

# Cyber Risk Landscape for Law firms

Law firms are considered particularly vulnerable to fraudulent attacks by criminals.



## Why?



Confidential information is firms' stock-in-trade



High value transactions



Client accounts holding large sums



Older technology more prone to attack



Smaller businesses – typically less sophisticated anti-fraud measures



173 law firms investigated by ICO in 2014



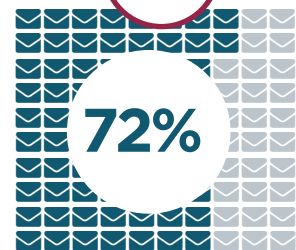
46% of all UK businesses identified at least 1 cyber attack in last year



73% of top 100 law firms hit by cyber attacks













Cyber incidents cost UK law firms £2.53m in the first six months of 2016



72% of reported breaches relate to fraudulent email



Staff in 58 out of 100 law firms clicked links in phishing emails (NCC/RSA simulated phishing exercise 2017)

Example Risk	PII Policy	Fidelity Policy	Cyber Policy	Crime Policy
 Data breach from external cyber attack	✓ <sup>1</sup>	✗	✓	✗ <sup>2</sup>
 Data breach from staff error	✓ <sup>1</sup>	✗	✓ <sup>3</sup>	✗
 Theft from firm's client account from telephone scam	✓	✗	✗ <sup>4</sup>	✓
 Client paid into wrong account following invoice hijacking (email interception)	✓ <sup>5</sup>	✗	✗ <sup>6</sup>	✗ <sup>7</sup>
 Theft of firm's money by third party	✗	✓ <sup>13</sup>	✓ <sup>8</sup>	✓
 Theft of firms money by member of staff	✗	✓	✗	✓
 Internet Service Provider failure	✓ <sup>1</sup>	✗	✓ <sup>9</sup>	✗
 Reputational and financial loss from computer systems failure from malicious attack	✗	✓ <sup>13</sup>	✓ <sup>10</sup>	✗
 Third party supplier data breach	✓ <sup>1</sup>	✗	✗ <sup>11</sup>	✗
 Regulatory defence and civil awards fines and penalties as a result of security breach	✗	✗	✓	✗
 Breach response costs	✗	✗ <sup>13</sup>	✓	✗ <sup>2</sup>
 Ransom request following computer systems attack	✗	✗	✓	✓ <sup>12</sup>
 Counterfeit cheques or bank notes	✗	✓ <sup>13</sup>	✗	✓
 Employee credit card fraud	✗	✓ <sup>13</sup>	✗	✓
 Costs incurred for fraudulent use of telephone line	✗	✓ <sup>13</sup>	✗	✓
 Utilities use fraud	✗	✓ <sup>13</sup>	✗	✓

1. Only covers client/3rd party claims arising from professional services covered by PII | 2. Data reinstatement costs only | 3. Certain cyber policies will also provide cover for general data breach. Check policy details | 4. Telephone fraud is not covered by all policies, but some may offer by optional extension | 5. If firm is proven liable for the loss, and a civil liability is incurred under the PII | 6. If firm's IT systems are confirmed as the source of the interception/breach, may be covered. | 7. The firm has not suffered a loss | 8. Limited and narrow (& only for specific cyber-crime incidents linked to a cyber breach) | 9. Business interruption due to loss of service covered but exclusions apply where due to infrastructure failure | 10. Cover to limit reputational damage from a cyber event | 11. Vicarious liability cover available | 12. Depends on policy | 13. Optional extension

**Policy covers vary widely and this guide to insurance covers is for general information purposes only and should not be relied on as a statement of cover applying under a specific policy. Contact Lockton for guidance regarding your particular cover requirements, and the terms & conditions applicable to any policies which you may have.**