corsica technologies

Top 7 Security Questions You Need to Answer For Your Business

Today's cyber threats continue to evolve and grow more sophisticated. There are phishing campaigns, malicious websites, ransomware, malvertising, DoS attacks, man in the middle attacks, brute force attacks and more. Yet, many businesses remain ill-prepared to combat them.

The reality is that without proper due diligence and an investment in effective network security solutions, a business that falls victim to a cyber-attack will face significant losses.

Which is why the best defense against cyber-crime is taking a proactive approach to network security. Here we put together 7 security questions that you can ask yourself in order to understand just how prepared your business really is (or isn't) for a cyber-attack.

Top 7 Security Questions You Need to Answer For Your Business

1. Can your employees tell the difference between a phishing email and a good email?

In an analysis of data breaches, Verizon found that 90% of them had a phishing or social engineering component. The lesson here is that no matter how strong your network security is, or how protected you think you are, one bad click by any one end-user on a phishing email is all it takes to create a disaster. End-user training and education cannot be overlooked when considering your network security.

---

2. Do you KNOW if your data is protected…or do you just think it is?

Proper data backups management means much more than just setting up backups…and then forgetting about them. It means testing the backups on a regular basis, deploying a hybrid solution that allows you to continue to function if disaster strikes, and having a plan for how to access the data when you actually need it.

3. Does your wireless network have unauthorized systems on it?

While a Wi-Fi network is now a staple for the modern business, how it gets configured and secured is an important consideration. Allowing guest access may be standard practice, but in doing so are you inadvertently allowing unauthorized users access to confidential business data? Having the right hardware and the right technical guidance are critical in protecting your information.

4. What do you have in place right now to protect your network?

Modern business demands a modern network security solution. Yet far too many businesses fail to invest the time and resources required to implement the layered approach that includes everything from firewalls management to patch management to end-user education and training. Start with understanding what you do have, and then identify what needs to be enhanced.

5. In the event of a disaster, will you be able to keep your business going at the most basic level?

Hope is not a strategy, and just hoping that your business won't get targeted is a losing proposition. By planning for WHEN - and not IF - you get hit with a cyber attack, you can implement the policies, processes and technologies that will allow you to operate "business as usual" even in the face of a cyber attack (or a data disaster created by human error). This type of Disaster Recovery planning can make the difference between simply surviving a disaster and actually thriving during one.

---

6. Are you at risk of being sued if an employees loses a laptop or mobile device?

In our always-on, always-connected society, mobility is a modern business need. But the secondary - and all too often overlooked - need is how to secure laptops and mobile devices against unauthorized use in the event they are lost or stolen. Your customers trust you to protect their data and in this new age of compliancy concerns, failure to do so could easily result in legal ramifications.

7. Who is actively managing your network security strategy?

Good network security is not a "set-it-and-forget-it" proposition. Businesses today face increasingly sophisticated threats every single day. In order to protect against them, you must actively manage network security, ensuring that security patches are applied, technology isn't out-of-date, threats are monitored 24/7 and end-users are educated and aware. Anything less is putting the heart of your business at risk.

Simplify and improve your IT strategy with Corsica Tech's managed IT solutions. You'll get timely support 24/7, fewer disruptions to everyday operations, peace of mind that the heart of your business is protected, and dedicated account management support from our top-notch team of friendly professionals. You already know good IT management is important – let us make it a priority.

corsica technologies
www.corsicatech.com

PH: 877-367-9348