A Set of Measures to Protect Your Business Data

How to Protect Business Data

Cyber-security breaches are a burning issue casting a sinister shadow over a business landscape. When it comes to hacker attacks, nobody seems to be safe, not even corporate giants with fat budgets. Almost every successful company either operates online or has a strong presence in the cyber universe. But, you are far from powerless against dark forces. What you can do is come up with a solid plan and proactive measures. You will have to allocate resources wisely, show due diligence, and put in some serious effort. Here is how to make it happen and preserve the integrity of your vital data.



A lot is at stake

Keeping consumer data safe is paramount. A single, major breach could tarnish the reputation of the brand in an instant and leave the budget in tatters. It is very hard to mend the fences once the sensitive data ends up in the wrong hands or is simply mishandled. So, to thwart the cyberthreats, you need to put a solid security plan in place, as well as suitable technological protocols and processes. The upfront investment of time and funds may seem unpleasant, but that is nothing compared to potential consequences of inaction.

Facing the learning curve

It all starts with a shift in mindset and building awareness. The good news is that you have plenty of resources at your disposal. Seek security checklists that regulatory authorities make available. Educate yourself and look into past incidents, if any. Hackers these days are pretty cunning and tend to use social engineering rather than brute force. Know also where your data is stored and identify sensitive information. Weigh the pros and cons of using cloud platforms vs. keeping everything on hard drives.

Multiple protective layers

There are some basic measures that every business should introduce. One of them is certainly using strong passwords. Random strings of numbers and letters are the hardest to crack, so steer away from words that actually mean something. Also, try to use different passwords for each service, keeping them all in a safe place. Next, obtain a robust antivirus and anti-malware tools. Remember that when it comes to security software, it is equally important to stay updated. Also, be prepared to pay a bit in order to acquire maximum protection.



Wireless network defense

Wireless networks are a particularly popular target for hackers. And when you have many devices connected to it, you are exposed to the heightened risk. That is why many companies try to use the strongest possible router encryption standards. What is more, they protect both a Wi-Fi network and router with passwords. These measures should lower the likelihood of hackers hijacking account information, files, and sensitive data. Finally, consider disabling the SSID broadcasting feature of the router.

Virtual Private Networks (VPNs)

Consider employing an appropriate VPN solution. In a nutshell, a VPN creates an encrypted tunnel through which all your data travels. In other words, it acts as an intermediary proxy between your computer and the internet. You can hide your IP address and make it appear as though you are located somewhere else. Just mind that not all VPNs are created equal, so do your homework and select the one that suits your business

needs and budget. Some platforms come for free, but enterprise-level products could offer a stronger protection.

A holistic approach to data security

Furthermore, it is highly advisable to separate business and personal accounts (and related data). That way, you can prevent one breach from wreaking havoc on both ends. Pay close attention to what you upload to the internet (cloud). Ideally, all sensitive and personal data should be encrypted and some processes like email encryption can be automated. Make sure to monitor network activity and use two-step identification as another security staple. Know that most breaches take place not because of state-of-the-art hacker attacks, but human error and omissions.

Everyone on the same page

This brings us to the key point– bringing employees onboard with data security. Namely, be careful about implementing Bring Your Own Device policy. Yes, it may bring increased operational efficiency, but also create new security loopholes. So, makes sure to communicate potential risks and provide necessary training. All employees should be involved in keeping data safe. A restrictive website permission and network access policy is one of the best ways to address the problem. You can always hire a cybersecurity specialist in case you struggle to come up with solutions.

On the safe side

In recent years, security invasions are plaguing businesses and the plight is not going to disappear in the foreseeable future. On the brighter note, there is much you can do to avoid falling victim to attacks. Start by fostering a sense of urgency. Plan for data breaches and embrace a preventive approach. Keep up to date with evolving cyberthreats and best practices. Encrypt data, generate strong passwords, train your employees, and bust the cohorts of viruses and malware.

Following these steps, you should be able to stay out of the harm’s way and keep customers happy.

The post A Set of Measures to Protect Your Business Data appeared first on Go Media™ · Creativity at work!.

https://gomedia.com/zine/insights/how-to-protect-business-data/