Protecting the future from cyber crime

Platypus Magazine spoke with Federal Agent Nigel Phair about his new book and the impact of high-tech crime as he sees it, and the challenges which lay ahead in controlling cyber crime.

"The consequences for business of technology-enabled crime includes financial loss, brand damage and, potentially, increased regulatory oversight. The move by organised criminal networks into cyber crime demonstrates how much money is to be made from this medium. These loosely-formed networks are different from what have been known as traditional organised crime groups, which are characterised by structure and a defined hierarchy. This new fluid structure of cyber criminals is becoming more professional and strategic in its endeavours."
extract from *Cyber Crime: the Reality of the Threat*

What are the challenges which lie ahead in policing high tech crime?

Nigel Phair: It is going to be difficult but not impossible. The challenge lies in investigators recognising the impact of technology across all crime types. There is going to be a strong technology element in almost any crime to be investigated, so they will need to be aware of what it is, where it's going and how it can be used both to enable and enhance crime. Investigators will also need to be aware of the avenues of enquiry they have that involve technology.

Can policing keep up with the evolution of cyber crime – or is this an unwinnable war?

NP: I don't like talking doom and gloom, but we do need to recognise that technology is always evolving and we need to be on top of it with our thinking and approach. It's not just about how it impacts on us from a criminal perspective, but about how technology can be used to increase productivity and conduct quicker, better, smarter investigations by actively embracing it.

From an organisational perspective, this is definitely being addressed. The AFP has been proactive in a number of ways by working with private sector technology providers (such as Microsoft) to find out what they are doing – now and into the future. It's putting a genuine strategic thought process into how we're going to address this issue and what systems we need to deal with what's going on today and what might happen in the future.

Author of *Cyber Crime: the Reality of the Threat,* Federal Agent Nigel Phair

For instance, three years ago no-one had heard of 'blogging' yet now it's ubiquitous.

We need to get younger people who use this technology continually, or who are studying IT, and get them involved in the organisation – literally pick their brains.

Does a cyber criminal fit a typical profile?

NP: In the past I would have said they were typically clever young kids who might deface a website then brag about it. But these days it's just crime and it's all about making money. The online cyber criminal is now focused on the proceeds of his crime – not the ingenuity of it.

Who do you see as being the most vulnerable to high tech crime?

NP: From a personal viewpoint, the home-user. The biggest issue at the moment is end-user compromise where the individual is using a computer which has been compromised by phishing scams and the like. However, as a society we really want people to have trust in the Internet and e-commerce

generally – and the police can play a very important role here. We need to be out there working with both government and the private sector, because they are the ones that own 95 per cent of the critical infrastructure.

What precautions can people take to protect themselves from cyber crime?

NP: In many ways it's all about thinking in real world smarts and adapting it to the cyber world. For example, when you queue at the automatic teller you make sure people don't see your PIN. Yet many people are going on-line and doing their Internet banking from an Internet cafe which could potentially be loaded with spyware. Having up-to-date antivirus and properly configured firewalls is also important. Similarly, if you receive an email from someone you don't know – you should never open it or any unknown attachments.

How will big business be impacted by cyber crime?

NP: The corporate world will be vulnerable from a range of mechanisms including external attack by hacking, insider attacks and 'denial of service' attacks which reduce the corporations' on-line ability. In addition to the basic perimeter security, businesses in the future will need what we call 'defence in depth'.

Where do you see the future of cyber crime going – in both criminal and geographic terms?

NP: Criminals will form vast global networks to conduct their attacks, without ever having to meet in the real world. They will harness their individual expertise or

buy it in from those who have it, discuss it all via encrypted chat channels, do the crime, then go their own ways and literally disappear into the ether.

NIGEL PHAIR

CYBERCRIME
THE REALITY OF THE THREAT
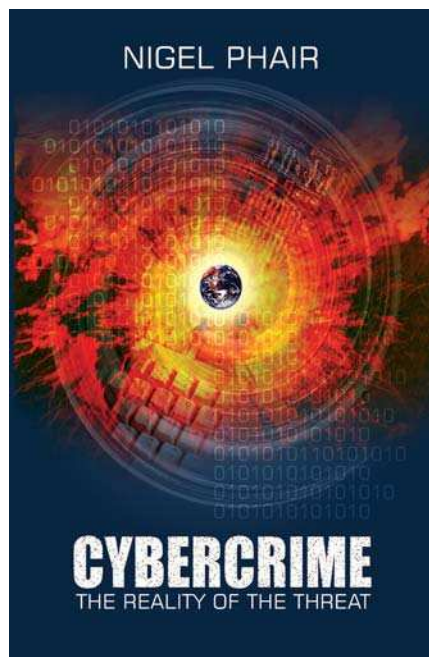
Geographically, cyber crime has largely perpetrated from Eastern Europe, but I am predicting a huge uptake in Asia and West Africa. The latter is already heavily involved in fraud and other criminal activity and this will be a logical way for them to move. Once they see how easy it is, dare I say, to make money and cause havoc, they will move more into this space. There is a huge population, getting better educated with a lack of real jobs, so it all points to the on-line criminal outcome.

Cyber Crime is published by E-Security Publishing.

"For organisations, IT security will become the fourth bottom line. Organisations need to compile a detailed information security strategy. Such a strategy needs to address and mitigate risks while complying with the legal, contractual and statutory requirements of the organisation, and supporting the business objectives. Since there is 'no silver bullet' for solving technology–enabled crime, given the nature of the problem it needs to be continually worked at rather than solved."