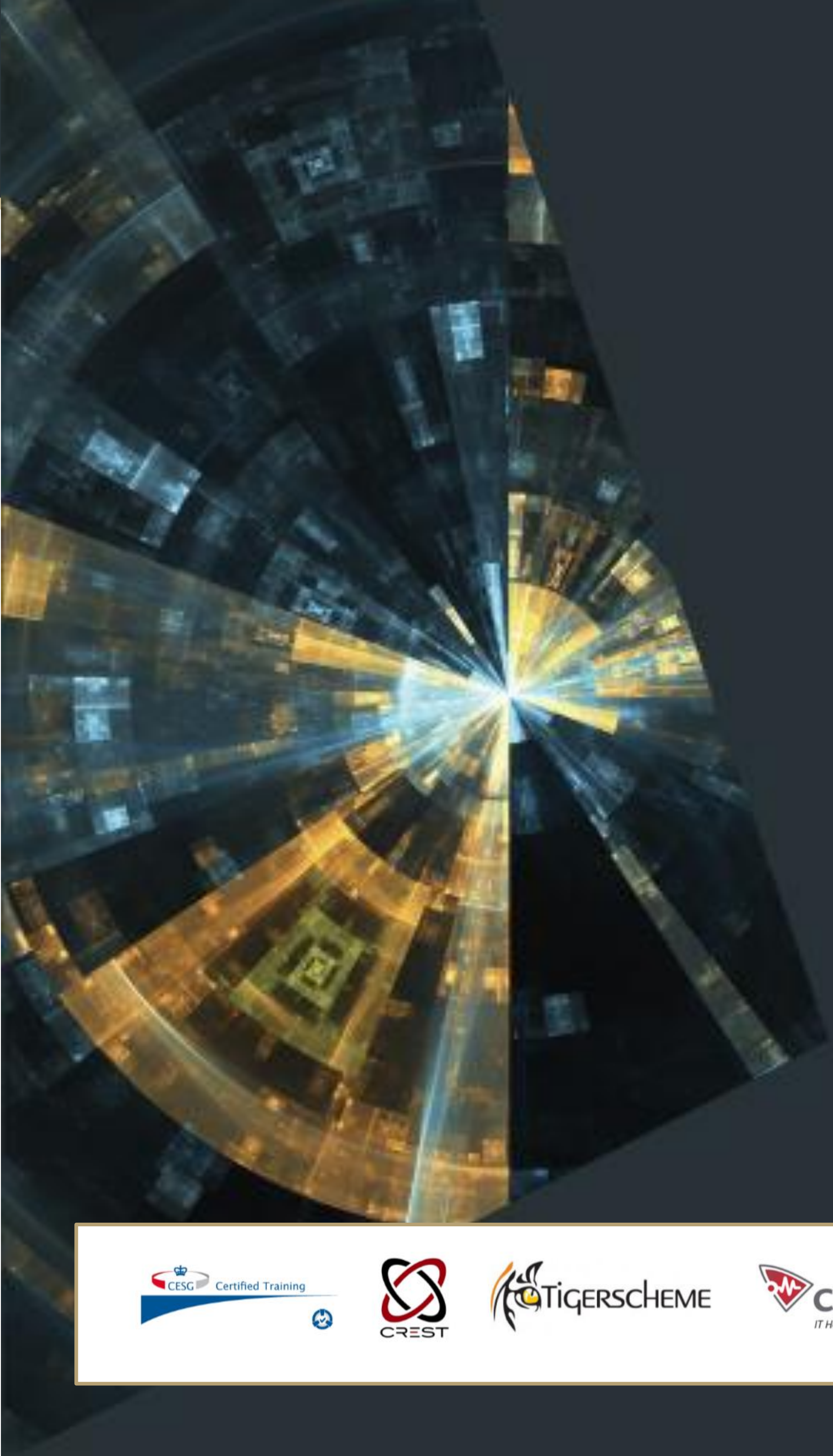

SME Cyber Digest

PGI

1st February 2017

- VPNs Not as Private as We Might Think
- 50% of Ransomware Victims Pay Up
- Insurance Company Fined for Data Loss
- An Essential Starting Point
- What is (was) Data Protection Day?

CESG Certified Training CREST TIGERSCHEME CHECK IT Health Check Service PCI DSS COMPLIANT Cyber supplier to: HM Government

Customer Services
+44 (0) 845 600 4403
pgicyber@pgitl.com

50% Of Ransomware Victims Pay Up

Whilst official guidance from cyber security experts and law enforcement is not to pay any ransomware demands, in some cases businesses and individuals are forced to do just that as they have no other option to retrieve their data. A new report by the Ponemon Institute called “The Rise of Ransomware” has revealed that 48% of businesses hit by ransomware admitted that they paid the demand. The report also found that whilst the average payment was $2,500, 7% of respondents admitted to paying more than $10,000 to get their data back.

There are several worrying findings in this report, not least that 49% of respondents said they were too afraid of public scrutiny to report the ransomware attack, and only a quarter had confidence that their existing security mechanisms would protect them from future attacks. As the majority of successful attacks are facilitated by phishing and social engineering techniques, having well-informed and vigilant staff will provide a good initial defence against possible infection. As well as ensuring your staff have an awareness of phishing techniques, another critical mitigation measure is to keep back-ups of your essential data and systems. Of the 52% of respondents that chose not to give in to ransom demands, the reason given was because they had indeed maintained a full back-up of critical data.

VPNs Not as Private as We Might Think

One piece of security advice we regularly share with our customers is the recommended use of Virtual Private Networks (VPNs) to increase personal security when using public WiFi networks. With a constant stream of media reports warning about threats to online security and browsing habits, mobile VPN apps are increasingly being used by millions of online users to hide browsing activities, bypass region-restricted content (e.g. the Great Firewall of China) and to protect data when using public Wi-Fi networks. However, academic research released last week claims that VPNs might not be as private as we think.

The research assessed the security and privacy features of 283 Android VPN apps, and found that not only did 18% of the apps fail to encrypt users’ traffic, but 38% injected malware or malvertising. Additionally, 80% of the tested apps requested to access sensitive data including user accounts and text messages.

While most of the examined VPN apps offered online anonymity, some app developers were found to be deliberately seeking to collect personal information that could then be sold on to external partners. As with any Android mobile app, we encourage users to ensure they only use the official Google Play store and conduct a degree of research into existing user reviews before signing up to a particular VPN service.

Insurance Company Fined for Data Loss

It was announced last week that the ICO has issued a £150,000 fine to Royal & Sun Alliance Insurance after the loss of the personal information of nearly 60,000 customers including names, addresses and bank account details. The data was lost after the theft of a hard drive device and the ICO found that appropriate measures were not in place to protect the financial information by preventing the theft from happening at its offices.

Although this incident was initially a physical crime and not cyber-related, it is a timely reminder of the importance of protecting personal information (the data on this hard drive was not even encrypted), especially with the forthcoming EU General Data Protection Regulation which comes into force next year and will carry significantly higher fines where companies are proved to have been negligent.

An Essential Starting Point

Unfortunately, the cyber threat landscape at the start of 2017 remains largely unchanged from 2016 and a range of new studies have found that cybercrime continues to increase. One of the first steps a SME can take to address cyber security concerns is to consider Cyber Essentials accreditation. The Government-backed scheme defines a set of controls which, when properly implemented, will provide organisations with basic protection from the most prevalent forms of threat coming from the internet (it is estimated that by implementing the controls, businesses can protect themselves from almost 80% of cyber threats). The scheme also offers a mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions.

There are two levels of certification – Cyber Essentials (CE) and Cyber Essentials Plus (CE+). CE certification requires a validated self-assessment which is approved by a senior executive and then verified by an independent Certification Body. This option offers a basic level of assurance and can be achieved at low cost, or as part of one of PGI's Digital Security Packages.

CE+ is more rigorous and offers a higher level of assurance through the external testing of the organisation's cyber security approach. This involves remote and on-site vulnerability testing to check whether the controls claimed actually defend against basic hacking and phishing attacks.

CE accreditation is also becoming an increasingly important requirement in the adoption of cyber insurance policies for businesses throughout the supply chain. Whilst larger firms have taken big strides in improving cyber security, they still face significant risks through their exposure from third parties such as service providers or product suppliers who are typically less well protected. The highest profile example of this was the Target breach in which data from 110 million customers and 40 million payment cards was stolen after the company was initially breached via an air-conditioning provider. It is likely that insurers too will now use CE as a mechanism for rational pricing of risk. Whilst the cyber insurance industry is still relatively immature and less than 10% of companies are believed to currently have cover, insurers recognise that having CE certification is a valuable indicator of a mature approach to cyber security and, as more firms achieve certification, it will help lower premiums and expand the cyber-insurance industry.

What is (was) Data Protection Day?

Last Saturday (28th January) was officially annual Data Protection Day, and many information security organisations used the day to warn businesses and consumers about the numerous data privacy issues which will proliferate over the next few years. The clear messaging focus was the EU General Data Protection Regulation (GDPR), which will come into force in May 2018, irrespective of the UK's position with Brexit. Other considerations centred on the potential risks associated with cloud data storage. As more businesses and individuals look to public cloud infrastructure to boost capacity and lower costs, leading security experts warn that these may not offer the necessary security and data protection measures that will be increasingly required for critical data.

Visit Our Websites

Protection Group International:
www.pgitl.com

Protection Vessels International:
www.pviltd.com

Cyber Services:
www.pgicyber.com

Cyber Academy:
www.pgicyberacademy.com

Intelligence Services:
www.pgi-intelligence.com
www.riskportal.pgitl.com

JTip:
www.jtip.co.uk

Follow us on Social Media:

Customer Services
+44 (0) 845 600 4403
pgicyber@pgitl.com