Cyber Security Guidance Note

What is the cyber security risk?

Cybercrime in 2019 is estimated to cost the UK economy £27BN according to the Cabinet Office. This cost is associated with a number of differing cybercrime attacks, whether that be ID Theft, Fraud, IP Theft, Extortion, or Espionage.

At the highest and most complex level foreign intelligence agencies are behind such attacks, followed by large organised crime networks, finishing with opportunistic cyber criminals. It's worth noting that the majority of attacks are carried out by organised crime groups.

In terms of scale, an average of 0.4BN records are exposed per month, with 4.1 BN records exposed in the first half of 2019.

What do cyber-attacks target?

There are three major areas that cyber criminals attack, data, money, and service delivery. Data and money can be closely associated, as an example a record containing a small number of attributes, e.g. Name, DoB, Address, can sell for up to £120 per record. More directly data can be stolen or encrypted, and the owner held to ransom to restore this data.

Attacks on service delivery can be intentional, for example to bring down a website to cause loss of earnings or reputational damage. When consequential, such as WannaCry in 2017, the aim was to extort money, but the knock-on effect was mass service disruption within the NHS.

How do attacks most commonly occur?

The most common attack in 2019 have been;

1) **Hacking**, where networks or systems have been deliberately compromised to gain access to environments to allow data extraction. Examples of this can include Business Email Compromise via use of legitimate credentials or exploiting known vulnerabilities of web applications or IT infrastructure to gain access.

2) **Malware**, 'malicious software' can take many forms, most commonly Ransomware where systems are encrypted and only decrypted after Bitcoin payments are received(e.g. WannaCry). Spyware is also a common form, where non-intrusive applications run and log all activity, including usernames and passwords, used in order to gain access.

3) **Phishing**, or social engineering, where the legitimate 'user' is compromised to transfer the rights of that account to the hacker and perform malicious activities, e.g. supplier fraud.

Practical steps to protect

1) **Secure your internet** by ensuring that network-based firewalls and host-based software firewalls are installed, active, updated, and configured correctly.

2) **Secure your devices and software** by ensuring any default usernames and/or passwords are changed when a new device is purchased. Utilise Two Factor Authentication for secure applications, e.g. banking, email, etc

3) **Control who has access to your data and services** by regularly reviewing who has access to these, and what level of access they have. Administrative access should only be used to perform such admin tasks, and not as a default or regular permission.

4) **Protect yourself from viruses and other malware** by ensuring all your devices are protected by appropriate anti-malware solutions

5) **Keep your devices and software up to date** by ensuring parches and Operating systems are at the latest levels.

Note Cyber Essentials + , operated by NSCS, is an independent audit of an organisation to these standards and is being widely adopted as the minimum level of security throughout the UK.

Seric
4th Floor, 75 Bothwell Street, Glasgow, G2 6TS
www.seric.co.uk