Cybercrime is considered as one of the most lucrative crimes today. The odds of getting caught are also low for well-planned crimes. Businesses are prone to cyber attacks because of their increased dependency on computers and digital systems. The growth in attack surface leads us to the question of how businesses can shield themselves from cyber threats. These threats may come from skilled cyber criminals, but we must also not ignore endless potential threats such as viruses, social engineering, malware and ransomware, and opportunistic hacking.

Whatever is the present state of security at an organization, one must strive to build stronger defenses to mitigate damage resulting from cyber attacks or to prevent threats from becoming an actual attack. Here are 8 tips that can help businesses protect themselves from cyber attacks

## Assess your cybersecurity measures

Without assessing your current cybersecurity measures, it is not possible to build adequate defense mechanism. Conducting regular cybersecurity assessments are essential to a good cybersecurity program as it highlights your strengths and weaknesses. It can help you prioritize your resources and save time and money that is otherwise spent on wasted efforts.

## Train your staff

Unlike common belief, employees are the weakest link in every organization in terms of security. Often the least informed employee can unknowingly expose your organization’s information to cybercriminals in the least expected way. It is important to conduct regular bi-annual or annual cybersecurity trainings for the staff to teach and remind them about how they can adopt safe practices. Trainings must include how to keep strong passwords, avoid social engineering attempt, identify phishing emails, and keeping their systems malware-free.

## Keep your software updated

Software that is used in your company must be regularly updated and of latest version. Old applications are more prone to zero-day attacks that can penetrate your network, steal information, and cause severe harm to your systems.

Though antivirus programs regularly get updated automatically, other applications may not do the same. It is important to check and manually update your software, if required. Also implement vulnerability management process that checks for exposed vulnerabilities and missing patches. Apply the required updates and patches.

## Implement real-time threat monitoring

Cyber attacks can happen from anywhere anytime. To detect an attack right when it occurs and prevent it from causing further damage, implement 24x7 monitoring on your systems and networks. This can be done by using an incident monitoring software that alerts of suspicious activity or a data anomaly that indicates that the attack is underway.

## Create an incidence response plan

A part of your comprehensive strategy involves being ready for times when an attack actually takes place. No security measures are 100 percent foolproof, so it’s important to have an incident response plan in place to immediately act after a successful attack happens. A good incident response plan lays out the escalation path, the steps that must be taken, and the roles and responsibility of all individuals who will be a part of implementing the plan.

## Implement Access Control

Your employees use different tools and access different information depending upon their job and role within the organization. Not all employees need to know about every information and data related to all departments. It is best to restrict access of a particular tool, network, system or information to only those employees who need it for performing their job. Make sure that only administrators can access full functionality of your network or systems.

## Assess risk associated with third party vendors

Many breaches in large business and global brands were a result of attackers exploiting a vulnerability found in suppliers and third-party vendors. Even with the best of security practices, your organization can still suffer from a data breach due to negligence and poor security practices by your suppliers and distributors. When choosing a vendor, always asses their security measures and ask questions such as how do they dispose off data? What do they do to protect their networks? Do they train their employees about security best practices like you do? Are they adhering to the regulations applicable to them?

## Be vigilant about hardware theft and physical security

Lastly, it is as important to safeguard your physical assets as it is to protect your information assets. If your staff uses mobile devices, tablets, or laptops through Bring Your Own Device policy, you must devise a plan to have [secure devices](http://www.cardzgroup.com/ContactSmartCard.html) and protect your data remotely. Employees have sensitive organizational data on their personal devices. If they get stolen, your information is also at stake. As a bare minimum, ensure that your information is protected through encryption.

## Conclusion

To keep your business safe from cyber-attacks, it is important to stay diligent and practices effective security strategies. Using the tips mentioned above, you can align your activities to the threats and help save huge costs that may be incurred as a result of losses resulting from a data breach.