Risk Management: Cybercrime

Introduction

Cybercrime can affect us all and cyber attacks are becoming more common. A recent survey[1] highlighted that 43% of business overall had suffered a cyber security attack or breach of some sort in the last 12 months. Whilst large firms had suffered the most at 72%, 40% of micro firms had been affected; demonstrating that the software and techniques being used impacts on all types of businesses whether large or small.

Taking some simple steps is key to making sure you are protecting your firm from this growing risk.

Types of cybercrime

Cyberattack can come from a variety of sources: individuals, either inside or outside of a company; criminal gangs; or even state-sponsored.

The different types of cyberattack include:

- Social media exploitation – gathering information about an individual for gain.
- Hacking: trying to gain unauthorised access to a system. Unsecured Wi-Fi provides an opportunity for hackers, so sometimes working from home can be a risk.
- Ransomware: a type of malicious software designed to block access to a computer system until a sum of money is paid.
- Fake email to redirect money or information: changing bank details for the receipt of funds.
- Phishing: criminals obtaining information or passwords by deceiving staff into revealing them. This ranges from the simple, such as emailing people in a firm claiming to be from IT or HR, requesting their password details, through to the larger or more targeted approaches.
- Spear-phishing: where the attacker will look to social media for personal information to gain confidence and pose as a contact of that individual.
- Malware: harmful computer programs designed to record information and breach confidentiality. Often unobtrusive and aimed at gaining information, often delivered as email attachments.
- Denial of a service: overloading a server and causing downtime to inconvenience a firm.
- The insider: disgruntled and/or unfettered access by an employee.
- Trojan horse: a virus that hides on a system and remains undetected for long periods.

[1] DCMS Cyber Security Breaches Survey 2018

Good Practice to Adopt

General:

- Regular reviews of the effectiveness of online security, including password changes.
- Plan for worse case scenarios and add IT risks as a separate category in your Risk Register.
- Have a mobile working policy.
- Keep browsers, operating systems and anti-virus software fully updated;

Patching:

- Make sure you have correct licences.
- All software supported.
- Patches are up to date.

Secure configuration:

- Close accounts which are not used.
- Remove software you do not need.
- Change all default administration passwords to a strong password.
- Disable 'auto run' features.

Firewalls:

- Needed on office, device and home.
- Change default password to a strong one.
- Change every 60 days.
- Define what kinds of files are allowed through.
- Control and limit use of removable data devices e.g. USB sticks.

Access control:

- Do not work in 'Admin' account.
- Change admin password every 60 days.
- No users with the same username and password.
- Restrict staff access to only those files they need to protect against insider attacks.

Anti-malware:

- Up-to-date malware protection on all computers, smart phones and tablets.
- Set to update itself automatically and 'scan on access'.
- Regular scans of all files and website warnings.
- Make sure data is encrypted.
- Ensure unapproved devices are not connected to your system.

Bad Practice to Avoid

- Use of unsecured webmail or unapproved devices to transmit files.
- Guessable passwords and locally stored files.
- Inadequate training for staff on protecting data.
- Failure to keep systems up to date.
- No mobile working policies to protect system.
- Bring your own device systems where these are not vetted.
- Lack of access controls, so any staff can access all files.
- No backup in place.

Managing Cybersecurity

The Department for Business, Energy and Industrial Strategy (BEIS) recommends that entities see the managing of cybercrime as a senior management responsibility. Treating this risk as an IT-only issue can lead to important preventative measures being missed.

The laws that cover this risk include the:

- Data Protection Act 2018, General Data Protection Regulation, Companies Act 2006, Legal Services Act 2007 and Computer Misuse Act 1990.

As a member of CILEx and/or an entity, you need to meet the requirements of the CILEx Code of Conduct.

Clearly cybersecurity should be an ongoing process and not an event. When looking at steps you can take, the following may be the types of action that could help you minimise risk:

- Make sure you have systems in place to protect your firm if you fall victim to a scam.
- Keep information secure as the Information Commissioner's Office (ICO) is handing out large fines to firms losing information on unencrypted devices.
- Protect your data by encryption: see ICO advice.
- Include the following statement in your client care letter: 'We do not change our client account bank details, so if you do receive any advice purporting to come from the firm, please contact your named person in the firm immediately'.
- Ask your bank to contact you if any unusual transactions go through e.g. a faster payment when you never use this method.
- Have a regularly documented check of IT systems to demonstrate to your PII insurers the actions you take to mitigate risk.

Self-assessment and Training

The National Cyber Security Centre provides support and guidance to firms of all sizes.

The Cyber Essentials Scheme is a government-backed, industry supported scheme to help organisations protect themselves against common cyberattacks.

The Information Assurance for Small and Medium-sized Enterprises (IASME) standard was developed over several years during a Technology Strategy Board-funded project to create an achievable cybersecurity standard for small companies. We would suggest that firms complete the self-assessment questionnaire on the IASME website www.iasme.co.uk/index.php as a starting point for their cybersecurity needs.

There is an online training programme titled 'Cyber Security for Legal & Accountancy Professionals' developed in conjunction with HM Government, The Law Society and ICAEW. This is a free one-hour, four-module training programme, giving a basic overview to the problem.

Cloud Computing and Storage

Cloud computing is defined as access to computing resources, on demand, via a network.

We are all seeing the use of cloud computing coming more into our day-to-day lives (e.g. Amazon and Google), so it is no surprise that more law firms are turning to it as a means to store data.

Benefits

- Greater flexibility and scalability.
- Self-service provisioning, mobile working.
- Increased reliability and resilience in terms of business continuity and disaster recovery.

Risks

But those same benefits can also pose risks to a firm around:

- security
- accessibility
- confidentiality.

The issue with security of cloud storage is to get the certification of the supplier. The data in a cloud should be encrypted at rest and in transit, but won't be when read.

As has been raised in the press around Safe Harbour[2], the issue remains with where the data is stored. Often smaller cloud providers have it outside of the EU, but this can also affect other types of firms. The question then is what type of data you have and where is it.

Consider the following if you are looking to outsource your IT provision in this way:

- service
- internal actions
- security and confidentiality
- data protection
- access provisions
- business continuity.

Also, consider that by using cloud storage it often means that data tends to be accessed on a variety of devices, often outside of an office environment. So you need to think about whether this is secure. Checking that the correct protections are in place outside of the office is vital.

Resources

The Information Commissioner's Office Guide to Information Security includes a wide range of useful information for a firm.

Of particular help is the Cloud Computing Guidance for Organisations including a checklist (page 22) which could be used as a starting point to help ensure you consider all confidentiality, integrity, availability and legal considerations regarding personal data.

[2] Safe Harbour is the name of an agreement between the United States Department of Commerce and the European Union that regulated the way that U.S. companies could export and handle the personal data of European citizens.