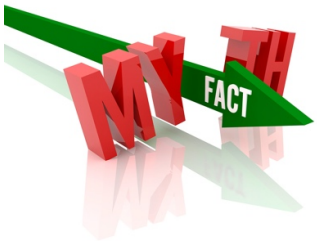
CISO ToGo
Technology Risk Consulting



Top 3 Cybersecurity Myths For Small and Mid-Size Businesses

If you follow ANY news these days, you can't help but become aware of more and more data, privacy, and/or security breaches, along with how customers of those businesses impacted are also affected by them.

To be honest, given the volume of these incidents, it would be understandable for small and mid-sized businesses to simply give up and believe that if larger enterprises are defenseless against them, then they must certainly be as well! Additionally, a common misunderstanding of small to mid-sized business is to believe that they simply aren't worth the hacker's time and effort, leading to even more haphazard cybersecurity practices. Quite the opposite is true, however, as most hackers have an even greater understanding of the value of the data they are stealing than the organization being compromised!

This sort of defeatist thinking can be very harmful to your business and leave your private data (and that of your customers) even more vulnerable. In fact, the growing number of disclosed incidents means that cybersecurity measures need to taken even more seriously! Appropriately implemented, these measures can effectively minimize your risk of a breach and will help to instill customer confidence.

Below are three cybersecurity myths that your business should simply NOT believe!

1. We're Too Small To Be Hacked

As mentioned above, a significant miscalculation made by small & mid-sized businesses is that they believe they are too small to be the target of hackers. This error in judgement can lead businesses to believe that they don't have to invest in their cybersecurity. However, the opposite is quite true. Hackers target small businesses because they are easier to attack. Since these organizations have a lot of data but little protection, it is actually easier for hackers to successful gain access to the information they want.

2. Cybersecurity Is IT's Problem

It's easy to push the problem to be the responsibility of the IT department (if you even HAVE an IT department!), but that thinking doesn't solve anything. The security of an organization's data is not an IT problem, but rather a problem for the business as a whole to ensure is addressed. Granted, the IT department (again, if there is one) needs to protect the data and understand how it's important, but the business needs to also understand how it's important, and how it can be appropriately secured, backed up and restored if it was to ever be compromised.

3. Antivirus Means We're Covered

Having a decent antivirus program is important and a good start … but it is simply NOT enough. Antivirus programs can protect you from certain attacks but won't be able to protect you from others. That's why it is crucial to have a multi-layered approach to security … thereby ensuring that you have other ways to cover your security needs. For instance, no antivirus program will ever be able to address human error due to phishing emails or other mistakes (this would require established cybersecurity guidelines for employees to follow).

The Bottom Line …

Small to mid-sized businesses need to be prepared for the risky world in which we live and operate … and that's where **CISO ToGo** can help. You will find that we understand the cybersecurity needs applicable to YOUR business and we are uniquely positioned to help you satisfy them! To find out more information, check out our services listed on our website (www.CISO-ToGo.com).