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

173 law firms investigated by ICO in 2014

46%

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

73% of top 100 law firms hit by cyber attacks

£2.53m losses

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

72%

72% of reported breaches relate to fraudulent email

58%

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

LOCKTON®

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

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