InfoTrust

netskope CROWDSTRIKE mimecast

EXECUTIVE SUMMARY

PROTECTING YOUR BUSINESS-CRITICAL DATA

PROTECTING AGAINST DATA LOSS

Data fuels businesses across all industries with email communications, cloud storage, and workforce mobility being fundamental to operations. However, the more data businesses collect, store and share, the greater the organisational risk. While much of the data held on local machines, enterprise databases, and cloud servers will be invaluable, every business stores a volume of personally identifiable information, trade secrets or intellectual property. Moreover, when business-critical data is lost, operations can grind to a halt.

Not all instances of data loss are as dramatic as a cybercriminal hacking a corporate website or a sophisticated social engineering attempt to steal sensitive information. Sometimes, data loss is caused by simple human error, weak passwords, or lost devices. However, whether caused intentionally or not, data loss can have a devastating impact. Ultimately, businesses need to be aware of the different types of data loss, the associated business risk and most importantly, measures that can be put in place to mitigate that risk.

Ultimately, businesses need to be aware of the different types of data loss, the associated business risk and most importantly, measures that can be put in place to mitigate that risk.

THE EVOLUTION OF DATA LOSS

Data breaches aren't unique to digital data. The fact is, data breaches have been a business risk for as long as organisations have maintained records and stored private information. Early breaches were caused when someone viewed a file without authorisation or found sensitive documents that weren't properly disposed of. These breaches were commonplace well into the early 2000s until public awareness began to rise. However, the threat of data loss has risen exponentially as businesses have become more dependent on digital services and cloud computing. Before the internet, cybercriminals had to transfer files to storage devices and physically remove them from the premises. Now, cyber threat actors can move files through cloud services and are far more difficult to detect within a network.

Today, data sharing is the basis for a vast number of business processes which in turn drive operations and productivity. With a typical enterprise deploying **more than 2,400 cloud applications** and over half of organisational data in the cloud, information has become more accessible and easier to share. Additionally, the increased use and overlap between business and personal devices only amplifies the risk of data exfiltration and exposure, alongside the opportunity for human error. The increase in potential attack vectors has led to a surge of **up to 10 million** multi-pronged or blended attacks a day, often with email at their core. The result, it is fair to say, that data protection is more challenging today than ever before.

THE BUSINESS RISK OF DATA LOSS

30% chance of a business experiencing a data breach within a two-year period, with the average cost of a breach now at a staggering $3.92 million.

News reports of data breaches are almost daily occurrences, with breaches that affect hundreds of millions of people being far too common. In fact, the chance of a business experiencing a data breach within a two-year period is now **almost 30 per cent**, with the average cost of a breach now at a staggering $3.92 million.

As we have discussed, data fuels modern businesses and drives operations. As such, data loss can have a significant impact and can affect many areas of a business:

- **Reputation** - while it may take years for a business to earn the trust of its customers, it can be lost overnight in the event of a significant data breach. This is only amplified if customer data is lost, and negligence is seen to be at fault.

- **Legal** - as every business is bound by data protection laws and regulations, data loss can expose them to legal actions, fines, and lawsuits. When a business becomes caught up in legal battles, recovery from data loss is even more turbulent.

- **Finances** - without access to business-critical data, organisations are left unable to generate profit as normal. Without suitable backups to work with, finances are stretched further as investment is required in recovering and restoring operations.

- **Productivity** - without access to the data they need to do their jobs, employees can be rendered unable to work and workflows can cease to a halt. This can impact top-level management too, as data-driven decisions become impossible.

The truth is that businesses can go bankrupt or permanently shut down due to significant data loss events. This is even more likely for small to medium-sized businesses, which may find it harder to recover. Therefore, it is vital that every organisation puts in place prevention and protection methods to reduce the risk and minimise the impact of data loss.

THE DIFFERENT TYPES OF DATA LOSS

To fully understand the risks and put the correct preventative measures in place, organisations need to understand the ways in which data can be permanently lost.

While data loss by malicious cyber attackers often hits the headlines, there are several types of data loss. Data loss, the destruction of data, can be intentional or unintentional and caused by both external and internal sources. To fully understand the risks and put the correct preventative measures in place, organisations need to understand the ways in which data can be permanently lost:

1. **Data breaches** - often the cause of data loss that gets the most attention is that of data theft by cybercriminals. Attacks often begin with phishing emails containing malicious links or attachments that enable data to be encrypted and withheld. Meanwhile, social engineering attacks trick victims into passing over sensitive information that is then used for malicious intent.

2. **Physical theft** - as workforces become increasingly mobile, the risk of theft or loss of devices continues to grow. Whether lost, stolen or disposed of improperly, the chance of that device ending up in the wrong hands and causing a data breach increases.

3. **Accidental data loss** - human error plays an enormous role. Employees can unintentionally send confidential emails to the wrong recipients, permanently delete files, or misconfigure servers. All of which can have a huge business impact.

4. **Malicious insiders** - while businesses may falsely assume their employees can be trusted, there is often nothing stopping them from leaking confidential information. This might be simply to cause damage, in the case of a disgruntled employee, or for financial gain if done in liaison with a cybercriminal.

There are other ways that data can be lost, such as hardware malfunctions, software corruptions, natural disasters, or simply a spilt drink on a device. Measures need to be taken to protect against all causes of data loss to ensure business continuity.

DEFENCE IN DEPTH

Ultimately, data loss can happen to any organisation at any time, which makes it vital for businesses to employ the right security tools.

Some of the most common causes of data loss come down to obvious errors with weak passwords, missent emails and misconfigured systems. However, with enterprises becoming more mobile and flexible, sensitive information is shared and accessed across more personally owned endpoint devices. Thereby extending and complicating the risk of data loss. Ultimately, data loss can happen to any organisation at any time, which makes it vital for businesses to employ the right security tools.

Data loss prevention (DLP) strategies help organisations put in place a framework to manage the evolving landscape and adapt to data security best practices, while still benefiting from enterprise mobility. There are several steps and security controls that organisations can employ to mitigate the different types of potential data loss:

- **Prioritise** - the first step in any DLP strategy is to determine which data is most business-critical and sensitive as this data is most likely to be targeted by attackers. Once prioritised, the data should be classified to inform policies on controls for storage, access, and exchange.
- **Control** - controls enable businesses to target the most common risky behaviours. Controls may involve authentication and approvals, limiting what users can transfer or share using software and automatically encrypting protected data when it is shared.
- **Access** - adaptive access controls enable safe business productivity by providing restrictions on certain activities. Defining and managing the roles and access privileges of users and devices to both cloud and on-premises applications is vital.
- **Monitor** - deep real-time visibility with contextual awareness of data across users, apps and devices are a vital part of DLP. By monitoring how data is used, businesses can identify unusual behaviour and implement notifications and alerts.
- **Educate** - training helps mitigate the risk of human error when it comes to data loss. Employees need to understand what data should not be shared or exposed and the consequence of their actions. Pop up alerts and automated reminders can also help keep the risk of data loss front of mind.
- **Backup** - regardless of the controls and processes in place, there will always be a risk of data loss. Having a safe, off-site data backup that is protected from threats around a data centre is essential.

PROTECTING YOUR BUSINESS FROM DATA LOSS

While there will always be a risk of data loss in the modern world, there are certainly many ways to reduce the risk. To mitigate the risk of data loss, organisations have to decide how they are going to share, monitor, and manage the exchange of data. It is a balancing act of convenience and caution, but by first classifying data and setting the right level of controls, businesses can reduce the risk while still benefiting from enterprise mobility.

To mitigate the risk of data loss, organisations have to decide how they are going to share, monitor, and manage the exchange of data.

Ultimately, strategies to mitigate or prevent data loss if an incident occurs should form an essential part of every organisations' backup and data protection strategy. To find out how InfoTrust can help you improve your data loss prevention strategy and protect your business, **request a consultation today.**