CSS PLATINUM

Monthly Security Newsletter.

Welcome to November's edition!

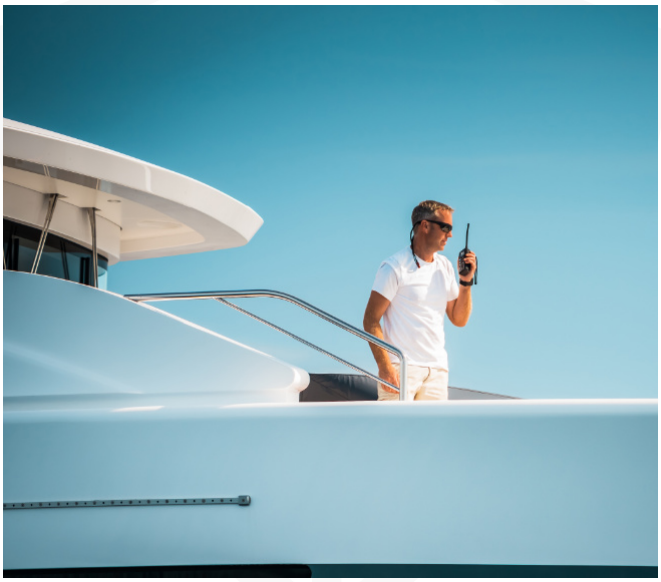
As we end the charter season, we see more superyacht organisations enquiring about cyber resiliency with us.

Unfortunately, every organisation is a target for cybercriminals, and the superyacht industry is no exception.

Our aim at CSS Platinum is to protect our Superyacht communities, ensuring guests, families, and employees are safe from cyber-attacks.

ISM cyber risk management regulations were introduced by the IMO last year to help provide compliance to the superyacht and maritime industries.

We explore how to achieve IMO ISM Compliance with our 6-step process starting this month with step 1 – understanding your current position and any vulnerabilities to your systems, processes, people or networks.



IMO ISM Compliance: How secure are you?

There are numerous stages to delivering cyber compliance against the IMO ISM (International Safety Management) Regulations.

CSS Platinum's **IMO Understand Service** provides a complete 360 assessment and report to assess the cyber-risk to your vessel, people, processes or technology against the IMO ISM Regulatory Compliance.

IMO CYBER COMPLIANCE

> "Knowing your vulnerabilities & associated cyber risks are the first steps to achieving cyber compliance"

Our **IMO Understand Service** will provide full risk assessment, gap analysis and technical penetration testing by our team of IMO cyber specialists to deliver a detailed roadmap and report demonstrating your commitment to Maritime Cyber Risk Management.

IMO CYBER RISK PROTECTED

A **complete report** of you maritime cyber risk resilience based against IMO Guidelines, including:

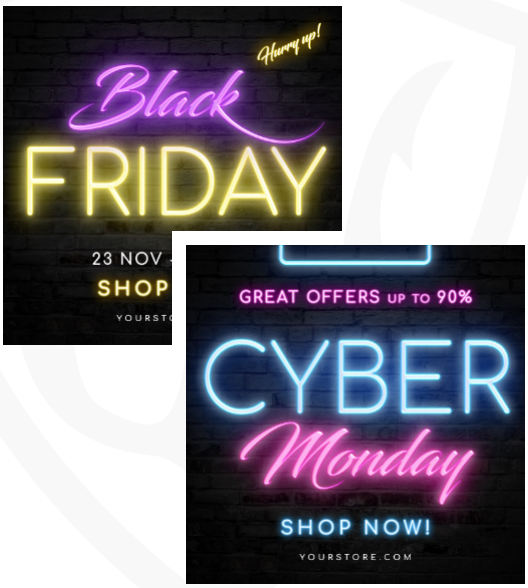
- **Bespoke Risk Register** for your vessel
- **Technical Penetration Testing** certification
- **Gap Analysis** against the IMO Cyber Compliance advised standards
- **Roadmap** for implementing governance and protections to meet the advised IMO Cyber Compliance standard

To learn more about the IMO ISM Regulation for Maritime Cyber Security or to request a call from one of our IMO specialists please click here

CSS PLATINUM

Monthly Security Newsletter.

Stay safe on Black Friday & Cyber Monday



Black Friday and Cyber Monday are just around the corner, and the internet is buzzing with deals. Unfortunately, cybercriminals are also gearing up for the increase in online activity. If you're not careful, you might be their next victim.

To protect yourself online, **follow these simple steps:**

1. Don't click on links in emails or social media posts.
2. Be careful when shopping online—don't use public computers or un-secure networks to make purchases.
3. Update your software regularly—it can help protect against viruses and malware!
4. Use strong passwords – check out our guide to password security below!

1 Use a strong email password

Any password should be at least 12 characters long but don't use birthdays, your name or family names and use different passwords for personal and work accounts!

2 Enable 2-factor authentication

If your password is compromised then this will help stop unauthorised access. 2-factor means in this instance, something you know (your password) and something you have provided (a onetime passcode) without these two items you can't access the account. All email providers have this option by default so if you haven't got it enabled, now is the time to get it activated.

3 Never open un-trusted attachments

If you receive an email with an attachment always check it is from a trusted source. Consider why the contact would be sending you a file. If in any doubt don't open the file it could be malware or ransomware.

4 Never click on unknown links

Links in emails can take you to undesirable websites where Hackers will look to steal sensitive data. Be vigilant and if you are not sure google the website to check if it is legitimate.

5 Emails can be intercepted

Whilst the connection to your email provider is usually encrypted, once it is sent to the recipient it must travel over many different systems on the Internet to get to its destination. Hackers can intercept emails and read the content before it arrives at its destination. Never put confidential or personal information in an email as it is not secure. Additionally, any files you attach will not be adequately protected.

6 Be aware of email schemes

Hackers will send you an email trying to impersonate someone you know. If the email has a sense of urgency and requires you to supply something right away it is usually a scam. The email will usually have spelling or grammatical errors in it also. If in doubt delete the email.