Cyber-crime cited as number 1 concern by brokers

We live in a digital society. From email to social media, smart phones to wearable tech we interact with the digital world on a daily basis. The more we interact, the more information that is stored. Unsurprisingly, the frequency of data breaches – the theft, loss or mistaken release of private information - is on the rise.

1 Who's at risk?

Today virtually all organisations collect and store personal information about customers, employees, service users and others.

HM Government research shows that 1 in 4 businesses reported a cyber breach or attack in the past 12 months[1]. And it's not just big businesses that are at risk, though it tends to be these that hit the headlines. Small and medium-sized businesses with fewer cyber security resources are particularly vulnerable. In fact, 74% of small businesses experienced a security breach in 2015, up from 60% the previous year[2].

Many organisations large and small, commercial and not-for-profit, now depend upon technology and social media to interact with partner organisations, customers, suppliers, donors or the general public. This exposes them to the risk of loss or damage to their technology assets as well as to the risk of crime, the potential cost of business interruption or loss of income, third party claims and perhaps most costly of all, reputational damage.

No surprise then that in our recent survey 84% of insurance brokers listed cyber/internet crime as the number one concern for themselves and their clients[3].

1 in 4 businesses
reported a cyber breach or attack last year

84% of brokers
list cyber/internet crime as their **No.1** concern

Ecclesiastical

2 So what can you do to protect your data and systems?

As technology and the way we interact with it continues to advance it may seem an impossible task. However, there are simple steps businesses should take:

1 Educate/train employees: Establish a written policy about privacy and cyber security, and make sure this is communicated to all employees. Educate employees on what types of information are sensitive or confidential and their responsibilities in protecting it. A large proportion of computer viruses attempt to gain access via email through malicious attachments and links. Make sure employees know what to look for and only open from trusted sources.

2 Secure computers: Require the use of strong passwords that must be changed on a regular basis. Keep security patches for your computers up-to-date. Use appropriate firewall, anti-virus and anti-spyware software and keep virus/spyware definitions up-to-date. Check your software provider's websites for any updates concerning vulnerabilities or associated patches. Train employees to never leave laptops or smartphones unattended.

3 Safeguard data: Ensure appropriate access controls are in place to protect and secure data. Use encryption to protect sensitive or confidential information stored on portable devices. Reduce your exposure by cutting back on the volume of data you collect and store only what is necessary.

4 Destroy before disposal: Don't just delete files or reformat hard drives as data can still be restored. Instead use software designed to permanently wipe the hard drive or storage device. Ensure you do this for all equipment not just computers; did you know many photocopiers scan documents and store a copy on the device's hard drive?

5 Update procedures: Make sure that your procedures comply with any applicable laws or legislation. Also, make sure that they align with any applicable industry required standards such as those that may be required by the Payment Card Industry (PCI) Data Security Standard.

This list is just a small sample and there is much more organisations can do.

3 Further help and information

An excellent source of more detailed information and help can be found at https://www.getsafeonline.org.

Get Safe Online is a public/private sector partnership supported by HM Government and leading organisations in internet security, finance and other sectors.

HM Government has also set up the Cyber Essentials scheme. This provides a set of controls which, when properly implemented, protect organisations from the most prevalent forms of threats coming from the Internet. The scheme also offers an Assurance Framework through which organisations can demonstrate to customers, investors and insurers they have taken these essential precautions.

4 Cyber insurance

Should the worst ever happen conventional policies may not cover many of the losses associated with cyber risks such as:

- Costs of dealing with data breaches
- Costs of dealing with cyber liability claims
- Business losses as a result of a cyber event.

“ *Having access to expert advice and support such as IT, legal, forensic and media relations when an incident occurs can help mitigate the financial impact of a loss or cyber event, as well as any reputational damage and disruption to your business.*” **states Tom Taylor, Ecclesiastical UKGI Casualty Account Director**

With this in mind and research showing that over 60% of organisations operating in some of our niche markets are also concerned about cyber-crime Ecclesiastical now offer an all-in-one computer, data and cyber risks policy. Aimed at small to medium sized organisations, cover can be tailored to meet individual needs and is available to any existing commercial customer or new commercial customer taking out an Ecclesiastical policy.

For more information get in touch with your usual Pound Gates contact.

Written by Tom Taylor, Ecclesiastical UKGI Casualty Account Director

This article is provided for information purposes and is general and educational in nature. You are free to choose whether or not to use it and it should not be considered a substitute for seeking professional help in specific circumstances. Accordingly, Ecclesiastical Insurance Office plc and its subsidiaries shall not be liable for any losses, damages, charges or expenses, whether direct, indirect, or consequential and howsoever arising, that you suffer or incur as a result of or in connection with your use or reliance on the information provided in this article except for those which cannot be excluded by law. You are free to choose whether or not to use the information provided in this article. You acknowledge that over time the information provided in this article may become out of date and may not constitute best market practice.

[1] Source: Cyber Essentials website.

[2] Source: Information security breaches survey 2015, Department for Business, Innovation & Skills, June 2015.

[3] Ecclesiastical research carried out by FWD Research, December 2016.

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