LOCKTON
UNCOMMONLY INDEPENDENT

Cyber Protection - In response to enquiries from law firms regarding cyber insurance, we are pleased to provide an overview of the cover provided by a cyber insurance policy, as well as an indication of the costs (see page 3)

It is 6pm on a Friday, you are about to leave the office for the weekend when you discover that one of your employees has innocently clicked on a fraudulent link attached to an email - your practice has been the victim of a phishing attack.

Hundreds of emails have already been sent out from their email address to other recipients, both internal and external, compromising highly sensitive data regarding your practice and your clients.

What do you do? Who do you need to notify? How do you need to notify them? By when do you need to notify them? Are the emails still being sent out from the affected account?

Unfortunately the above-mentioned scenario is not fiction. Law firms of all size and profile make attractive targets for cyber criminals and are experiencing an increase in cyber-attacks. One major reason is your access to confidential and sensitive client information, typically of great value. By your very nature, law firms often handle highly sensitive private and business information.

What did the practice do?

Upon discovery of the attack, the practice contracted **IT consultants** to conduct an internal investigation. It was determined that the hacked account had access to huge amounts of confidential data including daily reconciliations, invoices, client names, addresses and bank account details.

The business engaged a law firm and a **public relations consultancy** to assist with the investigation. The advisors recommended that the business notify all the affected parties. Notifications were sent and procedures put in place to manage client calls, offer credit monitoring and generally manage the process both practically and from a reputational harm perspective.

Regulatory authorities were notified and further investigations commenced.

The business suffered a considerable financial outlay to cover these incident response services including **IT, legal, PR, and credit monitoring costs**. The cost of responding to the regulatory investigation alone was significant.

The business notified a claim under its **cyber insurance policy** and was reimbursed by its insurer for all costs over and above their chosen excess, up to their limit of liability.

Does your Professional Indemnity Insurance policy include cyber cover?

Whilst your SRA Minimum Terms and Conditions Professional Indemnity policy goes some way to protect funds that you are holding on behalf of your clients, the true impact of a cyber attack goes far beyond the monetary amount held in your client account.

In our experience, the most frequent cyber-related causes of loss are described as follows:

Phishing – the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details where the cyber criminal disguises themselves as a trustworthy entity in an electronic communication.

Ransomware – having hacked into a network a cyber criminal then denies the business access to their own network, demanding a ransom in exchange for a "decryption key". Ransom demands have increased over the last twelve months and criminals are now also removing or encrypting client data, as well as demanding the ransom.

Data Breach – when a cyber criminal successfully infiltrates a data source and extracts sensitive information. This can be done either physically, by accessing a computer or network to steal local files where the disclosure is often inadvertent, or by bypassing a network's security remotely.

Business Interruption / System Failure – where an organisation is forced to close for a period of time as a result of a cyber attack, or where certain systems can no longer function properly as a result of cyber crime.

Coverage	Description	Is this coverage provided within an SRA regulated firms Professional Indemnity Policy?
Breach Event Cost Reimbursement	Coverage for IT Forensic, Legal, PR and crisis management costs incurred in responding to a cyber incident.	No
Cyber Extortion Reimbursement	Coverage for costs in responding to a ransomware/ extortion incident, including any potential ransom paid (subject to legal and IT Forensic advice).	No
Digital Asset Loss Reimbursement	Coverage to replace or repair damaged or stolen digital assets/ data.	No
Business Interruption Loss Reimbursement	Coverage for the impact to net profit/ loss from a cyber incident, including extra expenses.	No
Breach Event Liability	Coverage for a third party claim resulting from a data breach or cyber security incident.	Yes
Regulatory Liability	Coverage for a regulatory investigation from a data breach or cyber security incident.	Yes