Cyber Risks & Liabilities

November/December 2019

Government Data Reveals Biggest Cyber-risks of 2019

The National Cyber Security Centre (NCSC) recently released their 2019 annual review, outlining the top forms of cyber-attack that both UK individuals and organisations experienced this past year. As 2020 approaches, be sure to review the following data points for a better understanding of the biggest cyber-threats facing your organisation and best practices for bolstering your cyber-security programme.

- **Phishing attacks**—The NCSC removed over 177,000 UK-based phishing websites from the internet this past year. Cyber-criminals use these sites to trick users into unknowingly revealing their personal information. This technique has consistently become more sophisticated and destructive over time. Use these tips to reduce your organisation's phishing risks:
    - Train employees on how to detect and report any signs of phishing (eg emails from unknown senders, suspicious links or unsecure web addresses).
    - Conduct routine software updates.
    - Install anti-malware and virus protection on all organisational devices.
- **International threats**—Of the 1,800 cyber-incidents that the NCSC has handled, a significant portion of attacks came from hostile nations—including Russia, China, Iran and North Korea. To mitigate your organisation's international cyber-threats:
    - Ensure compliance with all GDPR requirements regarding international data operations.
    - Communicate with your local authority if you suspect an international cyber-threat.
- **Payment card fraud**—The NCSC detected over one million instances of suspected payment card fraud this past year. If your company utilises e-commerce, this is a top concern. Implement this guidance to limit your risk of payment card fraud:
    - Make sure your organisation's website has the proper controls to prevent hackers from infiltrating your payment system.
    - Choose a trusted payment processor for all online transactions.

More than anything, you need robust cyber-insurance to protect against these evolving threats. For more information and cover solutions, contact **Crendon Insurance Brokers Ltd**.

Crendon Insurance Brokers

Crendon Insurance Brokers Ltd

012145 45 100

www.crendoninsurance.co.uk

Here's How the UK's New Data Sharing Agreement Could Affect Your Organisation

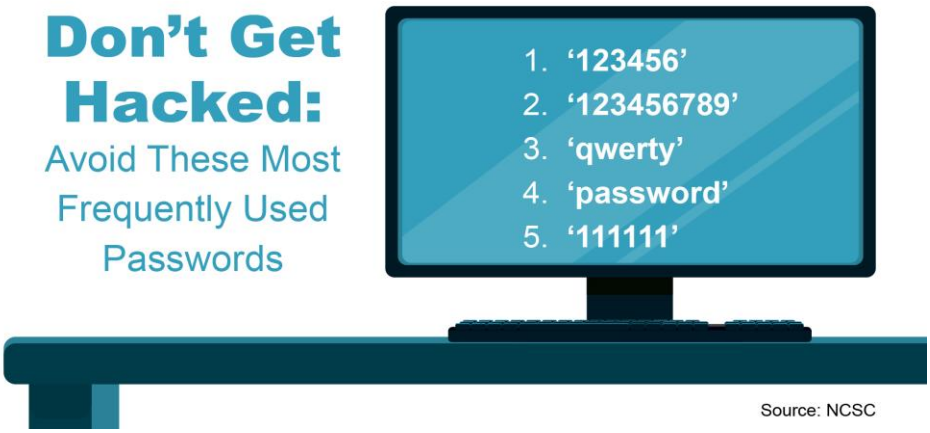
On 3rd October 2019, the UK and the US officially signed a new data sharing agreement in an effort to provide law enforcement agencies from both parties with more timely access to digital evidence held by international service providers (eg web hosts or social media platforms).

This agreement was motivated by both nations experiencing significant delays in retrieving digital evidence overseas for the purposes of investigating international criminal offences. Under this new agreement, such delays are expected to be reduced from months (or sometimes even years) to weeks.

While most organisations are unlikely to be impacted by this agreement, any UK-based business that has the potential to receive an international digital evidence request from the US should be prepared to comply with this new time frame.

Further, organisations and individuals subject to criminal investigation by US and UK authorities for data-related matters should be aware that evidence against them will be gathered faster than ever before. With this in mind, it's crucial to ensure that your organisation is maintaining GDPR compliance and storing data securely.

Although the agreement has not yet been published, Crendon Insurance Brokers Ltd will be sure to provide you with updates, compliance guidance and insurance solutions on the matter as soon as anything changes.



Are Your Devices Secure? Review These Password-cracking Methods

Password cracking is one of the most common ways that cyber-criminals gain access to sensitive company information. That's why ensuring your organisation takes appropriate steps to bolster password protection techniques is crucial in preventing a cyber-attack. Have a look at these top password-cracking methods, according to technology experts:

- **Dictionary attack**—This technique allows the hacker to quickly test simple one-word phrases to crack the user's password. Examples include 'password', 'administrator' or 'computer'.
- **Phishing**—Cyber-criminals can utilise email phishing to crack passwords by using a fake identity or website to trick the victim into providing their password. For example, the hacker could impersonate the victim's bank provider and send an email requiring them to log in to a fraudulent portal to manage their account information.
- **Malware**—This form of attack occurs when the hacker uses malware to record the victim's screen without their knowledge and screenshot their password.
- **Spidering**—This method entails the cyber-criminal studying information about your organisation and attempting to crack users' passwords with words or phrases connected to the company. Hackers might use your organisation's website, marketing materials or competitor information to compile potential passwords.

With these password-cracking tactics in mind, consider the following action items to strengthen your organisation's passwords:

- Establish password complexity requirements for all employees. This includes making passwords longer than eight characters, using upper- and lower-case letters, and including numbers or special characters.
- Restrict employees from using personal or company information in their passwords.
- Instruct employees to never share their password online.
- Have employees routinely update their passwords.
- Install anti-malware protection on all devices.

For more cyber-security tips, contact Crendon Insurance Brokers Ltd today.