As we move into 2022 the online digitised way of working is set to continue, and this will mean that businesses continue to be vulnerable to the threat from attacks from cyber criminals seeking to take advantage of the online nature of our lives.

At our Annual Legal Services Risk Management Conference held in November 2021 for England and Wales solicitors, attendees voted that the biggest risk facing their businesses was cyber security risk. The Law Society of Northern Ireland (LSNI) frequently warn of the dangers of cyber crime facing law firms and their clients. The LSNI has recently updated its guidance on managing the risk from conveyancing scams in its Call, Check and Confirm Campaign. In addition, the LSNI has issued two new email and website banners and all members are encouraged by the LSNI to add these to their emails and websites.

Data Security Incidents
The latest data breach statistics published by the Information Commissioner’s Office (ICO) for the second quarter of 2021/2022 covering the period of 1 July 2021 to 30 September 2021 confirmed that the reported number of data security incidents had increased to 207 from the previous quarter of 198. It is worthy of note that the lockdown restrictions were fully lifted on 21 June 2021 and the statistics for the next quarter will be released after 31 January 2022.

The ICO categorises the data breaches into ‘non cyber security incidents’ and ‘cyber security incidents’.

- Non cyber security incidents: which occur as a result of human error and includes data being emailed, posted, or faxed to the wrong recipient, failure to redact and the loss or theft of paperwork or data left in an insecure location.
- Cyber security incidents: which occur as a result of a cyber attack and include ransomware, phishing, malware attacks and unauthorised access.

Most common non cyber security incidents reported
The most common causes of a non cyber security incident reported to the ICO covering the period 1 July 2021 to 30 September 2021 were as a result of data being emailed or posted to the incorrect recipient and equated to 46% of the total breaches reported. Breaches of this nature occur as a result of human error often due to individuals working under extreme pressure either from clients or tight timescales and arise owing to a lack of attention to detail.

The table below sets out the data showing the top two most common causes of non cyber security breaches reported for the legal sector to the ICO for Q1 of 2021/2022 compared to Q2 of 2021/2022:

<table>
<thead>
<tr>
<th></th>
<th>Q1: 1 April 2021 to 30 June 2021</th>
<th>Q2: 1 July 2021 to 30 September 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data emailed to incorrect recipient</td>
<td>49 out of 198</td>
<td>72 out of 207</td>
</tr>
<tr>
<td>Data posted/faxed to incorrect recipient</td>
<td>28 out of 198</td>
<td>24 out of 207</td>
</tr>
</tbody>
</table>

Most common cyber security incidents reported
The number of cyber security incidents reported to the ICO covering the period 1 July 2021 to 30 September 2021 were considerably lower equating to 27% of the total breaches reported by the legal sector to the ICO, with phishing attacks (56%) being the most common cause closely followed by ransomware attacks.

We are periodically still seeing really simplistic cyber frauds which can be easily prevented by following the guidance issued by the LSNI in the Call, Check, Confirm campaign and ensure that all staff are made aware of this guidance.

The table below sets out the data showing the top two most common causes of cyber security breaches during Q1 of 2021/2022 compared to Q2:

<table>
<thead>
<tr>
<th></th>
<th>Q1: 1 April 2021 to 30 June 2021</th>
<th>Q2: 1 July 2021 to 30 September 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing attacks</td>
<td>37 out of 198</td>
<td>31 out of 207</td>
</tr>
<tr>
<td>Ransomware attacks</td>
<td>15 out of 198</td>
<td>17 out of 207</td>
</tr>
</tbody>
</table>

Cyber crime continues to grow and evolve and features as a priority risk for the LSNI. The National Cyber Security Centre (NCSC) published its annual review on 17 November 2021 which identified ransomware as the most significant cyber threat facing all businesses in the UK, not just law firms. The report identified that during the first four months of 2021 the NCSC handled the same amount of ransomware incidents for the whole of 2020 and was “three times greater than in 2019”.

The NCSC is urging businesses to sign up for its early warning scheme, which is a free service from the NCSC designed to warn organisations about potential cyber attacks on their networks, as soon as possible. It has also issued guidance about how to create a ‘cyber incident response exercise’.

Businesses need to detect and respond quickly and effectively to cyber breaches as doing so reduces any financial, operational, and reputational damage such incidents can cause. Running cyber security incident exercises can also assist firms establish their resilience to a cyber attack. It allows them to respond in a safe environment, at the same time as creating a culture of education and awareness and identifying areas of vulnerability which may require further investment or resources.

To pay or not to pay the ransom?
If you do experience a ransomware attack, the guidance from the NCSC and law enforcement agencies is that they do not “encourage, endorse, nor condone the payment of ransom demands”. There is no guarantee that you will be able to access the data if you do pay the ransom as your systems may still be infected. Furthermore, you will be putting yourself at risk of being targeted again as criminal groups will know that you are willing to pay the ransom.

Conclusion
Cyber security risk should form part of a business’ operational resilience strategy which will help identify, understand and manage any cyber related vulnerabilities to the business. Taking the following actions can help you prepare your organisation from potential ransomware attacks:

- carry out regular backups
- prevent malware from being delivered and spreading to devices
- prevent malware from running on devices
- prepare for an incident

Operating a cyber secure culture throughout the law firm by ensuring everyone receives the necessary education and training, as well as following the guidance issued by the LSNLI will help protect against these vulnerabilities and minimise the risk of cyber security incidents from arising.

Whilst the Master Policy continues to provide an indemnity following an alleged loss of data or money from the client account, we strongly recommend that you protect your business with an independent cyber crime cover which includes insurance protection for the costs of managing a data breach including regulatory fines, loss of data or money from the business account and business interruption costs following a cyber security breach.

We would encourage you to obtain a quotation from Margaret McDonald, margaret.mcdonald@ablinsurance.co.uk, at ABL to help protect your business from this ever increasing threat.

Dr Joanne Cracknell
Associate Director, Global FINEX
T: +44 117 976 9376 M:+44 7584 683 012
Joanne.Cracknell@WillisTowersWatson.com

Simon Hunter
Loss Management Executive
ABL Risk Solutions

We would encourage you to obtain a quotation from Margaret McDonald, margaret.mcdonald@ablinsurance.co.uk, at ABL to help protect your business from this ever increasing threat.
About WTW

At WTW (NASDAQ: WTW), we provide data-driven, insight-led solutions in the areas of people, risk and capital. Leveraging the global view and local expertise of our colleagues serving 140 countries and markets, we help you sharpen your strategy, enhance organizational resilience, motivate your workforce and maximize performance. Working shoulder to shoulder with you, we uncover opportunities for sustainable success — and provide perspective that moves you. Learn more at wtwco.com.