BIZCOMMUNITY

Few companies take cybercrime seriously enough

By Paul Vecchiatto

18 Jul 2012

Organised cybercriminals have the world at their fingertips, and South African companies should not think they are immune from hacking attacks.

"Large local companies need to be aware of the real danger of being targeted by cybercriminals operating across borders," says Dave Loxton, director and forensics specialist at Werksmans Attorneys. "The threat may be even more severe if your company uses a mailbox that resides in another jurisdiction. At the very least, you need to be aware of anti-hacking laws in other jurisdictions."

In South Africa, the law allows a company whose computer network has fallen victim to hackers to protect its interests by tracing the cybercriminals (often by hiring a skilled specialist to follow in the hackers' footsteps).

"In the United States, on the other hand, the law prohibits companies and citizens from tracking hacking activity beyond their own networks," Loxton says. "If hackers have breached a private network and left a footprint to follow, which then leads to the United States, only the Federal Bureau of Investigation (FBI) has the legal authority to go in pursuit."

When hackers have targeted a South African company, a request to the FBI would usually have to come from the bureau's local counterpart, the Hawks.

Hacking is potential threat

"Fortunately, there is a huge amount of cooperation with law enforcement agencies across the United States and Europe," says Loxton, adding that there is much less cooperation in countries such as Russia, Latvia and Bulgaria, where the authorities virtually turn a blind eye to cybercrime.

He says hacking has become so pervasive worldwide that it would be naïve for South African companies to regard it as a phenomenon far removed from their own businesses.

"In my experience, however, very few South African companies take cybercrime seriously enough to have a response plan in place and to give their staff training so they can recognise the warning signs of cybercriminals at work."

Lack of awareness of cybercrime could leave a company vulnerable to it.

"Companies that are the most exposed are those with large numbers of contractors," Loxton says. "It is virtually impossible

to hack into a secure company network without inside information, and hackers are constantly on the lookout for ways to plant informants. The more contractors you employ relative to permanent employees, the easier a target your company becomes."

Protect yourselves

Information that could be of use to hackers includes the existence of a weak company firewall and details of network upgrades or planned maintenance work. Firewalls would be shut down at such times, exposing the company to security breaches.

"A skilled informant would also be on the alert for inside information such as user names and passwords, or for opportunities to plant malware or keystroke monitoring software," he says.

Loxton advises companies to protect themselves by doing spot audits and security testing of their own IT networks, preferably using credible outside experts, and to arrange for their staff to undergo training.

"I also strongly recommend putting a response plan in place to deal effectively with the situation if your company network is breached. In a networked world, it is imperative to be aware of the risks of cybercrime and to be ready with a workable plan if worse comes to worst."

Source: *The Times* via I-Net Bridge