BIZCOMMUNITY

# Why SMEs should be looking at cyber insurance

By Colin Thornton

28 Sep 2018

For most small to medium-sized businesses in South Africa, budgets are tight and owners constantly have to prioritise spending. An expense like cybersecurity and thoughts of the nebulous world of cybercrime might be downgraded in favour of more tangible, urgent requirements - such as staff, physical security, and stock.

Source: pixabay.com

Yet as the risk of cybercrime becomes a daily reality for SMEs (it is no longer a case of if you get hacked, but when), business owners have to take a fresh look at budgets and reconsider where money is spent.

Now that ransomware attacks are happening almost daily – and will occur every 14 seconds by the end of 2019, according to Cybersecurity Ventures – businesses have to consider taking out cyber insurance to protect themselves against losses. Ransomware damages, alone, are forecast to cost industry up to $8bn in 2018.

## Cyber insurance, you say...does that even exist?

Indeed, for most local business owners, cyber insurance is a vague (and often, new) concept – yet it has been around for many years. Up until recently, cyber insurance was far too costly for the average small business – and was therefore not even a consideration. Now, however, given the prevalence of cybercrime in the business environment (cybercrime will cost a business up to R78tn by 2021, notes Cisco) cyber insurance has become far more affordable – and far more critical – for SMEs.

According to certain industry analysts, entry-level cyber insurance can cost between R5,000-10,000 per year, which is cheaper than many motor vehicle insurance plans. Moreover, in today's world, the chances of falling victim to a cyber attack are far higher than having a serious road accident.

## But why now?

Today, whether you are a sprawling multinational business or a three-man band selling coffee, your business is at risk of cybercrime. This is simply because every modern business relies on internet connectivity and digital services – thus providing access, in one form or another, to savvy hackers. Yes, even if you do the right thing, and have cybersecurity in the form of antivirus software and firewalls, hackers can still get in. Even the most well known of brands, such as British Airways, which presumably has an army of in-house IT brains, has been hacked.

Just recently, the airline announced that over 380,000 customers had their data stolen – putting these customers at risk of cyber fraud and financial loss. As a result, British Airways could face a huge fine, in addition to potential civil lawsuits (and massive reputational damage).

For business owners, it is critical to remember that cyber attacks, whether in the form of ransomware or otherwise (email phishing, etc), come saddled with a variety of costs – that arguably need to be covered by a robust insurance plan. Such costs can include potential ransom payments, loss of business/operational time, profit loss, reputational damage and lawsuits.
Also, given the increasing stringency of data protection legislation such as Europe's General Data Protection Regulation (GDPR) and the local Protection of Personal Information Act 2013 (PoPI), business owners must also consider the risk of fines/legal costs in the event of data loss or mismanagement.

Such laws emphasise the fact that as with traditional 'stock' within a business, data does not only require physical protection – it must also be insured in the event of theft or loss. Essentially, business owners now have a responsibility to protect their customers' data, or face the wrath of legislators who are under pressure to guard consumer privacy…

## Hyper Connectivity, Hyper Risk

Looking ahead, as the Internet of Things (IoT) whereby connected devices speak to each other, becomes more prevalent in the industry and in business, the cyber risk will only increase. While Artificial Intelligence and machine learning have the potential to provide an extra layer of security, business owners must still plan for the worst. The good news, however, is that as general awareness increases, financial services companies and insurers are beginning to introduce more innovative – and accessible – plans that can alleviate the risks of cyber fraud. Without doubt, however, if SMEs are not already looking at cyber insurance, they should immediately begin investigating…


### ABOUT COLIN THORNTON

Colin founded Dial a Nerd in 1998 as a consumer IT support company and in 2002 the business- focused division was founded. Supporting SME's is now its primary focus. In 2015 his company, merged with Turrito Networks who provided niche internet services outside of the local network. These two companies have created an end-to-end IT and Communication solution for SME's. Colin has subsequently become the managing director of Turrito. Contact him at info@dialanerd.co.za

- Understanding SA's 5G reality - 4 Apr 2019
- Why your business needs a cloud architect - 21 Feb 2019
- Privacy vs Profit: Will 2019 be the year of consumer paranoia? - 26 Nov 2018
- Why SMEs should be looking at cyber insurance - 28 Sep 2018
- Why your future digital ID should harness blockchain technology - 23 Aug 2018

View my profile and articles...