SUMMARY

Infosec Partners have designed a program of cyber education modules to be delivered to RINA members, initially as remote courses, but subsequently as physical training courses.

5 separate training modules provide expert education in distinct areas of cyber security, each delivered as a one day course.

Members can attend a course and gain a formal cyber certificate of course completion, and a further award for achieving a score of 80% or more on the final course test.

Any member that successfully completes and passes 3 of the 5 modules will be awarded a formal education certificate through an examination body (PECB/APMG).

All training courses delivered by certified GCHQ approved trainers and subject matter experts in the field of maritime cyber security.

All training courses will include practical examples, scenarios and simulations.

Training courses will include technical demonstrations of methods of protection from our technical cyber partner Fortinet.

Each module to be delivered 3 times per year, starting with modules 1-5 delivered on the week commencing 12th April 2021.

CYBER SECURITY TRAINING COURSES
ROYAL INSTITUTION OF NAVAL ARCHITECTS

InfosecPartners
CYBERSECURITY

COURSE MODULES

CYBER SECURITY TRAINING COURSES

ROYAL INSTITUTION OF NAVAL ARCHITECTS

InfosecPartners
CYBERSECURITY

MARITIME CYBER RISK MANAGEMENT

AND BEST PRACTICES FOR OPTIMAL MARITIME PROTECTION

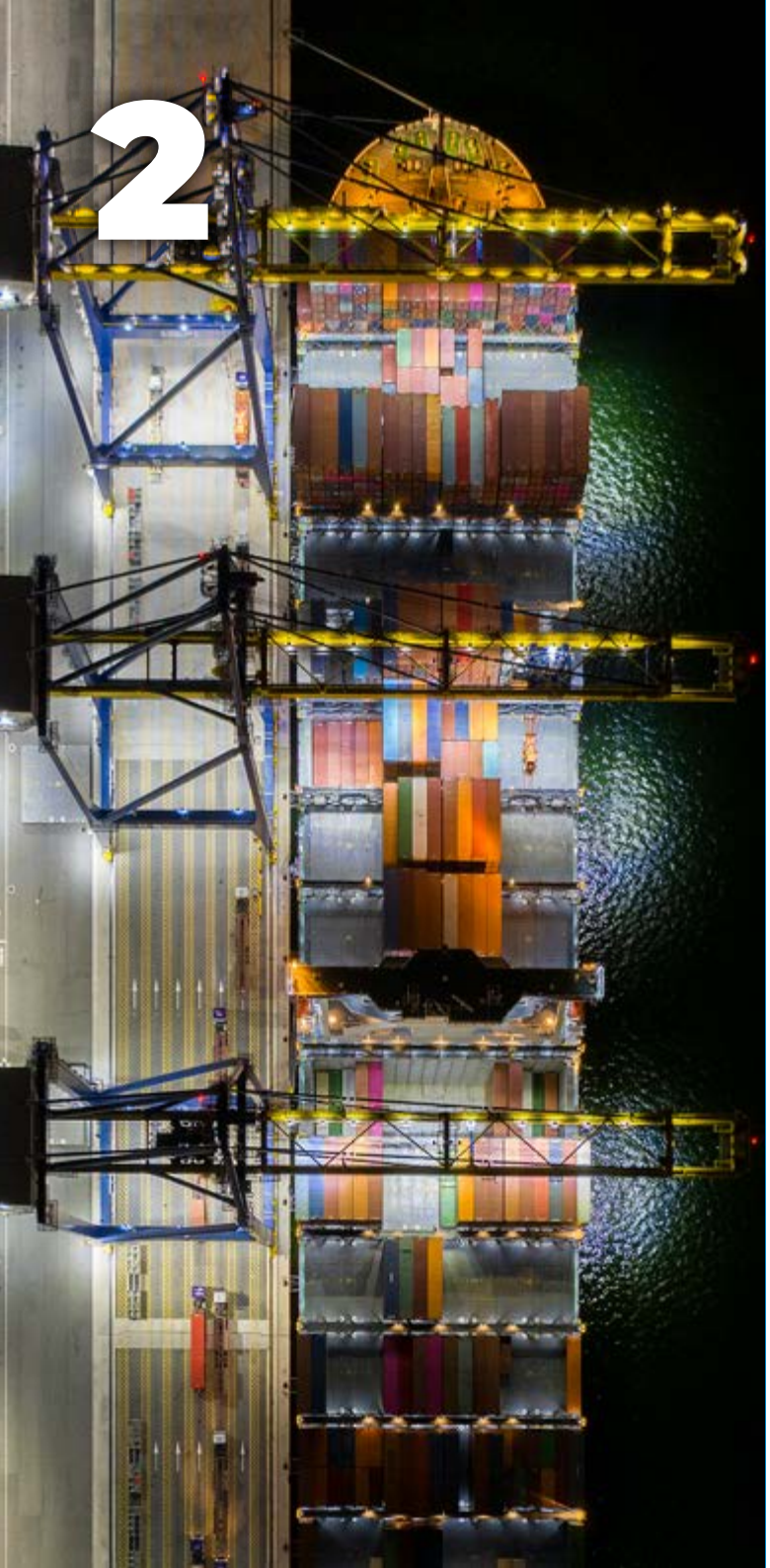
Provides a structured framework to provide owners, captains, management companies and crew assurance that cyber risks are appropriately managed and that there is both resource and process in place to detect and respond to potential cyber breaches.

High-level draft course content:

- How to identify information assets (IT and OT)
- How to identify the threats, vulnerabilities and risks associated with assets
- Assessing risk exposure
- Reporting on and tracking risks
- How to Carry out an effective cyber risk assessment
- How to Deliver an impact assessment
- How to conduct an effective risk assessment*
- Managing and, remediating risks
- Delivering a training and awareness programme
- Developing protection and detection measures
- Designing your on-vessel maritime cyber security action, and contingency plans
- How to create and implement an Information Security Management System (ISMS)*
- Legal compliance requirements (contractual, DPA, GDPR, IMO, employment, payments, etc.)
- Cyber incident management and liaison with law enforcement and third parties during an incident

* All risk assessment methodology covered will mirror IMO / ISO 27001 best practice

InfosecPartners
CYBERSECURITY



2

IMO CYBER RESOLUTION MSC.428(98), A FRAMEWORK FOR CERTIFICATION

AND ENSURING COMPLIANCE

Defines a formal program for vessels, fleets and third parties to achieve and maintain formal compliance to the IMO 2021 cyber regulations.

High-level draft course content:

- Preparing for and evidencing compliance to the IMO ISM code*
- What is maritime cyber security?
- What are the cyber security challenges affecting the maritime industry?
- What are the maritime cyber security compliance measures you need to consider?
- Understand the Confidentiality, Integrity and, Availability (CIA) triad
- Differences between IT and OT system
- Cyber Security best practices
- Identifying threats
- Identifying vulnerabilities
- Cyber Security, and safety management
- Real-World Lessons Learned from Maritime Cyber security Incidents
- Connectivity on a modern maritime vessel
- Preparing for a cyber security breach and your response
- Additional Maritime Cyber security Resources (ISO27001, NIST, etc.)
- Requirements and process for audits

* A complete set of documentation in support of, and by way of evidence of compliance can be provided at additional cost. This can also include customised consultancy, and staff awareness training.

InfosecPartners
CYBERSECURITY

3

TECHNICAL CYBER CONTROLS FOR MARITIME NETWORKS

ATTACK & DEFEND

Technical IT and security controls vary greatly in the level of protection they provide. This module demonstrates an example of a secure fabric of security controls designed specifically to protect the complex, critical environments onboard. This course also demonstrates an attackers view of attempting to subvert security controls in both low end security controls and also advanced levels of protection that are more robust against attack

High-level draft course content:

- Develop protection and detection measures.
- Design technical protection framework for vessels and ship to shore communications
- Design network segmentation of IT / OT / IOT platforms
- Define multi layered cyber controls based on best practice and risk assessment
- Deploy decoy and deception systems to act as early warning systems of cyber-attack.
- Design cyber security and IT control standards for all onboard electronic devices
- Protocol to identify and control all guest, crew, visitor and fixed devices
- How to utilise best of breed cyber controls to defend against active attacks
- How to regularly test cyber controls with simulated attack scenarios
- How to deploy devices on board to ensure that controls remain up to task
- How to identify and act on emerging threats to maritime assets

InfosecPartners
CYBERSECURITY

4

CYBER SECURITY TESTING, ASSESSMENT AND THIRD-PARTY REVIEW

This module demonstrates how Maritime IT & OT systems can be regularly tested to ensure they are free from serious vulnerabilities. Active penetration testing and passive vulnerability assessments highlight any security weaknesses in the design or operation of a vessels systems and highlight the impact of a potential breach.

High-level draft course content:

- Assessing cyber controls onboard and on shore
- Security assessment of vessel, yard, agent, management and third-party entities
- Passive review and vulnerability assessment
- Understanding of best-practice audit methodology
- Prepare and report on the findings of an information security audit
- Ongoing monitoring and auditing
- Through life management and remediation on shore and at sea
- Ensuring that documented controls are operationally sound and correctly deployed

InfosecPartners
CYBERSECURITY

5

GLOBAL RISK MANAGEMENT & CYBER INSURANCE

Many organisations are unsure how to effectively protect themselves when travelling or when away from their home base, cyber threats differ in impact and likelihood depending on what location the vessel, owner or crew are located in. The range of options to respond and recover also differs wildly across borders.

This module promotes a structured process for documenting threats and vulnerabilities, defining the appropriate level of both protection and response and how the security profile changes based on location and resource. This module also seeks to educate captains, owners, crew and yacht management companies on the benefits and pitfalls of cyber insurance and also the processes for invoking insurance in the event of any suspected or confirmed cyber breach..

High-level draft course content:

- Risks to a mobile workforce, global threats and hazards
- Duty of care, the law across the globe, lawful cyber monitoring and data protection
- Managing data – personal records/ medical information and access rights
- Impact, liability and penalties of incidents
- How to run a travel risk programme
- Cyber risk within a travel risk programme
- Organisational communications
- Secure communications
- Data transfer across borders
- Device protection while travelling
- Cyber insurance coverage, when and how to contact an insurance company
- Incident response and crisis management

InfosecPartners
CYBERSECURITY

LEAD INSTRUCTORS

MARK OAKTON

Mark is a recognised information and cyber security expert with over 25 years practical experience of both attacking and defending critical operational systems on land, air and sea. With renowned cyber expertise in the maritime sector, Mark brings war stories and advice from his time working on cyber security for ports and yachts during the Olympics, and from providing maritime cyber advisory and incident response for yachts, management companies, builders and owners.

In addition to working with maritime organisations, Mark has broad experience in critical infrastructure protection across a variety of sectors including Financial Services, Energy, Hospitality, Broadcast Media, and Aerospace. Having served on the board of an international insurance services business, Mark was responsible for ensuring the safe and secure configuration, build and launch of a leading SaaS platform within the insurance industry.

Mark is also the founder of Infosec Partners, a specialist cyber security company providing full-spectrum security expertise, protection and training to high profile individuals, sensitive government departments and global organisations. Through its VIPIT security offering, Infosec Partners provides personal protection to high net worth families at home and abroad, and its Highclere Crest business offers cyber expertise for the design and implementation of secure home, office and yacht automation.

Mark has trained and certified as a certified information systems security professional (CISSP), Certified Information Security Manager (CISM), ISO Cyber security lead auditor, Certified Listed Advisor Scheme consultant (CESG/GCHQ CLAS) and as a forensic investigator. He has taught Cyber security to operational and executive teams around the world, including training private groups on Crisis and Incident Management at the UK Defence academy.

As an established expert in cyber risk management, Mark is frequently called upon to provide thought leadership and expert opinion on developments in Information Security. Mark has advised the UK water regulators around cyber defence, has sat on Guardian round table events relating to cyber, and most recently he presented at the 2020 Superyacht Design Festival, highlighting how the superyacht industry is falling behind on cyber security, and was a guest panellist at the Yare Networking 2020 Cyber Security event.

InfosecPartners
CYBERSECURITY

LEAD INSTRUCTORS

RIZ OMAR

Riz has a wealth of experience gained over 19 years of working within the security industry. He started his career at the Policing Crime Reduction Group within the Home Office, working closely with government and law enforcement agencies to tackle organised crime and terrorism.

He has in-depth knowledge of the threats, risks and hazards faced by organisations, employees and travellers across the globe, and has gained extensive experience in security management, maritime security, anti-piracy, risk and crisis management.

Over the years Riz has implemented travel risk management plans for high risk environments, as well as designing emergency response and crisis management plans for specialist expeditions, such as the Nexton Mission.

Today Riz oversees and coordinates all of Priavo Security's global operations, managing and directing global deployments of specialist security teams across all land based and high risk maritime operations and transits.

With emerging technologies constantly redefining travel and transportation, Riz advises that there is a need for even the most mature security risk programmes to consider their security approach to ensure cyber resilience.

As an experienced security trainer, Riz designs and delivers tailored information and travel security awareness training for corporate organisations, including bespoke incident and crisis management scenario planning. Riz is also an associate lecturer on both the Security Risk Management Course and the MBA pathway at the Emergency Planning College, the national centre for resilience learning and development.

LEAD INSTRUCTORS

ALEX MARTIN

Alex is a Cyber Security Specialist who has worked in the field for 15 years. His experience spans from penetration testing, digital forensics advising on architecture and configuration to implementing policies and frameworks within complex organisations. He has delivered security training throughout his career to date and prides himself on breaking down complex topics to a range of technical abilities within his audience.

Prior to joining the team at Infosec Partners, Alex was a career soldier, specialising in Intelligence and Cyber Security. His role saw him conduct cyber threat assessments and investigations around the globe - with the scope different from small inbuilt controllers in specialist military equipment to enormous wide area networks and cloud environments. Alex's experience of maritime cyber security includes forensic examination and penetration testing of vessels deploying to high threat environments.

Since joining Infosec Partners Alex's role has included consultancy to external organisations (including RINA themselves) and the implementation of their security strategies. Alex leads much of Infosec Partners' testing and response activities and therefore knows what to look out for and which controls to prioritise to achieve the greatest effect.

Alex holds academic qualifications in Computer Science and additional qualifications in Digital Forensics, Penetration Testing and Governance. He is qualified to the highest level of military cyber practitioner and taught Cyber Threat Intelligence and Cyber Incident Response courses to NATO leaders on a bi-annual basis.

LEAD INSTRUCTORS

STEVE LUCAS

Steve is an experienced Information, Data and Cyber Security Consultant, with over 30 years serving varied government, law enforcement and commercial clients.

Having led thousands of successful engagements, Steve has been instrumental in many large-scale ISO27001, PCI DSS, SOC2 and Cyber Essentials certifications. He has led global audits across many regulatory environments including maritime operations, payment card industry, data protection, insider threat and the NCSC HMG Information Assurance Maturity Model for classified environments.

From testing cyber controls effectiveness onboard to the securing and formal certification of point of sale and card processing systems, Steve has acted as trusted advisor to shipping companies, ferry and cruise lines, private owners and management companies.

In addition, Steve has designed and achieved formal government certification for training courses relating to cyber security risk management, incident response and general staff awareness, which he has then delivered to the Police, radio networks, marine communications, and the global cruise network.

Certified by GCHQ as a government accredited trainer, Steve is a Certified ISO Cyber lead auditor (CISLA), a Certified Internal Auditor (CISA), a Certified Information Security Internal Auditor (CISIA), PECB certified ISO lead auditor, and an APMG Certified ISO practitioner.

Training courses designed by Steve have also been delivered through the UK leading NCSC approved training provider, where bespoke user awareness training has been tailored to individual client requirements and delivered on client premises or remotely via elearning.

LEAD INSTRUCTORS

CAPTAIN JOHN L. DAVID

John worked his way up through the Deck officer qualifications and ranks in a broad variety of vessels, trades and cargoes until, he was promoted to Master and given command of a 40,000 tonne multi-flex vessel. John has dealt with many problems encountered with cargoes, vessels and trades, including attempts at fraud, piracy and theft; allegations of shortage, contamination, loss and damage; he has had to deal with Charterers on various speed, performance, consumption, hold clean and safe port issues on behalf of his owners. He has also had to deal with death and major injury involving his crew and stevedores.

Whilst in command, John was closely involved in instigating and implementing various management systems, which have since become regulatory maintenance, ISM, and ISPS systems.

John has particular experience in main and auxiliary engine operation and systems of the vessels he served on, as this was one of the areas which caused many of the day-to-day practical problems involved in operating his vessels.

John spent 9 years working for Clyde's in their London office as a litigation claims handler specialising in claims that predominantly centred around technical issues arising out of contractual disputes.

Central to John's involvement in these cases was his ability to sift though existing evidence, advise on further evidence and in particular, go and obtain crucial evidence.

John also has experience in fire, collision and personal injury matters, where his investigative skills have provided the client with a comprehensive overview of the issues, facts and evidence in often very difficult circumstances.

John now provides the same investigative and advice services to clients working for Global Claims Management Ltd in the City of London.

John has worked closely with ship owners, Charterers and their P+I insurers; Hull and Machinery underwriters, claims handlers and brokers; Port and Terminal insurers; various other marine liability insurers; and the various cargo interests.

Captain John is also a frequent lecturer and presenter on a very varied spectrum of "marine-legal" topics in numerous countries and has been involved and chaired a major seminar on the Mariner and Marine Insurance.

InfosecPartners
CYBERSECURITY

CYBER SECURITY TRAINING COURSES

ROYAL INSTITUTION OF NAVAL ARCHITECTS

InfosecPartners

CYBERSECURITY