PDA Legal

Regarding: **Cybercrime and law firms: Facts of the matter**

Presented at: **Defending Law Firms from Cyber Attack Conference (organised by Salford University) at Etihad Stadium, Manchester**

Presented by: Bob Partridge, PDA Legal

Presented on: 10 May 2016

Contact us:
E: enquiries@pdalimited.com
T: +44 (0) 1372 879343

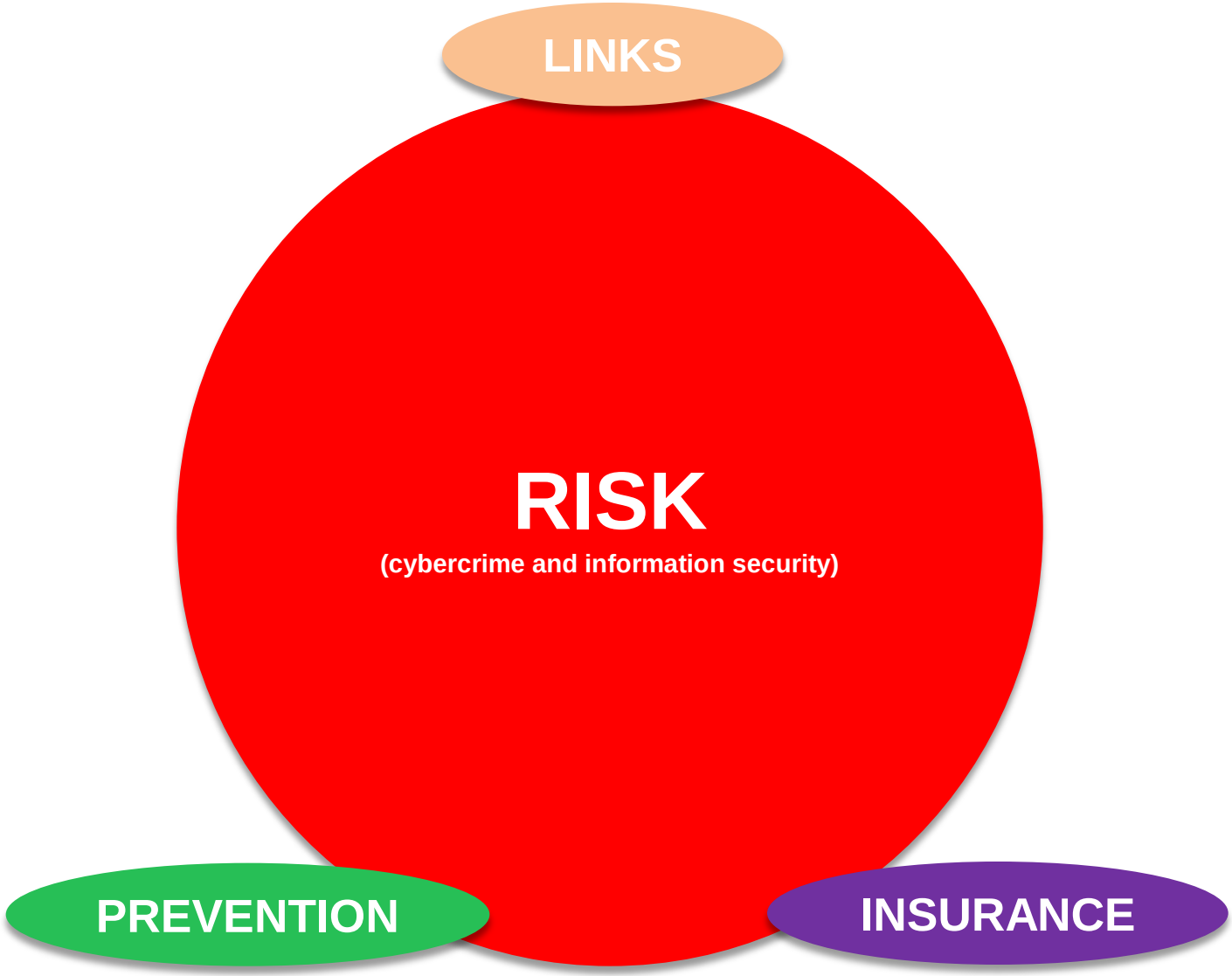
Cybercrime and law firms: Who are we and what do we do?

- Compliance Plans & Risk Registers
- Lexcel, CQS, ISO (inc. 27001) and SQM consultancy & assessment
- Authoring office and quality manuals
- Embedding quality and compliance processes
- Risk management (including AML and cybercrime)
- File review service and analysis
- Remedial action following audits (including SRA)
- Training in risk, compliance and management

www.pda-legal.com

Cybercrime and law firms: Never too big

Cybercrime and law firms: Overview



Cybercrime and law firms: The many faces of cybercrime

Cybercrime and law firms: You have been warned

- The legal sector is particularly vulnerable to cybercrime as organised gangs are attracted by the large sums of money being moved to and from firms (Law Society)
- Law firms are under a persistent threat from criminals seeking inside information (Law Society)
- Recent press stories identify that law firms are the ‘soft underbelly’ to their client’s data (Law Society)
- Cybercriminals consider law firms to be a “backdoor” to the valuable data of their corporate clients (FBI)
- If you openly demonstrate weaknesses in your approach to cyber security by failing to do the basics, you will experience some form of cyber attack (GCHQ)

Cybercrime and law firms: Figuring it out

1	first tier risk to National Security over next 5 years (NSRA – Nov 2015)
10	age of Finnish boy who found flaw in Facebook
12	age of youngest buyer of virus in 2015
17	average age of 'cyber attackers' (NCA)
49-200	days to detect a security breach
63%	of data breaches come from internal sources, either lack of control, errors, or fraud
80%	of online attacks preventable if firms followed simple guidance on the use of information systems (GCHQ)
>100%	increase in recorded crimes when online fraud and cybercrime taken into account for first time 2014/15
250k	new 'malwares' appear each day worldwide

October 2014 to April 2016

- **£85M** stolen from law firms
- **150** successful ‘raids’ on law firms
- **1500** ‘attempts’ on law firms (QBE)
- **349** reports of bogus law firms or individuals in 2012
- **726** in 2015 (+105%) (SRA)
- **19** security breach reports to ICO from legal organisations Oct-Dec 2015 (ICO)
- **48** ‘elite’ law firms hacked in M&A information (Gazette – April 2016)

Cybercrime and law firms: Risk Categories

- **Reputational (Strategic)**
  - "Don't trust that lot with your information."
  - "Local solicitors lose £thousands through hacking."
- **Operational**
  - Disruption to services e.g. DDoS attacks
  - Mistakes leading to attacks and losses
- **Financial**
  - How much does it cost the firm? (£4-60k +)
- **Regulatory**
  - Lots!
- **Insurance**
  - Will they still want us, and if so, what will they require of us?

Cybercrime and law firms: Responsibility – IoD Perspective

It is important that directors and owners realise they do not need to be cyber experts to understand the risk but do have policies and processes to deal with any situation...

(IoD)

DATA PROTECTION ACT 1998

Schedule 1 – Part 1

'The Eight Principles'

PRINCIPLE 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

SRA Principles 2011

7 Comply with your legal and regulatory obligations ….

8 Run your business …….. in accordance with proper governance and sound financial and risk management principles

10 Protect client money and assets

Cybercrime and law firms: Legislative Responsibility - 2

O(4.1) Keep the affairs of clients confidential

O(7.2) Effective systems and controls comply with Principles, rules and outcomes

O(7.3) Identify, monitor and manage risks to compliance ….. and take steps to address issues identified

O(7.4) You maintain systems and controls for monitoring … risks to money and assets entrusted to you by clients and others, and you take steps to address issues identified

O(7.5) Comply with ….. AML and data protection legislation

O(7.6) Train individuals to maintain a level of competence

Cybercrime and law firms: SRA accounts rules

7.1 Any breach of the rules must be remedied promptly upon discovery.

7.2 The duty to remedy breaches rests … also on all the principals in the firm. This duty extends to replacing missing client money from the principals' own resources … whether or not a claim is subsequently made on the firm's insurance or the Compensation Fund

SRA WARNING

If you identify that money is missing, you have a duty to take steps to ensure it is replaced, in full, immediately, from your own resources or a loan if necessary regardless of insurance claims. If not, intervention highly likely.

COMMUNICATIONS – ELECTRONIC SECURITY GROUP (GCHQ)

- Establish Information Risk Management Regime
- Maintain configuration security
- Ensure network security
- Manage user privileges
- Education and awareness
- Incident management procedures and processes
- Malware prevention
- Monitor IT systems and usage
- Control removable media
- Home and mobile working strategy

Cybercrime and law firms: Cyber essentials overview

1. Boundary firewalls and internet gateways

2. Secure configuration

3. Access control

4. Malware protection

5. Patch management

From October 2014, Cyber Essentials became mandatory for all suppliers of central Government contracts which involve handling personal information and providing certain ICT products and services.

Cybercrime and law firms: Lexcel requirements

- Register of relevant information assets of the practice and clients
- Protection and security of the information assets
- Retention and disposal of information
- Firewalls
- Secure configuration of network devices
- Management of user accounts
- Register of all software used by the practice (whitelisting)
- Training for personnel on information security
- Planned updating and monitoring of software

Cybercrime and law firms: The weakest links

- Mobile devices and social media applications are IT security's weakest links
  (Cyber Defence Report 2015)

- **SOCIAL ENGINEERING** - psychological manipulation of people into performing actions or divulging confidential information - a type of confidence trick for the purpose of information gathering, fraud, or system access

Cybercrime and law firms: Ponemon end user report 2016

- Negligent employees not following security polices, and devices they use in the workplace are greatest source of endpoint risk
- Malware targets mobile endpoints
- Laptops and smartphones are biggest endpoint security threat - insecure mobile devices in workplace increased significantly
- Employees' use of mobile devices and commercial cloud applications increase endpoint risk significantly
- More personal devices connected to the network (BYOD)
- Endpoint security is becoming a more important priority

INSURANCE ACT 2015

The insured must make to the insurer a fair presentation of the risk, containing:

- Every material circumstance which the insured knows or ought to know, or
- Giving the insurer sufficient information to put it on notice that it needs to make further enquiries re those material circumstances
- And in a reasonably clear and accessible manner and
- In which every material representation as to a matter of fact is substantially correct, and every material representation as to a matter of expectation or belief is made in good faith

Cybercrime and law firms: Cyber insurance questions

- What does the insurer define as cybercrime?
- What exclusions, e.g. perpetrator using firm's equipment?
- Any stipulations about the firm's protection systems?
- Any stipulations about maintaining security systems, e.g. software updates, anti-virus and patches?
- Homeworking?
- Terrorism?
- Retrospective cover?

Cybercrime and law firms: One minute risk assessment

- What is likelihood of occurrence?
- What would be the impact?
- On our Risk Register?
- If so, how high? - If not, why not?
- Is it in our BCP? - If not, why not?
- Who is responsible if something happens?
- Are we ready?
- Outsourcing!!!???
- External website developers & hosts!!!???

Cybercrime and law firms: Make an impact with an E-PACT

Endpoints and end-users

Patches (including updates), policies (and strict enforcement)

Access controls

Cyber Essentials

Training

Cybercrime and law firms: Contact for slides

This presentation is free to download at:

- www.pda-legal.com/cyber-crime
- www.pda-legal.com