KPMG
cutting through complexity

Advisory

Protecting your business from the malicious insider

Security breaches, theft of intellectual property and the loss of financial information and other critical-value data have reached epidemic proportions. The financial cost to governments, corporations and individuals amounts to hundreds of billions of dollars each year compounded by the effects of damage to brand and reputation.

"Many of these losses can be attributed to insiders," said Keith Lowry, guest speaker at a recent KPMG Breakfast Briefing in Sydney. "Insiders can cause more damage than external cyber-attacks but many organisations still have poor strategies in place to prevent serious and costly insider breaches. Executive teams need a new approach to these risks because the old security models and IT systems which focus on outside cyber-attacks provide very little defence against an inside job."

A unique insight

Lowry has a unique insight into insider threats. When he was Chief of Staff to the Under Secretary for Human Intelligence, Counterintelligence and Security, Lowry was closely involved in the Army investigation of Chelsea Manning. He led the Edward Snowden counterintelligence damage assessment team in partnership with the US Director of National Intelligence. He was also responsible for developing and publishing the US National Counterintelligence Strategy.

When the US Food and Drug Administration (FDA) needed someone to develop its first counter intelligence and insider threat program, Lowry was the obvious choice.

"The FDA employs about 20,000 employees and contractors and control literally trillions of dollars' worth of intellectual property (IP)," he said. "As part of its approval process, it must have access to the IP associated with just about every product that Americans eat or drink, medications they take and medical devices they use. Not surprisingly, there are many people who would like to steal that IP, so my team developed a program and a process to mitigate the risks associated with internal breaches of security."

Now, as Vice President, Business Threat, Intelligence and Analysis of Australian technology company Nuix, Lowry is using the same approach to help companies and government agencies around the world to identify and manage internal threats.

A huge problem

According to Europol, the total global impact of cybercrime has risen to about $3 trillion, which makes it more profitable than the worldwide trade in marijuana, cocaine and heroin combined. About a third of all cybercrime incidents and security breaches are reported as being generated internally, but Lowry believes the actual figure is much higher.

"Some organisations don't know when an insider breach has occurred, or they may be reluctant to report certain incidents," he said. "And, as we still don't have a standard definition of 'insider threat', many people aren't sure what it means. Nuix's definition doesn't differentiate between inside and outside because we believe that, regardless of their methods, once somebody has penetrated an organisation they're an insider."

Some insiders use their position to advance a personal, political or nation-state agenda. Others steal or leak high-value data such as credit card numbers and personal information to commit fraud or sell on the black market. And any organisation that holds valuable intellectual property is vulnerable to industrial espionage – the theft of trade secrets.

Lowry used a number of recent examples to illustrate the scale of the problem and also the skill and ingenuity of the perpetrators.

"The personnel records of everyone who works for, or has ever worked for, the US government have been taken, and it seems that someone had been inside the system for over a year collecting that data," he said. "Approximately $6 billion dollars has been laundered through Deutsche Bank over the last couple of years. Russian agent Anna Chapman and her compatriots were state-sponsored insiders tasked with gaining trust and access to the US financial and government sectors in order to steal information. And then there were the six Chinese nationals who took jobs in Silicon Valley microelectronics companies in order to steal trade secrets. They used this information to manufacture copycat parts for mobile phones which they sold to military and commercial customers in their own country."

Many criminals have devised ways to exploit the gap between when a breach occurs and when it is discovered. In banking and finance, this is about 90 days. In other sectors it's usually between 180 and 200 days, though it can be longer.

"Interpol has reported that organised crime groups are recruiting individuals, training them and then sending them to work in organisations, with the sole aim of getting to know the security systems, policies and procedures," Lowry said. "Once criminals understand them well enough to get around them, they embezzle a lump sum and leave the job so that, by the time their crime is detected, it's impossible to follow their trail. One Russian group recently amassed about a billion dollars by having different people steal up to $10 million each."

A more proactive approach

Clearly, organisations can't afford to be purely reactive.

"Perimeter defences are designed to keep outsiders from getting into an organisation's systems while incident response teams and security operation centres are mostly reactive – their work only starts after the breach," said Lowry. "These defensive measures are almost powerless against wrong-doers who are already inside the network, often with legitimate credentials that give them access to critical-value data."

Organisations can become more proactive by broadening the scope of cybersecurity activities to include policies and processes that limit opportunities for insider breaches and make it easier to identify anyone who poses a threat. However, Lowry conceded that detecting and deterring insider threats can present a significant challenge and that many organisations avoid the issues because they simply don't know where to start.

"In the proactive approach recommended by Nuix and KPMG, organisations focus efforts on very specific and definable targets – namely their critical-value data – and the very limited ways in which an insider could access, gather and infiltrate that data from their network," said Lowry.

They can then develop a proactive insider threat mitigation program that combines three key elements.

- **Understand and focus** – identify where critical-value data is located, who has access to it and how they can gain access.
- **Protect and disrupt** – use intelligence and analysis to identify insiders who pose a threat within the systems and networks.
- **Deter and detect** – have accurate and up-to-date cybersecurity and IT policies, training and forensic tools in place.

"A successful program is not just a piece of software," Lowry said. "It requires executive leadership and advocacy, clear policy and guidance, and workforce education and training. And it must bring together stakeholders from across the organisation including human resources, administration, legal, physical security, information security and information technology. With these elements in place, an organisation can address insider threats before they become messy and costly public problems."

Reporting a breach

In Australia, cybercrime is costing local organisations and individuals around $1 billion a year. In 2014 a data breach typically cost a large Australian company about $4.3 million, a rise of 33 percent over the last three years. There have been few public examples of insider breaches but that doesn't mean Australian organisations are less vulnerable. Disclosing a data breach is mandatory in the US but here reporting a breach is still voluntary so it's likely that many incidents go unreported.

"I think it's only a matter of time until mandatory disclosure is introduced but the issue is still a sensitive one," says Stan Gallo, Director of KPMG Forensic. "There are serious risks to consider – for example, a centralised repository of information on successful criminal behaviour could be a target in itself. But there are also strong arguments in its favour. For example, if victims shared information about a breach it could help other organisations to protect themselves against a similar attack. At the moment, the banks are very good at sharing information without exposing confidential material so perhaps that model could be replicated on a broader scale."

> **"I think it's only a matter of time until mandatory disclosure is introduced but the issue is still a sensitive one."**
>
> **Stan Gallo**

Gallo has seen boards and senior management becoming much more aware of insider threats, though people deeper in the organisation often believe that much more could be done.

"It could be that the message is getting lost somewhere in middle management," he says.

"This is a cultural problem and it needs to be treated as such," adds Gary Gill, a Partner and leader of KPMG's Forensic practice. "As with any other aspect of culture, the tone must be set at the top and pushed right through the organisation. Employees at every level need to know the nature of the risks and understand that everyone has a role to play in maintaining security. That means knowing how to respond if they suspect that someone is acting illegally – it's vital they feel able to speak up."

> **"Employees at every level need to know the nature of the risks and understand that everyone has a role to play in maintaining security."**
>
> **Gary Gill**

kpmg.com.au

Contact us

Gary Gill
Partner
Advisory
+61 2 9335 7312
ggill@kpmg.com.au

Stan Gallo
Director
Advisory
+61 7 3233 3209
sgallo@kpmg.com.au

August 2015. VICN13216ADV.