# Managing mobile security in South Africa

From smartphones to tablets, mobile devices continue to cause ongoing concern for IT teams responsible for information security. Sensitive corporate information can be easily transported, leaked, or lost while the Bring Your Own Device (BYOD) movement has dramatically increased the number of expensive security incidents.

Doros Hadjizenonos, sales manager of Check Point South Africa

Even so, corporate information, including sensitive customer information, is increasingly stored on personal mobile devices and not managed by the corporate IT department.

Check Point Software Technologies recently published its second mobile security report, revealing that the majority of businesses (79%) in the US, Canada, the UK, Germany, and Japan had a mobile security incident in the past year, with the costs proving substantial. The new report found mobile security incidents tallied up to over six figures for 42% of businesses, including 16% who put the cost at over R5.1 million.

To contextualise these findings for the South African market, Doros Hadjizenonos, sales manager of Check Point South Africa provides insight into trends driving mobile security in South Africa, challenges facing the South African mobile security market, top tips for businesses regarding managing mobile security and predictions for the future of mobile security in the South African market.

## Q. What are the top three trends that you see driving mobile security in South Africa?

A. i) The increasing mobility of the work force: the work force is becoming more mobile, which means that they require information to be available at their fingertips and, as such, require a solution to protect this information from getting into the wrong hands. The form factor of these devices makes them more prone to being lost.

ii) The rise of mobile device exploits. We are seeing an increase in the number of exploits on mobile devices (especially smartphones), which increases the security risk profile of allowing such devices to connect to the corporate network.

iii) Adhering to the Protection of Personal Information Act. The imminent Protection of Personal Information Act will hold companies responsible for loss of personal information. Assuming that these mobile devices have access to personal information about their clients makes it imperative to secure the devices as you would with a laptop or even a desktop.

## Q. Are the findings of the latest Check Point mobile security report in line with the SA market?

A. Mostly, yes. I would agree that the number of devices connecting to the corporate network is on the increase - 96% of companies surveyed in the report confirm this. BYOD most definitely creates challenges for security administrators and business owners, where a balance needs to be found between security and convenience. The report found that 63% of businesses do not manage corporate information on personal devices, and 93% face challenges adopting BYOD policies.

## Q. What are the key hurdles or challenges facing the South African mobile security market?

A. The major hurdle that I see is the impact of security exploits on the end-user. Security should be a business enabler and not an inhibitor. Users should be able to bring their own devices and use them for both personal and business practices, without compromising any functionality.

In addition, I believe that users need to be educated on the safe use of mobile devices, creating the need for companies to establish a security awareness programme - ensuring the security message is communicated to all employees.

## Q. What are your top tips for businesses when it comes to managing mobile security in South Africa?

A. i) Embark on a mobile security project to ensure that the enterprise data stored on mobile devices is secured. It is vital to choose a solution that minimises the impact on the end-user.

ii) Ensure that there is security awareness programme to educate users about the risks of mobile devices. This programme should also be extended to cover all devices that connect to the network, i.e. tablets, laptops, desktop PCs and notebooks.

## Q. What are your predictions for the future of mobile security in South Africa?

A. i) I believe that we will continue to see an increase in attacks targeted at mobile devices - smartphones specifically. South Africans have accepted and adopted a mobile device as a primary form of communication and I don't see this trend changing anytime soon. As legislation comes into effect I believe that corporates will take mobile security more seriously.

ii) The devices that are used in the workplace are not always corporate-owned devices - making managing BYOD more complicated. Looking ahead, I believe that corporates will place more emphasis on ensuring that corporate data remains secure, but at the same time not prohibiting employees from using their devices for personal use.