

## Ensuring security on the high seas

**It's not just pirate attacks which can endanger the life of the super-yacht owner, he's also at risk from cyber crime – even in the middle of the ocean...**

The world of the super rich knows few boundaries. Expensive toys are not to be coveted, they're to be used and enjoyed. And perhaps one of the most expensive toys a person can own is an ultra-luxurious super-yacht.

Not just any yacht, but one which comes with its own defence systems, helipads and aircraft hangars, multiple swimming pools, special holds for ski-jets, inflatables, even the odd Aston Martin and, of course, a full staff to ensure round-the-clock service and care, 365 days of the year.

While the luxury cruise ship is a floating hotel, the super-yacht is a floating palace and its dimensions and amenities on board are second to none.

The most expensive and luxurious yacht in the world today is said to be that of Roman Abramovitch. At 560 feet long and reckoned to be worth at least \$1.2 billion, it is said that Abramovitch's *Eclipse* will remain the world's most costly for a considerable time to come.

Requiring a minimum crew of 70, it has a swimming pool which can be dried and used as a dance floor, an additional pool and an aquarium, two helicopters, three boats and even a submarine. Of course there are the inevitable exclusive facilities which keep guests wined, dined and entertained for days and weeks on end. More importantly, it also has a state-of-the-art security system to protect Mr Chelsea Football Club and his guests. This system includes anti-intruder devices, missile detection equipment and anti-wiretapping installations.

A super-secure environment for a very high-net worth individual. But in simple 'speak', just how safe is *Eclipse*? How can Mr Abramovitch ensure that the millions he has invested in securing his beloved yacht – or even in his more inferior one, *Ecstasy*, worth only a mere \$129 million, or his much cheaper *Le Grand Bleu* worth only \$90 million – will allow him to sleep well in his bunk each night?

Can he be confident that whatever he does, whatever he says and whatever he communicates on his specially diamond encrusted Blackberry, is not being intercepted by some unscrupulous person on the other side of the world?

## *High Seas security/2*

Is he really safe on the high seas or is he, like so many other super-yacht owners, vulnerable to the ever-growing network of cyber thieves who will stoop at nothing to infiltrate the world of the uber-rich? The answer, says Massimo Cotrozzi, a European cyber fraud expert, is 'not really'.

Super-yacht owners may be able to invest in the same levels of security currently provided to the highest levels of government, specialist agencies, military users and professional clients - but that doesn't give peace of mind even in the middle of The Bermuda Triangle!

At a super-yacht security round-table conference in Palma in 2010, a group of experts from the yacht building and suppliers' industries pooled their knowledge and expertise to discuss a vision for the future. From the manufacturers' perspectives it was agreed that an integrated technical infrastructure which would be impenetrable could be the first step towards security on the high seas. It was generally regarded at the forum that many people are unaware of the risks they leave themselves open to when on the ocean wave, particularly regarding cyber crime.

Cotrozzi agrees with those discussions and reiterates: "Security at sea for super-yacht owners is not just ensuring that pirates don't get on board, nor terrorists attack – and there have been plenty incidents such as these hitting headlines of late. Security also covers cyber space and protecting against cyber crime is a huge consideration for everyone who owns a luxury yacht, regardless of its size."

Security is necessary for data 'at rest' – that is, in the computer, on servers or hand-held networks and for data in transit (ie data which we communicate over public, private or corporate networks). There is a common, but wrong, assumption that if a computer is 'at home' and connected to our own 'private network', then data is safe. Unfortunately passwords for wireless networks can be guessed and computers can be penetrated via unpatched system components.

"Today's super-yacht is not just a place for entertainment and leisure, it also doubles as a floating office," Cotrozzi said, adding: "...and this is why it is imperative that protection is installed to safeguard sensitive data which could reveal behaviours, habits or, as importantly, information like bank accounts and of course business dealings."

Cotrozzi, who has often during his career stepped on board luxury yachts to assess communications' facilities and advise on security safeguards, has drawn up a check list for readers to consider and insists: "Essentially, more advanced techniques than the regular 'at home' protection systems must be installed."

### **System encryption to protect sensitive data at rest**

It's not enough to protect data with passwords. Sensitive information requires the presence of fully encrypted partitions to enhance the protection capabilities and reduce vulnerability and access in case of hardware loss or system compromise.

### *High seas security/3*

In 'easy speak', encryption is basically a system designed to scramble a message so that it is unreadable to persons who don't have the passkey or methods by which it was made unreadable. The passkey and knowledge of the method used to scramble must be available to unscramble the message.

Encryption continues to protect even when the system is compromised or 'hacked' into from afar.

#### **Encrypt sensitive communications**

When data is transmitted, it generally flows through public networks with little or no control from the sender and the receiver. A recent incident Cotrozzi cites, involved one major provider who routed millions of unencrypted communications through China – a country now recognised for its unscrupulous hacking networks.

Network security is therefore a necessity in all business environments – and that includes the super-yacht. Data interception can be avoided if an encrypted network service is established between the yacht owner's location (this can be in the middle of an ocean or even in port) and a trusted personal location where the communication is then forwarded securely to the destination.

Additionally, when emails are sent or documents shared electronically, most of the time, systems do not allow for data encryption. In order to better protect one's information, a secure data storage and forwarding system must be set-up. This allows for one-to-one (or many-to-many) communication without too much effort.

#### **Anonymisation tools for browsing**

Personal information is attached to every internet communication we make, whether we're at home or on the high seas. Web sites we visit are gathering location, system and user information from our computers/laptops/telephones.

Additionally, internet providers gather all sorts of details – mainly for data retention reasons as required by law – and they do not allow for deletion of such information which they also use for user profiling and tracking. Such information could be hidden by using the appropriate tools and techniques which would safeguard information and location. These tools of course can only be acquired via cyber crime/fraud experts.

#### **Biometric identification devices**

The use of biometry is not as complicated as it was a few years ago – the science of capturing personal data simply from a fingertip scan has moved forward and it is now being used for all manner of security procedures including within the super-yacht environment.

Just using the unique properties of a fingertip impression can render as obsolete the need for a password to access systems and data.

### *High seas security/4*

This greatly simplifies the adoption of advanced security systems on board when it comes to accessing data directly. This is an additional security measure which is simple and easy to adopt.

#### **Mobile telephone call security**

Someone, somewhere, could be intercepting sensitive mobile telephone calls even when they are made from the middle of the ocean! However the same security safeguards apply to mobile phone devices as they do when communicating through computers.

Mobile communications can be encrypted point-to-point with people using the same compatible devices. In this way, no one can access any communication. Messages can also be encrypted and either seen for a limited amount of time as in SMS messages or accessible only with the sender's pre-registered authorisation.

This procedure, which is again set up on the mobile system through specific tools and techniques by specialist cyber crime experts such as Cotrozzi, will ensure that calls can neither be intercepted nor recorded.

So, the owner of the super-yacht has protected himself from cyber attacks while communicating with the outside world – but a huge question still has to be asked. How can the owner be guaranteed that his floating palace has not already been infiltrated with listening devices, either at source during boat-building, or during a refit?

Cotrozzi enlarges on this topic: "When buying or commissioning a new yacht, it is essential to ensure that other parties have not fitted special surveillance devices which could be activated externally to snoop on the occupants' activities or to intercept communications.

"With the help of specially trained counter-surveillance experts, such devices can be tracked through special 'sweeping' and either destroyed or back-tracked to the organisation which wanted the devices installed in the first place."

It may seem an unlikely situation, but in today's world, nothing is impossible. Safeguarding every avenue of security is essential for safety on the high seas.

"Just as it is essential to protect against malware – that is, Viruses or Trojans - arriving on computers or through mobiles, it's necessary that security is put in place to protect the very fabric of the super-yacht," Cotrozzi concludes.

In short, no-one can sail safely into the sunset – wherever that sunset may be – without ensuring every precaution has been taken to safeguard luxury life on the ocean wave.

### *High seas security/5*

But, as Massimo Crottozzi, our cyber crime expert underlines: “Security is always thought to be complex and complicated but all the suggestions I have made, when properly implemented, will become so seamlessly integrated into a person’s life that not only will data and the yacht be made more secure, it will lead to a happier and more relaxing life afloat.”

#