PiSYS .net

A COMCEN COMPANY

The Truth About Data Breaches

Have you secured your data?

We make IT easy

Real Data Breach in Numbers: Don't miss out on the chance to steer clear of these alarming figures

The cybercrime industry is constantly evolving, becoming more sophisticated. In a small business of 14 employees, the consequences of a data breach was devastating.

A single phishing email unleashed a cascade of events, leading to a fraudulent message sent to 796 CEOs worldwide, which raised alarms and attracted irate responses.

The breach, initially undetected due to hidden rules implemented by the attackers, exposed vulnerabilities in the organisation's Microsoft account, compromising valuable data stored on SharePoint and OneDrive.

TIME SPENT ON INVESTIGATION - IN HOURS

50 THE ADMIN TEAM	**30+** INSURER / LEGAL TEAM	**8** NATIONAL GOVERNING BODY (NGB)	**60** MSP IT PROVIDER
100+ CYBER FORENSIC TEAM	**14** INSURER / LEGAL	**14** NATIONAL GOVERNING BODY CEO	**30** GDPR CONSULTANT TEAM

DON'TS

- Open any email attachments that end with: .exe, .scr, .bat, .com or other executable files you do not recognise.
- "Unsubscribe" - it is easier to delete the e-mail than to deal with the security risks.
- Click embedded links in messages without hovering your mouse over them first to check the URL.
- Respond or reply to spam in any way. Use the delete button.

DO'S

- Check the email 'From' field to validate the sender. Check characters e.g. 'a' vs 'ɑ'.
- Check for so-called 'double-extended' scam attachments. A text file named 'safe.txt' is safe, but a file called 'safe.txt.exe' is not.
- Report all suspicious emails to the Pisys help desk.
- Note that www.microsoft.com and www.support.microsoft.software.com are two different domains (the first is real).

Data Maintenance: Ensuring Clean and Efficient Data Management

Your data is the most valuable resource , but without proper maintenance, they can become cluttered and inefficient, posing security risks and hindering analytics efforts.

One challenge is the accumulation of redundant, outdated, or trivial (ROT) data. This data occupies storage space, compromises data security and hampers analysis.

Neglecting data clean-up impacts data quality, increases storage costs and slows down processes.

Regular maintenance is essential.

Implementing data governance policies, defining data retention schedules and conducting periodic audits are crucial steps.

Unlock the true value of your data while ensuring security, compliance and operational excellence.

Contact Pisys today for effective data maintenance and optimised data management solutions.

Data Cleanup for **GDPR Compliance**

- **Conduct a thorough data inventory:** Identify all personal data stored in the organisation's data lake and categorise it based on GDPR requirements.
- **Implement data retention policies:** Define clear guidelines on how long personal data should be retained, considering legal obligations and business needs.
- **Assess data quality:** Evaluate the accuracy, completeness and relevance of the data. Remove any outdated, redundant or irrelevant information.
- **Obtain consent and update preferences:** Ensure that individuals' consent for data processing is obtained and documented. Provide mechanisms for individuals to update their preferences .
- **Implement data anonymisation or pseudonymisation techniques:** Remove or replace personally identifiable information (PII) to protect individuals' identities while retaining the usefulness of the data.
- **Strengthen data security measures:** Implement robust access controls, encryption and other security measures to protect personal data from unauthorised access or breaches.
- **Conduct regular data audits:** Periodically review and assess data stored in the data lake to identify and address any compliance gaps or risks.
- **Train employees on data protection:** Educate staff members on GDPR principles, data handling best practices and their responsibilities regarding data privacy and security.
- **Establish a data breach response plan:** Develop a comprehensive plan to detect, respond to and report data breaches in line with GDPR requirements.
- **Engage a data protection officer (DPO):** Appoint a qualified DPO to oversee data protection efforts, ensure compliance with GDPR and act as a point of contact for data-related concerns.

The Importance of Data Backup

Data backup involves creating a duplicate copy of your critical information to safeguard against potential issues like corruption, theft, loss or accidental deletion of the original files.

Imagine losing all your business data overnight. The consequences would be dire. Communication with clients would be impossible, projects would vanish, staff records would disappear and essential details about your products and services would be lost. And let's not forget about your financial data, invoicing status and more. Shockingly, nearly 70% of small businesses shut down within a year after experiencing a major data loss and a staggering 94% of businesses never fully recover from severe data loss. Take a moment to absorb these alarming statistics.

Considering the substantial number of devices that are inadequately backed up within companies and the insufficient attention given to data protection, the situation becomes even more concerning. If you wish to avoid becoming another statistic, it is imperative to prioritise data backup. This entails developing a comprehensive strategy and implementing a robust solution.

So, what data should you back up?

Ensure the safety of your business by prioritising the backup of essential files and documents. This includes financial data such as invoices, bills, statements, payable files and payroll information. It is equally important to back up customer data, supplier details, partner information, communication records, email accounts, applications, databases, project management files, personnel records, operating systems, configuration files and any other files generated by your team.

Don't overlook the significance of backing up mobile devices, which often contain sensitive data surpassing that of laptops.

Regularly review your backup scope to accommodate changes in infrastructure, new devices, solutions or services.

Consider appointing a Backup Administrator to oversee your backup strategy, including tool selection, defining the backup scope, managing the network and storage and establishing Recovery Time Objectives and Recovery Point Objectives. For small teams, outsourcing this responsibility to an IT support professional is a practical option.

We provide this service and would be happy to discuss it with you.

Data backup: How often is necessary?

Every day, without fail.

The frequency of your backups should align with the amount of data your business processes within a given timeframe. Failing to back up regularly could result in data loss between the last backup and a potential failure, known as the Recovery Point Objective (RPO).

For data-intensive businesses, a daily backup might not be sufficient. A shorter RPO reduces the risk of data loss but requires more storage capacity and network resources, which comes with a cost.

Alternatively, longer RPOs are more cost-effective but increase the potential loss of data.

While many small businesses opt for a 24-hour backup period, it's possible to establish tiered RPOs, prioritising more frequent backups for critical systems and longer RPOs for secondary systems.

Consider your Recovery Time Objective (RTO), which measures the time it takes to recover data from a failure point.

Minimising downtime is crucial for avoiding financial losses, so a shorter RTO is desirable. However, achieving a shorter RTO necessitates faster storage and technologies, resulting in higher costs. Typically, a few hours is considered a normal RTO for most companies.

Pisys RTO Calculator

Recovery Time & Downtime Cost Calculator

The cost of a technology outage can cripple a business. Use our Recovery Time & Downtime Cost Calculator to focus on a handful of simple metrics that might come into play during a downtime event, and start a general analysis of what an outage could mean to your business. The results of this calculator are meant to help estimate loss, and does not calculate actual loss.

https://www.pisys.net/rto-calculator/

Choosing the right data backup solution requires careful consideration.

With a wide range of options available, understanding your scope, Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) will guide you in making the best decision for your business.

These are the most popular solutions available right now:

Hardware appliances

These physical devices come with pre-installed backup software and storage, offering easy setup and configuration. However, it's important to note that if the appliance fails, your entire backup solution is at risk, requiring replacement and increasing recovery time.

Software solutions

Installed on your existing system, these solutions allow you to back up to a destination within your network. While you need to install and configure the operating software, they offer greater flexibility compared to hardware appliances and can be cost-effective.

Cloud services (Backup as a Service - BaaS)

The simplest option, cloud services enable you to run backups directly from the cloud. With no additional servers or systems required, it's easy to scale up storage as your business grows. Ensure your chosen provider complies with data protection legislation and has robust security measures in place for handling sensitive data.

Hybrid solutions

Combining local and cloud backups, hybrid solutions provide a robust and popular choice. By leveraging the strengths of both local and cloud backups, you can enhance data protection and resilience.

Introducing the 3-2-1 Approach: Securing Your Data Made Simple

One effective option that aligns with industry best practices and ensures secure data is the hybrid solution. **And it perfectly embraces the 3-2-1 approach**:

1. **Store your data in 3 places:** Safeguard your valuable data by maintaining three separate copies in different locations.
2. **Use 2 types of storage:** Employ two distinct storage mediums to enhance redundancy and protect against potential failures.
3. **Keep 1 copy stored off-site:** Ensure that at least one copy of your data is stored off-site, away from your primary location, to mitigate risks like physical damage or theft.

Choosing the right Backup Type

When it comes to backups, there are three main types, each offering unique benefits, speeds and operation methods:

ONE: Full backup

Capture a complete copy of all data you wish to protect. Initial backups usually begin with a full backup, which may take several hours to complete.

TWO: Differential (cumulative incremental) backup

Once the first full backup is done, you can switch to a differential backup. This method only backs up files that have changed since the last full backup. Differential backups are faster since less data is copied, but the data size grows until the next full backup.

THREE: Incremental backup

Similar to differential backups, incremental backups only copy changed data. However, they focus on capturing data changes since the last incremental or full backup. These backups are smaller and faster, especially when performed regularly. With advanced software, you can even back up data hourly or more frequently.

Choosing the Right Data Storage Solution

On-Premises Storage

Physical Servers
Advantage - Offers complete control over your backup data and enables fast data retrieval.
Disadvantage - Requires upfront investment in hardware, maintenance and physical security measures.

Network Attached Storage (NAS):
Advantage - Provides centralised storage accessible over the local network, allowing easy backup management.
Disadvantage - Limited scalability compared to cloud storage solutions.

Cloud Storage

Public Cloud
Advantage - Offers scalable storage options and high data availability. Service providers handle infrastructure maintenance, reducing your IT burden.
Disadvantage - Dependency on the service provider's infrastructure and potential concerns regarding data privacy and security.

Private Cloud
Advantage - Provides enhanced control over data privacy and security, allowing customisation to meet specific compliance requirements.
Disadvantage - Requires additional investment in infrastructure, maintenance and expertise for setup and management.

Hybrid Storage
Advantage - Combines the benefits of on-premises and cloud storage, providing flexibility, scalability and redundancy. Offers the ability to keep critical data on-site and leverage the cloud for additional storage and disaster recovery.
Disadvantage - Requires careful integration and management of both on-premises and cloud infrastructure, potentially increasing complexity.

Tape Storage
Advantage - Provides offline, long-term storage suitable for archiving and regulatory compliance. Offers cost-effective storage for large volumes of data.
Disadvantage - Retrieval times may be slower compared to disk-based storage. Requires manual handling and proper storage conditions to prevent physical degradation.

Off-Site Storage
Advantage - Adds an extra layer of protection against localised disasters by storing backups in a separate physical location. Provides geographical redundancy and minimises the risk of data loss.
Disadvantage - Requires additional logistics for transporting and managing backups in a different location. May involve additional costs for secure off-site facilities.

Talk to Pisys

We work in a challenging industry, this is true. The underground market for stolen data and hacking tools continues to thrive, fuelling cyber criminal activities.

But despite the inherent challenges posed by these ingenious cybercriminal attacks and data breaches, **you possess the ability to outsmart them.**

Your choice matters –

At Pisys, we understand that every business has unique needs when it comes to data backup. We go beyond a one-size-fits-all approach by providing customised solutions that align perfectly with your requirements, RPOs and RTOs. Our expert team will assess your resources and design a system that suits your business's specific demands.

We recognise the importance of making an informed decision, which is why we provide comprehensive information and guidance throughout the process.

We only take on a certain number of customers a year to ensure that we provide the best protection. Dont miss out - give us a call.

We implement backup and recovery solutions every day. To speak with an expert, get in touch.

CALL: 01792 464748
EMAIL: hello@pisys.net
WEBSITE: www.pisys.net

PISYS .net
A COMCEN COMPANY