FIBER-OPTIC NETWORKS AS A FIRST LINE OF DEFENSE IN CYBERSECURITY FOR BUSINESSES

HACKERS ARE CONTINUALLY CREATING NEW WAYS TO STEAL PRIVATE DATA. CASE IN POINT: CABLE TAPPING. THE VULNERABILITY OF CABLE INTERNET CAN'T BE TAKEN LIGHTLY. THE FACT IS, DATA THIEVES CAN EASILY HACK INTO CABLE INTERNET TO STEAL CRITICAL BUSINESS AND CUSTOMER INFORMATION. THE NEGATIVE IMPACT ON BUSINESSES IS STARTLING.

THE CONSEQUENCES

According to a 2018 study by IBM and the Ponemon Institute, a data breach can cost a company $3.86 million, on average. Small businesses that fall victim to hackers lose between $84,000 and $148,000. In both cases, aside from the obvious loss of business that comes with a breach, there are also many "hidden costs." From the negative impact on a business' reputation to the time employees spend on recovery and customer notification to legal and regulatory activities and fines, the cost of a data breach can cripple any company, whether large or small. In fact, 60% of small businesses shut down within six months of a cyberattack. It's easy to think it will never happen to you. But, when almost two-thirds of data breach victims are small to mid-size businesses, it's better to be safe than to risk your business and reputation.

LOGIX FIBER NETWORKS

THE SOLUTION

While protecting your network can be expensive and complex, requiring IT and security specialists that you may not have the resources to retain full time, there are steps you can take and solid alternatives to consider. For instance, the right network partner can serve as your first line of defense against cyberattacks. **Here are some things to consider:**

DEVELOP A NETWORK SECURITY PLAN

Every business should have a written (and thoughtfully prepared) network security plan in place. A thorough plan will include:

- **Acceptable use policy** to specify what types of network activities are allowed and which ones are prohibited.
- **Email and communications policy** to help minimize problems from emails and attachments.
- **Antivirus policy** to help protect the network against threats like viruses, worms, and Trojan horses.
- **Identity policy** to help safeguard the network from unauthorized users.
- **Password policy** to help employees select strong passwords and protect them.
- **Encryption policy** to provide guidance on using encryption technology to protect network data.
- **Remote access policy** to help employees safely access the network when working outside the office.
- **Software update policy** to ensure the latest patches and security updates have been applied.

INVENTORY YOUR CURRENT SECURITY TECHNOLOGIES

A secure business network should include the following technologies. The right network provider can deliver these critical security features.

- **Firewall** to keep unauthorized users off your network.
- **Virtual private network (VPN)** to give employees, customers, and partners secure access to your network.
- **Intrusion prevention** to detect and stop threats before they harm your network.
- **Content security** to protect your network from viruses, spam, spyware, and other attacks.
- **Secure wireless network** to provide safe network access to visitors and employees on the go.
- **Identity management** to give you control over who and what can access the network.
- **Compliance validation** to make sure that any device accessing the network meets your security requirements and security updates have been applied.

FOCUS ON RETURN ON VALUE VERSUS RETURN ON INVESTMENT

Seriously consider the harm a network security breach could do to your business, in lost revenue or as the result of customer litigation, for instance. Exactly what are your company's digital assets (intellectual property, customer records, etc.)? What are they worth? Ask yourself the hard questions:

- **Finances:** What is the potential financial impact of a network outage due to a security breach?
- **Disruption:** Could a security breach disrupt your supply chain?
- **Insurance:** Are you insured against internet attacks, or against the misuse of your customers' data? Is this insurance adequate?
- **Recovery:** Do you have backup and recovery capabilities to restore information, if necessary, after a security breach?

CHOOSE FIBER-OPTIC INTERNET

The right network provider can serve as your first line of defense against cyberattacks. Specifically, a fiber-optic internet provider can offer a secure network that is not at risk of cable tapping like a cable network. Unlike cable networks, fiber-optic networks are built with underground wiring, making it virtually impossible for hackers to gain physical access to your network.

ABOUT LOGIX AND LOGIX FIBER NETWORK FIREWALL

Since 1982, LOGIX has been providing enterprise-class, highly secure, fiber-based data and voice services that allow secure data transferring, video conferencing and streaming media for businesses. LOGIX Fiber Network Firewall creates a clean, secure connection to the internet, securing your business-critical data and blocking threats before they reach your network.

FINALLY, DON'T BE TEMPTED TO CONFRONT SECURITY CONCERNS WITH A PIECEMEAL APPROACH. INSTEAD, CREATE A SINGLE, UNIFIED STRATEGY THAT PROTECTS YOUR WHOLE NETWORK. MAKE SURE YOUR POLICIES ARE BACKED BY A NETWORK PARTNER WITH THE TECHNOLOGIES IN PLACE TO DETER CYBERATTACKS.

REQUEST A COMPLIMENTARY CONSULTATION

Contact LOGIX to learn more about safeguarding and protecting your business from cyber threats.

LOGIX FIBER NETWORKS

visit LOGIX.com or call 1-888-505-6449 to schedule a complimentary consultation.