CSS PLATINUM

Monthly Security Newsletter.

Welcome to November's edition of our Monthly Security Newsletter.

Cyber-attacks are ever-increasing. Unfortunately, every organisation is a target, particularly in our superyacht community, which is why we were delighted to be asked to feature in October's issue of Gibraltar Insight Magazine with an article that highlights cyber security risks and asks, "Could your business afford the impact of a Cyber Security attack?" See page 2 for more.

The CSS Platinum team have had a fantastic time meeting members of our community at the Barcelona ACREW awards and at FLIBS 2021. An amazing way to celebrate the end of the charter season!

CSS Platinum attend & secure the ACREW Awards as Official Security Partner

The CSS Platinum team were delighted to join our partner; ACREW at their prestigious crew awards in Barcelona last month. Everyone had a fantastic time celebrating in true 1920's style, safe in the knowledge that the event had been secured by the industry's leading cyber-security specialists!

Security Sponsor:

CSS PLATINUM

FLIBS 2021

Our US team were delighted to be a part of the Fort Lauderdale International Boat Show 2021. A great way to celebrate the end of the charter season with so many familiar faces!

CSS PLATINUM

Monthly Security Newsletter.

What would a cyber-attack look like to your business, and could your business afford it?

Privacy regulations have teeth

Internationally, there are an increasing number of compliance regulations whereby it is a requirement to protect against cyber-attacks. Widely known and leading the pack is the EU / UK General Data Protection Regulation (GDPR). This regulation requires that appropriate "organisational and technical" controls are implemented to protect personal data – by this, in the main, they mean cyber security. EU / UK GDPR are both extra-territorial, meaning regardless of the actual registration of your business, if you hold and/or processes the data of an EU or UK citizens, you must cyber-protect the data. Failure to do so could result in enforcement fines up to **£17.5M / €20M or 4% or global turnover** – whichever is greater.

Cost of damages claims

If your business is found to have transmitted a cyber-attack to a client or supplier due to insufficient or inadequate organisational or technological controls, and it has had a profound impact on strategic reputation, operational delivery, loss of intellectual property and/or personal data, you could probably expect to be sued for damages and the associated legal costs of defending your business. How would that affect your business?

Cost of management distraction

When cyber-attacks occur, they are all consuming, particularly if it is a ransomware attack and you have lost all digital access – no computer/device access, no website access, no management systems access. Nothing. All those tasks you were already juggling in your busy work life have just got interrupted, cancelled, or postponed while you concentrate on responding to the incident; communicating with shareholders, regulators, and insurers; and possibly having to inform and apologise to clients and suppliers. What would the cost of this be to you?

Reputation damage and loss of trust

When your clients provide their personal data to you there is an unwritten trust contract. They trust you to respect and preserve their privacy. Businesses spend huge amounts to recruit customers, but market analysis shows that an equitable amount is not invested in then protecting these clients. What would the impact be on your client's trust and your business reputation if you had to contact your clients to inform them that you had lost their personal data?

Most personal data stolen during a cyber-attack ends up for sale on the dark web for other cyber criminals to purchase and further target individuals. A single hack on your business, could lead to an individual being targeted multiple times over. How would you feel if it was your data? Would you want your business to be responsible?

There are a growing number of law firms offering group litigation action for damages to individuals who have had their data breached. Damages precedent is still being established, but currently are averaging at **£2000 per individual. If you lost 10,000 data records that could amount to £20m.**

So, in summary, while cyber security can feel like another compliance costs, the cost of a cyber-attack is likely to far exceed the implementation cost. Cyber security resilience is simply a baseline cost of doing business. For the full article please go to **https://cssplatinum.com/news/**