Cyber Security

comsec

Match Fit – Cyber Security

The growth of connectivity and the integration of IT (Information Technology) and OT (Operational Technology) makes all business better equipped to realise their "digital" potential, but with this increasingly "connected" environment come risks. James Ramm, Managing Director of Comsec Investigations Ltd explains more.

Complex interconnectivity means that physical equipment within organisations is increasingly likely to be linked to the internet. Whilst there is already awareness that data management systems are susceptible to cyber-attack, stadia systems such as lighting and ground watering have also been hacked. Whichever system is targeted, the outcome is similarly damaging - business disruption, reputational damage and financial loss.

Who are the victims? There are multiple examples of clubs both large and small, sporting organisations and individuals suffering targeted cyber-attacks. Team Sky, Keighley Rugby Club, the IAAC and Sir Mo Farah are examples, amongst many others, who have reported serious attacks.

Who are the perpetrators? Attackers range from tech savvy individuals, to sophisticated international criminal organisations, commercial or sporting opposition, terrorist groups and state sponsored hackers.

Why a cyberattack? There are many motives, including intellectual challenge, breaching cyber security as an end in itself, financial gain, reputational damage, political agendas, operational disruption and competitive advantage.

Protecting your organisation against cyber-attack demands a holistic approach.

Firstly, it's about ensuring that the people in your organisation value its assets and understand the vulnerabilities. Secondly, it's about a continuing programme of security review and testing of data management and physical security systems. Lastly, it's about recognising that professional security is not your core business and ensuring you engage with expert practitioners to deliver targeted penetration tests and security awareness training.

For more information on the Cyber Security needs of your company, please contact Comsec Investigations Ltd on + 44 (0)207 5537 960. www.comsechq.com

You can run, but you can't hide

The May 2018 deadline for GDPR Compliance is getting closer, and businesses and organisations of every size need to know how they will be affected.

During a celebration of RDS Global's 20th anniversary, the company's Technical Director, Rob Kay, spoke about the fast-approaching deadline for GDPR Compliance — while delivering a very important message to small businesses who think they can avoid the upcoming changes to the law.

Play by the rules

The GDPR law is specific, not an option, and will be enforced by the ICO (Information Commissioner's Office). However, with many smaller businesses feeling blinded by the sheer volume of the rhetoric and mantra being pushed from all angles, they may seek to ignore this issue in the belief that they will fly under the radar. This may be true, at least for a little while, but non-compliance will soon catch up with these businesses in ways they might not even realise.

While larger organisations are well prepared for the deadline, an audit of their supply chain will quickly highlight any businesses not playing by the rules like everybody else.

If that doesn't sound like enough of a warning, it's worth noting that customers and suppliers alike will insist on your certified compliance in order to continue doing business with you. Remain non-compliant, and you will quickly lose customers and clients.

RDS Global's team of Cyber Defenders will assist your business at all levels and implement the technology needed to safeguard against various types of cyber attack.

For more information please call us on **0330 221 1244** quoting fcbusiness
www.rds-global.com
#CyberDefenders #rdsglobal

RDS TAILORED IT SOLUTIONS

IASME Consortium ® GOLD Certified Company