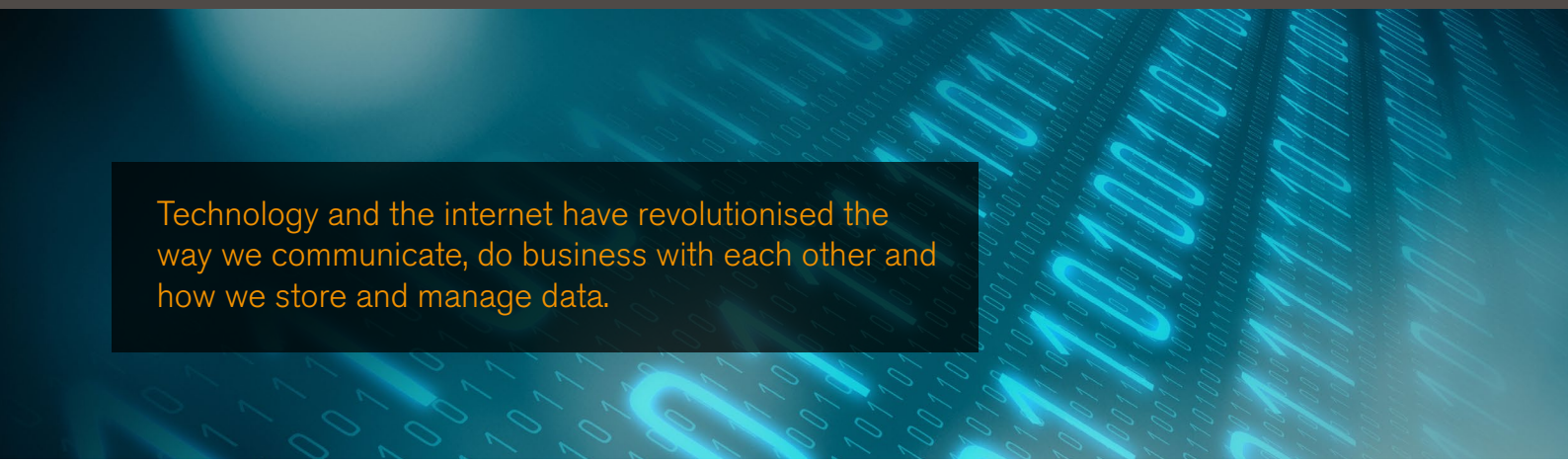
Cyber security



Technology and the internet have revolutionised the way we communicate, do business with each other and how we store and manage data.

Today organisations and businesses are ever more dependent on computer systems, the internet and technology such as smart phones and tablets to conduct business and carry out their day to day activities.

Unfortunately the explosion in technology and internet use has also seen a significant rise in those looking to exploit the technology for financial gain or to cause damage and interruption to systems and services. In addition, an organisation's own employees could also cause significant damage either through intent or by accident.

Many cyber attacks use indiscriminate scatter-gun approaches to target victims. If you're a small business, you're just as likely to be a victim of these scatter-gun attacks as a large organisation. Attackers may not know (or care) who you are until they get into your system.

Businesses large and small are being urged to protect themselves against cyber crime after the UK Government's Department for Digital, Culture, Media and Sport, Cyber Security Breaches Survey 2017 found nearly half of all UK businesses suffered a cyber breach or attack in the past 12 months.

A cyber security breach can damage an organisation in many ways ranging from disruption and data loss, damage through loss of intellectual property, denial of access to websites and services, physical loss or damage through viruses, ransomware and other forms of malicious software, reputational impact through damaged brand image and impaired customer relations.

In addition, legislation such as the Data Protection Act 1998, and the European General Data Protection Regulation (GDPR) which comes into force in May 2018, can impose penalties on organisations for not taking appropriate steps to secure or prevent access to data about individuals.

Cyber threats

Cyber liability and loss of data

Legislation such as the Data Protection Act 1998, and the European General Data Protection Regulation (GDPR) which comes into force in May 2018 place responsibilities on your organisation when managing, securing and using data. Failure to comply with these responsibilities may result in enforcement action by the regulator and the imposition of fines. At the same time, if the person or organisation to which the data relates suffered a financial loss, or harm to their reputation because of your failure to adhere to these responsibilities, a civil liability could be created.

Under GDPR individuals who suffer material or non-material damage as a result of an infringement of the regulations have the right to claim compensation. This means you could face compensation claims not only for financial losses but also for distress and hurt feelings, even when there is no financial loss. In addition you could also have to pay:

a) their legal costs (in the event you were unsuccessful in defending a legal action),

b) your own legal defence costs.

The costs to you following an unauthorised or inadvertent loss of data are not limited solely to legal costs and any amounts of compensation you may have to pay. You may incur further costs:

a) investigating the extent of the issue, which may include hiring professional persons to undertake this for you,

b) informing affected parties that their data has been lost or illegally accessed,

c) providing support to affected parties, which may include providing helplines and specialist help because of the effects of identity theft, and

d) reducing the impact of a loss of data on your reputation, which may include hiring Public Relations specialists.

In addition to any legal liability that may be incurred by a data loss, an organisation could also find themselves liable for damage to third parties through unintentional onward transmission of Malware, or through their computer system being maliciously taken over and involved in a Distributed Denial of Service attack (DDoS) on other organisations.

Cyber crime

Cyber crime has now overtaken physical crimes such as burglary or robbery. Cyber criminals are highly organised and are finding a myriad of new and more sophisticated techniques to access data and information for the purpose of financial gain and to commit fraud. This can result in money being taken from a bank account or credit arrangements (such as loans or overdrafts) being arranged in your organisation's name for the benefit of a fraudster. There is also an increasing risk of the use of 'Ransomware' where an attempt is made to extort money from you by preventing access to your computer system or files until a ransom is paid.

In the event that someone attempts to extort money from you, or hold your data or systems to ransom it's important that you do not pay the ransom demand without first seeking specialist advice. Paying even a small sum can result in an increased risk of you being targeted again in the future, as criminals share this information and in many cases, despite payment, access to the locked computer or files is not always restored.

Hackers will use any means available to find technical, procedural or physical vulnerabilities which they can attempt to exploit. They will use open source information such as LinkedIn and Facebook, and other social media to exploit user naivety and goodwill to elicit further, less openly available information, which they can then use to access to your computer systems.

1. **Phishing** - the fraudulent practice of sending emails purporting to be from reputable organisations/authorities in order to induce individuals to reveal personal information, such as passwords and financial information.

2. **Spear phishing** – The practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.

3. **Whaling** - The practice of sending emails ostensibly from a known or trusted sender in order to induce senior executives or CEOs to reveal sensitive information such as employee or customer data, passwords and other account details.

4. **Smishing** - the fraudulent practice of sending text messages purporting to be from reputable organisations/ authorities in order to induce individuals to reveal personal information, such as passwords and financial information.

5. **Vishing** - Vishing works like phishing and is carried out using voice technology i.e. phone or voicemail.

Damage to computer systems

Your systems may be damaged, have access denied or even destroyed by the use of malicious software, known as Malware, that can spread throughout a network. Systems may also be damaged through hacking (breaking security access codes to gain entry to your system). This may be as a result of criminal action for financial gain, hacktivism (hacking for political or other cause) or merely out of an individual's malicious intent or a need to 'show off' to their peers. Such incidents can incur expense in repairing damage to your computer systems including your websites.

1. **Malware** - software which is specifically designed to disrupt, damage, or gain authorized access to a computer system.
2. **Denial of Service** (DoS/DDoS) - a flood of simultaneous requests sent to a website to view its pages, causing the web server to crash or simply become inoperable.
3. **Web attacks** - websites can be defaced, databases with customer details can be extracted, malware can be inserted for download or the details of visitors to the site can be harvested.

Business interruption

Any incident of hacking, malware or ransomware attack may mean that your computer systems are out of action and could potentially leave you unable to trade or operate. This can result in loss of income, or additional expense to minimise the impact of this interruption to your organisation (for example, temporary hire of replacement computer equipment).

There is also a risk of reputational damage following a loss of data with customers losing confidence in your ability to protect their personal information. This potential loss of customers could also lead to a reduction of income as it may take some time to regain customers' trust and get back to pre-incident trading levels.

Cyber risk management

According to Ciaran Martin, CEO of the Government's National Cyber Security Centre (NCSC):

'The majority of successful cyber attacks are not that sophisticated but can cause serious commercial damage. By getting the basic defences right, businesses of every size can protect their reputation, finances and operating capabilities'.

In addition Government Communications Headquarters (GCHQ) estimate that approximately 80% of cyber attacks can be prevented or mitigated by basic information risk management.

There are a number of measures you can take to ensure you are prepared, but it's of vital importance that you have an incident management plan to ensure your organisation can respond quickly to, and mitigate the impact of an actual, or alleged, data breach. The introduction of GDPR will bring with it a requirement to notify a loss of certain types of personal data to the relevant supervisory authority within 72 hours of you first becoming aware of a data breach.

The National Cyber Security Centre has issued the following guidelines for small organisations that if implemented can help reduce the cyber threat and the impact a successful cyber event could have on your organisation.

Backing up your data

- Identify what data you need to back up
- Keep your back-up separate from your computer and restrict access. Consider using the ‘Cloud’ so the data is physically separate from your location
- Make backing-up part of your everyday business

Although the market is reasonably mature and most providers have good security practices built-in, we recommend you read the NCSC’s Cloud Security Guidance before selecting a provider.

Protecting your organisation from malware

- Install (and turn on) antivirus software
- Switch on your firewall
- Keep all your IT equipment (software and firmware) up to date (patching)
- Restrict the ability to download apps and software to designated individuals
- Control how USB drives (and memory cards) can be used.

Keeping your smartphones and tablets safe

- Switch on password protection
- Make sure lost or stolen devices can be tracked, locked or wiped
- Keep your devices and apps up to date
- Don’t connect to unknown Wi-Fi hotspots.

Using passwords to protect your data

- Make sure you switch on password protection
- Use two-factor authentication for “important” accounts
- Set minimum guidelines for passwords e.g. a mix of characters, numbers, upper and lower case
- Avoid using predictable passwords
- Change passwords regularly
- Help your staff cope with password overload with password managers
- Change all default passwords.

Avoiding phishing attacks

- Reduce the possible impact of successful attacks by restricting user rights to only those required for their job
- Provide staff training and consider how someone might attack your organisation
- Make sure your staff are aware of the obvious signs of phishing such as poor grammar and spelling, generic openings such as 'valued customer', calls to act urgently etc
- Encourage staff to report all suspicious emails and to ask for help if they think they might have been victim of phishing
- Report all attacks to the authorities (ActionFraud)
- Keep up to date with techniques used by attackers. Consider signing up to the free 'Action Fraud Alert Service' to receive verified information about scams and fraud in your area.

For more information download the guide from the NCSC website (https://www.ncsc.gov.uk/guidance/cyber-security-small-business-guide-pdf-version)

Source: National Cyber Security Centre – Cyber Security: Small Business Guide

If you need to improve your cyber security further, then you can also seek certification under the Government's Cyber Essentials scheme, which has the benefit of demonstrating to both existing and prospective clients that you take the protection of their data seriously.

(See http://www.cyberessentials.ncsc.gov.uk for more details).

If you are a larger business, or face a much greater risk from cyber crime, then the NCSC's 10 Steps to Cyber Security is a good source of information and can further enhance your approach to cyber security (www.ncsc.gov.uk/guidance/10-steps-cyber-security).

Compliance or alignment with a recognised standard, such as ISO/IEC 27001:2013 Information Security Management, can help you implement some of the above steps.

Useful links

http://www.actionfraud.police.uk/
(The National Fraud & Cyber Crime Reporting Centre. Cyber crimes committed or attempted against you can be reported here. Also contains useful information on how to protect your organisation against fraud, scam emails etc)

https://www.gov.uk/data-protection/the-data-protection-act
(overview of the Data Protection Act 1998)

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
(Information about the General Data Protection Regulation (GDPR) affecting UK law from May 2018)

https://www.iso.org/isoiec-27001-information-security.html
(Website for the International Organisation for Standardization who developed ISO/IEC 27001:2013 referenced above)

https://www.ncsc.gov.uk/guidance
(Website for the National Cyber Security Centre, useful information on how to protect your organisation against common cyber threats)

http://www.riscauthority.co.uk/free-document-library/RISCAuthority-Library_detail.s28-cyber-crime-overview-and-sources-of-support.html
(Website for Riscauthority – free download document regarding cyber threats)

https://www.ncsc.gov.uk/cisp
(CiSP is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business)

Ecclesiastical Insurance Office plc (EIO) Reg. No.24869 is registered in England at Beaufort House, Brunswick Road, Gloucester, GL11JZ,UK and is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

PD2819 1 02/18