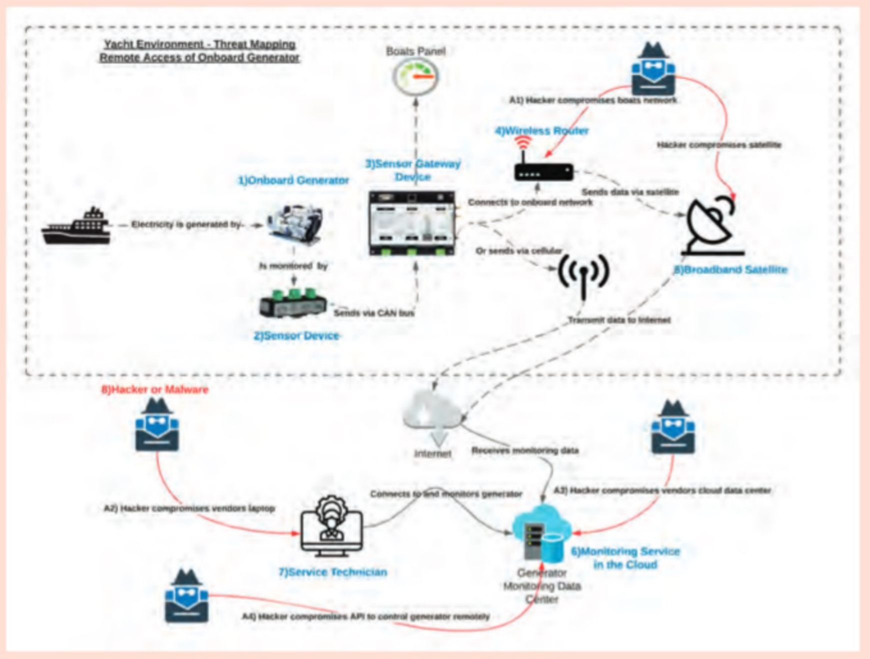
by **Alex Soukhanov** and **Will Perez,** *Moran Cyber*

REMOTE ACCESS: PROTECTING PRIVACY & SAFETY

Modern superyachts by character are the epitome of technology integration, from live-feed satellite communications and entertainment systems to state-of-the-art critical marine systems for navigation, engineering and propulsion, and vessel safety monitoring (referred to as Operational Technology [OT]). This integration typically is networked with extensive internet connectivity no matter where the vessel moves.


Yacht Environment - Threat Mapping
Remote Access of Onboard Generator
Boats Panel
A1) Hacker compromises boats network
4)Wireless Router
Hacker compromises satellite
3)Sensor Gateway Device
1)Onboard Generator
Sends data via satellite
Connects to onboard network
Electricity is generated by
Is monitored by
Or sends via cellular
5)Broadband Satellite
Sends via CAN bus
2)Sensor Device
Transmit data to internet
8)Hacker or Malware
Internet
Receives monitoring data
Connects to and monitors generator
A3) Hacker compromises vendors cloud data center
A2) Hacker compromises vendors laptop
6)Monitoring Service in the Cloud
7)Service Technician
Generator Monitoring Data Center
A4) Hacker compromises API to control generator remotely

The power of technology also is harnessed for optimized vessel performance, such as remote diagnostics and data collection, maintenance, voyage optimization and monitoring, remote control, and more. However, this evolution of digital access without security configurations and management as a priority also has increased risk of exposure to cyber vulnerabilities. In the context of superyacht ownership, this is a risk not only to privacy, but also to safety and is what makes maritime cybersecurity unique for superyachts.

Remote access to networks and systems on board is a prime example of something that should be closely monitored and managed – no different from physical access to the vessel. Remote access to networks and systems onboard can be via engine and equipment manufacturers, satellite communications providers, navigation system and software vendors, and security providers.

There are great advantages to remote access for technical representatives performing necessary functions. Fewer maintenance technicians physically visiting the vessel significantly reduces costs and preserves privacy for the vessel. Real-time diagnostics can be conducted in coordination with the chief engineer and captain, instead of waiting for a technician or diverting to a safe port for troubleshooting. An unscheduled and uncoordinated remote maintenance function on an operating marine engine at sea could be catastrophic. A compromised navigation system could prevent sailing and draw unwanted attention of the authorities and the public. These are two cases that actually have happened, and they were not cyber-attacks.

As an example, the diagram shown here depicts a typical remote-access system used to monitor and remotely maintain an onboard generator. In assessing this solution, there are seven systems at risk of being compromised by a hacker and four different attack entry points. Onboard the yacht, the sensor gateway device, wireless router, and satellite are the highest target systems for hackers. The shoreside remote management systems that are possibly vulnerable are the remote technician's computer and the cloud system collecting generator data and providing other computing services.

Guardian angel

Lastly, consider hiring a trusted service provider who is fluent with integrating marine system and the vessel's OT, is familiar with the vessel and maritime operations, and can serve as the vessel's guardian angel. This can be of particularly high value when the vessel travels to remote locations where technical cyber support may be limited, untrusted, or nonexistent.

Cyber threats exist along a spectrum in the same way as physical threats. Unauthorized access through the cyber domain should be treated the same as physical unauthorized access. And cyber threat actors and adversaries across a spectrum all should be treated the same – none of them belong on board. Simplify the problem by strictly limiting digital access to the vessel only to those who are trusted. Know whom you connect to, when, and why, and make no compromises.

1) Inventory and document systems onboard that have external connections.
2) Sign formal agreements for remote access.
3) Hire a trusted partner who can assess onboard remote access cyber risks and provide methods of reducing risks to the yacht.
4) Consider a secure cybersecurity threat-monitoring service to augment vessel operations, particularly as the vessel travels around the world.

Concentric has curated a team of specialists offering private maritime security against physical, cyber, and medical security risks. Moran Cyber provides security services to protect private vessels from cyber threats. For more information, visit www.concentric.io/family-office-maritime-security.