By Matthew Garrun, Garrun Group Insurance Brokers

THE CYBERATTACK PANDEMIC, WHAT CAN BUSINESSES DO?

A few years from now, the coronavirus pandemic may be a distant nightmare, but world experts are warning against a more discrete and equally destructive economic threat: cyberattacks, and they could come sooner than we anticipate.

Many South African businesses would not believe that we are already the sixth most exposed country to cybercrime in the world, according to the *Cyber Exposure Index*.

With South Africa in the throes of battling the Covid-19 pandemic, there have already been some major attacks impacting some notable South African brands. Covid-19 has provided a haven for attackers to exploit vulnerabilities in our current remote working, uncertain, anxiety-ridden environment.

The economic impact of cybercrime can be devastating.

According to the *Cost of a Data Breach Report* by IBM, the average cost of a data breach for a South African organisation is $3 300 000 (R56 000 000) with the cost per stolen record coming in at $155 (R2 635). These astonishing statistics should instill fear and swift action amongst our public and private sectors to protect their most crucial asset: data.

Most recently, local credit bureau Experian suffered arguably the most devastating cyber-attack in South African history. Sensitive data of some 23 million South Africans and 793 749 local businesses were compromised. With the largest banks already warning their customers to be on the lookout for cybercrime, the effects of highly sensitive data in the public sphere pose dangers for all South Africans for years to come.

It is often perceived that only large enterprises are targeted for attacks in South Africa, such as Telkom, Momentum, Nedbank, SterKinekor, City of Joburg, Life Healthcare Group and Liberty Holding. This view could not be more distant from the truth. The *State of Email Security* Report published last year by Mimecast stated that "53% of organisations experienced a business-disrupting ransomware attack, up from 26% a year ago". This implies that businesses across the spectrum are being severely impacted, showing cyber risk to be a silent force in further hampering the already brittle South African economy.

South Africa has not had a functional regulator overseeing and penalising the negligent acts of business in protecting their sensitive data. How much consumer data has slipped through the cracks and found its way into the public domain, often into the hands of exploitative cybercriminals? What economic impact have these non-existent regulations had on the South African economy?

The Presidency recently announced that the previously defunct Protection of Personal Information (POPI) Act will now come into force, effective 1 July 2021, allowing companies a year to comply.

According to the Act, businesses that do not conform to data protection policies, regardless of whether non-compliance is deliberate or not, can face harsh repercussions. Depending on the seriousness of the violation, the POPI Act can penalise businesses or individuals with fines of up to R10 million and a jail sentence of up to 10 years. Will the enforcement of POPI raise public awareness of the importance of protecting sensitive data? The answer to this could drastically shape our economy.

Although there is no silver bullet to protect a business from a cyber incident, there are some reasonable steps businesses can take to show due care. Due care could entail adopting a multi-layered security approach governed by enforced data security policies, updated regularly and tailored to the company. This approach is relevant to businesses of all sizes.

The first layer of protection is the effective implementation of security software and services. The primary function of layer one is to avoid access to your IT environment by unwanted cybercriminals. The next layer, often overlooked, carries significant value in protecting a business from being compromised. A robust cyber awareness training programme would ensure individuals within your business have cyber risk knowledge, displaying much-needed skepticism when utilising work email.

The last layer, seen as the final backstop against the irreversible impact of a cyberattack, is a Cyber Risks insurance policy. The vast majority of businesses in South Africa do not have this policy. The reasons range from the complexity of the product, brokers' unwillingness to engage in the cybersphere and low public awareness of risk.

The insurance facet is the final element of a holistic solution and would cover the dispatching of a cybersecurity firm to a businesses' premises to assist with the crisis and provide expertise in solving a ransomware attack.

This policy could be the difference between a business' economic collapse and financial resilience.

It has become indisputable that cyberattacks can destroy companies, livelihoods and economies. This is a risk no country can afford to ignore. A strong economy is built on protected networks.