Advancing network security while driving customer integration

A deeper understanding of your networks and the threats they face is a must for any business. We always talk about managing networks and network development — which are important — but network security is just as essential because if your networks aren’t secure, it can severely impact your business and its future.

Temps de lecture : minute

4 January 2023

When we talk about network security, it’s important to understand not just how it affects your company internally, but externally as well. For example, while it’s important to advance your network security for internal operations, like *network communications* between teams and departments, it's also crucial to think of network security with your customers in mind.

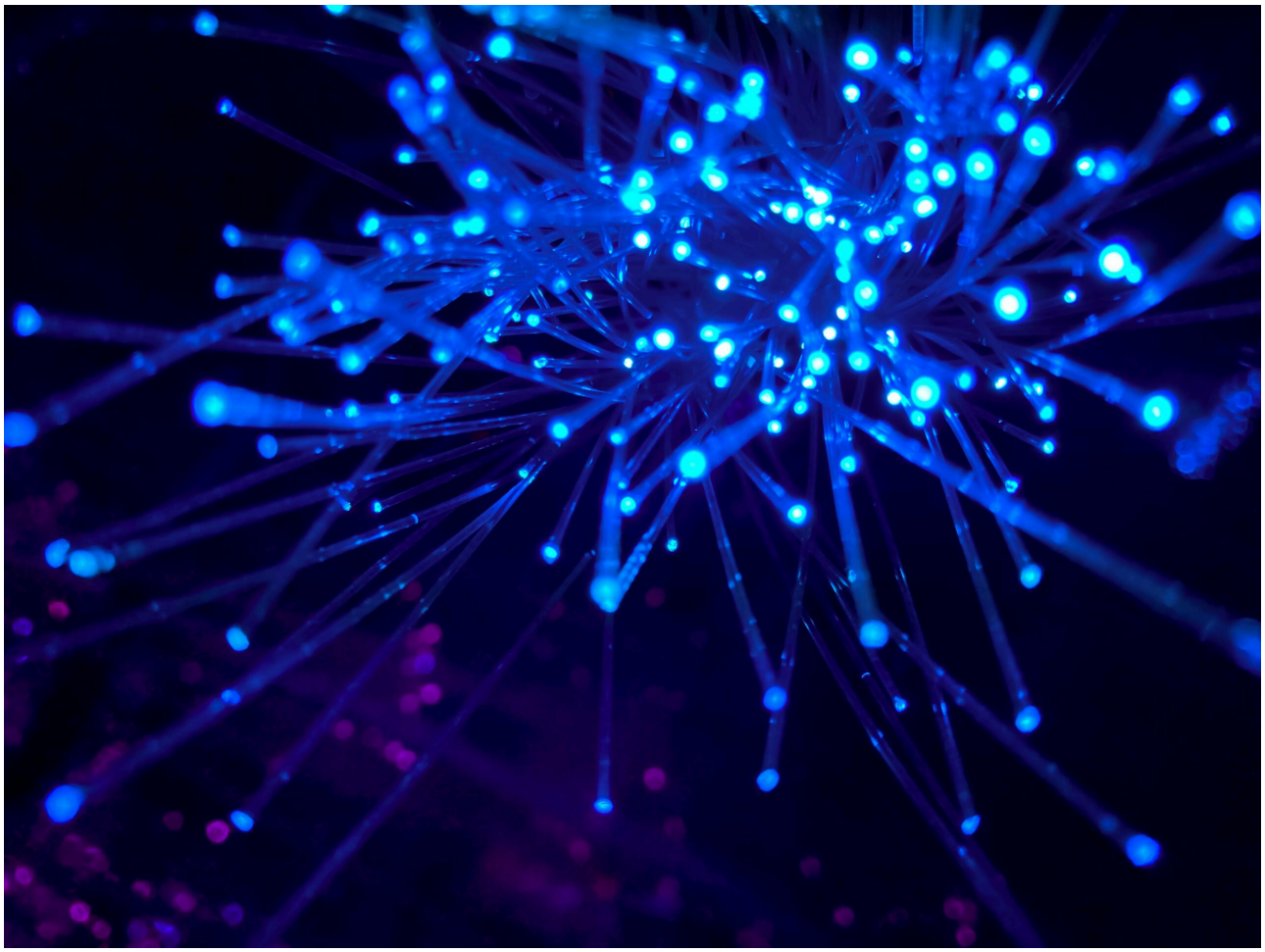
In fact, when dealing with customers, network security isn’t just a must to avoid data breaches; it can also help you improve customer satisfaction. Customers appreciate companies more when they go above and beyond to give them a quality experience, which includes upgrading your security measures to protect their sensitive data.

What are some of the most common network security threats?

In today's highly digital world, there are cyber threats coming from just about everywhere. Nothing is safe today unless you put the effort into developing a solid network security strategy. And being able to develop a

strategy starts with *knowing your cyber risk* and where these threats are coming from.

Look at the Internet of Things (IoT), for example. The IoT is essentially a network of connected devices or systems that has become increasingly popular amongst businesses today. Being more connected has numerous benefits, and this is a great advancement in technology. But when things are more connected, it also makes the data being shared and transferred more vulnerable. This makes the Internet of Things more like an *Internet of Threats*.



Read also
IoT: An Internet of Threats?

There are many ways that IoT networks and other network systems can be hacked or attacked. Some of the most *common network security*

threats today include:

- Malware attacks: This includes computer viruses, trojan horses, adware and spyware, rogue security software, and computer worms.
- Phishing scams: This involves someone or something pretending to be something else in an effort to gain access to sensitive data. The most common types of phishing scams are phishing emails, but phishing can also happen over the phone or through social media as well.
- DoS and DDoS attacks: These are common network attacks that target website servers. They essentially flood servers with data to overload and crash the system.
- SQL Injections: A lot of companies use SQL servers for their websites and applications to store user data. An SQL attack happens when someone inputs malicious SQL queries into the web application in an effort to steal sensitive user information.
- Privilege escalation: This is a group of networking attacks that cybercriminals use to increase their access to data by gaining unauthorised access to a network.

How improving your network security can boost the customer experience

When customers interact with your company, they are often sharing sensitive data with you through your networks, which makes them vulnerable and can put them at risk of having their information stolen. Thus, it is the duty of any company to prevent the misuse of a customer's information by improving its cybersecurity strategy.

However, advancing your security strategy to protect your networks and customer data doesn't just have the benefit of preventing data breaches. Upgrading your *cybersecurity can also improve customer satisfaction*.

Customers lose their trust in a brand when their data is compromised, and

the likelihood of them remaining loyal customers is significantly reduced. Not only that, but data breaches can tarnish a brand's reputation so much that it can struggle to gain new customers.

This is why network security is so important. When businesses take the time to focus on their cybersecurity, they strengthen their customer integration by ensuring their customers have a safer, better experience overall and are thus more satisfied.

Tips on improving network security with your customer in mind

There are many ways to improve your cybersecurity strategy. Whether you need *network security for a small business* or a more thorough and high-end security strategy for a bigger company, there are solutions for every business.

Some of the best tips for keeping your network safe and secure include:

- Conduct a network analysis. When businesses experience *network downtime*, they often conduct an internal and external analysis to determine the points of failure. And this same method holds true for improving network security. The best way to determine where your networks are weak and can be hacked is to conduct a thorough analysis, which includes doing something called penetration testing. Penetration testing is the process of trying to purposely hack your own network or system to help you expose vulnerabilities and deal with them before they become an issue.
- Upgrade to a secure cloud network. Another solution to both avoiding network downtime and improving your security is upgrading to a better cloud-based network. The cloud on its own is already a more secure way to store and share data, but you can also look into additional cloud security and cloud management to boost your overall

network and data security even more.

- Use a firewall. A firewall is essential as it helps secure and lock down the ports of entry that hackers often use to infiltrate networks and steal data. The stronger your firewall, the harder it is for hackers to find a way in.
- Update your firmware and antivirus software. Firmware is notoriously weak and leaves companies and their customers' sensitive data vulnerable. So it is crucial that you update your firmware to the latest versions often to avoid falling prey to firmware hacks. Antivirus software is also a must and should be updated regularly as well. Cybercriminals get more clever by the day, and they are constantly upgrading their attacks and viruses. So it is crucial to regularly update your antivirus software as this ensures it is up-to-date and able to handle the latest viruses and malware.
- Have a data recovery plan. Finally, every cybersecurity strategy should include a backup plan. No matter how hard you try, you can still get breached. But how you handle that breach can make a huge difference to both your company internally and your customers and their experience. The better prepared you are to handle a breach, the better you will be able to keep your customers safe and maintain their interest and loyalty.

Better security, happier customers

Network security plays a significant role in customer satisfaction. When customers are constantly having to share their information digitally, it increases their concern about their safety. So if you want to retain your customers, experience better customer integration, and expand your reach to new customers, you must make the effort to show them that you have their best interest in mind by keeping their data safe and secure.

Article by Indiana Lee