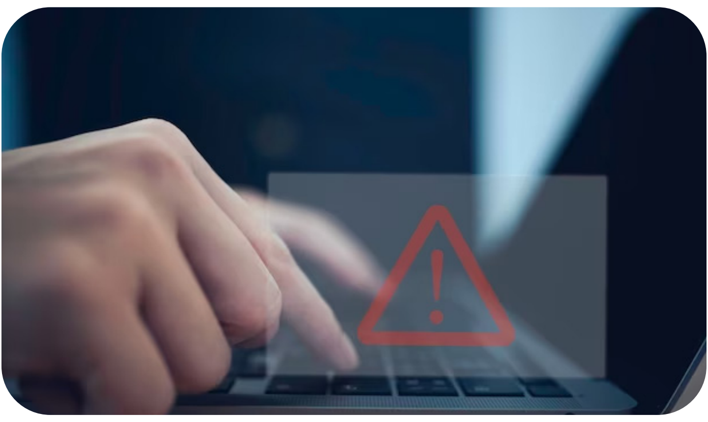
8 Ways to Prevent Data Loss

Data loss not only disrupt productivity for a short period of time but also leads to more permanent problems such as reputational risk, bankruptcy, closures, and fines. Although the cloud has helped many businesses improve remote collaboration and overall efficiency, they now have a massive attack surface that hackers can easily leverage.

Staying on top of data security and up-to-date with industry standards require you and your team's vigilance and risk-conscious mindset.There is no room for complacency when it comes to data security.

Preventing data loss can be challenging for both small and large businesses, especially if it flows through thousands of employees and when they're dispersed throughout the world. The good news is that you can easily prevent data loss by backing up your databases regularly, educating your employees about social engineering attacks, and installing antivirus software, among others.

Here are some of the important steps you can follow to keep data loss to a minimum.



Maintain periodic Data Backups

Data backups are easily the most effective step you can take to prevent data loss. As a rule of thumb, you should maintain multiple backup versions of your data. This way, if there's a problem with one system, you can fall back on the fail-safe plan. Try to make at least three backup copies of your data, especially if it's critical to your business.

Keep one copy in the cloud and the others on on-site physical servers. All these contingency plans will allow you to quickly recover your data in the event of a cyberattack or a natural disaster.

You should also maintain regular backups of your data to ensure they're operational when you need them the most. Maintaining data backups is important whether you use the cloud or maintain an on-premise physical server.

If this sounds like too much work for your core team members, consider hiring managed IT service solutions to regularly make and test backup copies.

Only Use Software from Trusted Vendors

Just because it's cheap or free to use doesn't mean it's safe and secure. The problem with free software from dubious companies is that it's incredibly easy for them to be used as a payload for malware and spyware. In fact, it isn't uncommon for malicious code to masquerade as legitimate software.

If you aren't sure whether the software is safe to use, consider looking it up and researching as much about the software as possible. Pay attention to online reviews from transparent platforms (such as TrustPilot) to look for red flags from real users. If you suspect that something about the software doesn't appear to be correct, consider looking for a more trustworthy alternative.

Remember, if it's too good to be true, it usually is. If you're not sure which software vendor to trust, feel free to schedule a conversation with professionals at Microsys here to learn more about your options.

Educate Your Employees About Social Engineering Attacks

Every security tool is only as good as the people operating it. It's a well-known fact that employees are one of the leading reasons for security incidents, including data loss. This is why it is extremely beneficial to educate your employees about social engineering attacks.

You should provide regular cybersecurity awareness training to your employees throughout their careers. This also means setting up a security-first culture where everyone has a responsibility for maintaining security. This is a great way of preparing your organization to prevent data loss.

You can also hire managed IT service providers at Microsys Inc to ensure that all stages of your business, from top management to operations, are safe and secure. Doing so will help your employees stay updated about the latest cybersecurity threats and how they can prevent them.

Set up Antivirus and Malware Solution

Your antivirus and malware software plays an important role in preventing data loss. Viruses and malicious code make it possible for hackers to penetrate your network and steal sensitive data. And it's not just your own business data that is at risk for theft; the data belonging to your customers, vendors, and employees are also at risk.

If you store credit card information, phone numbers, and other sensitive data, the impact of a data breach or data loss can be disastrous. This is why you should choose the right combination of antivirus and malware software to maintain your data regularly and prevent problems in the future.

PROTECTION

Update Your Network Infrastructure

Always prioritize security updates over everything else. The prevalence of zero-day attacks makes it easy for hackers to take advantage of unpatched software for accessing data. As a rule, you should keep all your operations systems and applications up to date for data protection. There should be no exceptions to this rule.

Moreover, you should also test your essential software regularly to ensure they are running as it should while also being extremely safe for use.

Restrict Access to Data

Employees and vendors should be on a need-to-know basis when accessing company data. You can use access management software to set up access levels and create policies on how company data is used. Access management software provides you alerts whenever an unauthorized entity gains (or tries to gain) access to restricted data. This will allow you to investigate the security incident to prevent data loss.

You should also ask all your employees to sign security agreements so they can commit to the prevention of data leaks while they're employed at your company.

Encrypt Sensitive Data

Encryption is the most effective preventive measure you can take for the prevention of data loss. Roll out end-to-end encryption to improve data protection. With the help of encryption, you can protect your data, whether it's in a private server, the cloud, or in transit.

The main goal of encryption is to scramble data using secret keys known only to the sender and the receiver. The proper implementation of strong encryption algorithms is an effective way of relying on data protection. Here are some of the most commonly used encryption algorithms:

- AES
- IDEA
- SHA 1
- RSA
- Blowfish

ACCESS GRANTED

Classification of Data

It may not be possible to protect all types of data on your service. This is why it helps to identify and classify the type of data you have. Once you have clarified your data, you should be able to devise policies on who can access it. Classification of data also helps you avoid storing it in unsecured locations and minimizes the risk of data loss.

For more information on how you can identify and classify important data, schedule a conversation with Microsys Inc professionals here.

Wrapping Up

Hope the above info helps you to understand and take preventive measures toensure safety and security of your company's databases. Some of these tips may be obvious, such as regularly backing up data and setting up antivirus software. But you would be surprised to learn just how many businesses miss out on the basics only to regret it later.

To learn more about how you can prevent data loss and stay up-to-date with data security and integrity, contact Microsys Inc here.

Click here to learn more!