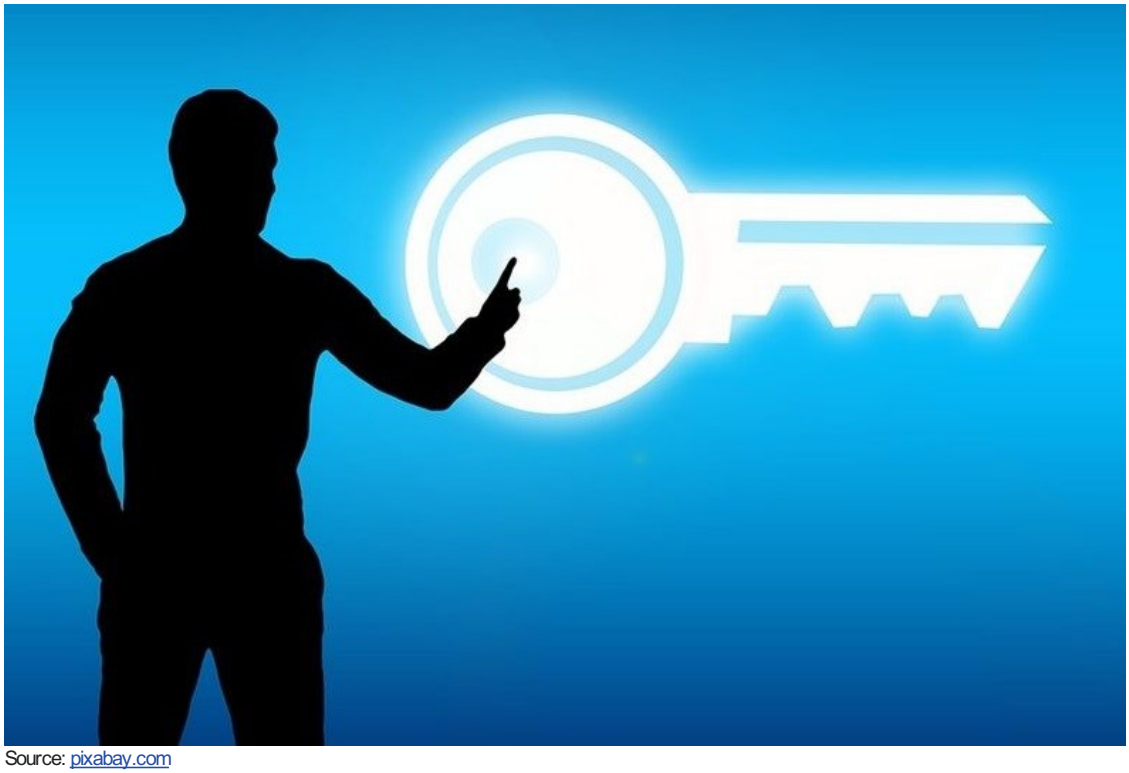
BIZCOMMUNITY

Control+Z your data

By Brian Pinnock

29 Mar 2019

As the world celebrates World Backup Day on Sunday, 31 March, it's worth taking stock of archiving and its growing importance in an age of exponential data and rising threats from cybercriminals.



Source: pixabay.com

The World Economic Forum believes cybersecurity is the fifth-greatest strategic risk facing the world in 2019, according to its latest Global Risks Report. Cyber threats are multifaceted: from government spying to election meddling, stolen passwords to impersonation fraud and ransomware, organisations are being challenged on all fronts in their efforts to secure their data and maintain business productivity.

It's become common belief that every organisation will at some point be a victim of a cyberattack. Despite their best efforts, no organisation is immune. Preventative measures such as advanced security and threat intelligence remain important aspects of cyber resilience, as does awareness training (to equip employees with the knowledge to spot potential cyberthreats and react appropriately). But there’s still the possibility that a new advanced attack could make its way through all the security controls you have in place, which means prevention alone isn’t good enough.

For those organisations that want to remain productive and access business critical information in the wake of a successful cyberattack or other business disruption - and I'd argue that is every organisation - effective archiving and recovery has never been more important. And considering the sheer volume of data most organisations have to process and store, the legislative and regulatory requirements they have to meet, and the ever-looming threat of cyberattacks, it's high time organisations dust off their archiving strategies and make some much-needed improvements.

The new shape and size of data

Organisations have more data than ever before. Thanks to highly advanced analytics, many are using their historic data to search for trends and other insights that can improve their decision-making.

The growth of the Internet of Things is set to vastly increase the volume of data that organisations have to contend with. Gartner estimates the total number of connected things will reach 20.4 billion by 2020. And we're not even touching on the vast volumes of structured and unstructured data generated by other sources such as email. In fact, IBM believes the world currently creates 2.5 quintillion bytes of data each day.

Just generating large volumes of data is not enough; organisations need to be able to quickly access the correct data in order to make empowered business decisions. And if business productivity is interrupted - whether by cyberattack or, in South Africa's case, power outages - organisations must be able to quickly restore access to important data. That’s not to mention the very real possibility of losing all data forever if they don’t have the right backup and recovery in place. This would be a catastrophe for any organisation.

Regulatory requirements add to the pressure: Europe's General Data Protection Regulation and South Africa's Protection of Personal Information Act both require organisations to be able to accommodate Right To Be Forgotten requests, which is only possible if organisations have effective e-discovery capabilities.

Breaking bad habits

A few bad habits are holding back efforts to build better archiving capabilities. The picture of a dusty on-premise catch-all with boxes full of tape persist, despite the technology maturing significantly. Settling for 'good-enough' search that sacrifices speed and accuracy for cost-savings tops the list.

Many organisations also underestimate the importance of e-discovery: that is, until the regulators come knocking, and they are unable to quickly produce the requisite data. Perhaps this is why 50% of South African organisations admitted to lacking total confidence in their e-discovery capabilities in a 2017 Mimecast survey.

Planning for unexpected downtime can sometimes be left to the lower ends of organisational priority lists. And yet 88% of South African organisations want uninterrupted access to email in the event of system failure or downtime. Part of the challenge is storing all data in a single location: a single successful cyberattack or mistaken delete could wipe out your corporate memory forever. Alarmingly, half of all organisations can't recover all their data after an incident.

Imagine the effect of a successful ransomware attack. More than 15% of South African organisations in a 2019 study by Mimecast and Vanson Bourne reported significant business impact from a ransomware attack over the past 12 months, with a further 27% reporting some impact. Alarmingly, 76% of South African organisations experienced downtime of two to five days following a successful ransomware attack. And for more than 10%, a whole week went by before they returned to a recovered state following a successful email-based attack.

So, what are organisations to do? I'd argue there are three key components to a successful archiving strategy that supports an organisation's broader cyber resilience efforts.

KPIs for archiving

In the Mimecast and Vanson Bourne study, 80% of organisations said data backup and recovery are extremely important components of a comprehensive cyber resilience strategy; 1% thought it not important at all. Ensuring it has the following characteristics will go a long way to supporting an organisation's recovery, business continuity and e-discovery efforts:

KPI 1 - Ease-of-use

The number one requirement for archiving solutions is ease-of-use: it must be sleek, intuitive, require minimal training and should be able to automate much of the data classification needed for e-discovery. End-users ultimately don't want to think of archiving at all: they just want to access the information they are looking for quickly and seamlessly and remain productive in the event of a disaster and downtime.

KPI 2 – Security

Pervasive fears over cloud security has stunted growth and adoption of cloud archiving services. That's why it's so important that it fits into a broader cyber resilience strategy that protects important data and can immediately restore business-critical operations in the event of a successful attack. Advanced threats may also sit dormant for days, so being able to recover to a point-in-time (prior to the malware insertion) is critical. Relying on basic recovery will allow the threat to re-emerge in the active mailbox.

KPI 3 – Speed

Let's face it, Google and its competitors in the consumer space have spoilt us. When you perform a search, you expect fast results. And you want to find exactly what you're looking for on the first attempt. Unfortunately, for South African enterprise archive search the average number of searches a user runs to find what they need is five; on average search queries took nine minutes. Search queries taking several hours are not unheard of either. Any modern archiving solution should boost productivity - not hinder it - through fast search, mobility, and easy access to information.

ABOUT BRIAN PINNOCK

Director of Sales Engineering at Mimecast
- #BizTrends2021: What the new year holds for cybersecurity - 6 Jan 2021
- #BizTrends2020: Cybersecurity trends predictions - 16 Jan 2020
- Control+Z your data - 29 Mar 2019
- #BizTrends2019: South African cybersecurity trends for 2019 - 21 Jan 2019
- #BlackFriday: Safe shopping starts with awareness - 22 Nov 2018

View my profile and articles...