Where there is an asset, there are also security risks. Almost all the big IT companies (Facebook, Yahoo, Alibaba, Sina Weibo, MySpace, Adobe, etc.) got hacked and there was a data breach.

You might wonder, “**Do I need cyber security for my small business?**”.

If this is the case for you then you are at the right place. Here we will show you reasons why you need cyber security for your small business.

Cyber security is the process to identify vulnerabilities in your systems and networks and secure them by fixing those vulnerabilities. Whether it’s a big company or a small company, if those businesses are internet dependent, there is a huge security risk.

So, are you at risk?

According to the Data Breach Investigations Report from Verizon, there were **1,037** incidents, with **263** confirmed data disclosure in 2021, and most of the compromised data was Credentials (**44%**), the personal data breach was **39%** and other data breach was **34%**, also **17%** medical data breach.

Why Are Small Businesses Targeted By Hackers?

Most of the black hat hackers target small businesses because they have less security protection.

Here in small companies, finding vulnerabilities is much easier on their internet-dependent asset compared to other big companies like Facebook.

Below you will see some key factors why black hat hackers target small businesses more?

Customer’s Valuable Data

Your customer’s valuable data is one of the main reasons why hackers hack small companies. Whether it’s a small or a big company the customer’s data gets the same priority by hackers.

The hackers search for credentials, credit card information, medical records, Social Security numbers, bank account details, and other important information.

After they have that data they can easily sell it on the Dark Web at a high price, and also can impersonate banks to get money. Most of the time they purchase technical items using credit card information.

Computing Power

It's an attack, where the attacker sends enormous amounts of web requests to a website or websites. The computers they have compromised then support to create those artificially generated requests.

Later the hackers sell this DDoS service or the botnet on the Dark Web.

Weak Security Mechanism

This is an easy reason why hackers choose to hack small companies. Most of the small companies just focus on their product or service selling and marketing.

They are not much concerned about the security of their assets. Some of them don't have any security at all. So, this creates a great opportunity for cybercriminals to hack small companies.

Money

Your money is the number 1 reason why hackers target small businesses. You may say, "Small business doesn't have a lot of money". You are right, but the hackers are not just targeting a single company they target multiple companies. All the points you saw earlier are just to make money.

And this is the reason why ransomware is such a popular method of cyberattack. According to the Data Breach Investigations Report (DIBR) from Verizon of 2021 93% motive for hacking was Financial.

In our daily life in cyber security, we often face posts on Twitter, Facebook, and other social platforms saying that their data server has been compromised, small businesses falling victim to ransomware attacks by evil hackers.

All these cyber-attack happen because of the absence of cyber security awareness and practices. Below you will see,

Common Cybersecurity Threats for Small Businesses

Phishing Attack

It’s a very well-known hacking technique, where social engineering and technical skills work together. In practical phishing, campaign hackers create fake websites similar to banks, social media, Amazon, etc. and add malware to those sites.

Then they share the malicious site URL using email or other media. According to purplesec, **1.5** million new phishing sites are created every month.

Ransomware

Ransomware is one of the most common cyber attacks that hackers use. It is malicious software that will encrypt all the files of your computer.

Most ransomware uses asymmetric encryption which is impossible to crack(till now). And hackers demand a ransom amount to decrypt all their files, although even if you pay the ransom there is no guarantee that your files will be decrypted.

Software Vulnerabilities

Here hackers exploit common vulnerabilities of the software/operating systems used by employers and hack into their systems. E.g vulnerabilities in WordPress, MS Excel, MS Word, Adobe, Windows(OS), etc.

Those are some very common cybersecurity threats, but there are countless other methods of hacking.

But don’t worry anymore about getting hacked. Because we are going to show you the best security practice that you can follow and secure the assets of your small business.

Common Practice to Prevent Cybersecurity Threats

When it’s a matter of Cybersecurity threats prevention a lot can be done. But here you are going to know some must-take action to prevent cybersecurity threats.

Employee Trainings

That’s right you have to train your employee, from the information provided by CyberSecurityIntelligence 90% of breaches are caused by Human Error.

Technology can’t take action on its own (Artificial Intelligence is still developing), so there must be a human to command it for some action.

By training your employee about cybersecurity awareness and cybersecurity threats you are turning them into insider protection. So, the biggest disadvantage will be your biggest advantage.

Perform vulnerability assessments

In a vulnerability assessment, a pentester will perform a scan for vulnerabilities on digital assets, using both automated and manual approaches. This is a good way to know how secure your company is from the outside.

Then you can fix those vulnerabilities via your developers or you can also hire some professionals.

Deploy IDS(Intrusion detection) and IPS(Intrusion Prevention) software

The work of IDS is to monitor a network, which sends security alerts when detects suspicious events on a system or network.

And the IPS works as a shield between cyberattacks, it stops attacks from reaching targeted systems and networks.

Create DLP(Data loss prevention) Program

DLP is a process of stopping data breaches by detecting potential data breaches or data ex-filtration transmissions.

Final Words

Thanks for your time! I believe that now you have a good understanding of, “**Why does your small business need cybersecurity?**” and also “**How can you protect your**

business from those cyber threats?”

If you like this, make sure to share it with others so they can understand the importance of cyber security. As always, for any doubts or questions, please leave a comment below, or reach me on Instagram.

Pranjal Singhal

I am a freelancer Cybersecurity researcher and a digital marketer. I have already helped Top IT Giants to secure their web applications and maintain a safe environment for their users. Sharing and Caring is my motive. I love to guide beginners about making a successful career in the cybersecurity industry.