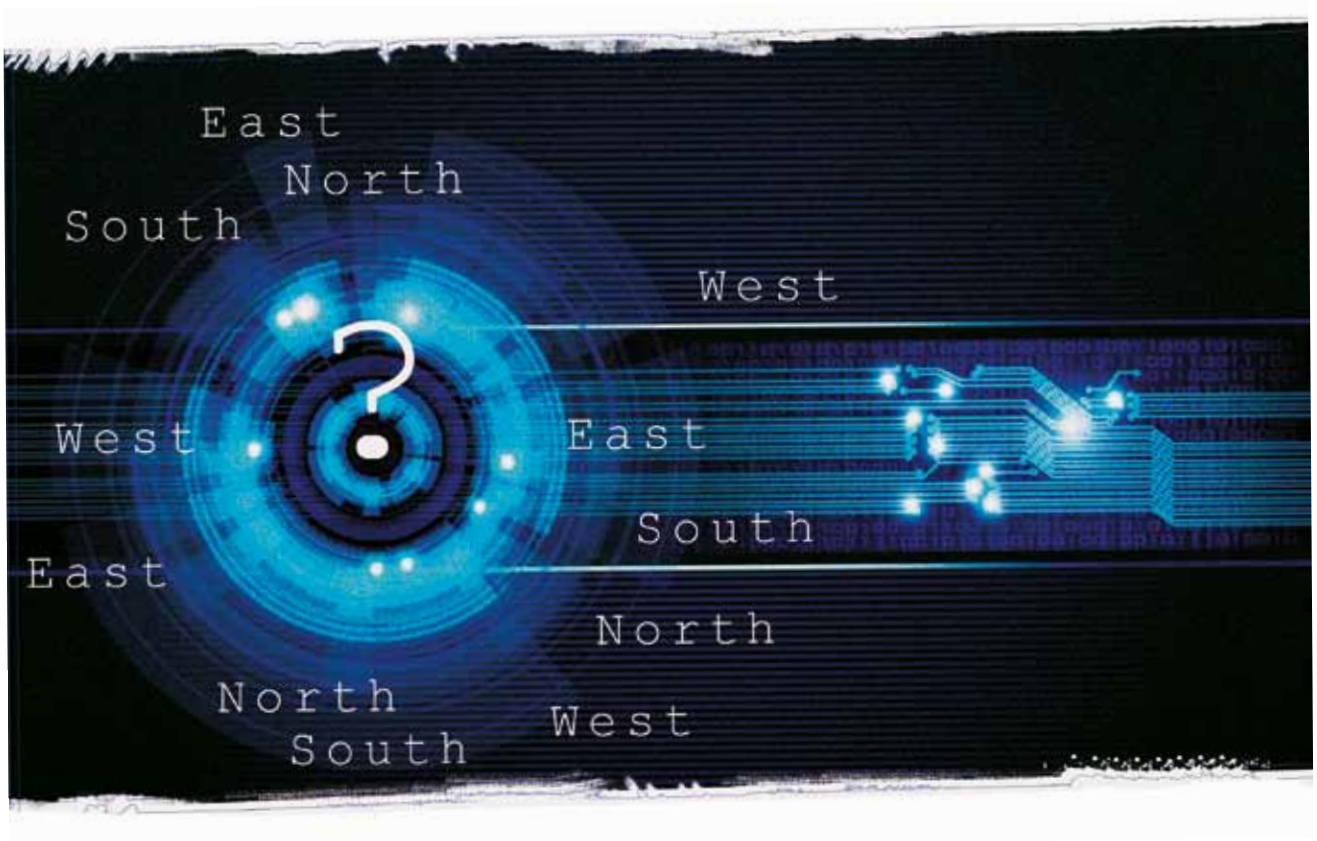
IN THIS SECTION
- Understanding cyber crime and digital piracy
- Security solution from Selex Elsag

The dangers of digital piracy



The threat of cyber crime can no longer be defeated by simply updating anti-virus software

EXPERTS AGREE THAT CYBER CRIME IS NOW THE MOST SERIOUS THREAT TO SUPERYACHT SECURITY. BUT WHAT IS IT — AND HOW CAN IT BE PREVENTED?

MICHAEL HOWORTH INVESTIGATES

MANY IN THE industry believe that armed piracy (such as that seen off the coast of Somalia) is the crime most likely to affect superyachts. And, as a consequence, many owners have begun investing in a variety of sophisticated measures to protect their yachts from similar physical threat. Often of military specification, this can include laser beams, citadels, and escape pods. For today's superyacht owner, feeling safe and protected at sea has never been more important.

However, even with the world's most high-tech security measures in place, superyacht owners and crew could still be leaving themselves exposed to another equally aggressive, yet far more insidious form of attack — cyber crime — which can take place without anyone onboard being aware.

"There's a general attitude that physical security measures are the priority onboard superyachts, but in fact electronic control systems are much more likely to be subjected to hacking and other criminal digital threats," explains Dan Hooton, founder of British cyber crime specialists, Spearfish Maritime Security. "Superyacht owners are ideal targets for cyber attacks and they're most vulnerable at sea."

Hooton also believes that cyber crime can no longer be defeated by simply staying up to date with the latest anti-virus software programs.

"Whilst anti-virus software can help, it's simply unable

to provide sufficient protection.

"In 2010 alone, a staggering 250m new digital security threats emerged — a figure which is set to increase every year from now on," he says.

Gaining access

Anyone looking to compromise a superyacht's electronic security has a host of access points to choose from, and it needs just one access point to be breached for a yacht's entire network to be opened up.

These weaknesses have been well-known to electronics experts for some time but, unfortunately, they are still misunderstood by even the most experienced of crew.

For example, modern GPS units can now be made to display incorrect latitude and longitude positions by being fed counterfeit signals.

Sailing into unfamiliar waters without knowing that the yacht is displaying misleading navigation information can have serious implications — placing those onboard in danger of wrecking or kidnap.

Criminal access to a superyacht's communications system can also compromise internal and external voice systems, giving hackers access to conversations via onboard computer systems which are likely to be highly personal or business sensitive and therefore extremely valuable to criminal gangs.

Onboard husbandry control systems — which are networked into the communications system — can also be compromised, enabling a hacker to alter the internal environment of the vessel.

The satellite televisions, games consoles and entertainment systems aboard all superyachts are also at risk from harmful infiltration.

Increasing threat

So, whether the intention is to defraud, steal information, or take full control of a superyacht, there is no doubt that many owners are placing themselves at both personal and professional risk through inadequate security protection across the whole of their onboard network.

And with cyber crime attacks now increasing in frequency and sophistication on an almost daily basis, it has never been more straightforward for criminals — be they business competitors, organised mafia, gun-totting pirates, or terrorists — to invade a superyacht's electronics and communications systems. SB

CONTACT DETAILS

- **SELEX Elsag**: www.selexelsag.com
- **Spearfish Maritime Security**: www.spear-fish.com
- **Yacht Technologies**: www.selexyacht.com

DIGITAL PIRACY PREVENTION & SECURITY

LEADING THE FIGHT against cyber crime in the superyacht sector is one of the world's leading electronics security firms — Selex Elsag — whose new Cyber Security Operations Centre (SOC) is being launched at the Monaco Yacht Show. Selex Elsag says that it will, for the first time, allow superyacht owners to use a fully integrated end-to-end cyber security service from a single contractor.

"Cyber crime can affect networks anywhere in the world, regardless of whether you are on land or at sea," explains John Hodder, head of superyacht operations at Selex Elsag. "And it comes in so many forms that no network is immune — not even the navigation system.

"Our new integrated system offers a highly robust infrastructure because it is designed and maintained to be resilient against all cyber security threats. And not only do these solutions include the design and configuration of security into the onboard network from day one, but now, thanks to Cyber SOC, they also include a range of embedded cyber security services."

John Hodder is leading the fight against superyacht cyber crime

Selex Elsag's Cyber SOC, located in the eastern Italian port of Pescara, has already been providing remote cyber security and monitoring to public and private sector clients for more than a decade.

It currently serves more than 5,000 customers, providing a round-the-clock service to ensure client networks and systems are protected to the highest standards against cyber crime and insider threats.

Finmeccanica Group, which operates the Cyber SOC, is also currently responsible for 70 per cent of all UK military and intelligence data encryption.

Security benefits

Central to the system is the installation of a special interface into the superyacht.

This interface has unique capabilities known only to the experts at the SOC, but Selex Elsag claims it provides cyber security of almost military specification. It provides a range of benefits for superyacht owners and operators including 24-hour global remote monitoring designed to guard against cyber threats while addressing security issues before they become damaging.

For example, the system can detect whether or not a yacht is going off course due to GPS spoofing by monitoring the strength of the satellite signal. If the signal is too strong the captain is alerted because there will be a good chance the position of the yacht has been compromised.

A continuous analysis of network traffic and user behaviours ensures that anomalies arising from threats or inappropriate behaviour are identified and responded to in a timely manner.

"At Selex Elsag we are now able to provide the superyacht industry with the same level of security as that required by government departments, major commercial enterprises, and critical national infrastructure providers," says Hodder.

"And we're able to do it by supplying and managing highly secure systems solutions for superyacht navigation, communications and entertainment operations."