THE SAPS WEBSITE HACK: A WAKE-UP CALL THAT WILL HIT BUSINESS AND THE STATE ON THE BOTTOM LINE

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Lucien Pierce | May 30, 2013

Reports in this week's media of a cybersecurity breach of the South African Police Service's website are a foretaste of bigger and more damaging information security breaches to come.

Both the State and Business regularly downplay information security breaches. Major corporations and government institutions in jurisdictions such as the United States, the United Kingdom and Puerto Rico have lost millions of rands in financial and reputational damage as a result of cyber-security breaches. The State and business in South Africa ignore the reality that losses of this magnitude will soon be happening in here. Like in those other jurisdictions, losses will be as a result of reputational damage, damages claims and statutory penalties.

Three high profile examples of cybersecurity breaches immediately come to mind. A breach of Sony's Playstation network saw the data of 100 million customers compromised. It has already cost Sony US$200 million, with 58 class action suits still outstanding. Google, yes Google, suffered an embarrassing cyber-security breach when researchers demonstrated that they were able to hack into Google's Sydney office's building management system (they could have taken over its operating system and accessed other control systems). Perhaps more relevant to South Africa, given Eskom's and the City of Johannesburg's roll-out of smart electricity metering systems, was where a Puerto Rican electricity utility's smart meters were hacked. These resulted in the US Federal Bureau of Investigation concluding that the utility was losing up to US400 million per annum.

The reasons for cyber-attacks vary from stealing financial assets, intellectual property or sensitive information to making social or political statements, as was the case in the SAPS hack (the reason for this hack was apparently to protest the Marikana incident). The outcomes for the targets of such cyber-attacks are always negative and include:

- The cost of remedying the information security breach e.g. replacing the stolen assets, and if customers or third parties were affected, providing some sort of compensation to them to try to retain relationships with them after the incident;
- Upgrades to cyber-security systems and protection;
- The loss of customers or business;
- Litigation; and
- Reputational damage affecting customer or investor confidence.

Both the State and business also seem to forget the statutory and best practice recommendations that apply to them. Those that immediately come to mind are (bearing in mind that certain industries and State departments have their own specific information security provisions):

- The Protection of Personal Information Bill ("**POPI**"), which provides for the protection of personal information, the standards of protection to be applied and penalties for non-compliance;
- The Consumer Protection Act, which has similar provisions regarding the protection of consumer information and penalties; and
- Chapter 5 of the King III Code Of Governance Principles for South Africa, 2009 ("**the King III**

Code") dealing with the Governance of Information Technology.

If Just POPI and the King Code are considered, it becomes evident that both the State and business can no longer afford to take cyber-security lightly.

POPI contains a number of information protection principles. It obliges a responsible party (such as the SAPS) to secure the integrity of personal information in its possession or under its control, by taking appropriate, reasonable technical and organisational measures to prevent the loss, damage or unauthorised destruction of personal information and unlawful access to or processing of personal information. In doing so, the responsible party must have regard to generally accepted information security practices and procedures.

Whilst POPI is not currently applicable, the King III Code may well apply to many. Paragraphs 32 and 33 of Chapter 5, deal crisply with the legal aspects of information technology risk management. They state:

"*IT legal risk arises from the possession, ownership and operational use of technology that may result in the company becoming a party to legal proceedings. When considering the company's compliance with applicable laws, rules, codes and standards, the board should ensure that IT related laws, rules, codes and standards are considered. Companies must comply with applicable IT laws and consider adherence to IT rules, codes and standards, guidelines and leading practices.*"

The simple question a court or tribunal will ask when considering an information security breach complaint, will be whether the party complied with IT rules, codes and standards, guidelines and leading practices. If the responsible party did not comply, then there may be various adverse consequences.

The day is fast approaching where a simple press release, down-playing the seriousness of a cyber-attack or information security breach, will not be enough to dispose of any reputational and financial damage to the State and business. They would do well to heed the requirements that laws and standards are complied with.