bullseye
Communications. Cloud Technology. Peace of Mind.

Communications Security –
Keeping Your Information Safe and Secure

Like many other tools, security technology is evolving – in part because threats are becoming more complex. What used to be simple attacks on one device have evolved to target every device on a network. This problem means the technology that was top-of-line several years ago is probably outdated today. As a result, 62% of organizations plan to increase cybersecurity spending in 2020. Of those, technology companies will see the biggest increase (73%) followed by manufacturing (68%) and retail/wholesale (67%). (source: Enterprise Strategy Group)

And because there is no such thing as a future-proof solution, businesses need to continually evaluate the security around their communications technologies. Many businesses may believe they are too small to be targeted, but the reality is that their lack of security requirements and resources makes them a more desirable target.

This is a critical error. Regardless of size, industry, or nature of their business, every company needs security to guard their information.

"Ignorance is Bliss" – A Dangerous Mentality

In some cases, business leaders believe what they have in place is good enough – that the surface defense security implemented years ago will suffice, or that their information is safe because they haven't been hacked. Again, critical errors. Companies need to look at defense in depth and have different types of network security in place so if a breach occurs in one segment of the network, it cannot extend to other, potentially more-critical segments.

This is especially true in today's business environment with the emergence of IoT solutions and an increase in employees working remotely – a trend that is expected to continue for some time. Additionally, technology over the past few decades has become an increasingly integral aspect of the workplace. From email correspondence to financial transactions, professional networking, and collaborative work documents, technology is crucial for businesses to stay connected and operate efficiently.

Be Smart, Safe, and Secure

One trend in communications security is **zero-trust connectivity**, which gives the company control over what each computer can access. Zero-trust connectivity differs from a traditional virtual private network (VPN) in that companies can give access to specific applications on specific servers without opening access to other applications on the same server. Leveraging this new technology can prevent unwanted access to greater and potentially unknown segments of the network infrastructure. Another approach related to zero-trust connectivity is **segmenting** internal networks so servers, computers, and even different departments operate on different networks. This approach ensures that if one network gets attacked, only those on that network – not the entire organization – are affected.

Another related trend is **endpoint protection**, which puts security on the laptop – not just the network. If the user's computer becomes compromised, it can be isolated from the corporate network until the trouble has been remediated. And with more and more people working remotely, this trend makes sense. Why have security solely on the network in the office when many people are externally accessing via individual laptops and access points?

There's even the use of **artificial intelligence (AI)** in communications security software. Today, software can do some behavioral analysis – something security software doesn't traditionally do. These days, malware is rarely reused, so with hackers making custom malicious, you need software that looks for malicious execution and not just definitions from a blacklist. Also, with AI security software, there are shared databases so when a vulnerability is found in one company or computer, details can be shared across the globe to prevent it from happening somewhere else.

We're even seeing the use of passwords evolving. **Two-factor verification** requires the traditional username and password but adds another method of verification such as a text message to a cell phone or a one-time use password to a multi-factor authentication application. In the past, this approach was used for specific activities – VPN for example – but as cloud-based activities grow, it's used more and more. Two-factor is also beneficial because many individuals reuse passwords or create simple ones such as "12345" or "password." To address the varying complexity and use of passwords, there is **password manager software**, which generates unique, long, complex passwords for all online accounts.

Take That First Step

Before your company's information can be safe and secure, you need to acknowledge that security is a priority. Work with the IT department to identify and evaluate your current processes, equipment, protection, etc. Consider bringing in a partner to review your current set up, identify needs, and create a course of action. As with any partner, be sure to find one that is knowledgeable, reputable, and provides services to companies similar to yours. Don't be afraid to dive in and learn more about your security – it's better to find and fix problems before they are used against you.

At BullsEye, we have experts to help clients identify security risks and find solutions to ensure their company information is safe and secure. If you'd like to learn more about security for your communications services, contact us at **877-438-2855** or **sales@bullseyetelecom.com**.