Failure of senior management to deal with this threat is irresponsible and likely to destroy the credibility and viability of a law firm with its clients and generally in the market place

Until a few months ago I like many probably thought that cyber threats were an IT issue and IT managers were charged with making sure it doesn't happen. I am afraid the buck stops at the top.

In reality it is much bigger than that because according to the PwC Law Firms survey in October, 41% of firms that suffered a breach pinpointed that it was caused internally by their own staff.

I attended a Cyber Crime Conference with a difference in Liverpool on 1st November organised by north-west law firm http://www.jacksoncanter.co.uk/ aimed at clients and potential clients. It was a major eye opener for the audience.

The Jackson Canter Group is a fast-growing and acquisitive business with six offices across the North West. Brian Cullen joined the business from outside the sector and was appointed as CEO following their acquisition of Lees Solicitors. They are enhancing their employment team and commercial offerings.

I also don't think it will be long either for commercial clients of firms checking that the commercial teams include a Cyber Crime expert to be proactive in advice on policy, post event communication and mitigation of the consequences

Already in the commercial world more and more companies will only deal with suppliers who have Cyber Essential Plus as a minimum need

Every firm these days must have a Cyber Policy recognising that security is a partnership between technology and people. To include training, awareness, staff empathy and perpetual re-assessment

One speaker said that *"The scariest statistic to come out in 2015 for me was that it takes 229 days on average between infiltration and detection, i.e. a criminal (hacker) on average spends 229 days in IT systems undetected, the amount of information that could be stolen and damage that can be caused in such a time is unmeasurable"*

Cyber Events – and unfortunately they are probably inevitable need a clear response and policy – too late for this methodology to be considered post event

- Containment
- Evaluation
- Ramification consideration and deployment of **mitigation plans – legal responsibilities including formal reporting, PR,**
- Remedial action – stopping it happen again

The event was opened by Joanna Kingston Davies COO of Jackson Canter and the speakers included Nat West Bank, the northwest police Titan team, MLS Advantage members

http://www.matrix247.com/ and https://www.xyonecybersecurity.co.uk/ , http://www.nasstar.com/ and Grant Thornton – a great line up.

Matrix and Nasstar are suppliers to Jackson Canter

I have followed some of them up post event.

charlie.edwards@xyonecybersecurity.co.uk says *"My advice to firms is to stop worrying and start mitigating your risk. Yes, you have received a barrage of malicious threats. Some will get past your technical controls you may or may not have in place. In the PwC Law Firms survey in October, 41% of firms that suffered a breach pinpointed that it was caused internally by their own staff. So you need vigilance across the firm, where there is immediate reporting of any malicious activity. Firms need a clear Business Continuity Plan and a strong Cyber Security Policy that is enforced and implemented across the business with training for all employees. Otherwise you will always run the risk of being another statistic. As the threats become more and more targeted, now is not the time for a generic response. Get your training right, using the latest threat intelligence, to create a resilient and vigilant workforce and mitigate your risk."*

nigel.redwood@nasstar.com says *"GCHQ believe that 80% of cybercrime is preventable through better process, policy and education for employees. That switches the emphasis from the IT team to the business owner - people, process and policy is not the IT team's domain alone. Our clients outsource their IT to us, however that does not mean they can stick their head in the sand and say IT security is Nasstar's responsibility and become complacent as a result. We have a dedicated Control and Compliance Manager who works with our Problem Management Team and Ethical Hacker daily to assess, reassess as react to the changing landscape. Who would have thought a "Ethical Hacker" would be a job. However unfortunately that is a reflection of the dangerous times we operate our economy in! To conclude, my message is that cyber security is a partnership and no longer the domain of the IT team alone!.*

Stephen Pritchard - ste@matrix247.com asks *"How many risks are currently being taken and are they HIGH, MEDIUM or a LOW risk to your firm?" Calculate this by simply drawing a few headings: Potential LOSS in money taken directly, CLIENT DATA RECORDS stolen and shared or exposed, FINES on your firm, company value loss due to REPUTATIONAL DAMAGE, loss of TRUST etc. The list goes on but a great start. Then ask, "What CAN be done to mitigate risk?"*

Steve also identified that Juniper 2015 research across 200 firms sights 74% of UK firms THINK they are safe, yet 55% of large firms and 45% of SME's were attacked last year and 29% of these resulted in a data breach. 87% of firms have a 'DR / Security' plan which is good, but ONLY 27% actually conduct a penetration test to check security works and ONLY 26% do regular training with staff around security procedures.

Steve also says *"March 2015 government figures now show the average cost of a data breach is £65,000 to SME's. So taking the above statistics, it is roughly a 1 in 8 chance your firm will both be attacked AND have a data breach* ***in the next year****. Therefore investing a minimum of £8k ANNUALLY in Cyber Security Awareness training, policies and tightening exposure in HIGH RISK areas is a wise pro-active approach for those responsible, which is ultimately the board, not the I.T. department. Juniper research tells us 65% of firms believe simply putting security policies in place will make them secure. I would challenge this.*

Working with security experts in each field, Matrix247 is currently offering a complimentary ***'Vulnerability Assessment Report (VAR)*** *security@matrix247.com"*
Similar services are offered by Nasstar and I also referred in the August issue to the service from http://www.d2na.com/

More Added Value for MLS Members

Apart from the good advice above I am pleased to advise that there will be additional members to the suppliers group starting in January and full details will be in the next edition of the Messenger

Bill Kirby is a director of Professional Choice Consultancy offering advice to firms on business issues from strategy, planning, business development, the effective use of IT applications and IT hosting for compliance, business continuity and DR. He can be contacted at billkirby@professionalchoiceconsultancy.com