Protecting an organisation's most valuable asset: why a solid data management and protection strategy is non-negotiable

By Pieter Engelbrecht – Datacentrix Business Unit Manager: Data Management Solutions

With businesses in today's digital economy having access to more data than ever before, a good data management and protection strategy is critical. Not only does proper data management allow for intelligent, informed decision making, it also reduces the risk of data loss, and, importantly, ensures that valuable data is secure and protected from theft and attacks.

We've seen many examples recently, both global and local, on what can happen when your data falls into the wrong hands.

Unfortunately South African companies are being increasingly targeted by cybercriminals, a point that has become more and more apparent over the past two years, as businesses had to rapidly make changes to their environments for remote working.

Ransomware is a particular challenge locally, with Mimecast reporting earlier this year in its State of Email Security 2022 report that 60 percent of South African companies had experienced a ransomware attack over the previous 12 months, a statistic that had increased from 47 percent in 2020.

The truth is that it's a case of when an organisation will be affected by a ransomware attack, not if, and therefore, similar to physical home security, it must have measures in place that make it more difficult for would-be criminals to gain access.

Best practices for data security

There are three best practices required for data management, namely: protection, detection, and recovery.

1. From a **protection** point of view, businesses must ensure that they have three copies of data at the very least – two copies on different

When it comes down to it though, a business must remember that a data management and protection strategy cannot operate in isolation – it must form part and parcel of a greater protection approach that includes other security measures, from firewalls, spam filters and email protection, to anti-malware, and point protection software.

storage types, and a third copy held off site on immutable storage.

2. For **detection**, it is important that any data backup and recovery solution implemented includes malware scanning and anomaly detection. Because there are generally few changes from backup to backup, your solution must be able to report on an out-of-character increase in change rates for instance, as this could indicate an anomaly, and will allow you to take swift action.

3. When it comes to **recovery**, the rule of thumb is that the sooner you know there is an issue, the sooner you can recover from it – by the time you receive that ransom note it's too late. Systems and solutions must be tested regularly, and it's also important to ensure that employees know how to use the solution and are comfortable with it, as there is an important people element when it comes to data management.

Encryption is also more important now than ever before, because even if data is taken, it is then more difficult for the cybercriminal to decrypt without the correct keys.

How do you go about executing a data management and protection strategy?

A solid data management and protection strategy requires several considerations.

Firstly, the company must get to grips with and understand its data. Around 14 to 17 percent of people's data is 'clean' data, which is the important and valuable information, and approximately 35 percent is redundant, obsolete and trivial (ROT) data, or information that has little or no value to an organisation any longer, although it is still retained. The balance is dark data, which is generally unstructured data that is unused, unknown and untapped.

There are clear risks in not knowing your data, particularly in light of the Protection of Personal Information (POPI) Act, from both a security and regulatory perspective, and so this is one of the biggest challenges to data protection and management.

Other important components of the strategy include data risk management, data access management and control, protection policies and procedures, standards and regulatory compliance, and data backup and recovery procedures.

When it comes down to it though, a business must remember that a data management and protection strategy cannot operate in isolation – it must form part and parcel of a greater protection approach that includes other security measures, from firewalls, spam filters and email protection, to anti-malware, and point protection software.

For more information please contact Elzette du Preez on edupreez@datacentrix.co.za