for Cyber security in maritime and offshore industries

Incidents

- ***Growing number of cyber safety and security incidents**, both **IT** (information technology) and **OT** (operational technology) impacted, and **limited transparency** and experience sharing*

➢ ***Examples with Hurtigruten, IMO, AIDA, MSC, CMA CGM, …***

Regulation

- ***International and national/regional cyber security** and data privacy laws and regulation implemented, and **financial impact** with charter requirements and insurance*

➢ ***ISM audits cover cyber risk from 2021, mandatory for all shipping companies***

➢ ***Flag / port state controls with risk of detentions (e.g. USCG CVC-WI-027)***

Digitalisation

- ***Increased complexity of vessels** with more software, automation and connectivity, and **cyber safety & security is a crucial enabler** for the maritime and offshore industry to safely realise the benefits of digital transformation*

➢ ***Digitalisation cannot be done safely without considering cyber risks!***

International Management Code(IMO) demands on cyber security

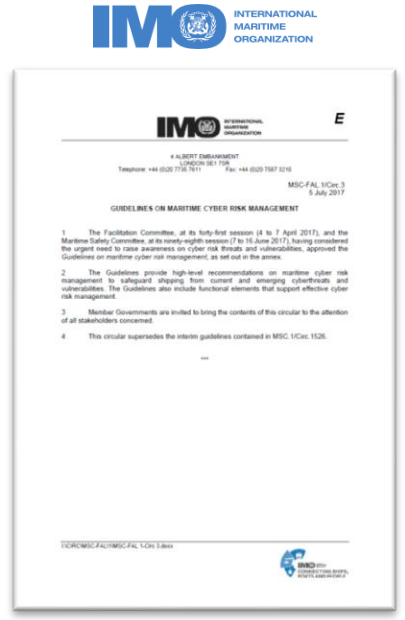
IMO has issued MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management.

The guidelines ***provide high-level recommendations on maritime cyber risk management*** to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management. The recommendations can be incorporated into existing risk management processes and are complementary to the safety and security management practices already established by IMO.

The Maritime Safety Committee(MSC), at its 98th session in June 2017, also adopted **Resolution MSC.428(98)** - Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages administrations to ensure that ***cyber risks are appropriately addressed in existing safety management system***, until the first Document of Compliance after 1 January 2021

Maritime Cyber Risk Management

- IT and OT systems,
- Cyber risk management: Cyber safety and cyber security,
- Intentional and unintentional events
- NIST structure: Identify – Protect – Detect – Respond – Recover,
- Referring to international best practices



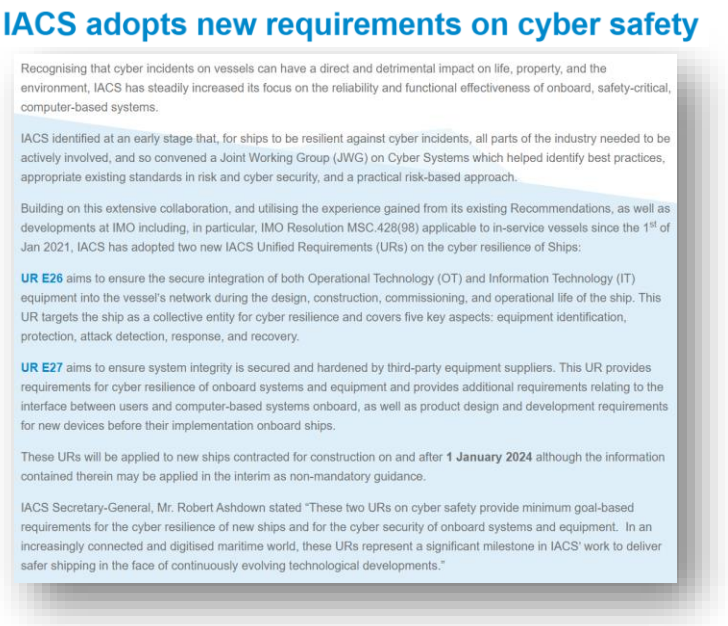
Examples of Vessel's Critical OT Systems

1 Bridge systems; .
2 Cargo handling and management systems; .
3 Propulsion and machinery management and power control systems; .
4 Access control systems; .
5 Passenger servicing and management systems; .
6 Passenger facing public networks; .
7 Administrative and crew welfare systems; and .8 Communication systems.

IACS just released Unified Requirements on Cyber Security for ships and systems

- Applies to new ships contracted for construction on and after **1 January 2024.** May be applied in the interim as non-mandatory class notation.
- **UR E26** to **secure integration of both Operational Technology (OT) and interfaces to Information Technology (IT)** equipment into the vessel's network architecture during the design, construction and commissioning of the ship.
- **UR E27** to ensure **system integrity is secured and hardened by third-party equipment suppliers** and provides requirements for cyber resilience of onboard systems.
- Ongoing work on a 3rd UR which looks at **survey requirements**.
- Supports owner with concrete barriers to meet IMO resolution MSC.428(98).
- Vendors of onboard automation and navigation systems should act now due to potential longer development process.
- DNV's current cyber security rules with more than 100 vessels & systems contracted is fully aligned with IACS URs, both being based on the recognized standard IEC 62443.

IACS International Association of Classification Societies



IACS adopts new requirements on cyber safety

Recognising that cyber incidents on vessels can have a direct and detrimental impact on life, property, and the environment, IACS has steadily increased its focus on the reliability and functional effectiveness of onboard, safety-critical, computer-based systems.

IACS identified at an early stage that, for ships to be resilient against cyber incidents, all parts of the industry needed to be actively involved, and so convened a Joint Working Group (JWG) on Cyber Systems which helped identify best practices, appropriate existing standards in risk and cyber security, and a practical risk-based approach.

Building on this extensive collaboration, and utilising the experience gained from its existing Recommendations, as well as developments at IMO including, in particular, IMO Resolution MSC.428(98) applicable to in-service vessels since the 1st of Jan 2021, IACS has adopted two new IACS Unified Requirements (URs) on the cyber resilience of Ships:

UR E26 aims to ensure the secure integration of both Operational Technology (OT) and Information Technology (IT) equipment into the vessel's network during the design, construction, commissioning, and operational life of the ship. This UR targets the ship as a collective entity for cyber resilience and covers five key aspects: equipment identification, protection, attack detection, response, and recovery.

UR E27 aims to ensure system integrity is secured and hardened by third-party equipment suppliers. This UR provides requirements for cyber resilience of onboard systems and equipment and provides additional requirements relating to the interface between users and computer-based systems onboard, as well as product design and development requirements for new devices before their implementation onboard ships.

These URs will be applied to new ships contracted for construction on and after **1 January 2024** although the information contained therein may be applied in the interim as non-mandatory guidance.

IACS Secretary-General, Mr. Robert Ashdown stated "These two URs on cyber safety provide minimum goal-based requirements for the cyber resilience of new ships and for the cyber security of onboard systems and equipment. In an increasingly connected and digitised maritime world, these URs represent a significant milestone in IACS' work to deliver safer shipping in the face of continuously evolving technological developments."

DNV

BEST PRACTICES FOR IMPLEMENTATION OF CYBER RISK MANAGEMENT

Cyber risk management guidelines by IMO provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyberthreats and vulnerabilities.

For detailed guidance on cyber risk management, users of these Guidelines should also refer to Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

Additional guidance and standards may include, but are not limited to:

1 The Guidelines on Cyber Security Onboard Ships produced and supported by **BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.** .

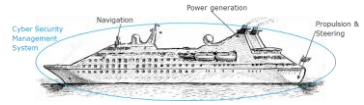
2 **ISO/IEC 27001 standard** on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). .

3 United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the **NIST Framework**).

Cyber Security in the Class scope for ships and offshore units

Cyber Secure Class Notation (DNV-RU-SHIPS Pt.6 Ch.5 Sec.21)

- **Pre-defined scope important and essential systems,** and based on recognized standards, different levels suitable for **all vessel segments**



Cyber Secure Type Approval (DNV-CP-0231)

- **Pre-qualify vessel system's or component's** security capabilities using DNV-CP-0231

Existing vessels

Cyber secure

Entry-level for all merchant vessels

- **For standard merchant vessel, security is ensured through policies & procedures, segmentation of networks/zones, secure remote access, etc.**
- **Aligned with compliance towards IMO Resolution 428(98)**
- **Intended for existing and newbuildings in of standard merchant vessel segments**

IACS UR 2024

Cyber secure (ESSENTIAL)

existing vessels with SOLAS essential system coverage

- **Essential** covers the above plus system security capabilities at **Security Profile 1**
- **~40 system requirements** from up to IEC62443-3-3 SL-1
- Primarily intended for **existing high end vessels** and **complex newbuilds**

Advanced projects

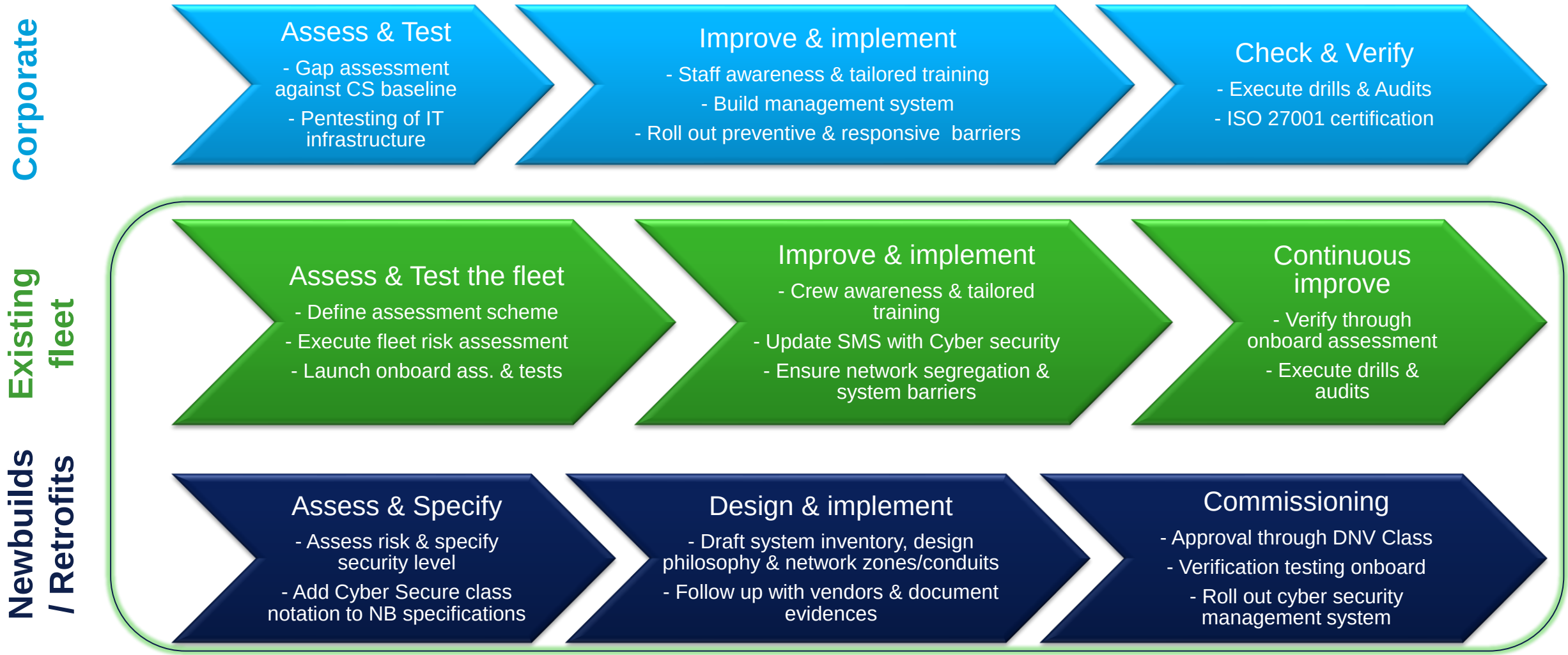
Cyber secure (ADVANCED)

complex newbuildings with higher security requirements

- **Advanced** covers above plus system security capabilities at **Security Profile 3**
- **~80 system requirements** from up to IEC62443-3-3 SL-3
- Primarily intended for **advanced ship segments and newbuilds** where cyber security is key focus area; typically require tailored solutions and higher investment

SOLAS: The International Convention for the Safety of Life at Sea (SOLAS)

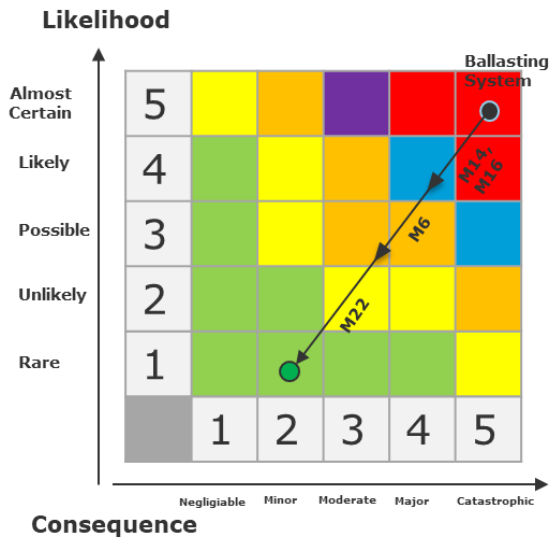
Overview of DNV's current engagements in Newbuilds/Retrofits/Existing fleet's



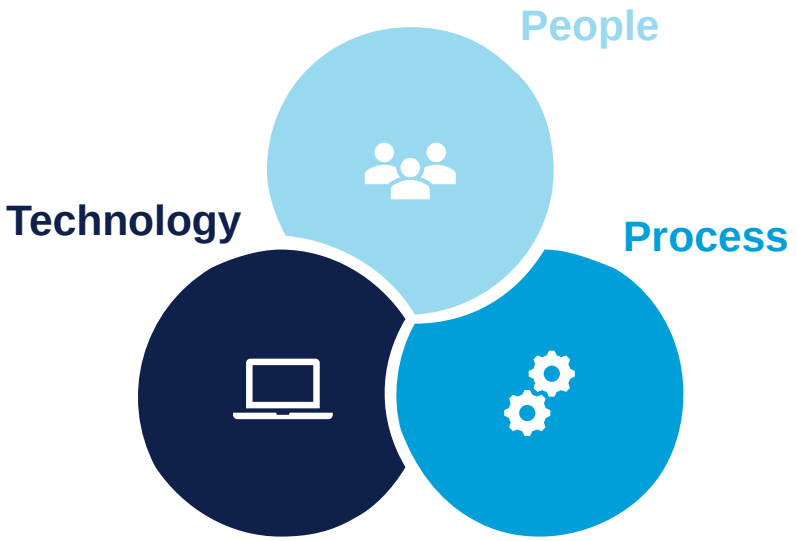
How do we cater to maritime cyber risk assurance services for ships in operation, newbuilding/retrofits and corporate

Assess/Test → **Improve/Implement** → **Check/Verify**

Evaluate the risk and define improvement plans



Develop barriers in all relevant dimensions



Provide independent assurance through certification

Initial onshore assessments

Assess

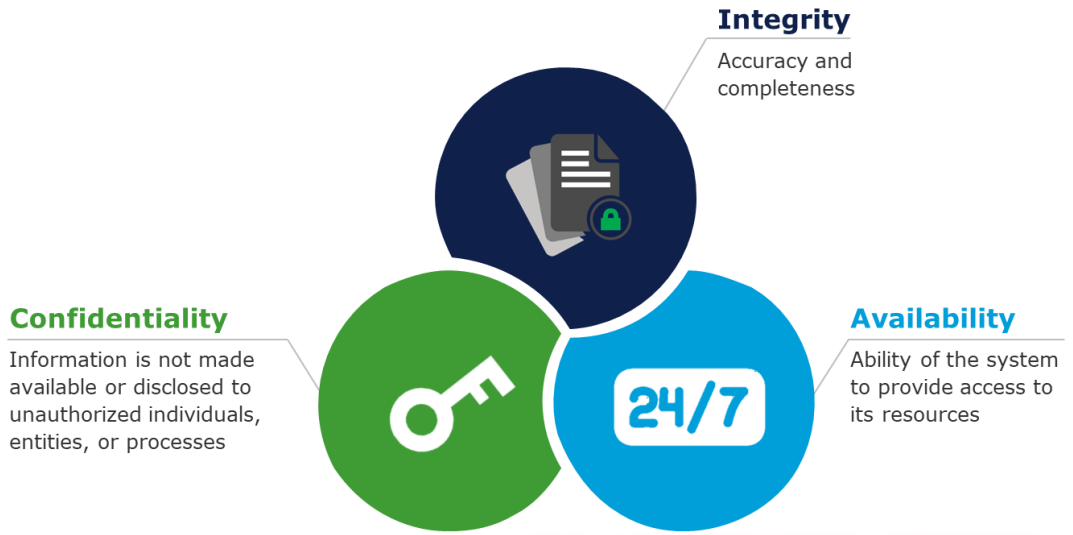
Organisational assessment

1. Leadership and commitment
2. Identify
3. Protect
4. Detect
5. Respond
6. Recover
7. Continuous improvement

Area Name	Checklist question	Examples of evidence	ISM code ref.
ELEMENT 1: Leadership and Commitment			
Roles and responsibilities	Are cybersecurity roles and responsibilities for the entire workforce established?	Job descriptions; Org. charts	3.2 3.3 A 3.3 A 3.5.1
Organizational objectives	Are priorities for organizational mission, cyber security objectives, and activities established?	Safety and environmental protection policy; CS Policy; MoM Management Review	1.2.2 2.1 A 3.5.1
Legal and regulatory requirements	Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, understood and managed?	Safety and environmental protection policy; CS Policy; Legal Register	1.2.3.1 10.1 A 4.1
Management commitment	Do the senior executives understand their roles & responsibilities for cyber security?	CS Policy; Interviews	3.3 4. A 3.3

- Consisting of ~ 25 areas & ~ 75 topics
- **Aligned with IMO requirements providing concrete questions to uniformly check cyber security resilience and compliance with the IMO requirements and more...**

Cyber risks assessment

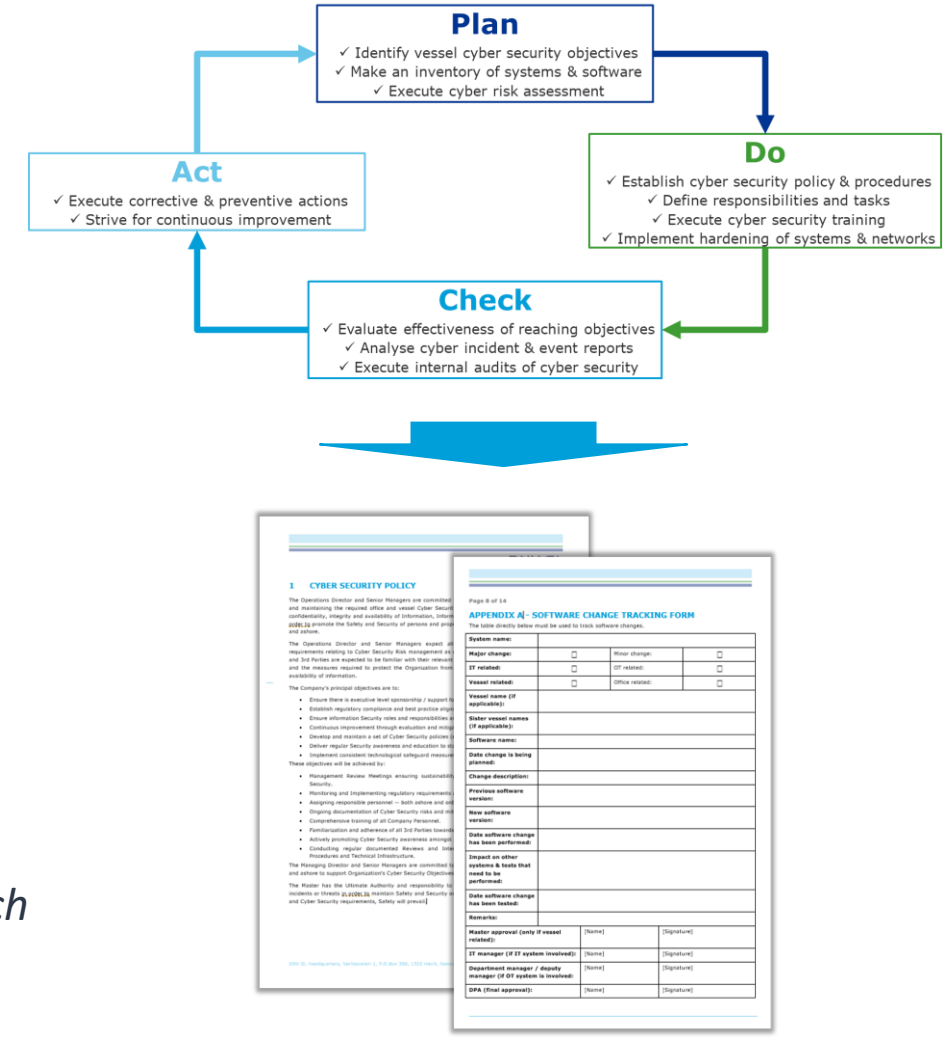


System group	R
Ballasting system	25
Propulsion & steering system	25
Power generation systems	20
Navigation planner	20
Stability Monitoring system	20
Man overboard system/CCTV	16
Muster Evacuation Monitoring	16
Energy management system	16
Environmental systems	16
Position fixing and navigation systems	16
Hospitality management	16
Security systems	16
Security Incident Report Platform	16
Emergency power systems	15
Inventory system	12

SMS and Technical Doc. Development

Improve

- Fitting into the existing SMS and tech. documentation
- Based on DNV's templates
- Workshops together with all relevant stakeholders
- In order to fulfil
  - the IMO Resolution MSC.428(98) and MSC-FAL.1/Circ.3**, required by most flag states**
  - the requirements of the DNV Cyber Secure class notation
  - or other stakeholder demands e.g. TMSA 3, NIST CS Framework, ISO 27001, NOG 104, RightShip



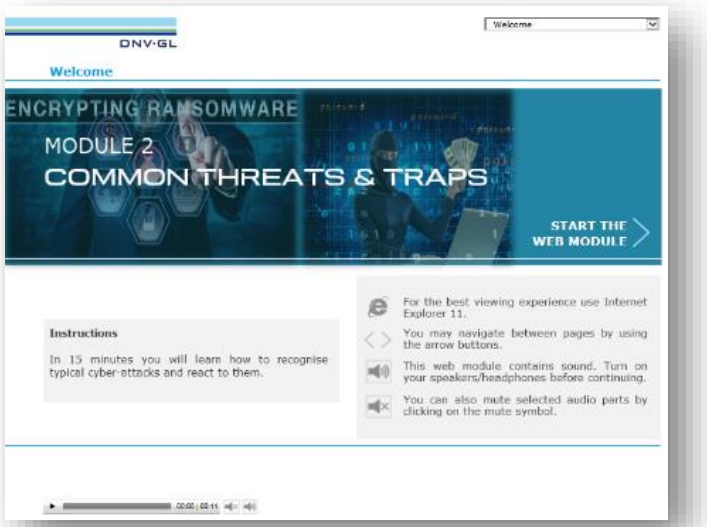
The safety management system (SMS) therefore ensures that each and every ship comply with the mandatory safety rules and regulations, and follow the codes, guidelines, and standards recommended by the IMO, classification societies, and concerned maritime organizations.

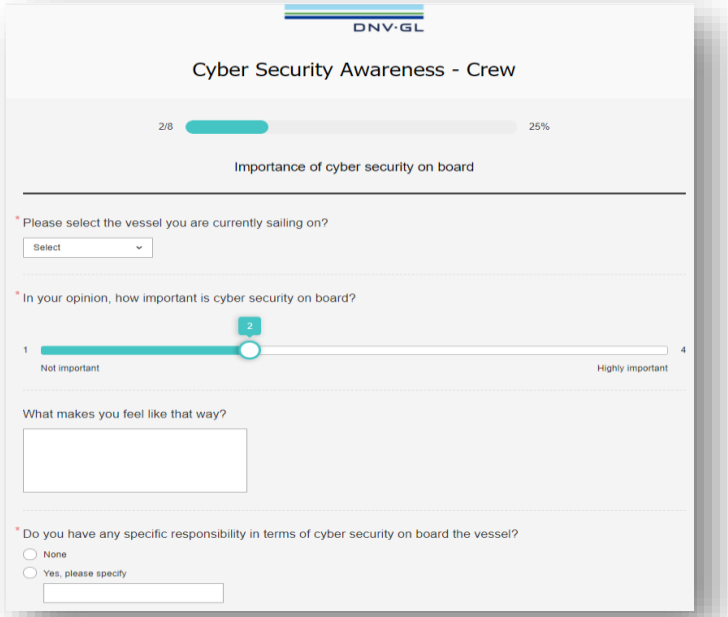
Training, drills and surveys

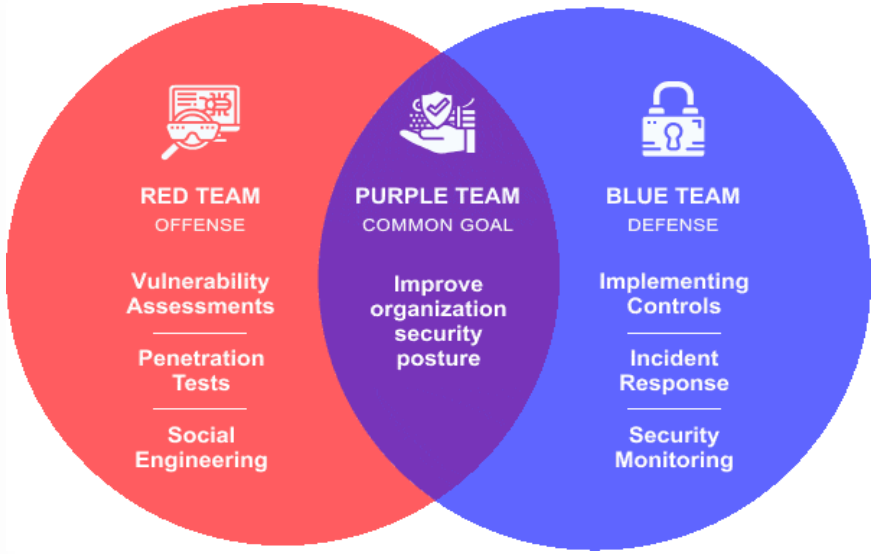
Implement

Different options

- E-learning courses
- Class room / online training
- On-board / on-shore tabletop exercises
- Online survey of crew
- On demand implementation support





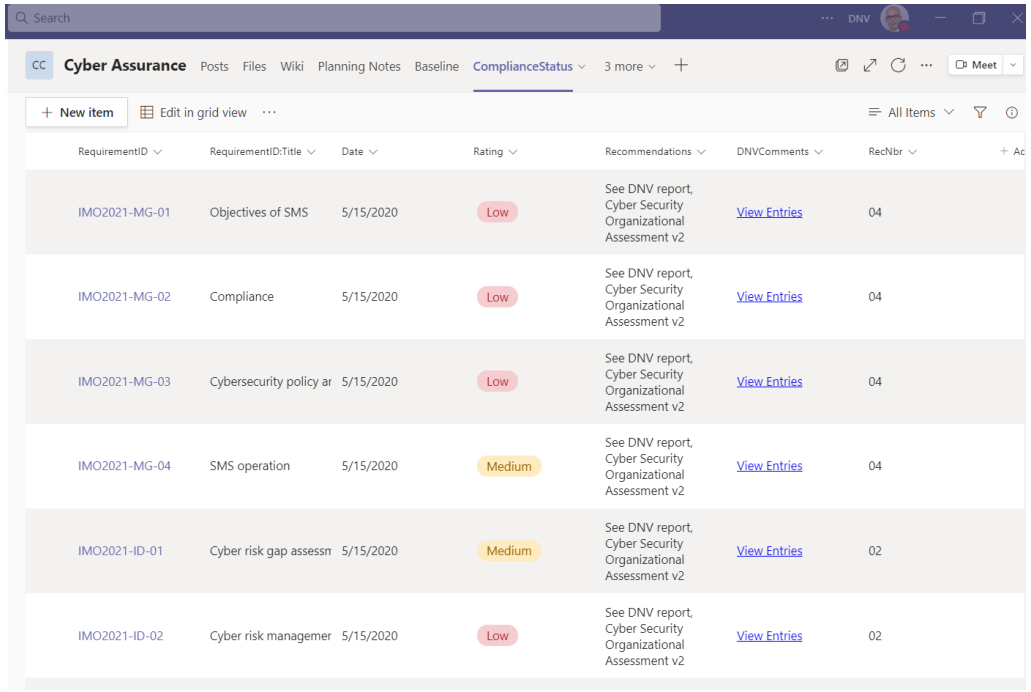


Tracking of compliance and checking of implementation

Check

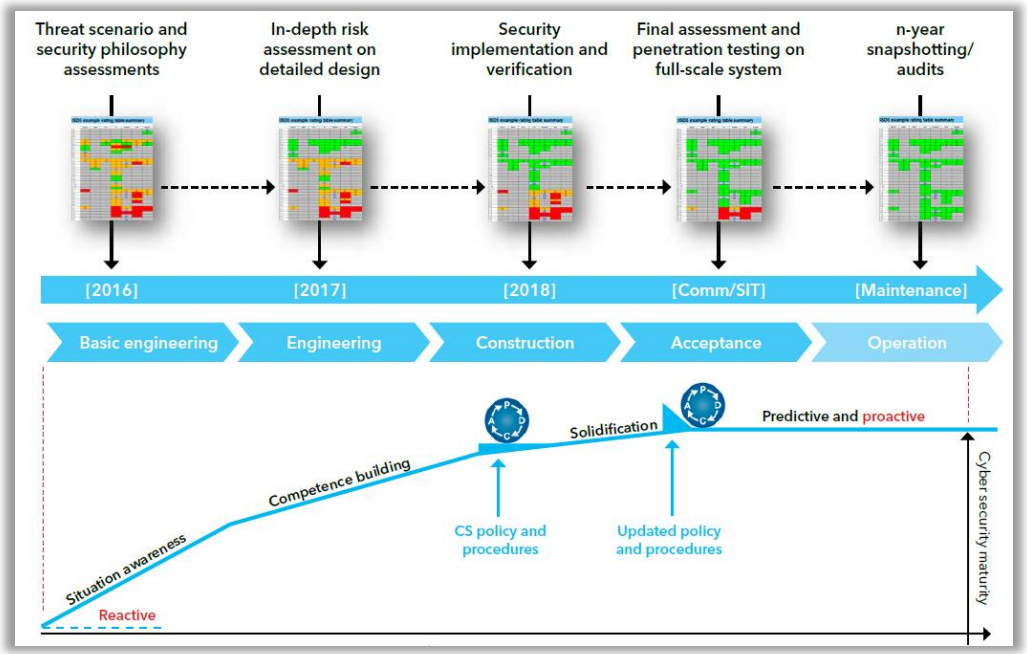
Ships in Operation

- Fleet approach: one/several vessel groups
- Effective implementation of cybersecurity requirements (from risk assessment, standards, external stakeholders)



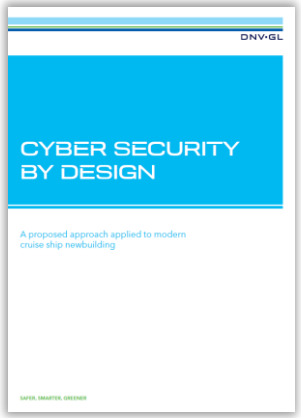
RequirementID	RequirementID:Title	Date	Rating	Recommendations	DNVComments	RecNbr
IMO2021-MG-01	Objectives of SMS	5/15/2020	Low	See DNV report, Cyber Security Organizational Assessment v2	View Entries	04
IMO2021-MG-02	Compliance	5/15/2020	Low	See DNV report, Cyber Security Organizational Assessment v2	View Entries	04
IMO2021-MG-03	Cybersecurity policy ar	5/15/2020	Low	See DNV report, Cyber Security Organizational Assessment v2	View Entries	04
IMO2021-MG-04	SMS operation	5/15/2020	Medium	See DNV report, Cyber Security Organizational Assessment v2	View Entries	04
IMO2021-ID-01	Cyber risk gap assessn	5/15/2020	Medium	See DNV report, Cyber Security Organizational Assessment v2	View Entries	02
IMO2021-ID-02	Cyber risk managemer	5/15/2020	Low	See DNV report, Cyber Security Organizational Assessment v2	View Entries	02

New Building



White Paper with:

Royal Caribbean Group

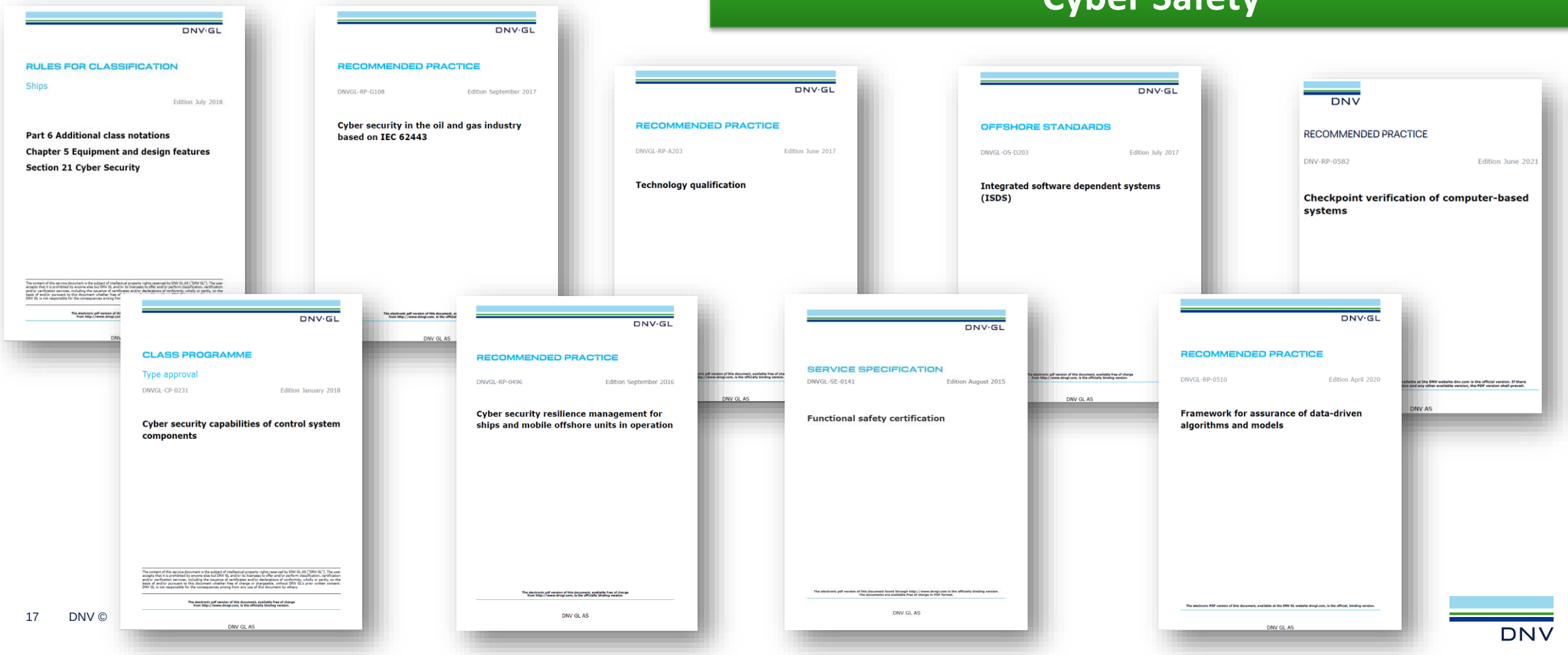


DNV

DNV has followed up with support to the industry

Cyber Security

Cyber Safety



The Cyber Priority

The state of cyber security in the energy industry

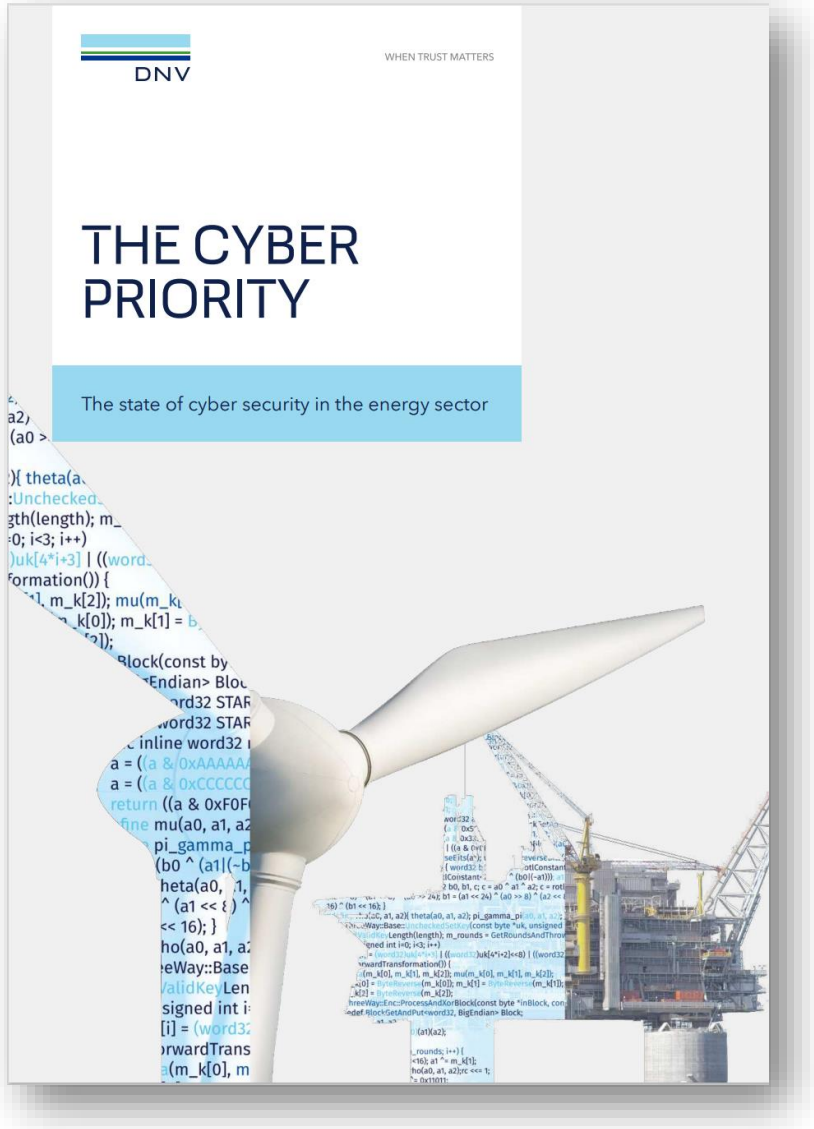
Introducing our research

- How real is the industry's awareness of the threat?
- What action is being taken to prevent it?
- Where is investment being prioritized?

948
Energy professionals surveyed

98
Countries represented

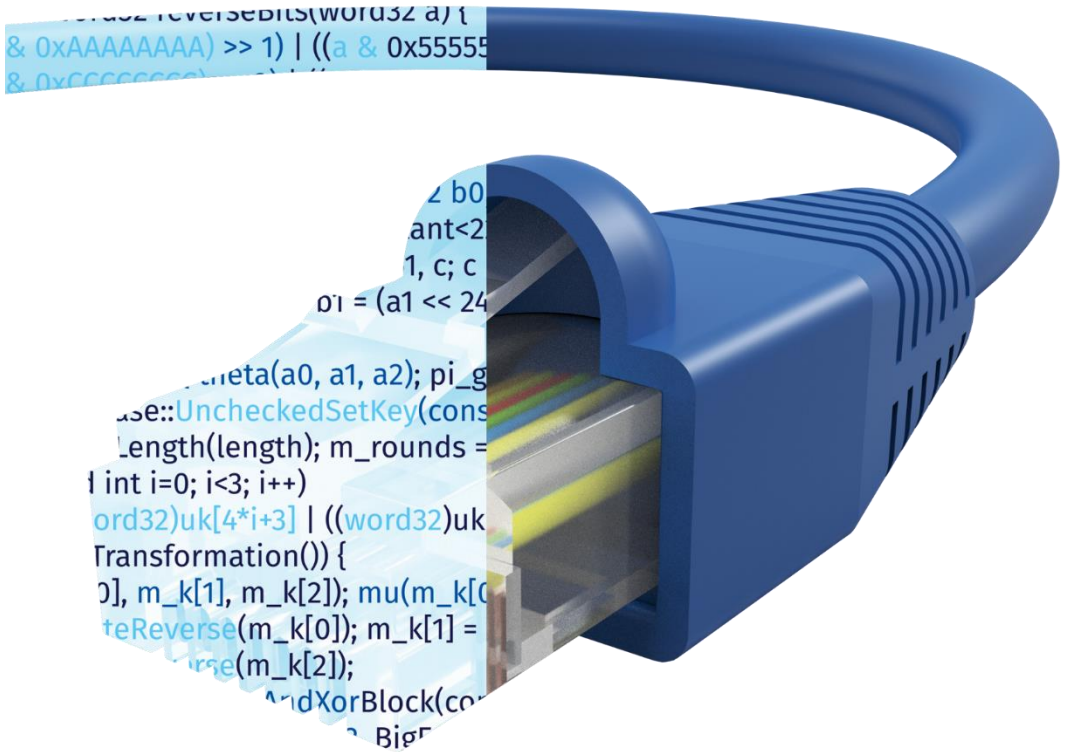
64%
Support, develop or operate operational technology



In-depth analysis of our survey findings published in a new report.

Download from: www.dnv.com/cyberpriority

Cyber risks are emerging



The energy sector now appears among the top three industries reporting cyber attacks

The sector has been tackling IT security for decades

Securing operational technologies is a more recent and urgent challenge

Operational technologies are becoming more networked and connected to IT

This opens the back door for hackers to access and take control of critical infrastructure.

Thank you!

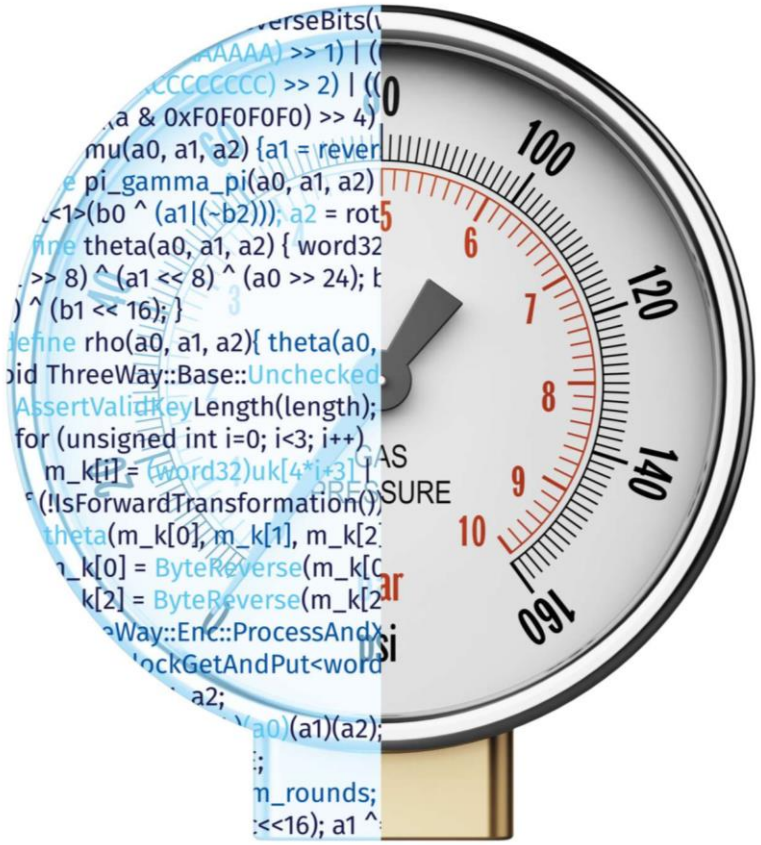
Svante.Einarsson@dnv.com
+49 175 49 100 74

Vijayan.manogara@dnv.com
+65 96427273

www.dnv.com

Some key findings

An industry waking up to the threat



Energy professionals anticipate that a cyber attack on the industry will compromise life, property, and the environment within the next **two** years:

85%

Think **operational shutdowns** are likely

84%

Anticipate **damage to assets and infrastructure**

74%

Expect an attack to cause **environmental harm**

57%

Think **loss of life** is likely

Defensive action is lagging

6 in 10

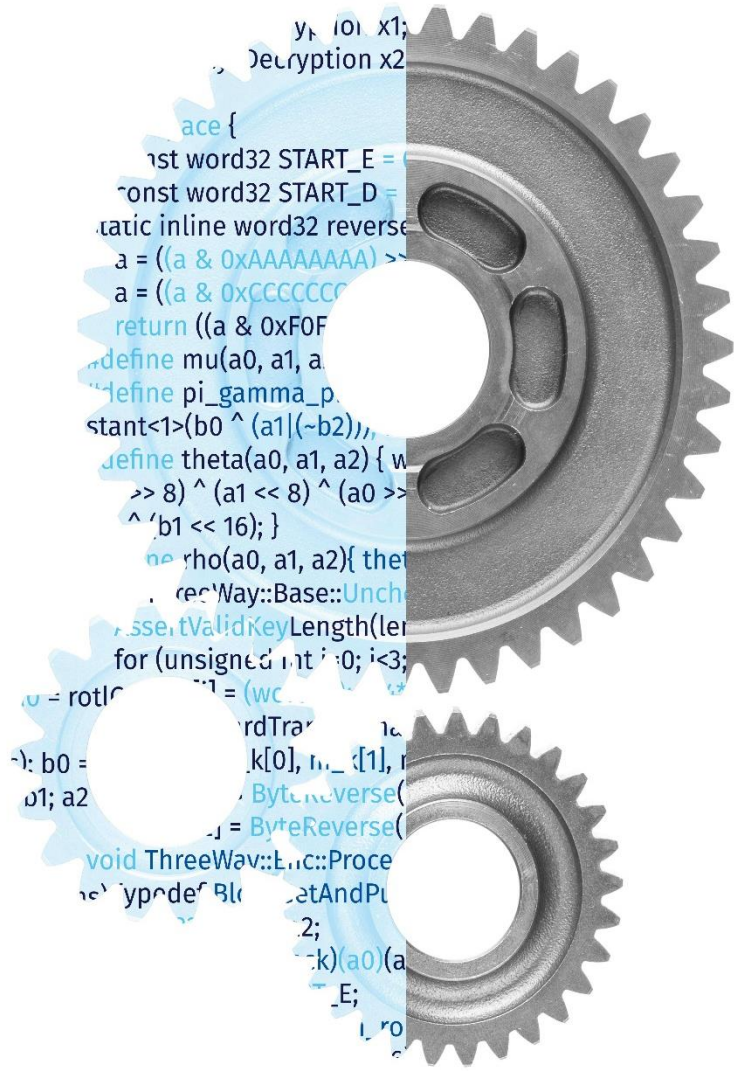
C-suite executives acknowledge that their organization is **more vulnerable to attack than ever before**

4 in 10

C-suite executives **expect to make urgent improvements** in the next few years to prevent an attack

35%

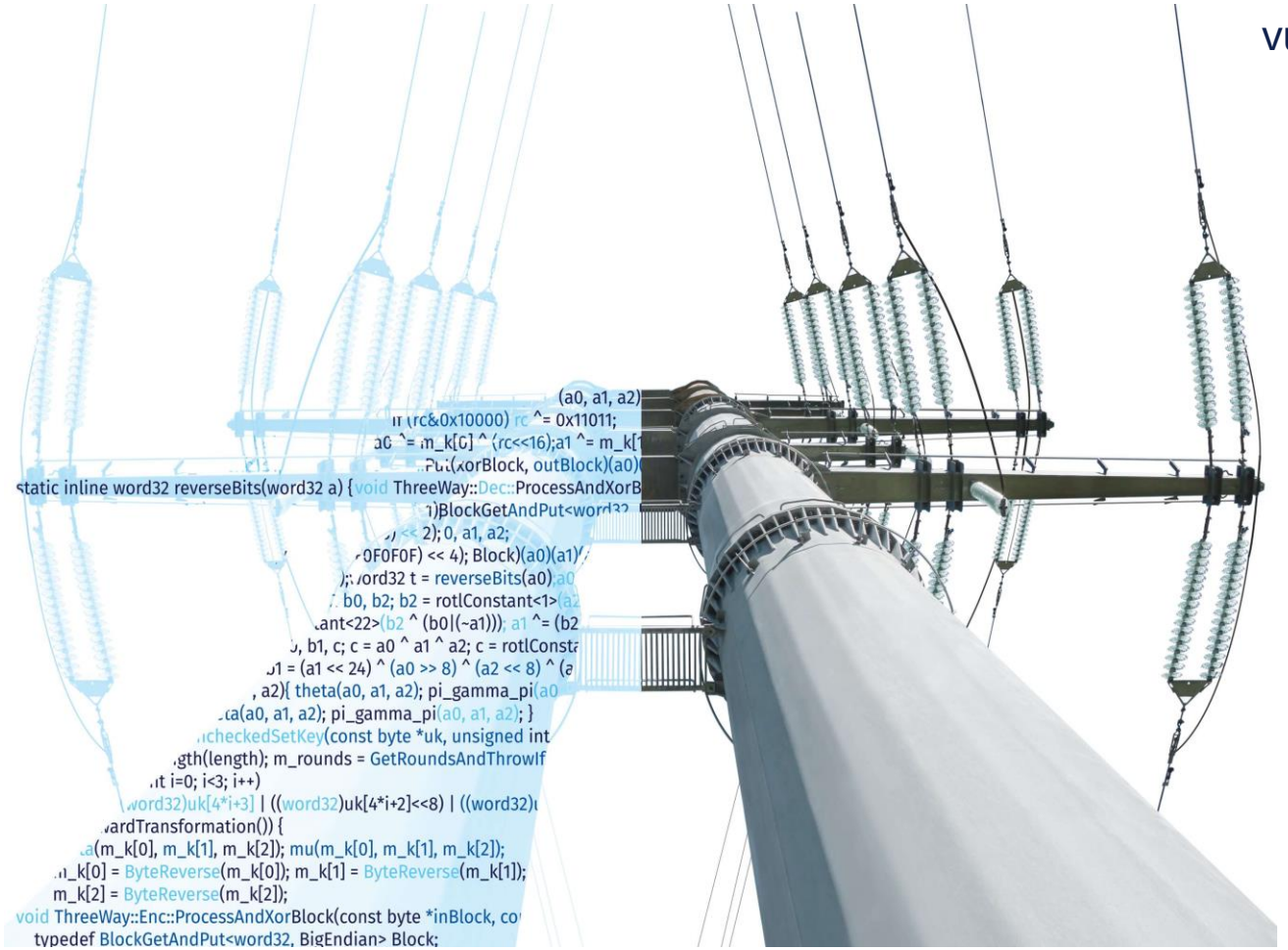
of respondents think their business would need to be impacted by a major incident before it would spend any more time or money on its defences



Our view:

- Companies who ‘wait, see and hope for the best’ are exposing themselves to significant risks
- This draws parallels to the industry’s approach to physical safety over the past 50 years
- Investment is needed before a cyber security issue becomes a safety issue.

Supply chain blind spots are appearing



Stronger cyber defences start with knowing where you are vulnerable to emerging cyber threats.

Only 28%

of energy professionals working with operational technologies say their company is making the **cyber security of their supply chain a high priority** for investment

Our view:

- If suppliers have undiscovered vulnerabilities, buyers are also vulnerable
- Energy companies should pay close attention to assuring that equipment vendors and suppliers comply with security best practice.

Greater focus is needed on the first line of defence

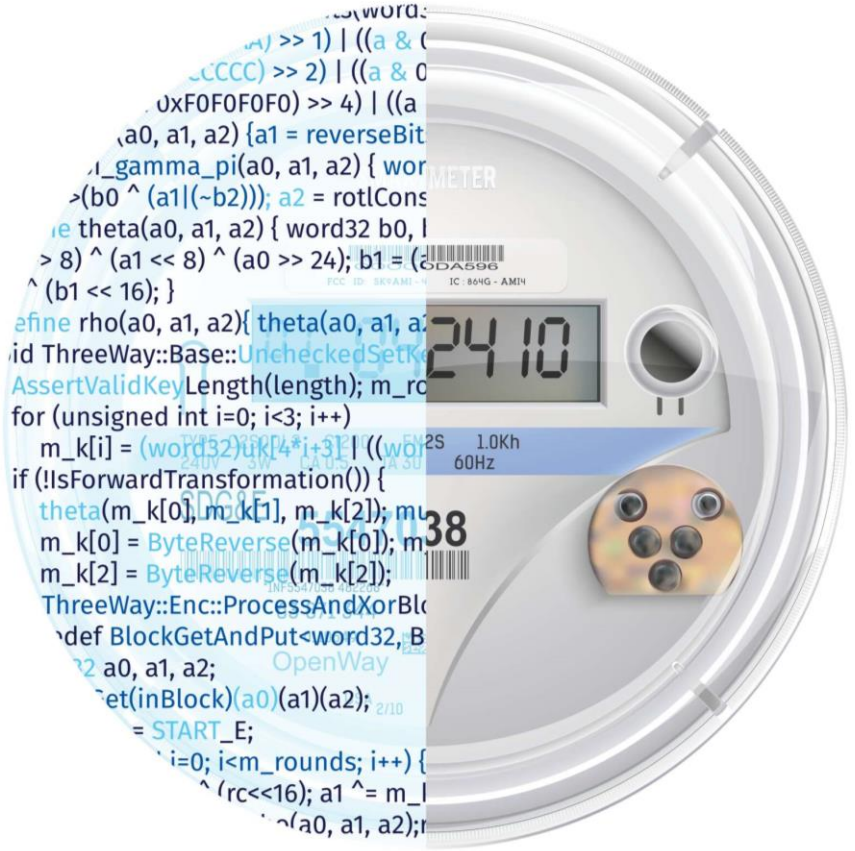
A company's first line of defence in the fight against cyber crime is its people.

3 in 10

energy professionals assert confidently that they know exactly what to do if they were concerned about a potential cyber risk or threat

6 in 10

think that the cyber security training they receive is effective



Our view:

- There is a need for companies to carefully evaluate investments in keeping their people well informed of how to spot potential criminal attempts
- Effective workforce training, combined with having the right cyber security expertise in place, can make all the difference to safeguarding critical infrastructure.