[Title:] Four cybersecurity considerations for when it happens, not if

[Subtitle:] A free cybersecurity assessment will identify vulnerabilities

[Client:] XYZ Solutions

Cybersecurity attacks are a little like shark attacks—most people know they're possible, but they tend to happen to *other* people, so nobody prepares for them. But cybersecurity is a very real problem. (And, for the record, thousands of times more common than a shark attack.)

As a broadband service provider, the cybersecurity of your customers is in your hands and protecting their data on your network is crucial to your reputation and your ability to do business. With that in mind, here are four cybersecurity issues you should know about and consider. **Below these four points, find out how to get a free security assessment from XYZ Solutions.**

1. **Risk analysis.** When it comes to risk, there are many categories to consider: devices, systems, data, personnel, supply chains, suppliers, third party vendors, and so on. Any of these (and more) might be the culprit—however unintentionally—behind a cybersecurity breach. Completing a risk assessment and, better yet, having a risk management strategy, is vital. Identifying cybersecurity risks is also a key requirement of many federal and state broadband grant programs.

2. **Security patches.** When automated reminders pop up letting you know that a security software update is available, what do you do? Do you maintain the security of your systems by installing security patches? It may be a hassle to update your software again and again, but there's a reason those patches exist: they often solve cybersecurity issues or vulnerabilities. Many cybersecurity breaches are due to unpatched software (estimates vary from a third to nearly 60%).

3. **Antivirus software.** Antivirus tools help protect you from the most common cybersecurity attacks: viruses, "Trojan horse" attacks, spyware, ransomware (which is on the rise), and many more. Antivirus software is not created equal—often you get what you pay for—but it's a key component of any cybersecurity arsenal. Business News Daily sums it up: "Although antivirus software can't completely protect a business's systems, these solutions are still necessary."

4. **Network configuration.** Network setups include varied devices like servers, switches, firewalls, routers, and systems for domain names, intrusion detection, and more. The U.S. Cybersecurity and Infrastructure Security Agency says, "These devices are ideal targets for malicious cyber actors because most or all organizational and customer traffic must pass through them." You can't stop an end user from clicking on a malicious link, but your customers expect their broadband service provider to maintain a secure network.

Cybersecurity is—or at least it should be—among the most pressing issues for broadband service providers. XYZ wants to help you and your customers stay safe. For a limited time, we are offering a **free security assessment**. We'll review your IT infrastructure and create a personalized audit of your network—absolutely free.