CSS PLATINUM

Monthly Security Newsletter.

CSS Platinum Newsletter June Edition

Charter season is in full swing, and the team at CSS Platium have been busy keeping our customers safe and secure. Our Co-Founder Mike Wills was delighted to speak on a panel at the Superyacht Investor event last month, detailing the threats of cyber attack to a superyacht – click to read the article here.

The team have been busy providing Yacht Audits in the US and Europe also, learn more about Yacht Cyber Security Audits below.

Behind the scenes:
What to expect with a Yacht Cyber Security Audit.

CSS Platinum help our clients' meet data and cyber security regulations by providing Cyber Security Yacht Audits, but what do they provide and what can you expect when commissioning a Yacht audit?

We spoke to CSS Platinum's Head of Information Security, Doug Lucktaylor to learn more.

What are the reasons for taking a Yacht Cyber Security Audit?

Superyacht and Maritime regulators like the IMO have set guidelines for the security and safety of vessels, employees and anyone who boards a boat. Cyber Risk Management regulations were introduced as part of the ISM Code in January 2021, and cyber security policies must be demonstrated to meet these guidelines.

Many of our clients are due their flag audit and must meet cyber security regulations. By speaking to a cyber security specialist like CSS Platinum and commissioning a yacht cyber security audit, you can demonstrate that steps have been taken to meet the Cyber Risk Management Guidelines.

Why are regulators demanding that cyber security policies are enforced?

My background is within the finance industry, which is heavily regulated to ensure data is protected securely.

If your data is not secure, then not only are systems exposed but also the people who work and use them – customers, employees etc. We have seen fines in the multi-millions for breaches of security in the aviation industry so, it's no surprise that a high-profile industry such as the Superyacht industry is now being held to a higher level of security.

How does a Yacht Audit work?

CSS Platinum work to a fixed AMA framework (Audit Maturity Assessment) that focussed on three pillars: people, process, and technology to provide a complete 360 audit.

We review all the systems on the boat, from servers, networked connections, and all devices from iPads through to air conditioning units to streaming devices - anything on or off-site that transfers or stores data will be assessed for vulnerabilities.

We also review the policies in place, who has responsibility, what can and cannot be accessed and by whom and then what happens if something goes wrong?

We are looking to put the measures in place to prevent security threats and additionally address reactive policies if ever breached; can you access information logs to demonstrate accountability and remediate them?

What does a Yacht Audit provide?

The audit usually takes place over a two day period. The analysis then provides an audit report which is presented to the client with recommendations on the current security posture. It contains both high and low level details of the findings and gives a detailed breakdown of the areas that should be looked at in order of criticality. These are linked back to the requirements and controls that need to be put in place to meet cyber security risk management guidelines.

Learn more about Yacht Cyber Security Audits here

CSS PLATINUM

Monthly Security Newsletter.

Phishing attacks target high-profile individuals: Are you the 'Whale' within your organization?

Phishing, the malicious email attack format that successfully impersonates a trusted sender, continues to be the most significant online threat to businesses of all sizes and industries.

These Phishing emails are sent in huge volumes to entire organizations or groups, knowing that at least 1 or 2 recipients might take the bait and unwittingly share their sensitive data or access, however, not all phishing attacks use such a wide net, a more sophisticated and specialized phishing attack genre known as "whaling" is crafted for selected high-profile individuals. These present desirable targets due to their influence level and direct access to sensitive information, security settings, and finances.

Cybercrime organizations expend a much greater effort and resources –and exhibit a much higher degree of creativity– in their mission to exploit these high-value targets.

Best Practices for mitigating the threat of whaling attacks, and to help prevent people from falling for them:

1 NEVER click on links or download suspicious attachments.

Most phishing attacks end with a call to action – usually clicking on a link or opening an attachment. As soon as you spot a link where you're supposed to click, you should be suspicious. If you think the link is legitimate, navigate to the browser and type the URL instead of pasting it. Most attackers use URL shorteners and look-alike domain names to trick victims.

2 Take note of aggressive or forced urgency, or demands

This is a critical component of a whaling attack and should be met with healthy skepticism. Attackers seek to create an emotional response in which you overlook suspicious details and instead worry about the impending deadline or threat.

3 Verify requests before you act

Examine the sender's email address. Is this request something that falls within your typical job duties, or that of your team? Is this email address one you have seen before? Is it in the correct format? Why is the CFO requesting that you transfer thousands of dollars into an offshore account? Verify the authenticity before acting if something seems unusual.

4 Practice good cyber hygiene

Restrict your personal information on social media Remember that the internet is a public place, and protect your privacy according to best practices, avoiding oversharing behaviors such as geotagging, and detailing of professional responsibilities or processes.

5 Awareness is key

Training/education should be on ongoing effort – enhance your human firewall by promoting a security-minded culture within your organization. To effectively avoid these email-based threats, your employees must first be aware that such a threat exists. Make sure they know the red flags and appropriate process for reporting suspicious emails or incidents while on the company network.

Learn about the people training that CSS Platinum can provide to ensure you and your organization is secure from cybercriminals
https://cssplatinum.com/maritime-cyber-licence/