Professional Practice Solutions

Detail makes a masterpiece

Professional services firms are increasingly being seen as easy targets for cyber-attacks and the frequency of these attacks is increasing: most recently one of the 'big four' accounting firms was hit by what it describes as a "cyber incident".

As these attacks increase in sophistication, organisations need to understand their security risks and put in place the right level of controls to help mitigate the threat.

In this email, we share three recent articles that we have written focussing on how organisations can evaluate their level of risk and how to better prepare themselves against this type of attack.

Five stages of cyber security maturity

I thought you might be interested in a report we have launched entitled 'The cyber security journey – from denial to opportunity'. The recent spate of cyber-attacks is keeping cyber risk at the top of the business agenda and as such investments are being made. Our new KPMG/BT report looks at each of the stages businesses go through to gain true leadership in the management of their security risks.

The report warns businesses against falling into dangerous traps as they deal with the complexity of securing a digital enterprise. These include being stuck in 'denial' and 'worry' phases at one end of the spectrum and 'false confidence' and 'hard lessons' at the other end.

Download the report.

IT Internal Audit: Multiplying risks amid scarce resources

Technology risk is pervasive and continually changing. It is a critical time for IT professionals and internal auditors of IT, who must build plans to provide assessments of, and insights into, the most important technology risks and how to mitigate them. IT Internal Audit (ITIA) must keep abreast, and wherever possible anticipate, fast-moving developments in technology. In particular, ITIA must plan, deliver and, when necessary, flex its audit plan in such a way that it responds to these changes in the most appropriate, efficient and effective manner. And it must do so within the budgetary constraints imposed by the organisation, facing competition (both internal and external) for resources.

To find out how ITIA is responding to these challenges, KPMG's global network of firms surveyed ITIA representatives of 250 organisations, both large and small, that are operating in a wide range of industries around the world.

Key findings:

- ITIA is currently focusing on core operations risks, such as unauthorised access or changes to critical business applications. But respondents anticipate a significant shift in attention in 2018 toward emerging risks, such as robotics and the Internet of Things (IoT). ITIA will need to build holistic assurance over these new risks across the organisation to cover key components such as cyber defences around data, applications and infrastructure.

- ITIA faces the task of obtaining the appropriate skilled and qualified resources to assess fast-changing risks and to increase the use of tools and technologies such as data analytic technology and automated workflow tools.
- Forty-three percent of respondents say their ITIA budgets are likely to be stable and 8 percent say they may fall between 2017 and 2018. Thirty-eight percent say they may rise. If budgets are not, at least, maintained, there is a danger that ITIA will not be able to perform its job of providing adequate assurance over all the different kinds of risks, not just those affecting core operations.
- The chief area of concern is whether ITIA has the skills required to provide assurance over the most important technological risks to the organisation. ITIA respondents say they face talent shortages in many risk areas they are auditing. The biggest resource gaps are in cyber security, followed by D&A, and privacy.
- One area of need is the ability to use D&A for various purposes in ITIA. Only a quarter of respondents say they use analytics for continuous auditing, monitoring and assurance techniques; the remainder use it in an ad hoc way.
- Assurance is typically delivered through direct internal and external audits, rather than by leveraging the assurance work done by the organisation's independent assurance specialists. The implication is that many organisations lack an integrated approach to assurance.

Insuring your business against evolving cyber threats

I thought you might be interested in a report we have launched entitled 'Closing the gap – Insuring your business against cyber threats'. In this report, KPMG in the UK joins with DAC Beachcroft and Lloyd's of London to provide a unique cross-sector assessment of the various cyber threats facing companies today. It also details the total financial impact of data breaches and analyses the costs associated with recent high-profile cyber-attacks.

Download the report.

KPMG member firms have over 3,000 cyber security professionals. KPMG can give you the support and guidance in mitigating the unavoidable risks outlined in the report that come with operating in an increasingly digital world.

Our view is that these type of attacks will continue to increase and organisations need to act now to put in place the relevant controls and safeguards to mitigate the risk to their clients and their business.

If you have any questions or comments, please feel free to contact me and I would be happy to arrange a meeting at your convenience to discuss any of the above.

Paul Spicer
Head of Professional Practice Solutions
KPMG

kpmg.com/uk

Produced by Create Graphics I Document number: | CRT087937 | 171024