How Much Does Cybersecurity Really Cost?

The majority of data is now stored online, but cybersecurity is a preventative measure that some companies need more than others.

April 23, 2021 5 min read

Opinions expressed by *Entrepreneur* contributors are their own.

With the tremendous advances in technology, the majority of business data is now stored online, making cybersecurity a must-have for all companies. However, cybersecurity is a preventative measure that some companies need more than others.

Before choosing a company to trust with your data, it's important to make sure you've taken the following steps.

Decide who will be responsible for your cybersecurity policies

- Even if you enlist another company, you still need someone within your firm to be the high-level decision maker, especially if there is a breach and action is required.
- Always plan, making sure you have the proper procedures in place is essential if you want to operate effectively.
- Define all staff members' responsibility for

cybersecurity, and make sure they know the consequences should they or your company fall victim to a cyber attack.

- Review your current policies regarding internet access (if you don’t have any, create some) for all company-owned devices. You can also make a list of products, software and employee devices on company property. Create an annual review for this, including staff training. Warn your staff about the risks involved in connecting to the internet, while demonstrating cyber breach prevention measures. They need to know that everyone is vulnerable to having their information stolen. Provide training and teach them how to spot phishing, viruses, malware and spyware, in addition to any other means by which various malefactors may attempt to seize access. Your staff needs to know the difference between a security breach and a data breach and how each can occur. Also educate them on who to inform should they fall victim to any breach.
- Ensure you have physical security for your office building, data center(off-site and on-site) and staff, especially if employees travel home with company devices.
- You need to set password policies and encryptions for all data.
- Make sure you have decommissioning procedures in place. Not all employees leave on good terms, but even those who do are potential targets. Have your IT department log all employees who own or lease company property. Record all employee IDs and set reminders for password renewals. For example, IBM has a 90-day policy for all devices, apps and software passwords. And back up all devices before wiping them clean.

Related: A Casino Gets Hacked Through a Fish-Tank Thermometer

Look at an outline of considerations when planning your cybersecurity procedures and policies. However, hiring a company with cybersecurity expertise can help you manage, implement and maintain your plans to keep your business, staff, and data safe and secure.

Costs involved in cybersecurity

Like any business decision, you need to research and compare options before planning out your next steps; cybersecurity is no exception. Many companies provide cybersecurity, so the first step is to get a list of all the best services, and then compare the plans, features, and prices.

The consequences of falling victim to a cyber attack can be detrimental to your brand and reputation and may also result in financial loss. To ensure that your organization is secure, it’s crucial to balance the threat with the business’s risk appetite and your skill set in-house before considering the appropriate technical controls or deciding what kind of external resources are needed to help support you. Considering these different elements will allow you to develop a cost-effective cybersecurity programme best suited for your organization’s needs and size.

Cost analysis and planning

Cybersecurity risk assessment. Most companies allocate an entire budget to cybersecurity; this is a mistake. Instead, complete a risk assessment to understand what risks can lead to:

- Software or operational downtime.
- Loss of business, customers, money.

- Damaging a company’s reputation.
- A data breach or security breach. You can use tools to complete the analysis, like risk matrixes, which can help you understand, budget and address unforeseen threats.
- Size analysis. Hackers and cyber attackers can have a variety of motivations from addressing political injustice, gaining money or releasing privileged information to the public. However, no one knows until it’s already happening. A bank or financial institution is a good example. The hackers can release information, steal it, sell it to another company, or simply access clients’ money.
- Operations and activities. Create an operations model for your business, outlining your cybersecurity needs. Decide whether you want the unit to be in-house or outsourced. Include activities like training, staff awareness policies, procedures, security tools and upgrades. You can add any factor that might be necessary for your business model.

How much to spend

As we’ve discussed above, multiple factors play a part in cybersecurity. So let’s dig a little deeper. No company has the same budget for cybersecurity, but many include it in the budget for the IT department. Your account needs to fit into your business size and risk evaluation.

According to CyberShark, industry leaders like IBM feel that “a healthy cybersecurity budget should make up nine to 14% of your overall IT department’s annual budget.” The reality is, you might spend less than 6% of your budget on risk management and security.

Related: A Ticking Time Bomb: Mainstream Messaging Apps Are Killing Your Company's Security

No business can predict when or how they will get a cyber threat, but they can fortify vulnerable systems in advance. A cyber attack can make or break a company depending on how prepared they are. Look at it this way: Cybersecurity is an investment, not a liability.

https://www.entrepreneur.com/article/367141