How to build a cybersecurity plan for your small business.

## Description

The primary focus of small business owners is to grow their businesses. So they spend all their time and resources on administrative and other business tasks. They tend to neglect IT security due to limited staffing and budgets.

Because small businesses do not operate on as big a scale as large corporations, they also think they are not at high risk of a cyber attack.

But all businesses, regardless of size, are now operating digitally to some extent or another. This means that small and medium businesses are also vulnerable to cybercrime. According to a study conducted by IBM in 2021, 52% of small businesses had experienced a cyber attack in the previous year and 10% had experienced more than 10 cyber attacks.

## Why cybersecurity is vital.

Cybersecurity is the process of protecting and recovering computer systems, networks and devices from data breaches and cybercrime. As businesses continue to rely on technology for their business operations, they can remain susceptible to a myriad of cyberattacks.

There are some statistics to show the volume of cyberattacks. For example, an average of 30,000 websites are hacked every day and one company falls victim to cyberattacks every 39 seconds. And 60% of companies globally have experienced at least one form of cyberattack.

Cyber breaches can cause financial losses as well as damage the company’s reputation and customer trust. According to a recent report, businesses with less than 500 employees lose about 2.5 million per attack. Such effects can be very devastating for many small businesses.

Companies need to have a cybersecurity plan to protect themselves from cybercriminals. The common types of attacks on small businesses include phishing attacks, malware attacks (trojan horse, spyware), password hacking, ransomware attacks and insider threats.

## How to build a cybersecurity plan for your small business.

As more companies shift to remote working and incorporate newer technologies in their daily operations, it's important to protect these systems and networks from any infiltration. Below are some actionable steps to help you develop a cybersecurity plan for your business.

## 1. Assess your risk.

Every business is different and faces different types of cyber threats. During a cybersecurity risk assessment, you should identify important digital assets, potential threats for each and the consequences. A business can be attacked through email, web servers, network infrastructure, wi-fi access, data storage, phishing, software, bots, financial systems, etc.

## 2. Identify the potential consequences.

Cyber attacks can be very dangerous and hard to recover from. 60% of small businesses that fall victim to a data breach or cyberattack go out of business within six months. The results of a cyberattack may include stealing of private customer data, theft of money or business data, reputational damage resulting in loss of customers and sales, and legal consequences such as fines and regulatory sanctions.

## 3. Acquire the skills and resources or outsource.

Small businesses need to understand the potential risks of a cyberattack and build cybersecurity plans to help mitigate such risks. You can hire a cybersecurity specialist or outsource the function. Alternatively, small business owners can educate themselves or their employees on how to prevent cyberattacks. An online cybersecurity certificate teaches everything there is to know about securing a business from cyberattacks.

## 4. Install the best cybersecurity software.

Cybersecurity software helps to protect networks, systems and applications from unauthorised data access, cyberattacks and identity theft. Some types of cybersecurity software include antivirus, encryption tools, network security monitoring tools, firewalls, wifi protection, anti-malware, PKI services, endpoint protection, and cloud security tools.

## 5. Develop strong access control protocols.

An access control strategy will help companies determine and regulate those who need access to certain resources. To keep authorized users from entering the network, you can create personal accounts for all your employees and encourage them to use strong passwords. You can also limit employee access to servers, data systems and network administration.

## 6. Conduct regular data backups.

Regular backups are an integral part of data security. They ensure that important files and information are preserved for easy recovery. Hardware malfunction, computer viruses, human error and cyberattacks are common causes of data losses. You should always back up, safeguard and securely manage your data including those stored in the cloud.

## 7. Implement regular software updates.

Cybercriminals often enter computer networks through the vulnerabilities of outdated apps. It's important to install software updates on all network equipment, employees' computers and mobile devices. New software versions help to address old vulnerabilities, stay safe from emerging threats and improve upon features.

## 8. Develop a response strategy and disaster recovery plan.

A disaster recovery plan (DRP) is a well-documented approach that describes how a company can bounce back after an unplanned incident. It consists of steps that employees can take to resolve data loss and recover system functionality. An online certificate in cybersecurity teaches how to develop a DRP so business can resume after a cyberattack or other forms of disaster.

## 9. Run a penetration test.

After securing your business network and implementing cybersecurity strategies, you need to perform a penetration test. You can hire an ethical hacker or penetration tester to try to infiltrate your network to determine if there are weaknesses. This is necessary for eliminating any vulnerabilities and enhancing the security of your digital assets.

**Category**

1. Technology

**Date**
08/29/2025
**Author**
huubster