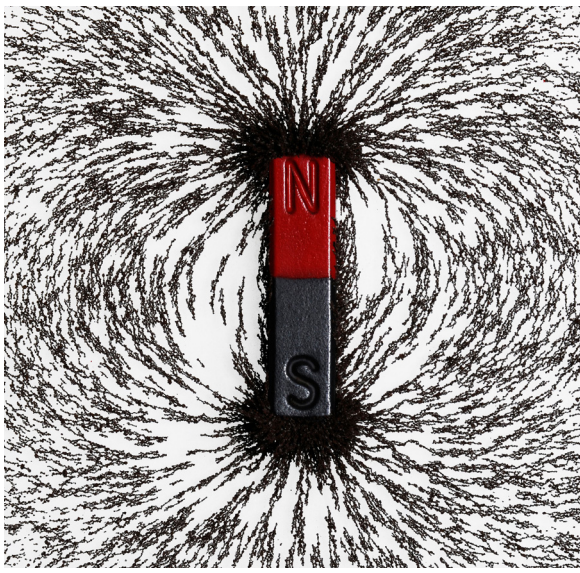
Deloitte.

Risk Angles

Five questions on the evolution of cyber security



An interview with Mike Maddison, Deloitte UK partner and leader of cyber security consulting for Europe, the Middle East and Africa and closer look by Sid Maharaj, Technology Risk Partner, Deloitte Australia, and Tommy Viljoen, National Lead Partner Security, Deloitte Australia.

While cyber security used to be considered an issue primarily for the IT team, these days it is an agenda item for the entire C-Suite. What's changed? It's not just the frequency of media reports on cyber security breaches — if anything, these are merely symptomatic of a larger shift underway. Cyber crime is fuelled by increasingly sophisticated technologies along with relatively new trends in mobility usage, social media, and rapidly expanding connectivity — all in the hands of more organized online criminal networks. In this environment, an intelligent and evolutionary approach to cyber security is key to staying ahead of cyber criminals — and the competition.

In this issue of Risk Angles, Mike Maddison tackles five questions on cyber security frequently voiced by clients. Then, Sid Maharaj and Tommy Viljoen take a closer look at how big data can be used for intelligent security.

Question	Mike's take
What shift in cyber security is currently happening?	The shift has to do with the fact that today's cyber security efforts require guarding against a broader range of challenges. New and emerging technologies, trends in mobile usage, social media, well-funded and organized foes, round-the-clock attacks, and more, have pushed this issue to the forefront. Cyber risks are becoming more complex in nature and can have a direct impact on everything from share prices and revenue streams to regulatory compliance and brand reputation. Traditional information security practices can address a large number of risks, but true cyber security demands capabilities — people, processes and technology — be built on intelligent security rather than just information security.
How real are cyber threats for companies not typically targeted by cyber criminals?	The threat is very real. All highly-connected and digitally reliant organizations are a target. Banks, for example, are an obvious target for cyber criminals. But what about everyone else? Our experience shows that cyber criminals seek out the easy targets, wherever they are. Consider retail. Retail companies can house massive volumes of customer data, and as a result are seeing an uptick in fraud problems. Companies caught up in geopolitical struggles are also prime targets, whether for criminals, political actors, or activists. Think you're not an obvious target? Think again.
How should we respond to the threats of today's digital environment?	The right response depends heavily on industry, on market conditions, social trends, you name it. But you can quickly reach a more informed answer to the question of resource requirements by taking inventory. What assets does your organization have that would be valuable to others? What are the threats to those assets? Which groups or individuals stand to benefit from compromising those assets? For many clients, this is an exercise they've never undertaken, focusing instead on information assets. But in a world in which highly diverse, highly organized external groups seek to do harm, information assets are only part of the story.

Question	Mike's take
Is there value from taking an intelligent approach to cyber crime?	Absolutely. Facing up to the challenge of managing cyber risks can help companies take advantage of new technologies, processes, channels, and alliances. These efforts also lead to supply chain optimization and the ability to operate with confidence in current and new markets.
Can we predict cyber crime rather than simply respond to it?	While there is no way to predict every possible threat, of course, many companies are developing capabilities that result in real time threat analysis, detection, and prevention. Build an understanding of your information assets and what risks could impact them. Then, determine what data you have, or need, in order to develop actionable intelligence. Of course, you cannot preempt every threat, but having a smart response plan can play a big role in minimizing the impact.

A closer look: Big data for intelligent security

By Sid Maharaj and Tommy Viljoen

In the context of cyber security, it is tempting to think of big data primarily as a treasure trove of valuable information — information that must be vigorously guarded from cyber criminals. Of course, that is true. With massive volumes of data at their fingertips, a breach in security that gives cyber criminals access to such data could be catastrophic.

But there is another, equally important way to understand big data in this context: As a potentially powerful weapon in the fight against cyber crime. The use of predictive and real-time analytics for security and the ability to source information on rogue web sites, rogue activity, threat actors and threat events as well as visualization and threat chaining, are allowing companies to explore possible future attacks — helping them rethink risk and identify opportunity to stay ahead of cyber crime before it reaches the present.

Could your organization be putting big data to use as part of its cyber security strategy? The short answer: If you have access to big data on your users, systems, third parties or customers, the answer is almost certainly "yes." The real question should be how quickly can you start putting it to work?

For more information, please contact:

Mike Maddison
Partner
Deloitte UK
+44 20 7303 0017
mmaddison@deloitte.co.uk

Sid Maharaj
Partner
Deloitte Australia
+61 2 6263 7160
sidmaharaj@deloitte.com.au

Tommy Viljoen
Partner
Deloitte Australia
+61 2 9322 7713
tfviljoen@deloitte.com.au

Henry Ristuccia
Partner, Deloitte & Touche LLP
Global Leader
Governance, Risk and Compliance
Deloitte Touche Tohmatsu Limited
+1 212 436 4244
hristuccia@deloitte.com

Vikram Bhat
Principal
Deloitte & Touche LLP
+1 973 602 4270
vbhat@deloitte.com