9 QUESTIONS

for your IT provider to assess your company's vulnerability to cyber attack.

Did you know that small businesses are just as vulnerable to cyberattacks as large Fortune 500 companies? Sure, you've heard about the attacks on Target, Equifax and Marriot, but cyberattacks on small businesses are more prevalent than you think. According to a recent report by Ponemon Institute, 67 percent of companies with less than 1,000 employees have fallen victim to a cyberattack, and 58 percent have experienced a data breach.

What's more, in 2019, it costs companies on average $114,000 to recover from a data breach and 60 percent of small businesses could go out of business due to damages associated with a cyberattack.

Why do so many companies fall victim to a cyber attack?

Because these businesses aren't preparing to meet these attacks head-on.

They are making the common mistake of spending their money on protection, when they should be spending it on detection. Detection can identify and eliminate the risk before it becomes a huge problem.

What about your business - is it safe from a cyberattack or data breach?

Not sure?

One way to put your mind at ease is to ask your IT provider what they're doing to protect your business. If they say, "we've got it covered," don't be so sure. Probe further.

To find out how if your business is vulnerable to cyber attack - here are 9 questions you can ask, followed by the answers you should be getting to let you know how vulnerable your business really is.

Question 1: How do we enable our employees to keep our data protected?

What you should hear: 94% of malware is delivered via email, so employees are the first line of defense. We provide regular cyber security awareness training including phishing simulations and training videos to provide them the current information they need to help us keep things safe.

In addition to providing Security Awareness Training for our staff, we also have email security filtering on all email accounts to minimize email scams and a documented process for reporting a cyber incident.

Question 2: Do we have password policy and how is it enforced?

What you should hear: It's critical that we not only enforce our password and acceptable use policies, but we document them, too. Would you like to see them?

Even with a password policy in place, there are no guarantees that credentials aren't stolen by other means, such as a phishing email scam that tricks a user into giving up their credentials. For this reason we also monitor the Dark Web to ensure we're aware of any stolen credentials and that user names and passwords are safe.

Question 3: Do we have client data or personal information on our network and is it properly protected?

What you should hear: We do have client data, including personal information, on our network, but rest assured, it is properly protected with the most up-to-date methods. If it's not, our business reputation could be at risk and the financial ramifications could be brutal. In addition, we also ensure our encryption service meets our compliance requirements.

Question 4: What are the top threats to our business right now?

What you should hear: Threats are always changing and evolving. For context, 300,000 new pieces of malware are created every day. These could be viruses, spyware, adware or something else all created with one goal in mind: to ransom or steal our data. And that's just one example of the types of threats that are out there, so it's important that I stay current on what's trending and how to prevent it from becoming our issue.

In addition to Anti-Virus software updates, our company has also deployed Endpoint Detection and Response to detect any potentially malicious behavior happening from the inside of our organization.

Question 5: If we are attacked, how fast would we know it?

What you should hear: According to Cyber Observer, the average lifecycle of a data breach is about 11 months. On average, it takes about seven months to detect a breach, and an additional 4 months to contain it. That's a lot of time. We not only protect our busines with antivirus software and a firewall, we also use Advanced Endpoint Detection software and a Security Operations Center to provide 24/7 monitoring of our network to immediately detect, shutdown and isolate any system on our network that may become infected.

Plus, we use an advanced backup solution that protects our backups against an insider attack. If a bad actor got ahold of our credentials and got into our servers and backups, even with the correct credentials they would not be able to permanently delete, corrupt or encrypt our data backups.

Question 6: If we are attacked, how quickly could we resume business as normal?

What you should hear: Since we have the right tools in place to detect an attack as it happens, the damage will be minimized, which will reduce the cost and time to get us back to business as usual.

We also have Disaster Recovery Plans in place which include encrypted backups saved to our secure data center if other layers fail to prevent an attack. What's more, this secure data center is accessible from anywhere at any time so if even if we're not at our office we can access the remote data center servers.

Question 7: Do we have a cyber-attack response plan?

What you should hear: Yes. In addition to providing the blueprint for how to respond to and recover from an attack, we also have cyber insurance. Most cyber insurance policies require a response plan to bind coverage.

Question 8: Do we have backups of our mission critical data in two or more locations and when was the last time the backups were tested?

What you should hear: Having simply a backup is not good enough. We have backups in at least two locations with Insider Protection that protects us against an insider attack and accidental deletion. The integrity of the backups is verified daily and if there is a failure, we are notified. Finally, Insider Protection makes a secret copy of data that can't be found by anyone.

Question 9: When was the last time our company had a risk assessment?

What you should hear: We advocate hiring an outside vendor to do a full risk assessment every year. They identify any vulnerabilities in our environment, help us proactively identify potential security concerns as well as suggest areas of improvement so we can keep the business safe.

Because threats change so quickly, new solutions are created to help meet those threats. A risk assessment can also provide an understanding of the current landscape and threats, and what solutions are available to help prevent them.

If your current IT provider isn't giving you the right answers to these questions, contact RYMARK for a free risk assessment. We'll give you the information you need for achieving IT security and proven guide to help get you there.

Request Your FREE Risk Assessment:

Call: (651) 328-8900

Email: info@rymarkIT.com