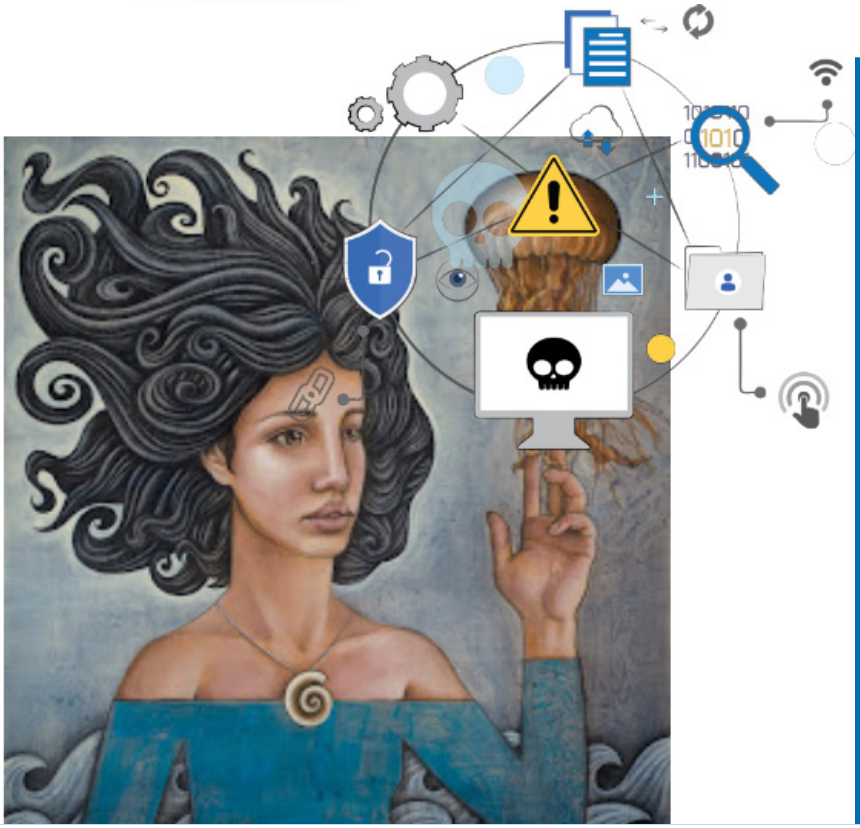


Project CETO: enduring cyber- security for superyachts

Superyacht stakeholders in Cyber Security Resilience are a bit like participants heading towards a potential family crisis.

On the one side of the partnership is the super yacht owner. Owning a super yacht is a luxury for the world's financial elite due to the exorbitant cost of buying and maintaining one. It is a vessel for the super-rich.

On the other side are the people who run the vessel. They are usually well presented, hard-working, fit, healthy and discreet. They are not wealthy.

There are incompatibilities between the two. One has power and money. The others are chosen to be respectful, well-mannered and not to make a fuss.

There is a third party. Guests on Super yachts are what cybercriminals call high-value targets: A list personalities and influential wheeler dealers. All rich pickings in the world of extortion.

Like relatives, thrown together at a family gathering, guests can unknowingly or inadvertently open the door to cyber criminals to an insidious attack.

Successful cybercrime can have unforeseen results, such as loss of reputation, especially by the yacht owner, exposure to blackmail and significant extra costs if the super yacht is disabled.

Relationships between owner, captain, crew, and guests can be tested leading to friction, disharmony and in the worst cases a "family breakup".

Yet if the parties can work together, many potential security loopholes can be avoided. There are benefits all round.

That is what Project CETO is designed to do. Bring owners, ship brokers and crews together with a common purpose, mutual understanding and a united approach to digital protection of their super yacht and assets.

Lord Louis Mountbatten, who claimed to be an odd-job man and, in 1966, became British Computer Society President, had a good look at what made a successful warship and came up with the idea of "Working Up" crew, officers and other members of the team together.

This is the approach taken by Project CETO to cyber security protection on super yachts and which has, as a starting point, the IASME Consortium based in the UK. IASME delivers the UK Government Cyber Essentials scheme and other cyber security certifications.

The organisation works alongside a network of almost 300 expert organisations across the UK and Crown Dependencies to help advise and certify organisations of all sizes. Learning from experience, IASME also runs a number of commercial schemes, including the Maritime Cyber Baseline (MCB) aimed at Superyachts.

CETO is a Cyber family guidance initiative. It is the first vital step in a full assessment of the yacht, surveying all Information technology (IT) and operational technology (OT) systems, documentation, policies, and processes. It determines the optimum cyber security posture as a starting point and most importantly considers the cyber resilience strength and weaknesses of all who sail onboard.

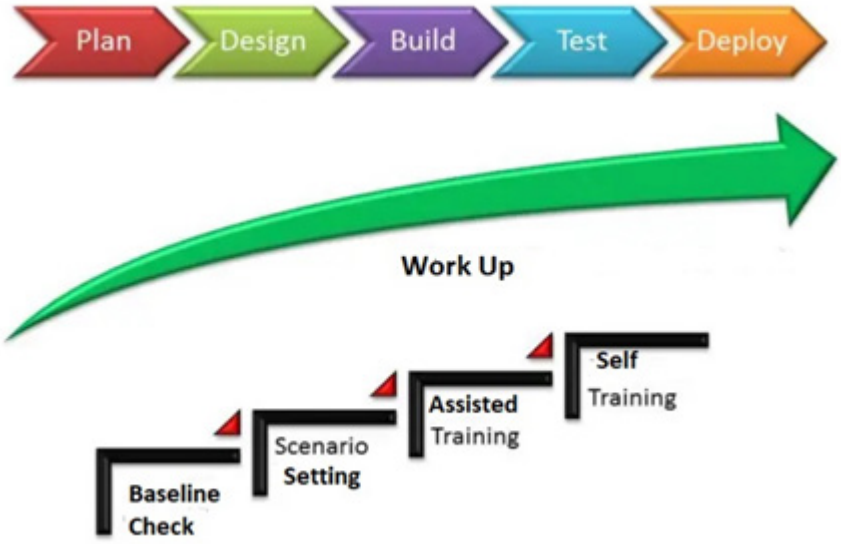
Built around active feedback, CETO provides bespoke training and awareness for all the crew, from junior deckhand through to captain and the owner. Its aim is to instil confidence, awareness and of a culture of regular self- training, with outside help only necessary to address new threats or circumstances.

CETO brings together the delinquent son who uses the internet without caring about the risks of inserting malware onboard; the younger members of the crew who may present the biggest risk to data and yacht systems as they lack rounded knowledge of the basics; through to the well qualified, but cyber naive engineer who leaves passwords in full view. It invites the Owner to participate rather than adopt a tendency to pass the responsibility onto the Captain.

Most superyachts are now fully outfitted with technology, from GPS and navigation systems to electronic chart displays, information systems and wifi.

High-tech super yachts with wealthy owners thus create the perfect combination for ransom -hungry hackers and extortionists. In an undisclosed phishing fraud, an Owner was defrauded of over $11 million in one transaction.

CETO "Work Up" progresses via the Baseline check to some simple scenario setting. This can be carried out onboard via assisted training and then self-training.



The assisted training focuses on building assurance, awareness and most importantly, practical cyber protection of the vessel and its personnel. It covers both IT and OT to provide comprehensive and enduring protection for the vessel, the crew, the owner and their guests.

Assisted training addresses the human aspects, since a majority of cyber security related attacks are attributed to human involvement. This bespoke training has already proved to be very effective in stopping staff from inadvertently causing costly cyber security incidents.

This type of training discusses and imparts current cyber security threats and subsequent threats to information including: negligence, phishing, insider threat, malware, technical surveillance etc. Specific modules can be incorporated to cover other security threats such as Email, Web (includes strong passwords and safe internet browsing), Mobile Communications, Wi-Fi, and the handling of sensitive information.

The aim is to stabilise, inject and take forward progressive Best Practice, including looking at the steps to take if the superyacht is suspected of being the victim of an attack.

Owners are not forgotten. Although it is best if they participate in the Work Up together with the others onboard, special modules can be created by experts, for C level stakeholders.

Although CETO is aimed at onboard personnel (including guests) it can be extended to train and make cyber aware land-based staff. This might include understanding of crisis management plans and relevant responses to this.

In Summary what CETO does is:

- Promotes cyber security for Superyachts
- Treats cyber as a ship wide safety challenge
- Develops and practises insight sharing between the crew and Owner
- Starts from a proven, practical and relevant baseline
- Focuses on the people on board working collectively for common good.
- Covers non digital **fall-back** option(s) which can be practised by those on-board when it suits them

Malcolm Warr

Malcolm has spent a lifetime in the Maritime Industry and has worked at all levels of Corporate and SME management - both ashore and afloat: And for Governments and the pub;lic sector. He now specialises in Maritime Cyber Security policy and development and chairs international conferences which include discussion on Superyacht protection -physical, digital, superyacht design and especially relevant training to protect very valuable assets, the crew, guests and the owner.