It’s a common misconception that cybersecurity is only for larger organizations. In fact, small and medium businesses often fall trap to security breaches because they are easier to target due to weak security measures. Hence, SMEs should be careful not to think that they are too small to be noticed by cyber criminals.

It’s easy to understand that small businesses don’t want to invest in cybersecurity due to their limited resources and small budget. However, in today’s era where every business directly or indirectly depends on the internet, it’s hard to completely ignore the necessity of adopting cyber security best practices.

It does not necessarily mean that you have to invest heavily. Instead, the focus should be on preventing the occurrence of a security breach with basic best practices. Let’s look at some of these practices for your small to medium-sized business for ensuring cybersecurity in your organization.

### Draft Cybersecurity Policies

Creating policies does not cost much investment. It only requires your knowledge and understanding of complying with security standards and frameworks. In order to ensure that these policies become well-documented within your organizational culture, draft them thoroughly and support them with checklists and schedules to ensure that new process are effectively implemented.

### Backup Data

### Ransomware attacks are on the rise, where the hacker steals and encrypts data unless they are paid a ransom amount. Even if the ransom is paid, there is no guarantee that the data will be retrieved in its original state. Instead of covering costs of both ransom and downtime, it’s better to safely back up your data on another location.

### Cloud services are common for backups. Not only do they allow data access from any location, they also offer security that is far more sophisticated.

### Review Access Permission

### Access control is one of the most basic steps towards ensuring security. A simple way is to restrict access to shared files and confidential applications according to job roles. Only provide it to people who are relevant to the specific source and need it to complete their job. Revoke access once it’s no longer needed by an individual. Do not give unlimited access to anyone only on the basis of seniority. Also revoke access soon after an employee leaves your company or changes a department.

### Consider Risks of Remote Working

### COVID-19 pandemic has made remote work a regular part of work culture. As convenient as it is in the current global crisis, it’s important to consider the risks associated with remote working. The more entry points are added to a network for cyber criminals to exploit, the more is the risk of a potential breach. Employees working from personal devices and unsecured WiFi can be dangerous for the business, and there is no check-and-balance to ensure they don’t use these mediums while working remotely. The only way to counter this threat is by creating a policy for employees to follow. It should state best practices for employees for using their own devices, including security software installation as well as installing patches as soon as they arrive.

### Train Your Employees

### Conducting training and awareness sessions is a good practice, but unless employees get a practical knowledge of why cybersecurity is important, they may not take it seriously. Its important to conduct simulations and security breach drills to give the staff a fair idea of how to avoid potential breach and act after a breach has taken place. Also teach them the importance of adopting password best practices such as keeping strong passwords and never to keep the same password twice.

### Implement Multi-Factor Authentication

### Two-factor or multi-factor authentication is common for businesses such as banks, ecommerce stores offering [online transactions](http://www.cardzgroup.com), and social media accounts. It adds an extra layer of security to a user’s accounts and does not allow anyone to access it even after entering a password unless they authenticate it with a second factor such as a code or a biometric impression. If you are offering services that require customers to create accounts, enable multi-factor authentication to ensure that your customer’s data remains secure. Encourage employees to do the same.

### Use Security Software and Tools

### In addition to password managers and cloud backups, invest in a good anti-malware software. Even after training, many employees tend to fall prey to phishing emails and other social engineering traps. Anti-malware can filter out phishing emails to prevent them from being successful. Also implement a firewall as your first line of defense to create a barrier between your network and attackers.

### Encrypt Confidential Information

### Enable network encryption to ensure that your data is securely transferred online without any threat of interception by a man-in-the-middle. Encryption will transfer your information into a secret code and prevent it from being tampered, read, destructed or stolen.

### Above all, make cybersecurity a part of your workplace culture.

### By combining regular trainings, new processes implementation and software updates for emerging threats, you can make significant improvement to your resulting business cyber security.