

Why is safeguarding business data crucial for digital success?

 By [Iniel Dreyer](#)

18 May 2023

Data management and protection are crucial for the success of businesses in a fast-paced digital age. Consequently, companies must develop and uphold a strong plan to manage and secure their data, considering the increasing threat of cyberattacks and evolving legal requirements. This raises the important query: What defines a reliable data management and protection plan, and how can enterprises safeguard their security effectively?



Iniel Dreyer, MD at Data Management Professionals South Africa (DMP SA)

Identifying, Locating, and Classifying Data

Businesses must first identify the type of data they have, locate it, and classify it. From there, companies can build a plan that fits their organisational objectives by understanding the relevance of the data they possess and where it is located.

Furthermore, it is critical for businesses to have a strategy in place to protect sensitive data and address risks like ransomware, malware, and natural disasters.

Businesses should consider the following questions when they identify and categorise their data:

Which data needs to be restored initially in order to maintain business operations? Is the appropriate data viable and available? Does the data recovery process correctly prioritise your critical data?

A business can recover the data that is most important for carrying out business operations if it can promptly respond to

the questions above and understand its recovery time objective (RTO).

Having the appropriate resources to support the strategy is also crucial. When something goes wrong, such data loss caused by ransomware or a natural disaster, it could be too late to start looking for suitable IT service providers or resources.

Applying best practices

Businesses must be able to govern who has access to their data, and multifactor authentication is an effective and excellent tactic from a security standpoint. To access or modify the data in this way, at least two authentication methods would be needed.

Encrypting data in flight and at rest is an additional layer of security that can prevent breaches. This occurs frequently when data is transferred between storage mediums, like the cloud, or between on-premises locations. Most businesses tend to spend a lot of money defending the perimeter from outside attackers while overlooking the likelihood of inside threats.

They must guarantee that the data is secure from threats coming from both inside and outside the organisation.

Keeping compliant

In terms of the regulatory landscape, companies must ensure they are following all regulations that are applicable to them and their industry by understanding what data they have and where it resides. Regardless of whether their data is on-premises, in the cloud, or a combination of both, businesses should think about a solution that offers a "single pane of glass" view of all storage platforms (hybrid).

The solution should also be flexible and economical, allowing a company to pay just for what it uses at the time. This highlights the "as-a-Service" approach, which ensures a company only pays for what they use and support is provided by professionals who are knowledgeable on how to build, administer, and more importantly, respond if something goes wrong.

There are IT service providers who help businesses identify and manage their data, and assist their clients with data protection compliance activities in line with applicable legislation. Ideally, they provide compliance-as-a-service (Caas) to help with the process.

oo<https://www.bizcommunity.com/Article/196/159/237427.html> | embed]]

Over the past year, ransomware attacks have been at the top of the list when it comes to data threats. Insider threats, along with social engineering, are also high-ranking risks as companies do not always suspect a threat from within.

Therefore, it is important for companies to be vigilant and develop a comprehensive data management and protection strategy.

In conclusion, an effective data management and protection strategy is critical to the success of any business in today's digital age. By identifying the nature of their data, implementing best practices in terms of security, complying with relevant regulations, and using appropriate tools and solutions, companies can mitigate risks and protect their data from threats.

ABOUT INIEL DREYER

Iniel Dreyer is managing director of Data Management Professionals South Africa (DMP SA), a European specialist in complete solutions for secure and reliable data management. He is passionate about Information Technology and started his career working in a Personal Computer (PC) upgrade centre but gained extensive international experience early on in his career working on a number of international projects.

- Why is safeguarding business data crucial for digital success? - 18 May 2023
- Demystifying DMaaS and why you need it - 3 May 2019
- When it comes to managing your data, trust the experts - 28 Mar 2019
- Can you trust a local data backup provider? - 13 Nov 2017
- Extract more value from your backup than just 'backup' - 20 Feb 2017

[View my profile and articles...](#)

For more, visit: <https://www.bizcommunity.com>