This Month

- **Essential Availability to Clients**
- **Poor call handling can cost a fortune**
- **Essential Security – Breaches can cost a fortune and credibility**
- **More Added Value from MLS Advantage**
    - **Specialist legal security validation**

Essential Availability to clients

Every year for the last three years around the Christmas period I have had a bit of a rant at law firms closing their doors to potentially vulnerable – mainly private clients from a couple of days pre-Christmas until 2nd January.

I know everyone wants to have a break but people still die, families' feud and people even lose their jobs. This is becoming more and more unacceptable to clients and potential clients and as were are now law firm businesses client satisfaction is on our list of responsibilities.

Some firms are already using specialist outsourced support from Moneypenny https://www.moneypenny.com/uk/ – telephone answering and call prioritising for communication and Document Direct https://www.documentdirect.co.uk/ for the production of documents. Not just for the Christmas period but for out of hours and volume demands – good return on investment.

Something that helps prove the point was a small firm that on its website provided some telephone numbers for calls during the period. They received about 50 messages during the time and following response gained multiple Probate, Family and Employment business

Call Handling Opportunity

Whilst on the topic of availability to clients. How and when people within our businesses who are trying to contact via the telephone brings up management information from telephone systems about how long they ring, how quickly answered, length of calls – all of which can have an impact on in bound enquiry conversions and client retention. Very costly if not done correctly. Where do your teams sit on the enquiry conversion scale which ranges from 22% to 70%.

During January, Claire Smith, head of business development at Moneypenny did a social medial blog

https://www.moneypenny.com/uk/resources/blog/the-6-crimes-of-modern-day-call-handling-for-law-firms/

This highlighted the 6 crimes being committed by many law firms with call handling

- Endless ringing and slow response times
    - 69% will not leave a voicemail
- Disinterested and robotic receptionists
    - Early empathy is critical
- Assumptions about call handling
    - Process should be part of induction
    - Shared diaries, organisation charts
- Hit and miss service
    - Guidelines for consistency
- Unreturned calls – lost goodwill and lost business
- Answering machines turned on too early

- 10% of calls outside of hours
- Answering for half an hour before work and half an hour post would be a start

Essential Security – Breaches can cost a fortune and credibility

Interesting responses from the New Year's **Revolution** proposals from last month's piece http://www.professionalchoiceconsultancy.com/articles/January2020.pdf which included some great common sense actions and some difference from the 2019 edition. One major feature that I emphasised again in April 2019. http://www.professionalchoiceconsultancy.com/articles/April_2019.pdf was the absolute need for the management of the firm to take accountability for security – not to abdicate, not to show inertia and not to assume. Security and compliance risk is a major and worsening issue. We cannot just leave it to our in house IT teams or third party managed service providers or even hosting companies. All three groups need the necessary qualifications verifying. "Following the principles" is just not good enough.

These considerations are also not just for IT but also telecoms and datacomms – we have also consider the dangers around the use of mobile phones and laptops. October 2018 article.

The prevention of third party access to our client's data for private and commercial clients is absolutely essential. Plus increasingly commercial clients will be expecting validation if you are on their supply chain.

From a business development point of view the firm being able to up front declare their genuine compliance is a bonus.

Frightening statistics

86% of breached businesses thought security in place

52% of people "in the cloud" have been breached or attacked

49% were breached through own devices

47% of breaches were holding personal data

43% of all businesses attacked

37% of breaches led to loss of finance and data

Our technology needs validation, regular testing, on-going review and regular knowledge discussions with in house IT or managed service/hosted suppliers

Our staff need training, awareness and competency testing – vigilance and vulnerabilities must be discovered. This should also sit alongside a comprehensive social media policy and practice.

Firms need policies and procedure to ensure realistic governance dependent on their work-types and IT and telecoms infrastructure

Third party and independent expertise is an essential consideration and if breaches are prevented it should not be regarded as a cost but a return on investment.

Added Value

Manchester Law Society has in January made a significant addition to its Advantage group with the signing up for collaboration of https://mitigogroup.com/ a specialist, nationally operational business

operating from Cheshire. Principle liaison with partner Damian Wasey damianwasey@mitigogroup.com. They also offer a cyberdoctor@mitigogroup.com service and bespoke programmes for each firm.

Conversations with them gave some **interesting response to fundamental questions**

- Q: As a law firm, undertaking a mix of commercial and private client work, will we really be a target for cyber criminals? Why would they possibly want to focus on us?
    - *A: Most cyberattacks are not specifically targeting your firm. They are high-volume indiscriminate attacks that hit every business connected to the internet. These automated attacks are seeking out weaknesses in your business technology, applications, the vulnerabilities in poorly trained staff and any inadequate policies or procedures. If you have vulnerabilities, you will be hit and may then become a target for more focused attacks.*
- Q: We have an IT company that look after our computers and systems. Are we right to assume they are covering cybersecurity?
    - *A: I am afraid the answer is almost always no, for at least 2 reasons. Firstly, the effectiveness of the attacks has grown significantly as cybercriminals become increasingly sophisticated. Secondly, the growth in cloud-based software, mobile phone usage and remote working has dramatically increased the attack 'surface' available to cyber fraudsters. This means cybersecurity is now a specialism and not 'general practice'.*
    - *Ask yourself the following question. Who is undertaking the security risk assessments required by law? Do they know your legal, professional and regulatory requirements as regards technical security? Are they pressure testing your technology defences? Who is providing your cyber awareness training? Who has advised on the appropriate policies and procedures? There will be areas within your business where you need more specialist cyber advice viewed through the eyes of a cyber security professional.*
- Q: Our IT company performs regular system back-ups which comforts us when we hear about ransomware attacks; however, we've heard from a friend in another firm who has paid a ransom when their back-ups didn't work? How can this happen?
    - *A: This is the scary thing about ransomware. Most people believe that their IT back-up system is set up correctly, but usually it is not. Nor has it been tested against a ransomware scenario. Ransomware may come for example, via an email from an infected 3rd party, or by a device with a vulnerability connecting to your network. Ransomware encrypts (locks-up) every file in your business and historic back-ups can be lost (overwritten) if they have not been set up correctly.*

      It's important to understand how your back-ups are set up. You should sit down with your back-up provider and get them to talk you through exactly how it would work in a ransomware scenario and get them to prove to you that encryption won't lock or overwrite all your backed-up copies.

      More importantly, put the proper defensive protection in place (technology, training and governance) so that your firm won't suffer the damaging effects of a ransomware attack.

      Ransomware is becoming increasingly common. Please don't wait for an attack to test the resilience of your back-up, rehearse it now!

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