THE LOOK OUT

PROFESSIONAL RISKS NEWS

LAW FIRM TARGETED BY CYBER CRIMINALS

In This Issue...

Jim Brindley discusses a recent data breach affecting a law firm. Through good training and risk prevention procedures the firm avoided suffering a loss of client money but were left managing, and responding to the consequences of a data breach.

HOW IT CAN HAPPEN - A REAL EXAMPLE

A law firm recently reported a cyber incident to us, which because of good due diligence from both the law firm and their clients, theft of client money was avoided. Although they were fortunate not to suffer any direct financial loss, the incident caused significant disruption, stress and cost to the law firm. The hack was detected after two clients had spotted unusual email content and activity, they both reported the suspicious emails to the firm within hours of each other.

The management agreed that two separate incidents reported so close to each other was no coincidence. After extensive investigation they discovered their IT systems had been compromised for a ten day period before it was detected. The hacker had gained access to their Outlook and installed a tool which allowed them to be “blind copied” into emails which partners and senior fee earners were sending and receiving.

Jim Brindley
Account Executive
TLO Risk Services Ltd

TRAINING AND CYBER AWARENESS

The firm had recently conducted a series of cyber awareness training sessions with management and staff alerting them to the dangers of cyber-crime. This was also relayed to their clients via emails, client engagement letters and verbal discussions during meetings and telephone conversations. This training and advice ultimately saved their client from suffering a financial loss.

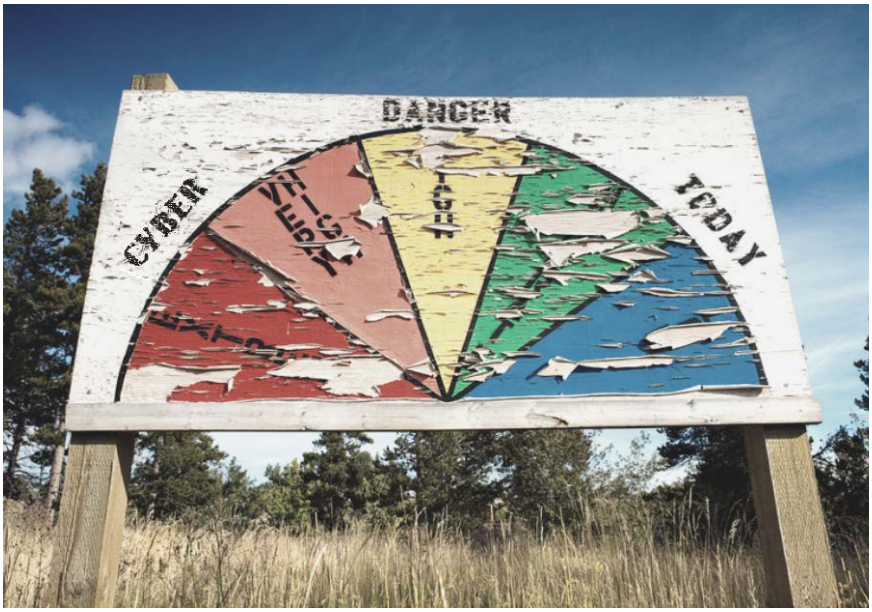
CONSEQUENCES OF A DATA BREACH

Unfortunately, whilst the law firm avoided a professional indemnity claim, the management had to respond to the consequences of the data breach, determining which confidential information had been compromised and which clients had suffered a data breach. The firm had sent and received close to a thousand emails and attachments during those ten days and it was crucial that each email and its attachments were checked.

The firm had a regulatory responsibly to report the data breach, both to the SRA and to the Information Commissioners Office (ICO), with full details of how the breach occurred, the type of data lost, and the potential impact to their customers. The firm also had to inform the clients affected by the data breach and explain what personal and confidential data had been compromised.

In addition to the cost of employing an IT company to investigate, repair and improve cyber security, the data breach had a serious impact on their business. Along with other financial costs resulting from the data breach, vital fee earning time was lost whilst partners tried to manage the situations.

EVER INCREASING CYBER RISK



The SRA recently published that in 2017, 157 cyber-crime related incidents had been reported to them, with losses of £10.7m in clients' money. Email modification accounted for 70% of these incidents. Reports of data breaches to the SRA increased in 2018 and it is likely to increase further, particularly with the new reporting requirements of GDPR.

It is essential that law firms treat cyber-crime and the protection of client data as one of their key risk exposures when assessing and reviewing their risk management plan. Firms need to adopt the necessary risk prevention methods to help avoid, detect and manage cyber-crime and data breaches. The recent statistics from the SRA on cyber incidents, suggest it is only a matter of time before security systems are attacked.

KEY PREVENTATIVE MEASURES

Training Staff - keep up to date with latest scams.

Alerting clients to the risks - Via email correspondence, client care and engagement letters and in meetings.

Email awareness - check senders email address and be wary of links and attachments.

Software - Only use up to date operating and virus software.

Encryption - Secure mobile devices and deploy dual authentication to vital management software.

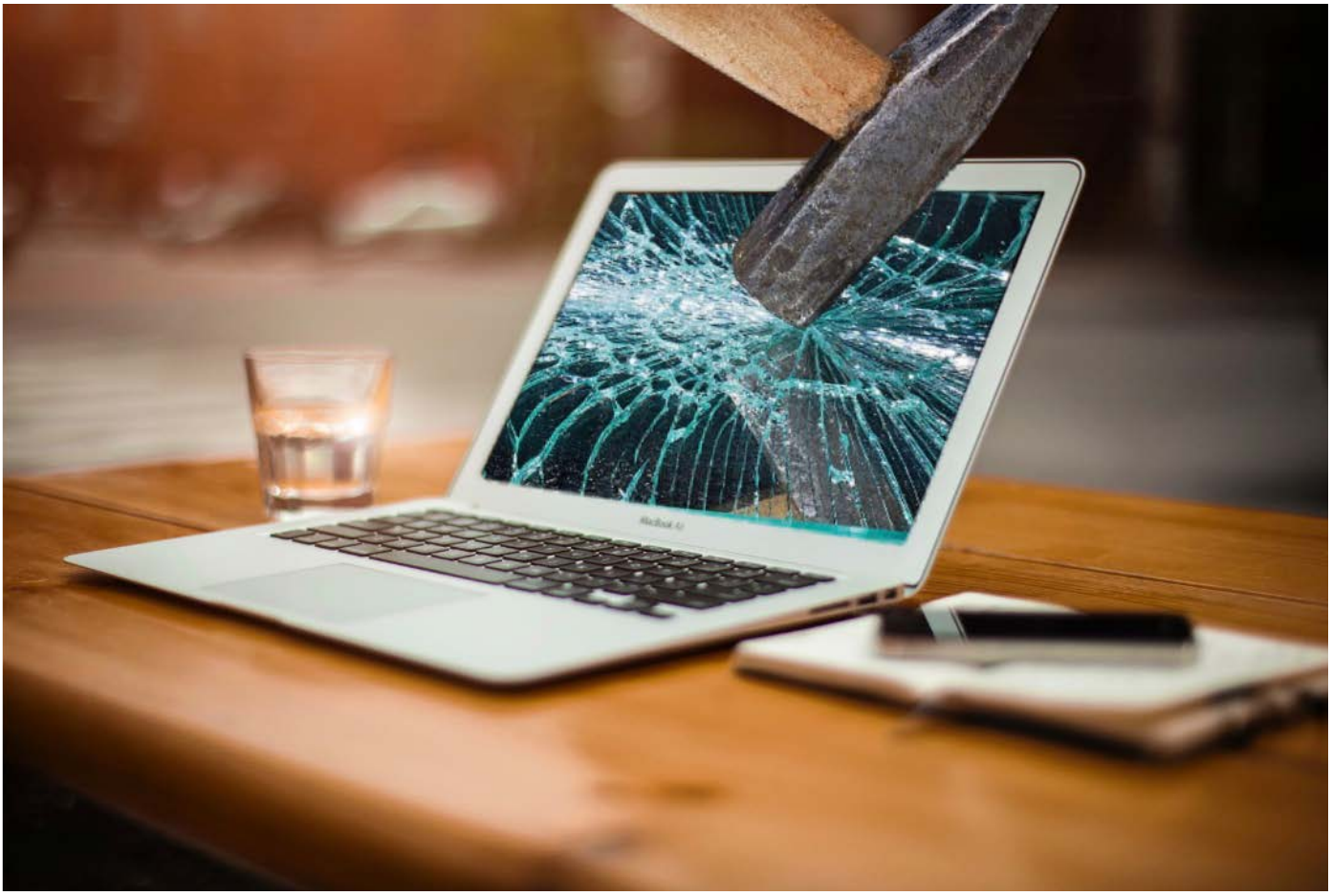
Passwords - Create strong passwords that use numbers and case sensitivity.

Impact following a Data Breach

- Interruption to your business service and function, i.e. loss of fee earning time
- Costs associated with potential payment of Ransomware
- Recovery and Investigation costs
- Replacement of any damaged hardware
- Public disclosure and reputational impact

Five steps to manage IT security

- System Hardening – reducing risk by eliminating superfluous programs and apps
- Patching – updating and fixing software after vulnerabilities are identified
- Logging - Tracking information on a computer to discover the if, when and how
- Vulnerability scanning – Identifying and fixing potential laws in IT security
- Monitoring – collecting and any analysis information to detect suspicious behaviour



Key steps to managing a Data Breach

- Assemble a management team to respond to a breach.
- Have a written data breach procedure and plan, and test such a plan.
- Are you able to evidence IT security and logging?
- A plan to manage any fall out of a breach with the public, press and regulator(s).

CYBER LIABILITY INSURANCE

Given the ever-increasing risk of cyber-attack to law firms and the resultant losses suffered, many practices are now turning to cyber liability insurance to protect them in the event of a cyber incident.

There are a vast array of cyber liability policies now available to law firms and the choice can be bewildering. Some policies offer very small elements of protection and advice following a cyber incident, these generally are of low cost. The more comprehensive cyber liability policies offer far greater protection and levels of indemnity but come at a higher cost.

When a firm is seeking cyber liability insurance, consideration should be given to how the insurance policy will respond following a breach, what elements of the breach will be insured, and will the indemnity provided be sufficient to protect the firm for their losses? The more comprehensive Cyber liability policies provide cover for costs associated with a cyber-attack, such as:

- Immediate Incident Response costs
- Hardware and rectification costs
- Crisis management and Communication costs
- Privacy breach costs
- Theft of money following a cyber crime (lower limits and restriction)
- Business Interruption and Denial of Service
- Ransom costs
- Regulatory fines (where insurable by law)

For more information on cyber training and cyber liability insurance please contact us.

TLO Risk Services Limited

Professional insurance The Personal Way

0121 212 9090

contactus@tlorisk.com

www.tlorisk.com

If you are interested in reviewing your insurance arrangements for 2019 and would like to find out how TLO Risk Services can assist your firm, or wish to discuss the above matters, please contact James Brindley on 0121 2121 9090 or james.brindley@tlorisk.com

TLO Risk Services (TLO) is a privately owned insurance broker. We specialise in helping firms that provide professional advisory services, from accountants and law firms, through to investment agents, surveyors and estate trustees. For more information visit www.tlorisk.com or speak to our experts on 0121 212 9090 or 020 7183 4925