It seems like I hear about a U.S. business getting hit by a new, major cyberattack every week. As a whole, cybercrimes have increased by 600% since the start of the Covid-19 pandemic. In all the uncertainty of the past year, one thing we can be certain of is that cybercrimes will only continue to increase. In fact, 69% of organizations no longer believe that attacks can be prevented through antivirus software, and 61% of cyberattack victims were small businesses. At this point, the question is not if you will experience a cyberattack, but when, and how bad.

For decades, the go-to system for securing a network was the 'castle and moat' technique where all outside traffic was considered a threat, but everything within the network was considered safe and cleared for access. 'Castle and moat' security systems are outdated and no longer effective at preventing breaches. Businesses formerly had corporate data centers with contained networks, but with the ubiquity of cloud-based services combined with internal applications, it no longer is safe or effective to trust all internal traffic. With the 'castle and moat' notion of security, when an attacker gains access to the network, they can easily move through the internal systems. Furthermore, due to the pandemic, employees are accessing company networks through a myriad of outside areas, blurring the perimeters of once clearly defined networks, and requiring more comprehensive security systems to be put in place.

One such security structure is called zero trust security. Zero trust security is an umbrella term for an assortment of different applications and system management techniques. The core concept behind zero trust security is the belief that businesses should not automatically trust anything (devices or users) within or outside their networks. Essentially, this means putting in place administrative policies and applications that require authentication of all users and devices before they can connect to the network.

The foundation of comprehensive zero trust security begins with micro-segmentation and granular perimeter enforcement. This means that you are protecting your network by dividing all data and programs into distinct segments for each user's workload, providing access to only what they need. Also called identity and access management, this style of data and program compartmentalization is used for employees as well as customers and partners to ensure that no user could be compromised and lead to a breach of all the data on the network.

Your login process:

After creating a solid security foundation through micro-segmentation and granular perimeter enforcement, the next step is securing the login process. Humans are fallible, so often, the biggest risk to your network is a user making a mistake and compromising their login. While an attacker would not have access to the entire network through proper micro-segmentation, it is still an enormous security risk. To prevent the compromise of individual users, you need to maintain one digital identity per user and modify it as needed depending on use. Not only is it important to verify a user's identity through their login credentials, but it is also crucial to verify all aspects of their access including the device they are using and where they are accessing the network from.

One of the easiest and most important parts of identity and access management is multifactor authentication. The simple addition of a login prompt on another of the user's devices is an enormous obstacle for an attacker even if they have the rest of the login credentials. A 2020 Forrester survey found that 53% of information workers secure their passwords insecurely, creating a security risk of massive proportions. When passwords are stored in plain text, it is extremely easy for an attacker to gain access to your login credentials. With the addition of multifactor authentication, your account is infinitely more secure, even with a password stored in plain text. The simplest way to secure all your accounts is through password management software that encrypts your passwords, allows you to autogenerate passwords, and

has a system for multifactor authentication. One of the most popular systems is Last Pass, which we discuss in more detail here.

For administrators:

There are a variety of systems that can be used in identity and access management. They provide administrators with the tools needed to manage their users at all levels. Administrators need to be able to change user roles, track user activities, and enforce corporate or government policies to ensure system security. Also, administrators need the ability to manage company devices against physical compromise, so these applications provide the ability to deauthorize or wipe stollen or missing devices. Identity and access management software allows administrators to do this efficiently and on an ongoing basis to ensure the safety of your data.

Zero trust security is not a simple fix but is a broad term to encompass the ongoing efforts of IT administration that are required to secure your business from cyber-threats in a time when anyone and everyone is at risk. Zero trust security is not a one-size-fits-all approach to security. Instead, it requires an in-depth understanding of your specific business's needs and data flow through your systems to create efficient and comprehensive protection against threats.

Team Tobin is committed to a better technology experience. We will work with you to understand the complexities and nuances of your business's technology needs and provide an efficient and comprehensive approach to zero trust security, tailor-made to best suit your individual needs. Every business has unique needs and expectations, so by working with our team, we can provide exceptional service that specifically suits your business.