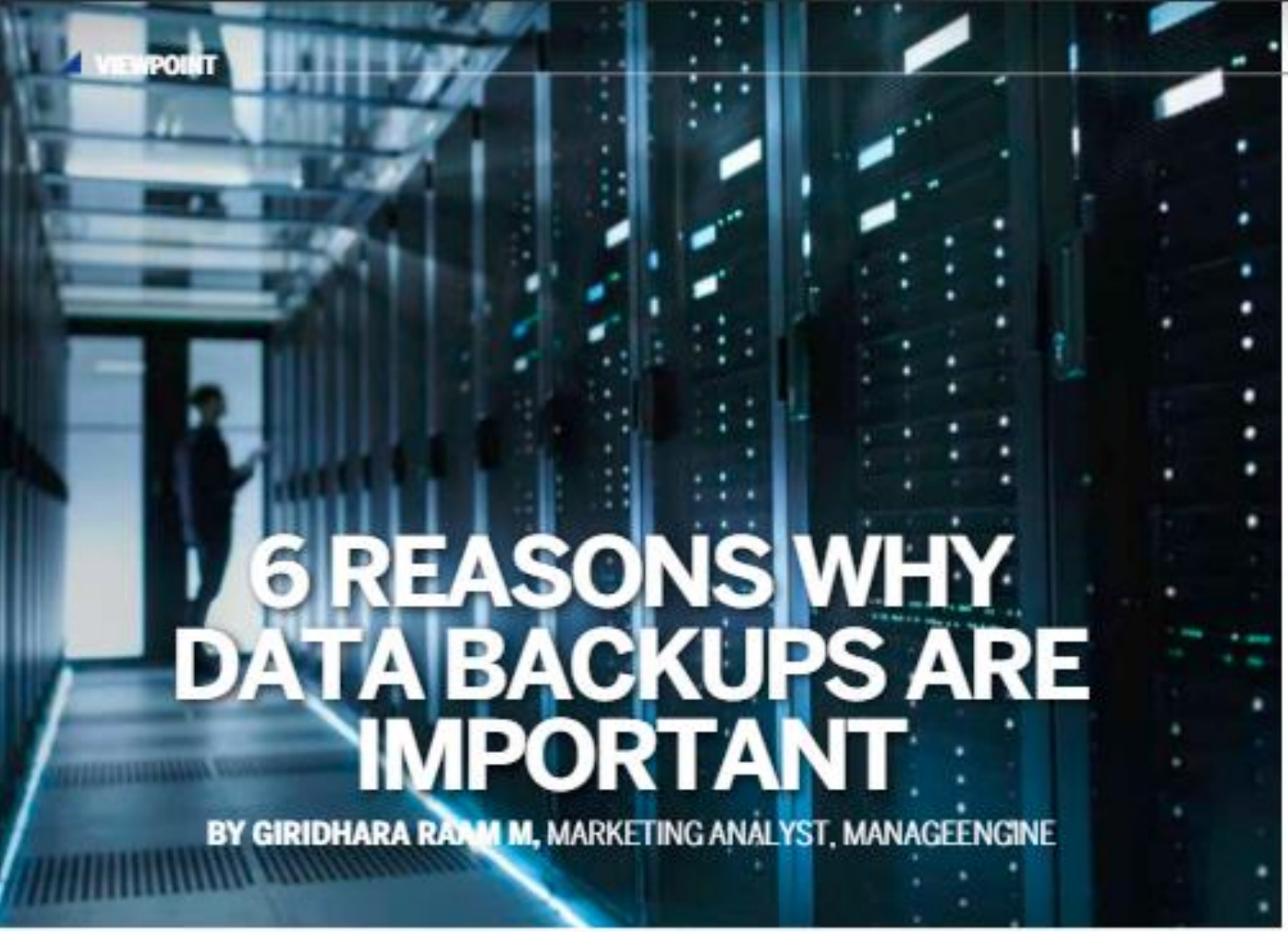

6 REASONS WHY DATA BACKUPS ARE IMPORTANT

BY GIRIDHARA RAMM M, MARKETING ANALYST, MANAGEENGINE

The increase in ransomware attacks and high-profile data breaches over the last few years has reinforced the importance of data security. Recent research indicates that an average of 2,244 cyberattacks happen globally each day, and many of these attacks are targeting sensitive business data. Large enterprises are clear treasure troves of data in the eyes of hackers, but small and medium-sized businesses (SMBs) are often targeted as well. Businesses are becoming more dependent on data in the 21st century, which means the demand for data security is increasing.

However, data security isn't just about protecting data from malicious outsiders; remediation is a critical aspect of data security. While you can't predict when data loss will happen, you can make sure your business has the right solutions to recover its critical data. IT managers are responsible for implementing the right data backup and disaster recovery procedures in their businesses. Mentioned below are a few reasons why your business needs to perform data backups and implement a disaster recovery solution:

1 Preventive measures don't always work

Businesses should take a proactive approach to cybersecurity by equipping themselves with network security solutions, strong firewall configurations, and patch management tools, but they also need solutions for mitigating data loss. SMBs are clearly not immune to having their data stolen or encrypted by ransomware, but according to research by Nationwide Insurance, 68 percent of SMBs don't have a disaster recovery plan. Every organisation, big or small, needs to have a plan for mitigating the aftermath of natural disasters, server downtime, and other complex situations.

2 Cyberattacks are constantly evolving

According to a CNN report,

> "WHILE YOU CAN'T PREDICT WHEN DATA LOSS WILL HAPPEN, YOU CAN MAKE SURE YOUR BUSINESS HAS THE RIGHT SOLUTIONS TO RECOVER ITS CRITICAL DATA. IT MANAGERS ARE RESPONSIBLE FOR IMPLEMENTING THE RIGHT DATA BACKUP AND DISASTER RECOVERY PROCEDURES IN THEIR BUSINESSES."

the average small business hit with ransomware in 2017 lost over $100,000 due to downtime. What's more, these businesses struggled to recover their encrypted data, if they were able to recover it at all. Ransomware is just the tip of the iceberg in terms of cyberattacks; malware, DDoS attacks, data breaches, supply chain attacks, and zero-day exploits are a constant threat.

These cyberattacks usually target sensitive business information stored in the cloud or on-premises. The frequency of cyberattacks has increased thanks to digital transformation, which has become a key driver for businesses in every industry. Businesses today are seeing a massive influx of data for every activity from lead generation to customer conversion, and attackers are ready to capitalise on this steady stream of data.

3 Natural disasters can halt business in an instant

According to Clutch, 60 percent of small businesses that lose their data will shut down within six months. Although data can be lost in many ways, you should never underestimate the occurrence of catastrophic natural disasters. Regardless of your business' size, you need to prepare for storms, earthquakes, fires, and any other natural disaster that could shut down your servers and data centers.

4 Lost data hurts your brand's reputation

According to a study by Small Business Trends, 58 percent of businesses don't have a backup plan for data loss. What businesses need to consider is that, in addition to the above points, data loss leads to a loss of customer trust. Being known as a company that has lost data, especially customer information, won't do your business any favors. In fact, having a poor reputation will likely lose you customers and may impact your organisation's productivity since new employees might hesitate to join your company.

5 Cloud computing demands additional backups

Moving your on-premises operations to the cloud can save your business money and reduce its management efforts, but the cloud isn't without its risks. When businesses store their corporate data on the cloud, they're placing the security of that data into the hands of the cloud provider.

6 Insider threats are often unseen

You never know whether one of your employees will pose a threat to your business' data. A disgruntled employee could easily steal or erase business-critical data if you don't have proper security controls in place. According to a survey by CA Technologies, 56 percent of cybersecurity professionals say regular employees pose the biggest security threat to organisations, with excessive access privileges being the main enabler of insider attacks.

Having proactive data backup procedures in place can add additional security for your business. It also allows you to handle any unforeseen data loss situations, keeping your productivity and brand stable. Since data loss can happen at any time and in a multitude of ways, just making backups is a good place to start. However, keeping consistent backups is the key. If a disaster strikes and your last backup is six months old, your business will have a hard time recovering. Likewise, your data backup plan should be coupled with a disaster recovery plan. This will give you an extra hand when you need to restore your failed devices as quickly as possible. Your corporate data management procedures should include software that automatically creates backups and makes restoring from different backup versions as easy as possible.

Additionally, the 3-2-1 rule is often recommended for maintaining backups: keep three total copies of your data, in two different mediums, with one copy stored off-site. Maintaining physical backups even if you use cloud storage is advised in case your cloud provider experiences downtime or faces a breach.

Best practices for data security

When it comes to databases in particular, here are a few security best practices that could help your business fight against database takedowns and breaches:

- Define strong password policies.
- Remove stale user accounts.
- Change the default username for admins.
- Restrict user privileges.
- Encrypt sensitive business data.
- Keep applications and firmware up-to-date.

Special note should be placed on that last point. According to Gartner's predictions, 99 percent of vulnerabilities exploited by 2020 will continue to be the ones that security and IT professionals have known about for at least one year. This extends beyond just databases and is something to keep in mind for all data storage operations.

Lastly, you need to audit employee login and logoff behaviour, manage USB connections, and provide employees with only the minimal amount of privileges needed for them to complete their work. You don't want to have an air-tight storage and recovery plan unraveled by a malicious insider or an irreversible mistake.