The risk of underestimating cyber threats

By Rudie Raath, who heads up the Security portfolio at Datacentrix

Cybercrimes have been on the increase at a global level, with 2020 breaking all previous records for data breaches and cyberattacks. And the African continent has not escaped this unscathed, with South Africa, Kenya and Nigeria seeing the biggest increases in cybercrime locally.

South Africa has, in particular, experienced a surge of ransomware incidents more recently. The real fact is that many companies face the fear of data encryption by cyber attackers, who are able to purchase the software, and an instruction guide on how to use it, via the dark web for a paltry amount, as little as R2,000 in some instances.

These attacks are not focused on any particular industry, but more on companies where data is critical to running operations. This is due to the fact that a Bitcoin payout for decryption keys is far more likely if the organisation under attack is unable to operate without those systems. The unfortunate truth is that no company is safe from these attacks - even if you spend all the money in the world.

The protection of the infrastructure is no longer the focus for businesses today; it is all about the data. Cybersecurity is now closely intertwined with the application and infrastructure and, in particular, the actual data. Therefore, a multi-disciplined approach is required, one that understands the system architecture, its dependencies, and the location of all the data. Many companies to date are still blissfully unaware of the location and validity of their backups until the day they are required, only to find that it does not work.

Protecting the data must take priority, and with the technologies available in the market today, it is possible to secure your data copies through regular, immutable backups. Some of these solutions are even able to scan backups for possible ransomware scripts, or processes timed to trigger at a point in time.

The question posed here then is, if backup tapes are dead, could they not be considered as the potential safety net that protects companies? Could this legacy technology be the answer?

An area of concern would clearly be that, should an organisation be targeted and its data encrypted, how long would it take to restore systems – are you prepared to pay the price of this downtime? Or worse, are you prepared for loss of data? How would this affect your business operations and customers? Would you perhaps be liable to pay fines or penalties?

These are the difficult facts that every organisation must consider when assigning budgets to IT operations and innovation. The mitigation measures against cyber threats requires a higher level of discussion within the business, and can no longer be isolated between engineers around the water cooler.

An important facet of this process is choosing the right partner to support you on this journey - one that understands technology integration, infrastructure monitoring, cybersecurity threat mitigation technologies, data protection, governance and risk frameworks – and making the decision to do this quickly. Time is not on the side of the unprotected company.