CLIENT:	**ISACA**
PUBLICATION:	**AFR.com.au**
PUBLISHED:	**15 October 2013**
CIRCULATION:	**Online**

http://www.afr.com/p/technology/business_understanding_of_cyber_57sx365889CqsImhnmzO2M

Business understanding of cyber attacks a decade out of date

PUBLISHED: 9 HOURS 2 MINUTES AGO | UPDATE: 1 HOUR 48 MINUTES AGO

The motives behind APTs are as old as civilisation itself, but the methods being used are right up-to-date. **Photo: Frank Maiorana**

CHRISTOPHER JOYE

Current approaches to defending the most sophisticated and destructive form of cyber-attacks targeted at businesses are likely to fail because they are focusing on attacks conceived a decade ago, according to a new study published by a global IT body, the Information Systems Audit and Control Association.

The author of the ISACA study, David Lacey, said so-called advanced persistent threats (APTs), where hackers gain access to networks and lie low to collect confidential information, are worryingly on the rise.

“The motives behind APTs are as old as civilisation itself: espionage, sabotage, crime, terrorism, warfare and protest,” Mr Lacey said. “What’s not old is the ramp-up in attacks and their mounting sophistication.”

Mr Lacey was previously head of IT security for the UK Foreign & Commonwealth Office, the Royal Mail Group, and the Royal Dutch/Shell Group.

In September *The Australian Financial Review* revealed that the number of serious cyber-attacks on Australian government assets had jumped 39 per cent in 2013 and was 205 per cent higher than 2011 levels, according to the Defence Signals Directorate.

Last week a “sophisticated” Russian-speaking hacking crew penetrated Adobe’s networks and stole details on 2.9 million credit cards and “source code for numerous Adobe products”, a company spokesman said.

Mr Lacey said ISACA’s message to company boards was that conventional protective measures, like firewalls and anti-malware systems, were “not up to the challenge of defeating today’s APTs”.

CURRENT SECURITY NOT ENOUGH

“Companies need to understand that their current security will not protect them from the new threats we are seeing emerge,” he says.

“These are long-term, professional threats from organised crime, foreign intelligence services, military agencies, hacktivists and potentially terrorists who are able to walk through the average - business’s defences, bury deep inside, and stealthily steal and exploit critical information.”

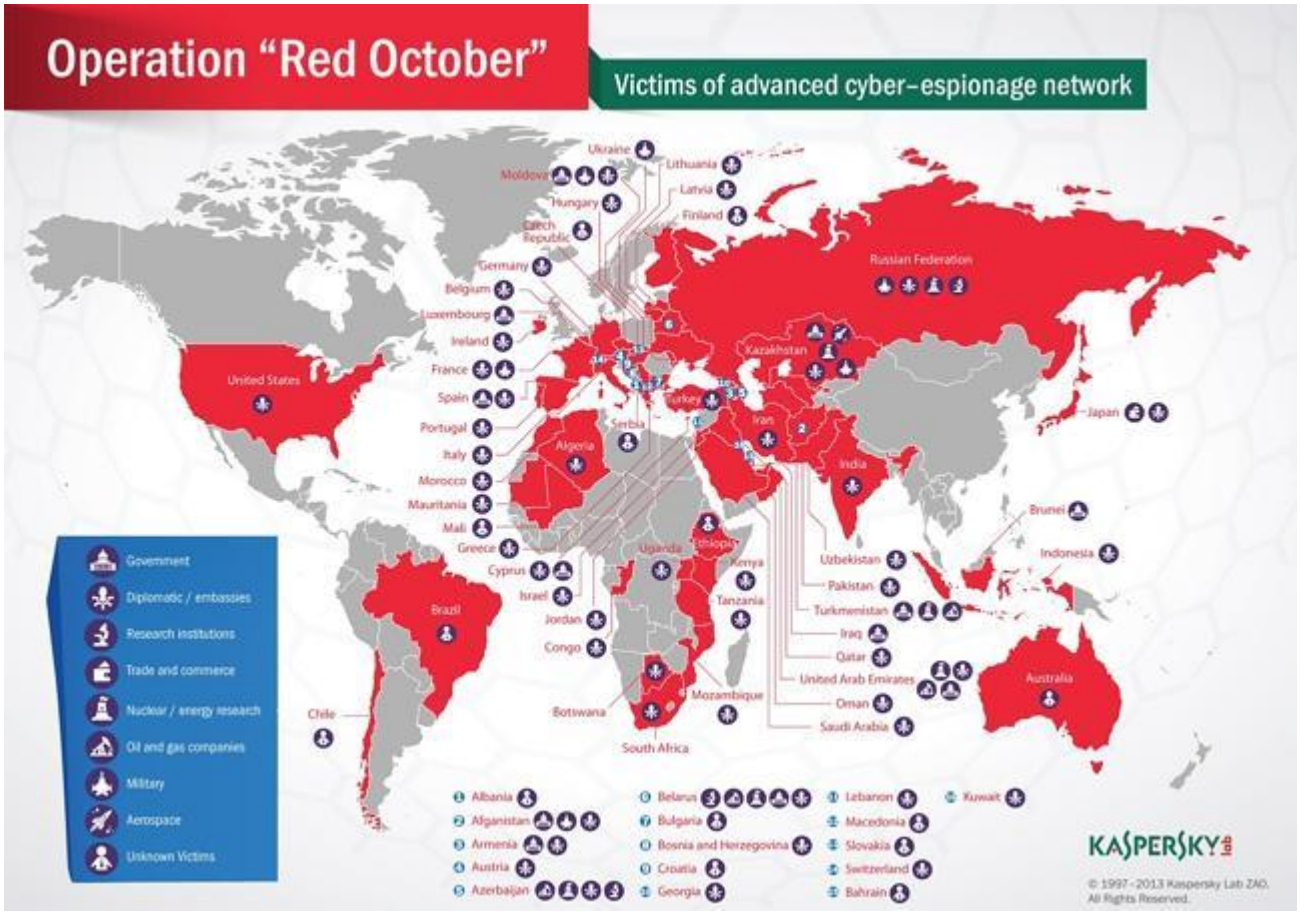
In a survey of IT security professionals last year, ISACA found that one in five worked in an organisation that had been the subject of an APT attack and 63 per cent said they believed it was only a matter of time before their enterprise was targeted.

ISACA is a not-for-profit certification body for IT professionals and has more than 100,000 members in 180 countries.

Mr Lacey said that just as “armies were designed to fight the last war” the same was true in the digital security domain where threats were constantly evolving.

“Most APTs are not discovered for three to five years – so the ones we are hearing about today were developed five years ago,” he said.

The *Financial Review* revealed last month that the Department of Prime Minister and Cabinet, the Australian Federal Police, and three of the four major banks had all hired the US firm, FireEye, to help them combat APT threats.



America's National Institute of Standards and Technology defines an APT as an attack that: "(i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives."

Mr Lacey believes the private sector continues to chronically underestimate online risks and under-invest in mitigants against them. "Businesses are happy to take risks and keep their fingers crossed. If they do spend any money, it will normally be on the cheapest possible solution. So price, not security, rules," he said.

"Few businesses have the incentive to rip out all their insecure systems and replace them with hardened substitutes. Imposing more regulatory compliance will not work either.

"The only thing that will fix this will be a great big incident that causes so much damage that company boards say, "Okay whatever it takes – we are going to secure this properly."

Asked what businesses should be doing, Mr Lacey said "companies have to raise their game across the board from basic counter-measures, like firewalls, through to more comprehensive APT detection and monitoring techniques that look for signs of abnormal activity inside their network".

ONE ATTACK, MULTIPLE SOURCES

“Some companies may need to also consider “trusted hardware” and keeping their most valuable secrets away from “open, internet-exposed networks,” he said. Mr Lacey said APT attribution was becoming harder as attackers got better at concealing identities.

“When the Red October APT was revealed, four experts attributed four different sources to it,” he said.

In January ,Kaspersky Labs published a detailed report on a five-year long “advanced cyber-espionage” campaign named Red October that had “successfully infiltrated computer networks at diplomatic, governmental and scientific research organisations, gathering data and intelligence from mobile devices, computer systems and network equipment.” Red October hit numerous Eastern European countries and targets in the US, Africa and Australia.

Dr Lacey said APTs were also “spreading down supply chains to company’s outsourcers, legal advisers, and accountants who often have information and access but are not well defended.”

“We know that SMEs don’t have real security – they’re not interested in it, and often cannot afford it,” he said.

Asked whether cyber risks were being exaggerated, Mr Lacey responded, “Frankly, the movie *Die Hard 4* will probably prove to be understated”.

He said societies will have to get used to living in a world where online spying is more prevalent, as a trade-off for technological progress.

“There are both opportunities and threats with technology, and they are getting bigger and bigger. If we end up in a situation where you can’t do anything without half the world spying on you, so be it. But there will be many other positives, including better products and services, to compensate for these costs.”