

Cyber criminals ‘fish in so many pools’

A leading authority on cyber security maintains that the call on global companies and commercial interests to recognise and safeguard against the threat posed by cyber criminals and financial criminals is largely being heard and the matter is now getting the attention it deserves.

Sir Rob Wainwright, a partner at Deloitte and formerly executive director of Europol, said he no longer sees many examples of large companies who don't grasp the importance of online security.

“The challenge is translating that into meaningful action and knowing what to do but there is a consensus of better practice emerging around the idea of challenging this climate of fear,” he said.

Sir Rob stressed, however, that while people must view cyber for the serious threat that it poses to our economy and our lives, and recognise that it is not going to go away, it can still be managed.

He warned that there are still many mistakes being made by companies and individuals who are being exploited and exposed to scams operated by sophisticated criminals who can cause chaos.

Some of the fundamentals of even the basic security architecture are very often not put in place and criminals are finding it so easy to keep stealing data.

“Some criminals are very adept at exploiting new technologies for their illicit gain,” he said.

Data breaches are illustrative of the fact that criminals, by and large, are opportunistic and they can see that the illegal acquisition and exploitation of personal data is still easy and very good business, he told delegates.

“They are able to fish in so many pools where personal data is found in so many different sectors, including in government, in the commercial sector and the health sector which is particularly interesting for them because personal health information is four times as valuable because it is so rich in personal detail,” Sir Rob highlighted.

“They are able to do that and keep coming back for more because, in many cases, we are still not good enough at closing the door even after we've been burgled once or twice,” he said.

The Deloitte expert said while some cyber-criminals are more aggressive and more sophisticated, a lot of cyber-crime is not “top-end fancy stuff” as up to 90 per cent of it is repeat behaviour and is manageable.

He said it is imperative that companies identify the risks and realise how vulnerable they are and that efforts are made to really understand the threat, monitor and respond to it and use the technological tools available to counter the threat.