Regulations forcing businesses to be prepared for cyberattacks

Hackers are constantly conceptualising new and innovative ways to gain unauthorised access to private networks, cybercrime and the risk thereof are increasingly making headlines. While the motive is often financial, it could also be purely malicious.


Gillian Wolman

High profile data breaches which have been reported on in the media recently highlight the implications of such cyber-attacks. Hackers gaining access to Ashley Madison's website last month resulted in millions of account details being exposed, while the hack of Sony Pictures last year saw the public release of confidential information belonging to the company, its employees and their families. Both incidences have led to lawsuits and claims that the hacked companies didn't have sufficient security in place to protect their sensitive data.

An unpredictable risk

Gillian Wolman, head of litigation at Risk Benefit Solutions (RBS) - one of South Africa's largest independent insurance and risk specialists - says cyber attacks and crime are not always associated with large companies and that smaller businesses are also very much at risk. Small and medium enterprises should also therefore be contemplating the potential impact of a data or privacy breach, as well as an ever-increasing extortion exposure.

"The reality of doing business in the modern world is that businesses are almost completely reliant on technology. While legislation requires businesses to protect their customers' confidential information, many businesses remain unprepared or unprotected due to the technical nature of the necessary security or the associated costs."

KPMG's Global CEO Outlook 2015 report revealed that although cybersecurity is one of the five top risks that CEOs are most concerned about, only 50% of the CEOs are fully prepared for a cyberattack.

The KPMG report explains that cybercrime is an unpredictable risk, and according to Greg Bell, KPMG's US Cyber Leader, until recently, there has been too much attention focused on prevention and not enough on protection and response.

Protection against the costlyness of cybercrime

Wolman says that in South Africa, the Protection of Personal Information (POPI) Act requires local businesses to realise the importance of not only compliance to the Act, but also have financial cover in place should they fall victim to a cyber attack. "Non-compliance to the Act could have disastrous consequences for businesses. Harsh penalties of up to R10 million, as well as 10 years imprisonment, are a very real possibility for business owners and directors that fail to prevent network breaches."

She explains that the Act provides for financial compensation to affected parties in the form of damages awarded, which could bankrupt a business faced with a class action lawsuit originating from a legal situation involving a large number of people.

The A Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity report, released last week by specialist insurer Allianz Global Corporate and Specialty, revealed that cybercrime in South Africa costs the economy close to R6 billion annually, and approximately $445 billion a year globally.

Wolman says that RBS has witnessed an increase of local business' enquiring and purchasing cybercrime insurance should a data breach occur. "Business owners have started to realise how costly the effects of cyber hacks can be, and are therefore putting measures in place to protect themselves financially. In the event of a law suit, the business will be responsible for paying legal fees, judgements or settlements and other court related costs, which can be extremely costly and potentially bankrupt a business.

"A cyber liability policy will protect businesses against a "network security breach" or a "data privacy breach", and insurers will cover first party and third party claims, loss of business income, notification expenses, crisis management expenses, associated regulatory fines and penalties to the extent insurable by law, as well as direct financial and consequential loss. Each underwriter may however have different terms and conditions."

©Benoit Daoust via 123RF

The cost of a damanged reputation

Wolman adds that apart from impacting a business' operations, cybercrime can impact the reputation of a business to a greater extent. "If a company doesn't manage the crisis effectively and fails to sufficiently inform its internal and external stakeholders, the backlash can result in the closure of a business - if the cybercrime and the fallout didn't already do so. Cybercrime cover therefore also extends to the cost of public relations and marketing to ensure that the business can keep trading and meet its legal obligations to notify the public."

The POPI Act is going to revolutionise how organisations manage personal information and data, says Wolman. "Although complying with the legislation is most certainly going to affect a business's bottom line, these costs will be significantly less compared to the fines potentially placed on transgressors. Businesses need to be preparing more comprehensively for the POPI Act, especially in light in the rise of cybercrime in the country. Business owners should be seeking guidance from their brokers to ensure their business is complying with the Act and that it is protected from possible cybercrimes," concludes Wolman.