YOU WILL BE BREACHED: TIPS ON LIMITING LEGAL LIABILITY UNDER THE PROTECTION OF PERSONAL INFORMATION ACT

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Lucien Pierce | March 20, 2017



It was reported over the past weekend that 15 computers were stolen in a burglary at the Office of the Chief Justice, in Johannesburg. The media reported that the computers held the information of 243 South African judges and about 1,800 support staff. Other important South African state institutions like the state arms procurement company, Armscor, and the South African police also had potentially damaging cybersecurity incidents during 2016. There are likely to have been others, but until South Africa's Protection of Personal Information Act, 4 of 2013 ("POPIA") becomes effective, there is no legal obligation to disclose such incidents. Once it becomes effective, not only will you be required to report any breaches, but you may also be liable to fines of up to R10 million and imprisonment for up to 10 years.

Cybersecurity incidents typically involve the loss or theft of valuable trade secrets or the exposure of sensitive personal information, usually through a breach in an information security system. If you're saying to yourself: it'll never happen to my organisation, you need to think again. James Comey, the US FBI director highlighted this at the height of the US' war of words with China, over the activities of Chinese hackers. He said "*There are two kinds of big companies in the United States. There are those who've been hacked by the Chinese, and those who don't know they've been hacked by the Chinese.*" Hacks and reaches are very real prospects, take the allegations against the Russians' regarding the United States Presidential elections. The reality is that whether they are bored teenagers, criminal syndicates or spies acting on behalf governments, there are people out there who are trying to get to your organisation's valuable and sensitive data.

The consequences of a cybersecurity incidents are dire. The Word Economic Forum's Global Risks Report 2016 reported that cybercrime alone cost the global economy US$445 billion. McAfee reported in June 2014, that the value of cybercrime in South Africa is estimated at 0.14% of GDP. US retailer – Target has spent about US$148 million so far dealing with the fallout from the theft of the records of 110 million shoppers. Sony Corporation's PlayStation breach has cost it over US$171 million and saw a 12% devaluation in its share price. The better prepared your organisation is for when a cyber incident does occur, the less reputational and financial damage it is likely to suffer.

Below are five steps you should follow to ensure that you are prepared.

Assemble your crisis response team long before an incident happens. It's no longer something for just "the IT guy" to deal with. It definitely wasn't the IT guy who had to explain the 12% drop in its share price to Sony Corporation's shareholders. Your dream crisis response team should be made of the company's governing body or directors, its lawyers, its public relations people and the information technology team. The directors are necessary, because they will bear ultimate responsibility for explaining any reputational or financial damage that the company suffers. The lawyers, because there are bound to be a few laws that would have been broken and a few contracts that would have been breached. The PR people are going to have to understand the implications of the cyber incident because they are the ones who are going to have to deal with the media and put some spin on the story. The IT guys will of course have to immediately investigate the source of the breach. Make sure that there is a formal incident response plan and that all team members are aware of it, so that when the inevitable does happen, everyone is singing from the same hymn sheet.

Implement best practice, policies and procedures. When you're summoned to appear before the Information Regulator or when you appear in court as a result of a civil action for losing sensitive personal data, you want to be able to show that your organisation did what would have been expected of it. For example, you should be able to show that you set your information security systems up in a way that segmented data to ensure that people only access what they need and no more. You should ensure that, if employees are to be trusted with sensitive information, they should at least have had their backgrounds checked. You must be able to show that you trained your employees on information security and that you provided annual refresher training. Ensure that any work related mobile devices your employees use, are governed by an appropriate use policy, that they are encrypted and that they are capable of being remotely "wiped".

Conduct an information security gap analysis (or an audit if you can afford it). Arrange for external information security specialists to do the necessary network and information security testing to determine whether you have implemented what would be regarded by the industry as appropriate and reasonable for your organisation. Review the contractual arrangements you have with suppliers and customers. Check whether the agreements have provisions which limit your organisation's liability if you are responsible for damages caused by a data breach. Ensure that the agreements you have with your suppliers indemnifying your organisation against any damages that they or their staff may cause as a result of an information security breach. Check whether your current insurance policy covers you for cyber and information security incidents. Most insurance products don't, so you would be wise to determine whether a separate cyber insurance policy is necessary. Make sure that it covers your organisation for legal fees, damages, penalties, public relations and data restoration and remediation costs. Importantly, try to ensure that the policy covers acts that occurred prior to the policy, because hackers may already be on your network.

Act decisively when the cyber breach does happen. The first thing you should do is try to get independent information security and data protection attorneys in for advice. The reason for this is that if the attorneys are in charge of dealing with the cyber security breach, whatever information they collect during the course of the investigation, is likely to be privileged. This means that if the independent attorneys brief the investigators to conduct a report on how the breach occurred, no matter what the findings of the report are, even if it finds that the company was negligent, it may always be argued that the report is legally privileged. This means that in the face of an investigation by the Information Regulator or where court action is commenced against the company, that information will not have to be disclosed to the Information Regulator or the plaintiffs and will not be capable of being used against you. On the other hand, if a third party investigator conducts the investigation without the final report being legally privileged, the report may at some point have to be handed over to the other party, no matter how damaging it is.

Finally, do not delay remedying the breach. If you are required to by law, report the breach to the authorities as soon as possible (of course once you have taken advice from your advisors). The authorities, together with your own advisors, will then determine how best to deal with the breach. For example, in certain instances, it may even be necessary to observe the hacker's activities on your network in order to try to trace the hacker's location.

Reputational harm, civil claims and regulatory fines can cripple your organisation. You can limit the damage by taking some or all of the steps we have recommended. They will go a long way to reducing the risk your organisation may face in the event of a cyber-incident happening.