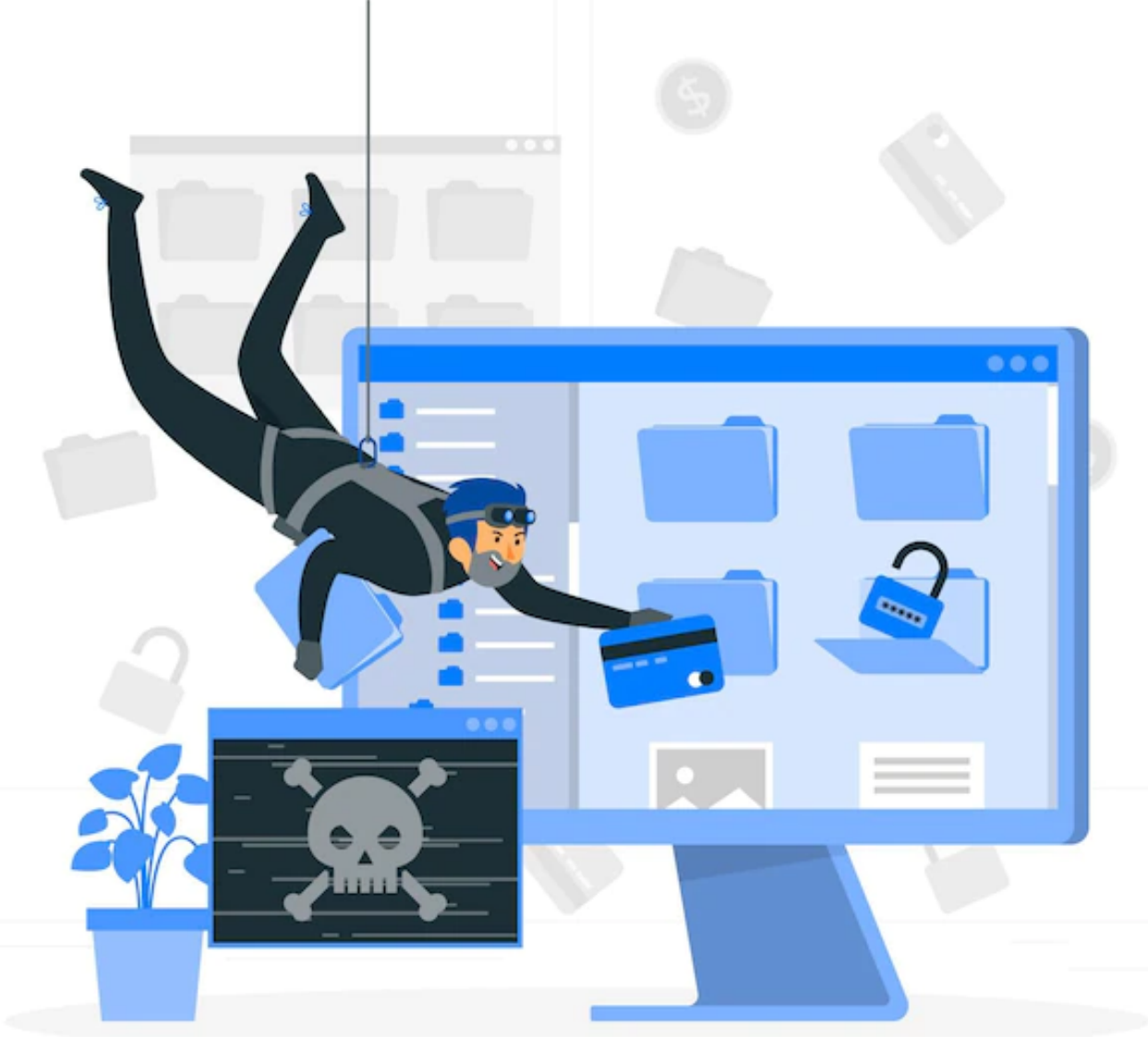


Practical Ways of **Preventing Data Breaches**

In the context of countless data breaches that have made news headlines in recent years, the old adage, "prevention is better than cure," definitely applies to cybersecurity.

Responding to a data breach is a chaotic and complex task. Even if an organization is well prepared to respond to a data breach, the repercussions may be too severe to recover (including financial, reputation, and operational damage).

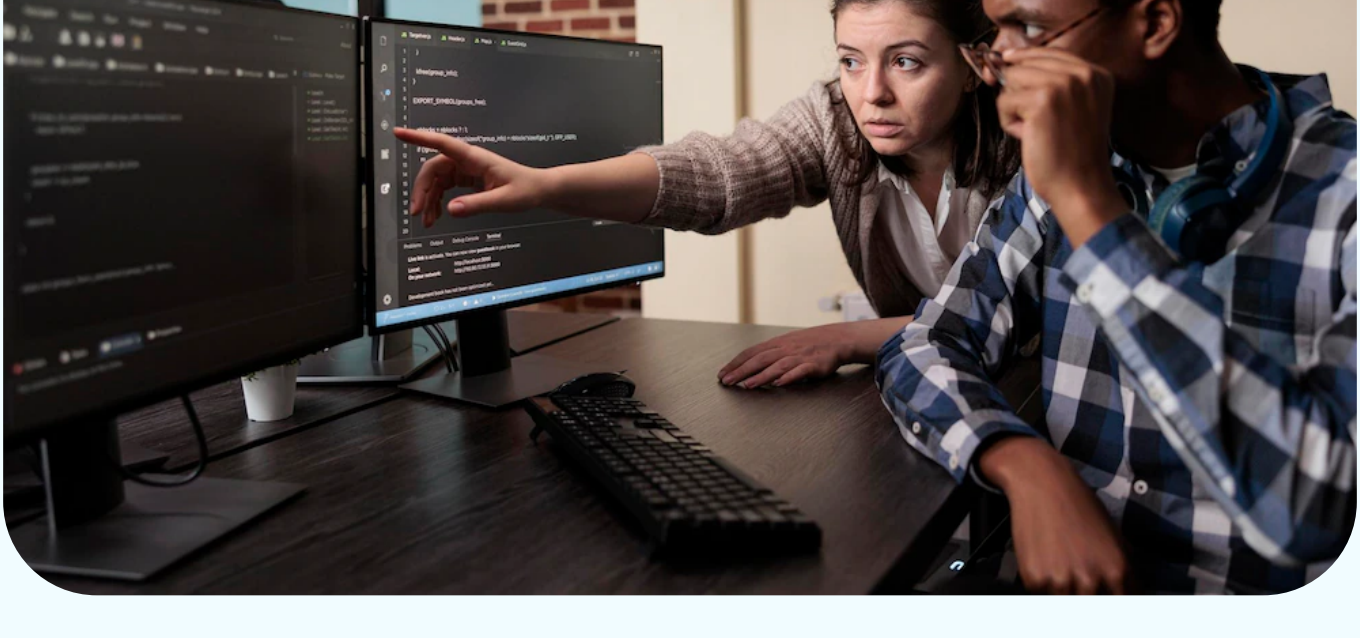
This is a problem because the cyber landscape is constantly evolving, with new threats emerging. Nearly every business has a growing digital footprint that makes them vulnerable to data breaches. There is a need to take proactive, as opposed to reactive, approaches to evaluating your digital activity and keeping up with the latest cybersecurity practices.

What Are **Data Breaches**

A data breach occurs when unauthorized personnel gain access to sensitive data. Top priority for cyber criminals in data breach attacks include credit card numbers, social security numbers, driver's license numbers, and trade secrets (such as source code, marketing material, and customer lists).

In other words, if someone isn't authorized to view the target data and manages to access or steal it, the organization is said to have suffered a data breach.

Data breaches can have devastating consequences for the target organization and their clients, vendors, and employees whose data has been outed. Businesses can be on the receiving end of costly litigation, massive fines, reputational loss, and loss of license. This is why companies, regardless of the size of their digital print, must constantly evaluate their cybersecurity measures and adapt to malicious behavior.

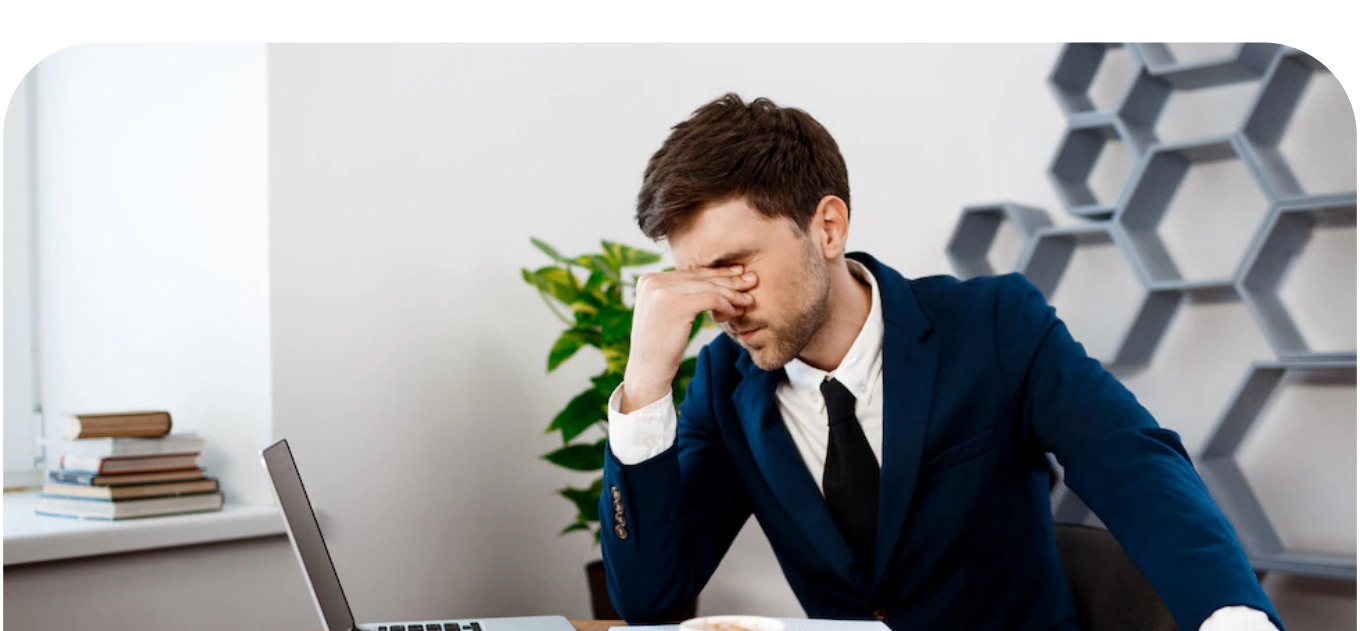


The Potential Ramifications **of a Data Breach**

The potential ramifications of a data breach depending on the organization, industry, and scale of attack. Data breaches in the finance industry can have more devastating consequences compared to the manufacturing industry. Businesses should measure the potential impact of a data breach as it applies to their organization in order to develop an appropriate cybersecurity posture.

Loss of Reputation

Loss of reputation is arguably the biggest impact of a data breach because most customers would not do business with the company, especially if it failed to protect their data. This can translate into a loss of sales and brand devaluation (which takes a long time to build). The failure rate of small businesses gets even higher if and when they are exposed to a data breach.



Theft

Businesses, both big and small, are vulnerable to data breaches. In fact, cyber-attacks are commonplace with smaller businesses because they are usually perceived to have less sophisticated defense mechanisms. For most cyber criminals, the theft of sensitive data leads to a bigger paycheck than stealing money.

Intellectual property theft is also damaging to businesses, with many companies losing years of trade secrets and copyrighted material which results in the loss of their competitive advantage in the market.

It is worth noting that intellectual property theft is slightly more difficult because businesses can identify who stole their IP and bring them to court. In any case, this can be a serious problem if litigation isn't possible (especially in countries where IP laws are non-existent).

Fines

Data breach fines are nothing to sneeze at and can amount to several millions of dollars (or euros). For example, Marriott was hit with a $23.8 million fine for a data breach where hundreds of millions of guest records were exposed after their reservation database was compromised. The GDPR, in particular, is unrelenting when it comes to protecting consumer rights and has issued over $193 million in fines in 2020 alone.

Many small businesses may be unable to afford these fines and may have to close operations.

Steps You Can Take to **Prevent Data Breaches**

In most cases, most businesses can take measures to prevent data breaches, as we will discuss below.

Employee Awareness

This may sound too obvious, but a lack of employee awareness is the biggest threat to an organization's cybersecurity posture. You should educate your employees on protecting their data from being compromised. This can be done by teaching them how to make stronger passwords, changing them frequently, and helping them identify social engineering scams (such as phishing emails and other conspicuous activities).

Establish Data Security Procedures

Your organization should establish procedures for employees to diligently follow without fail. These procedures should be reviewed and updated based on the latest cybersecurity threats. This includes best practices such as encryption, strong password policy, 2FA, user activity, and endpoint security.

In addition, it is recommended to implement role-based access control to restrict data access based on an employee's role within the organization. Various access management tools can be used to enforce appropriate restrictions in place and protect your data. This includes SolarWinds Access Rights Manager and ManageEngine ADAudit Plus.

For more information on which software is ideal for your business, we recommend getting a thorough evaluation from our cybersecurity experts at Microsys Inc.

Regular Data Backup

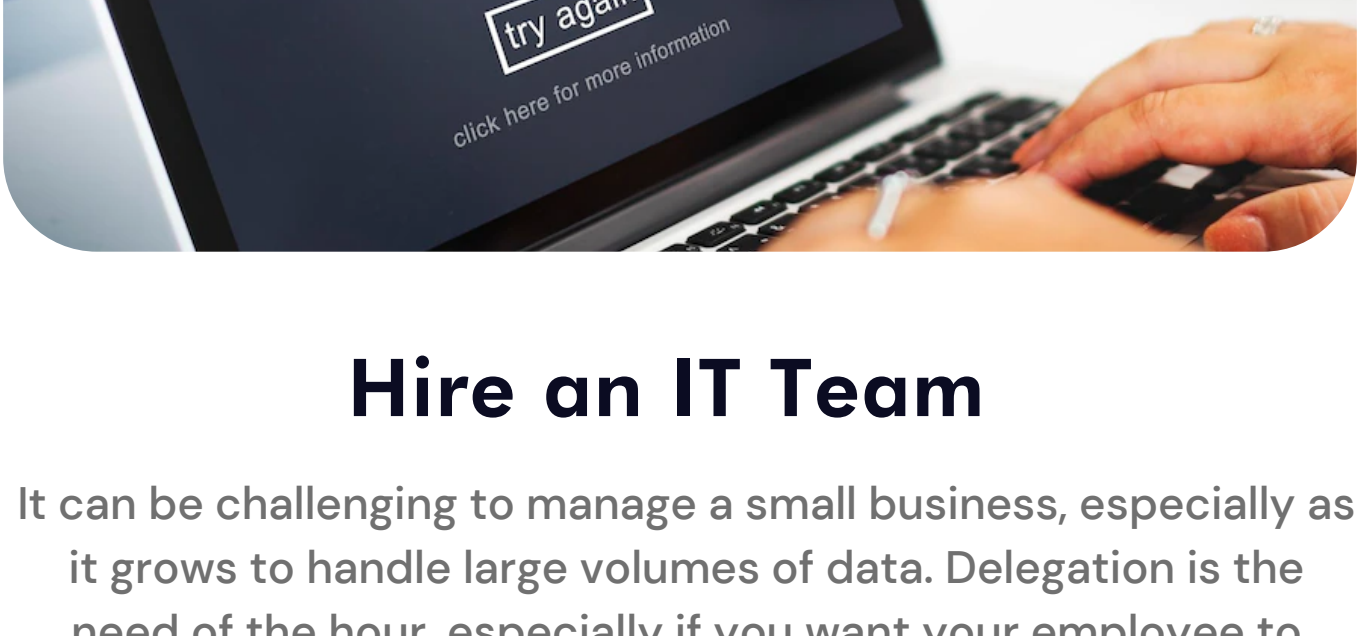
Data breach attacks can delete all your data and hold it for ransom for monetary compensation (usually in the form of crypto coins because they are harder to trace). You can render most ransomware attacks useless by backing up your data by making physical copies on a separate hard drive or a cloud server.

Data backups are also useful because they help you recover data in case of a natural disaster, server crash, or an accidental loss of data. You can hire IT teams to make remote backups on a regular basis to ward off the threat of ransomware attacks and server outages.

Implement Security Software

Professionals recommend installing security software and updating them regularly. Install patches when they become available. Ignoring a patch for a long time could make you more vulnerable to data breaches, especially because cyber criminals become aware of loopholes in outdated software.

Different types of security software are available for businesses, including anti-spyware, anti-virus, and firewalls. These tools, coupled with an IT team, will ensure that you have a strong cyber security posture.



Hire an IT Team

It can be challenging to manage a small business, especially as it grows to handle large volumes of data. Delegation is the need of the hour, especially if you want your employee to focus on the core areas of the business instead of worrying about their cybersecurity posture.

With Microsys Inc, our consultants will help you identify gaps in your cybersecurity posture and ensure that your business stays safe using PCI-compliant security tools.

Click here to learn more!