KPMG

Professional Practice Solutions

You've built your business on building trust

Insight Dinner – Tuesday 15 May 2018 – Post-event summary

The realities of Cyber Threats, Security and Appropriate Responses

KPMG's Professional Practice Solutions team were again proud to host another successful Insight Dinner on Tuesday 15 May in KPMG's client meeting and engagement space at Number Twenty Grosvenor Street, London.

The event was hosted by Paul Spicer, Head of Professional Practice Solutions; Martin Tyley, Head of Cyber, National Markets and guest speaker Paul Edwards, Chief Financial and Operating Officer, DLA Piper who shared their thoughts, ideas and insights into cyber threats, security and appropriate responses and what can happen when it goes wrong.

Below, Martin shares his high level summary of topics discussed and themes to consider along with Paul's five top tips firms should consider if they want to prevent a cyber attack.

Please do get in touch if you would like to explore anything you feel would be beneficial to you and/or your firm.

From Martin Tyley

There has always been loss of data but now we are seeing a changing nature of the threat and uncertainty as technology and threat actors evolve and increase in sophistication and capacity.

Martin introduced us to a wide array of threats we should all be aware of and should be recognising as significant risks to the sector. Highlights included:

Data loss and leakage

Data losses can arise through external actions but are more likely self-inflicted through human error, misadventure or procedural failure. In 2018 we still hear stories of unencrypted laptops or paper documents being left on trains, these are not difficult challenges to prevent. Data leaks can also arise through malware infection or concerted cyber-attack. Of course data losses can result in reputational damage, and with GDPR now being enforced, financial penalties or even preventing that organisation from being able to operate.

The good news is, most data loss scenarios can be mitigated by reviewing existing working practices, addressing bad habits, reinforcing existing security and data protection controls, and forward planning (recovery and damage limitation strategies).

Malware and ransomware

Today, malware is commoditised – "ransomware as a service" and toolkits allow cyber criminals to reuse old code to achieve new objectives. Unpatched flaws or bugs in network protocols, software interfaces and hardware simplify the attack and expedite the malware spread; some malware is crafted to attack specific legacy systems through its built-in backdoors. It can take only one response by one employee, to a malware popup or email, to trigger malicious code that massively disrupts business operations, exposes data to theft or damage, and damages reputations.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The good news is, many infections can be thwarted by combining security tools (such as inbound email content scanning and antivirus/antimalware) with end user education and ongoing communication with vendors and suppliers. There are also numerous free online resources which report on current and emerging threats on a daily basis. Vendors and service providers can provide guidance on how to ensure their own systems can be kept secure.

Email: The gateway to theft and fraud

In the early days, this was mostly amateurish stuff like spam emails offering a finder's fee to anyone who could help move an inheritance out of a country – people had to be naïve or greedy (or both) to fall for it. Today, modern email-driven fraud is carefully crafted, without obvious spelling errors and can be difficult to spot. Friday Fraud was a simple example of these tactics in practice. Between 2013 and 2015, cyber criminals used online tactics (e.g. phishing emails) to steal £85 million from British law firms by targeting the conveyancing transactions which are routinely processed on Fridays; the theft amounts for each attack ranged from £65,000 to £1.9 million.

The good news is, because this level of attack is so dependent on exploiting routines or procedures to effect a redirect, it is possible to spot and thwart these attacks – email security systems can spot tell-tale signs like spoofed email addresses or flag messages with risk based on the appearance of key words. Also, procedures can be tightened to provide sanity checks where context or lexical analysis is insufficient, for example if any external email instruction to redirect a payment is automatically challenged and independently verified irrespective of its sender, then most fraudulent requests will be intercepted before any damage is done.

Spear-phishing, whaling and CEO fraud

Here are two eye opening statistics: According to an alert in May 2016 by the FBI, 17,642 organisations from the US and 79 other countries had fallen victim to whaling and CEO fraud between October 2013 and February 2016, with combined losses exceeding $2.3 billion. The Email Laundry (a threat research company) simulated whaling attacks to see how effective their approaches could be – and achieved a 90% success rate.

The reason these attacks are so difficult to counter are because they are multi-staged, intricately planned affairs which are tailored to the victim organisation. By impersonating president or C level they make it difficult for lower grade members of staff to raise suspicions. They may research, and emulate, established business patterns and practices, hierarchies, patterns of behaviour, and even the format and language of internal email communications, for weeks or months. By the time they issue a spoofed instruction to transfer funds or data, it will appear completely above board to all but the most attentive, suspicious observer. Some fraudsters will go as far as making a call before and during an ongoing transaction to further convince the unwitting actors that it is a bona fide request.

Then Martin provided insight into how tier one banks perceive the legal sector following a KPMG cyber security review of the supplier environment.

During 2017 KPMG reviewed 40 legal firms, including 40% of the firms present at the Insight Dinner on 15 May, and we identified 726 findings and a higher number of findings per organisation when compared to any other industry sector. Poor controls in relation to Risk Management, Access Control and Monitoring accounted for around 60% of the total number raised. Many reasons of those findings had common causes:

1. The nature of the business determines the way data is generated and accessed:
    - — Data in the legal sector is extremely mobile and transient, for example handwritten notes being prepared during face to face contact with clients.
    - — Much of it may be contained in working documents and hard copies – for example in case notes and contracts.
    - — Independent and ring-fenced teams develop their own ways of working with, or storing, sensitive client data.
    - — Unstructured data can be held in disparate ways: in email chains, on USB drives, in hardcopies, scanned document management systems, in shared folders and sites, or in the cloud.
2. The way IT and related security may be perceived as a support structure or overhead, instead of being seen as a business enabler:

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

- Partners' ownership of responsibilities is orientated around serving client need rather than developing and enforcing standards and controls.
- Senior Management teams may be unaware of how technology advancements and evolving IT threats create new business risks.

Martin was keen to ensure the audience left with some KPMG take-aways to help them consider how their own organisations were postured.

1. Be aware of your internal and external obligations (including regulatory and legal obligations, such as GDPR)
   - Educate your staff as to the risks and their obligations.
   - Examine and address any working practices that conflict with these requirements.
2. Revise your internal policies and procedures in respect of compliance and risk
   - Access to client data – Intellectual Property, Sensitive Personal Information and Business Critical Information.
   - Access to business data – HR, financial, CRM and case management systems.
   - Transport and storage of working data – use encrypted drives and storage devices, and secure paper documents in transit.
   - Disaster recovery and damage limitation strategies in place (in case the worst does happen).
3. Review and monitor
   - Consider the need for a dedicated data protection role.
   - Perform regular checks on existing technological safeguards e.g. firewalls, antivirus and email content security.
   - Ensure your security officers know how to keep abreast of any significant new threats.
4. Test all your defences on a regular basis
   - Never assume that existing policies, procedures, technical safeguards and user education is enough– complacency is the biggest risk.

Martin concluded by noting the need for a strategy and sustained and evolving cyber capability development if an organisation intends to better secure itself and stay on top of risk. A good starting point is to invest time in reviewing business continuity and IT disaster recovery capabilities and testing them with involvement from across the organisation, not only IT.

And from Paul Edwards

We were very fortunate to have Paul Edwards, Chief Financial and Operating Officer at DLA Piper, in attendance as a guest speaker who outlined DLA Piper's own experience of the cyber incident that they fell victim to in June 2017. This session provided a real life experience of the issues that need to be dealt with and built on many of the points made by Martin in his earlier address. In conclusion, Paul recommended five points all senior management at professional practices should be considering to ensure they are prepared:

1. An open network helps the bad guys too
2. Trusting third party software should not be an assumption
3. Plans are worthless, but planning is everything
4. External advisors are critical
5. The IT team needs air cover

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Our events in the legal sector

This dinner is one in a series aimed to bring you thought-provoking insight into real-time topical issues and challenges that you're likely to be grappling with. If you're receiving this email you're already on our invite list for this event. We will also be running events specifically aimed at CEOs, CFOs; CIOs; HRDs so if you'd like your colleagues to be invited, do get in touch.

If there are any subjects you'd like to see covered at a future event, please let us know.

KPMG in the legal sector

We have brought together some of the best professionals from across our firm with relevant insight and experience in the legal sector. We strive to co-ordinate and deliver a collaborative approach to your business whatever challenges you encounter – looking to the future and the bigger picture with you. Our service offering document gives an overview of our specialists. Please get in touch if you would like to speak to our specialists.

kpmg.com/uk/professionalservices

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in the United Kingdom. The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Designed by CREATE | CRT093978 | 180611