KPMG
cutting through complexity

Lifting the lid on cyber risk.

Stan Gallo, a Director in KPMG Forensic and former Queensland Detective, has seen all manner of nefarious activities from both sides. At KPMG's Risk Leader's Roundtable, he shared five key insights into emerging threats of the evolving cyber risk environment and how to manage them.

Think like a cyber criminal

Cyber criminals are increasingly focused on information. They will be eyeing what data you have, what it's worth and how they can extract it. It's important to understand that mentality so you can better protect against potential attacks. It's equally important that everyone takes ownership of cyber security. Cyber security is not an IT problem. Whilst IT is a key component of any solution, it is a strategic risk issue that should be considered from the board level down. It has to be tackled with a 'Tone from the Top' approach.

Collaboration is key

Government and business need to collaborate to find a solution to cyber risk. Neither Government nor business alone have the capacity to deal with the threat adequately – particularly given the multi-jurisdictional nature of many variants of cyber attacks. Government organisations have the legislative strength and legal reach, whilst business has the funding, flexibility and global reach. A collaboration is in everyone's best interests. We need to enhance models for sharing intelligence.

Data loss has wide ranging effects

External criminals are targeting transactional data, but authentication, personal and commercially sensitive data are on the agenda. Internally, intellectual property theft is the key challenge, but can be expensive and difficult to pursue.

Under newly proposed legislation, data loss incidents may come with compulsory reporting implications and, of course, potentially severe reputational consequences. The multitude of recent intense media coverage of high profile data breaches is a case in point.

What are the top cyber risks business are facing?

Connectivity is on the rise It has been reported that around 75 percent of Australians own a smart phone and 47 percent a tablet[1]. The Internet of Things means our daily lives are unbelievably connected, so we're much more vulnerable. Consider the connectivity in your home, office, car, etc. For example, Smart TVs can monitor and record voice through in-built cameras and microphones.

Data breaches beyond retail In 2014 retail breaches abounded; in 2015 it will be all about breaches in the health sector, where security is perceived as being weaker and personal information records are of higher value. Regulators are now on board with privacy legislation and there is discussion in parliament about mandatory disclosure for data breaches.

Unparalleled media sharing via social media, cloud and through remote access means a lot of confidential information is now more vulnerable. Available data is actively mined by marketing organisations, companies themselves – and by criminals. Social engineering is alive and well.

Internal data theft There's a big focus on external threats, but don't ignore the insider threat. We know data is valuable but organisations don't always understand how much value they hold and where it is stored. If you want to understand your organisational risk, you need to first know what the crown jewels are and where they are stored. Often we find it is not where you think they are.

[1]http://www.adnews.com.au/adnews/answering-marketers-prayers-smartphone-penetration-hits-75

What are the key specific threats to be aware of?

Ransomware is moving to the next level: Cyber criminals are likely to mature in their approach to Ransomware, moving from attacking single machines to entire networks, the cloud and mobile devices. Proactive detection is getting increasingly more difficult.

Email breaches are becoming more sophisticated: Businesses are not the only ones leveraging technology to enhance old processes. These days fake emails that aim to defraud use correct logos, company information and specific individual related information. There has been a recent spate of well-tailored emails targeting finance people, enticing them to make payments on false invoices and approvals. A tried and true fraud method that leverages current technological capability.

Denial of service attacks are evolving: These denial of service (DoS) attacks send millions of commands to deny access to, or collapse servers. Now we're seeing them used to hide other breaches that occur whilst the focus is on responding to the attack, and valuable data is being stolen.

Simplicity in attack: Information regarding cyber-attack methodology and applications to assist are becoming more commonplace. SQL injection attacks can be accomplished using tools with user friendly interfaces with little in the way of programming skills required. It was reported that one Australian organisation had 1 million passwords extracted using this method.

Social engineering: New ways to commit old offences. The integration of technology assists everyone – not just the good guys. People are inherently trusting by nature and the baddies will take advantage of this. On the back of the Snowden leaks, some companies had their sites targeted as it was alleged that they provided user information to the NSA. It is thought that in one instance the domain name servers (DNS) were changed via social engineering to redirect traffic.

Cyber-crime does not respect geographical boundaries and, as early adopters of technology, Australian businesses are at risk. The ubiquitous nature of technology means that now, more than ever, a practical but robust, defense strategy needs to be implemented. It should be driven from the most senior levels of the organisation, ingrained as part of the organisational culture and be supported by the information technology infrastructure.

Contact us

Stan Gallo
Director
KPMG Forensic
+61 414 507 742
sgallo@kpmg.com.au

kpmg.com.au

April 2015. VIC N12862ADV