It is often assumed that cybersecurity is a matter of concern for only large businesses and enterprises as they are more vulnerable to threats than other small and medium businesses. This is not entirely true, because in reality, small businesses equally face threats from cyber criminals. The reason is simple. Large corporations have more awareness, invest in protecting their valuable data and implement solutions to secure their informational assets. Startups and small businesses, on the other hand, have limited knowledge and budget and often overlook spending on cybersecurity, considering it as a secondary issue. This attracts cybercriminals who consider them to be easy targets.

A number of security experts have cited various reasons why small businesses attract criminals.

* Lack the expertise and budget for providing thorough security defense
* Don’t have dedicated cyber security specialists on their payroll
* Employees lack security awareness
* Security defenses may be implemented but are not always kept up to date
* Lack of risk awareness and risk management policy and procedure
* Failure in securing endpoints

Let us look at 10 important reasons why startups and small businesses should pay attention to cyber security.

1. **Hackers Want Information that Small Businesses Have**

While small businesses and startups may not have as many risks as large corporations, they do have employee and customer information. Hackers are interested in getting personal or financial information such as social security numbers or banking details, and small businesses are easy targets for them. Since criminals need [credit card or banking credentials](http://www.cardzgroup.com/ContactLessSmartCard.html), this information needs to be protected as much as possible.

1. **A Cyber-Attack Can Destroy Your Startup**

Startups and newly established businesses can be very fragile. They need to take many things into account and calculate risks in order to be successful and grow into an established organization. If your organization suffers a breach of data in its initial phases, not only will it cause reputational damages, it can also give you a major blow on your finances.

1. **Cyber Criminals are Always on the Lookout**

Cybercriminals never stop looking for opportunities to conduct malicious attacks. Since small businesses and startups are plenty in number, they present a big market for exploitation. Large corporations have the capability to enhance their security system and ward off hackers, pushing them to look for smaller and easier targets.

1. **Non-compliance can be Costly**

Cost of non-compliance with cybersecurity practices can be more costly than that of compliance in case of data breach. For compliance, you have to invest in cybersecurity solution alone, while in case of non-compliance, you will have to bear data breach costs, reputational costs and operational costs. Just like large corporations, small businesses also deal with technologies, processes and people, all of which can be targets of a cyber-crime. Hence, it’s misleading to think that small businesses don’t have to comply with data security regulations.

1. **Businesses Need to Attract and Retain Employees to Grow**

Professional and knowledgeable employees now understand the importance of their online privacy and security. If a potential or existing employee finds out that your workplace is not safe and is putting their personal data at risk, they will not like working for you. This may not seem like a reason big enough to implement cybersecurity, but for startups that already find it difficult to attract talent, it can be a matter of concern.

1. **Downtime can Break Small Businesses and Startups**

In the event of a data breach, most of the times hackers bring down critical network infrastructure and websites through DDoS attacks or other methods. Larger organizations are able to survive such attacks because of their resources to withstand them, such as redundant servers. Small businesses, however, simply don’t have such resources. Most of the times, they are unable to recover from such losses and shut down. According to the US National Cyber Security Alliance, [60% of small businesses close down](https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/) after falling victim to a cyber attack or data breach.

1. **Partners and Customers May feel Reluctant Working with You**

If your startup is not following safe security practices, people outside your organization such as third parties and customers may notice this and be hesitant in doing business with you. A potential partner will never want to work with an organization which can impact its business and put its assets in danger due to unsafe practices. They will always see you as a liability.

1. **Implementing Cybersecurity can Ensure Productivity**

In addition to reputational and financial damages, data breach incidents can destroy productivity in the workplace. When employees don’t have access to their networks and work files, they are not able to do their jobs. Small businesses and startups will be diverted towards recovering from the breach, ignoring other business operations. The best way to avoid this is to ensure cybersecurity best practices, to prevent potential data breaches.

1. **Cloud Services also Need to be Secured**

Because of their unmatched utility and affordability, startups and cloud services are adopting cloud services. Hackers are aware of this, of course, and cloud related cyber attacks have considerably increased as a result.

1. **It can Prevent Lawsuits and Legal Liabilities.**

Have you heard of instances where an organization had to deal with a lawsuit because an employee accessed prohibited content on a workstation? A cybersecurity solution can help detect and prevent employees from watching inappropriate content from workplace. It can also prevent legal liabilities that you may face from customers or suppliers when there is a data breach in the absence of cyber security practices.

**In a Nutshell**

Cyber threats are continuing to increase at an exponential rate, and small businesses are at risk of losing their finances, data, productivity and sales. Because any organization can become a prime target, it’s important to take all important steps for safeguarding their business technologies, information and processes. While small businesses may not be able to afford investing in hiring security experts or comprehensive high-priced security solutions, they can use other affordable services such as VPN tools and adopt cyber security best practices to succeed in the long run.