BIZCOMMUNITY

Yahoo breach highlights the need for cyber insurance

The cyber attack on Yahoo.com's email servers in 2014 put at least 500m of their users' personal information at risk, and highlights the liability companies face in keeping this kind of information safe.

Under South Africa's fairly new Protection of Personal Information Act (POPI), companies could in similar circumstances, face up to a R10m fine or 10 years imprisonment for a company director.

R6trn lost in global cybercrime

"Cyber security is a big concern for businesses and individuals. South Africa's GDP is estimated to lose about R5,8bn annually to cybercrime, according to a recent McAfee *Global Cost of Cybercrime* report. Internationally the report places that number is closer to $445bn (R6trn). Cybercrime is increasing globally and steadily becoming quite a phenomenon in the business industry," Gillian Wolman, head of litigation at Risk Benefit Solutions.

© Maksim Kabakou 123rf.com

One of the growing trends in cybercrime is the application of ransomware, which encrypts all of the information on a company's servers, she says. "Criminals often use this type of attack to extort money from businesses, promising to decrypt the company's files for a fee."

"Usually the programmes only encrypt company information, and no data is actually taken off the servers. Still there is no way to be sure that the criminals did not get access to the information and companies are still under obligation to report it to their clients and authorities. They also face the same possible penalties and loss of business," Wolman notes.

No covered by traditional insurance

While the business sector is becoming aware of the issue, Wolman says that companies need to start adapting to this emerging threat more rapidly. "In terms of risk management, more businesses need to start putting processes in place, that are properly managed and having a transfer mechanism in the form of an insurance policy in place, are paramount. The liability that companies face if they do not have these, could easily send them into liquidation."

Wolman points out that cyber claims are not covered under traditional insurance policies. “Policies such as general liability, business interruption and computer all risks only cover claims where there is physical damage, while professional indemnity provides limited cover for third-party data loss, but generally only in relation to the provision of professional service.”

As a result, businesses require dedicated cyber policies that cover first-party expenses, loss of business income notification expenses, crisis management expenses as well as the associated regulatory fines, says Wolman.

“Also keep in mind that any insurance policy will have its terms and conditions, and companies are only adequately covered if their risk management procedures are up to standard. Therefore, up-to-date security software, proper password protection and the right data security procedures are all the company’s own responsibility,” she adds.

Being hacked is inevitable

More business owners have fortunately started to realise how costly the effects of cyber attacks can be, and are therefore putting these measures in place to protect themselves financially.

“Cybercrime is fast becoming one of the biggest threats facing organisations. It is no longer sufficient for businesses simply to guard the network perimeter with a firewall and install antivirus software on endpoints. Companies need to continually monitor the evolving threat landscape, and understand that being hacked is no longer a risk, it is an inevitability,” concludes Wolman.