Peregrine
TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

CYBER SECURITY CONCERNS

2019 RESEARCH VESSEL OPERATORS COMMITTEE

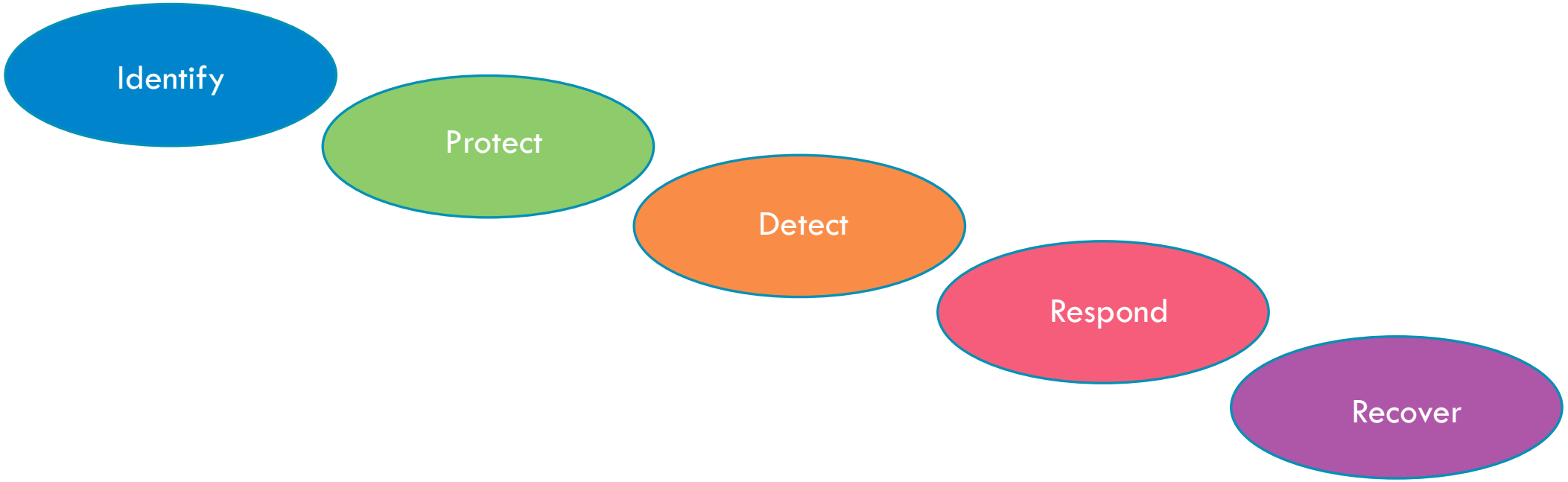
Dave Wolfe, Vice President

EXECUTIVE SUMMARY

- In June 2017, the International Maritime Organization (IMO) released a Maritime Safety Committee (MSC) resolution that addresses Maritime Cyber Risk Management in Safety Management Systems
- This resolution "affirms that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code"
- The resolution also encourages administrations to "ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after **1 January 2021**"

IMO FUNCTIONAL ELEMENTS

- The IMO has identified 5 functional elements in their guidelines that support effective cyber risk management (i.e., NIST CSF). These functional elements are not sequential and all should be concurrent and continuous in practice.



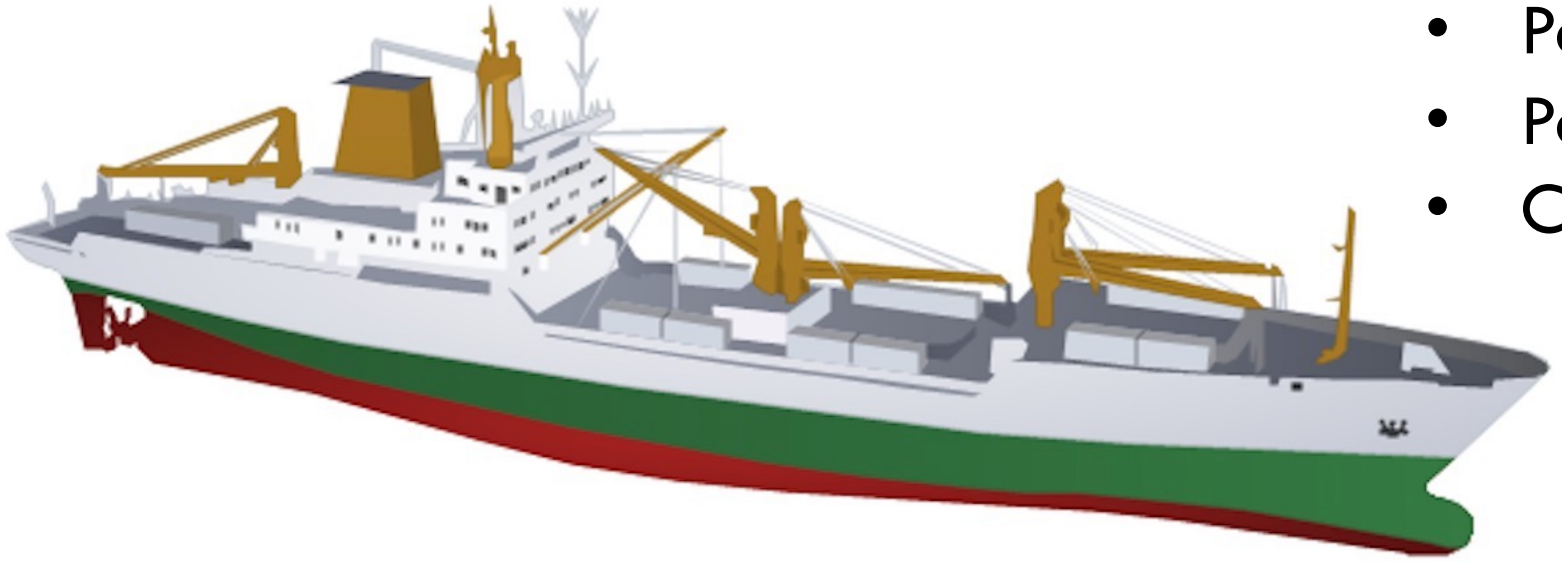
IDENTIFY

- Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations

- Define Cyber responsibilities and create a Cyber Risk Management Team
- Asset Management: Perform Inventory (i.e., systems, software, users, vendors)
- Map the ship's key functions and systems and their potential impact levels using the CIA model, taking into consideration the operation of OT systems
- Conduct risk assessment to identify threats and vulnerabilities

EXAMPLES OF MARITIME THREAT VECTORS

- Navigation Systems
- Ship Safety Systems
- Propulsion Management
- Cargo Management Systems
- Passenger Management Systems
- Passenger Access Systems
- Crew Personal Device Network



Source: ConceptDraw.com

PROTECT

- Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations

  - Cyber Risk Awareness Program
  - Acceptable Use Policy
  - Access Control
  - Network Segmentation
  - Data Security
  - Maintenance Procedures

DETECT

- Develop and implement activities necessary to detect a cyber-event in a timely manner

  - Detect Anomalies and Events
  - Monitor Traffic
  - Keep Logs
  - Security Continuous Monitoring
  - Reporting Responsibilities
  - Deploy and Update IDS

RESPOND

- Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event

  - Investigate Notifications
  - Response Planning (IRP)
  - Internal/External Communication Channels
  - Incident Analysis
  - Mitigations

RECOVER

- Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event

  - Restore capabilities that have been impaired
  - Back Up Data and Protect Backup Storage
  - Maintain/Establish Redundancies
  - Develop Recovery Plan
  - Capture Lessons Learned
  - Update Plans

GUIDELINES AND METHODOLOGIES

- Additional Guidance and standards may include, but are not limited to:
  - The guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and UMI
  - ISO/IEC 27001 standard on information technology
  - National Institute of Standards and Technology (NIST) 800-53 Special Publication
  - Recommended Procedures 153-163 from the International Association of Classification Societies (IACS) summarized below
    - Software maintenance, contingency plan, physical security, network security, network architecture, data assurance, integration and inventory of computer based systems on board
    - Manual/local control capabilities for software dependent machinery systems
    - Vessel System Design
    - Remote Update/Access

SUMMARY

- This new IMO requirement is based on IP and OT systems, and Peregrine is uniquely situated to support UCSD SIO, because our SMEs have not only conducted RMF efforts at the Naval War College, Naval Information Forces and INSURV, but have also been conducting vulnerability assessments (VA) focused on control systems (CS) for the DoD over the last four years under two contracts from OASD EI&E (Platform Resilience Mission Assurance C5-17-0005) and UAV Cyber Study (HQ0034-14-C-0209)
- Peregrine is currently in talks with the University of California – San Diego (UCSD) to provide services to their 3 ships that include:
  - Security Assessments/Audits
  - Penetration Tests
  - Policies and Procedures Support
  - Risk Management Support
  - Training and Education Support

PEREGRINE QUALIFICATIONS

Peregrine TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

- Peregrine is an SBA 8(a) certified, Alaskan Native Corporation (ANC), small disadvantaged business (SDB)
- Corporate Fully Qualified Naval Validator (C0124) with QNVs on staff
- Skilled in using industry standard methodologies to secure IT/OT
- Key contractor writing Facility Related Control System (FRCS) instructions for DoD
- Certified by the International Standards Certifications review committee for ISO 9001 and ISO 27001
- Experts in cybersecurity compliance and vulnerability management. Highly adept at providing cybersecurity support services and managing DoD Information Assurance (IA) workforce requirements

QUESTIONS?

Dave Wolfe, CISSP, PMP

Vice President

Office: 757-234-6664

Cell: 757-871-4379

dwolfe@gbpts.com

www.gbpts.com

BACKUP SLIDES

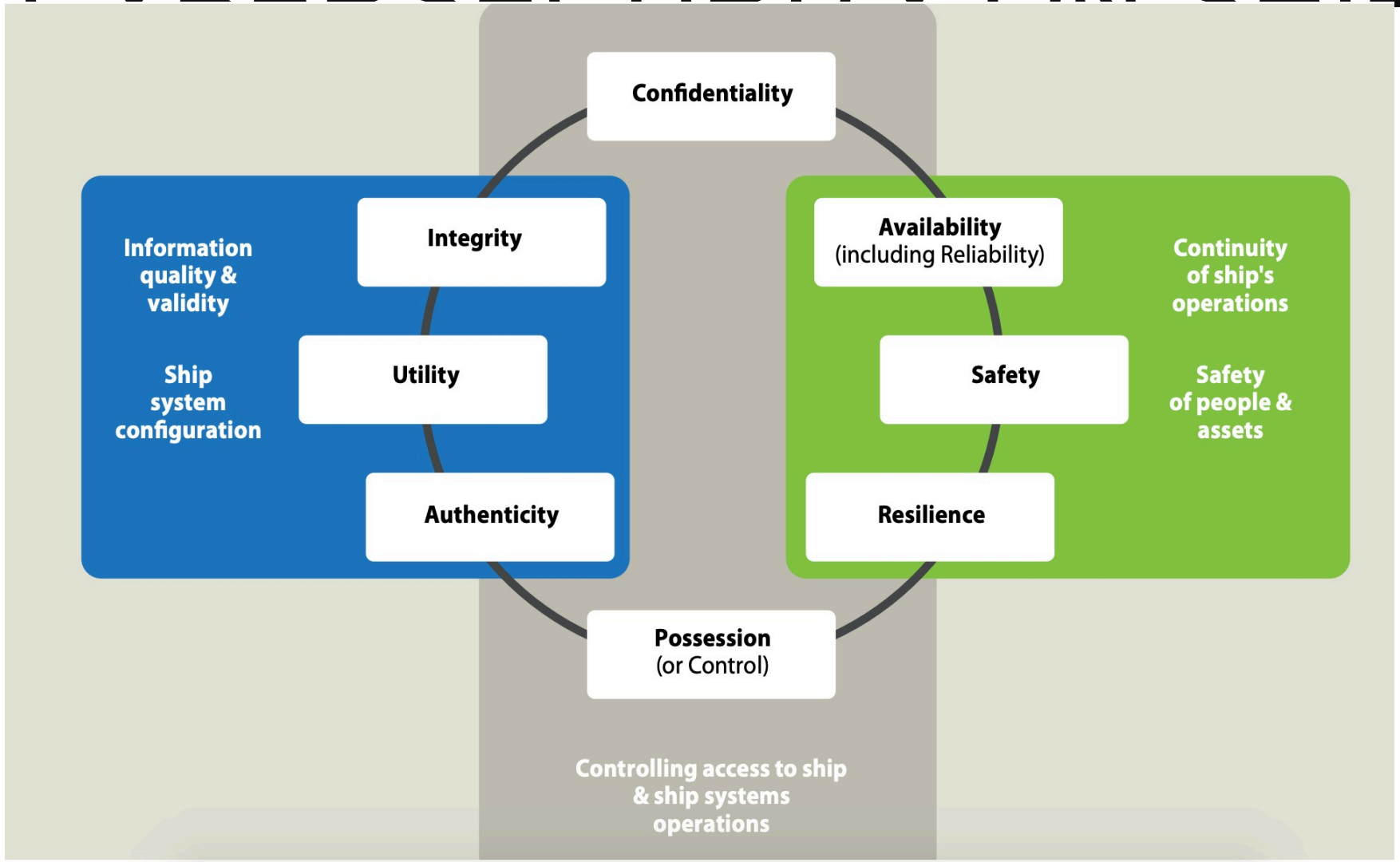
DIRECTIVES

- ISO 27001
  - A framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes
  - Developed to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system
- DFARS 252.204-7012
  - The Defense Federal Acquisition Regulation Supplement, or DFARS, has been working to encourage DoD contractors to proactively comply with certain frameworks in order to achieve this goal. Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is the latest mandatory addition.
  - Under the Clause, all contractors must comply with the National Institute of Standards and Technology's Special Publication 800-171 (NIST SP 800-171), a framework that lays out how contractors must protect sensitive defense information and report cybersecurity incidents.

UNDERSTANDING THE THREAT

Peregrine TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

ATTRIBUTES OF CYBERSECURITY ON SHIPS



Source: Code of Practice: Cybersecurity for Ships

RISK MANAGEMENT PROCESS (NIST CSF)

Peregine TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

Identify

- Inventory ship systems/ assets/data
- Define personnel roles
- Conduct risk assessment to identify threats and vulnerabilities

Protect

- Access Control
- Awareness & Training
- Data Security
- Processes/Procedures
- Maintenance
- Drills/exercises

Detect

- Anomalies/Events
- Continuous Monitoring
- Detection Processes

Respond

- Response Planning
- Communications
- Analysis
- Mitigation

Recover

- Backup/restoration of cyber systems necessary for ship operations
- Capture lessons learned
- Update plans

PEREGRINE APPROACH

- Peregrine proposes a 3 phase approach to identify and address vulnerabilities:
  - Phase 1: Pre-Assessment
  - Phase 2: Ship Assessment
  - Phase 3: Review and Reporting

PHASE 1: PRE-ASSESSMENT

- Map the ship's key functions and systems and their potential impact levels using the CIA model, taking into consideration the operation of OT systems
- Review detailed documentation of critical OT and IT systems, including their network architecture, interfaces, interconnections, and the ship's maintenance history
- Establish contractual requirements and obligations that the shipowner/ship operator may have for maintenance and support of the shipboard networks and equipment
- Support, if necessary, the risk assessment with an external expert to develop detailed plans and include producers and service providers
- Identify main producers of critical shipboard IT and OT equipment

PHASE 1: PRE-ASSESSMENT (CONT)

- Identify the following inventory requirements:
  - Software
    - Name and publisher
    - Installation date, version number and motivations
    - Local and remote roles
    - Generic accounts
    - Dedicated accounts
    - Access Control list with read, write and execution rights
    - License numbers
  - Network
    - Protocol name and version
    - Listening ports and existing outgoing IP connections
    - Listening interface (for non-IP)

PHASE 2: SHIP ASSESSMENT

- Assess the ship's network, systems and devices to identify any vulnerabilities that could compromise or result in a loss of confidentiality, integrity or availability. Below are areas of focus:
  - Roles and responsibilities of users
  - Software defects, vulnerabilities and unpatched systems
  - Configuration of computers, servers, routers and firewalls
  - Cyber security documentation and procedures for connected IT and OT systems
  - Data flows and access points
  - Access management design
  - Unmanaged network interconnections

PHASE 3: VULNERABILITY REVIEW AND REPORTING

- Following the assessment, each identified vulnerability will be evaluated for its potential impact and the probability of its exploitation
  - This takes into account impact to the mission as well as factors as they relate to the ship as a whole
- An executive summary will be provided that includes a high-level summary of results, recommendations and the overall security profile of the assessed ship
- Technical findings will be provided as a breakdown of discovered vulnerabilities, their probability of exploitation, the resulting impact, and appropriate technical fixes or mitigation advice
- A prioritized list of actions will reflect the effectiveness of the measure and the applicability

PHASE 3: VULNERABILITY REVIEW AND REPORTING (CONT)

- Safeguards will be implemented to prevent the occurrence of adverse cyber events on onboard. Some areas that may be addressed could include patch management, separation of duties, credentials user accounts, data backup procedures, event logging and encryption for data at rest
- An appendix will state the activities performed by the cyber risk assessment team and the tools used during the engagement