ClearCom
IT Solutions
ASSESS | MONITOR | AUTOMATE | PROTECT

Frequently Asked Questions About Your
Free Cybersecurity Risk Assessment:

QUESTION #1:

Do I have to notify my current IT guy or company that you are running this assessment?

A: No! Your current IT company or guy DOES NOT NEED TO KNOW we are conducting the assessment. In most cases, it's actually better that they are NOT aware that our security assessment is going on. The worst thing we can do is provide your IT guy advance warning that a test is coming. If they always knew that an attack was imminent, then your network would probably be better protected. Nearly everyone can prevent an attack they know is coming; it's when they don't know it's coming that you're most vulnerable to an attack.
As a CEO myself, I understand that you have to delegate and trust, at some level, that your key employees and vendors are doing the right thing – **but it never hurts to validate that they are**. Remember, it's YOUR reputation, YOUR money, YOUR business that's on the line. THEIR mistake is YOUR nightmare.

QUESTION #2:

If you find a compromise, virus or security violation during the risk assessment, do you have to report me?

A: No. Please understand that EVERYTHING WE FIND AND DISCUSS DURING THIS ASSESSMENT WILL BE STRICTLY CONFIDENTIAL. We are not obligated to report any of our findings to anyone other than you directly.

You should know that according to state laws, you *may* be required to tell your clients and/or patients if YOU have exposed their data, records and information to cybercriminals, and we would recommend you abide by the law. But we are not the police or the FBI. We are here to help you put a plan in place to prevent that disaster from happening.

QUESTION #3:
How intrusive is the assessment? Do you have to install any software on my computer network during the assessment?

A: Our assessment is completely non-intrusive to your network. Neither your employees nor your current IT company or guy will even know we are performing the assessment. During our initial meeting, we will cover a number of different options for assessing your network against cyberattacks, which may or may not include specialized diagnostic software tools. We will discuss these options with you in person and will never do anything on your computer network without your complete agreement.

Either way, this assessment will provide you with verification from a qualified third party on whether or not your current IT person is doing everything they should to keep your computer network not only up and running, but SAFE from cybercrime.

QUESTION #4:
How long will this take? Will my system be down at all during the assessment?

A: Your time investment is minimal; one hour for the initial meeting, 1 hour at your office to independently conduct our assessment and one hour in a second meeting to go over our Report of Findings. Your computer network will not be slowed down or taken down by this assessment.

QUESTION #5:
Are we too small to worry about getting hacked? We don't have anything a hacker would want to steal.

A: WRONG. For starters, small businesses are the #1 target for cybercrime groups because of their inability (or unwillingness) to implement proper security protocols. You're *easy prey*.

Second, not all cyber-attacks are about stealing your data. Ransomware attacks, like the recent WannaCry worm, are about **stealing what's valuable to YOU and extorting money**. Hackers corrupt ALL of your customer records and e-mail addresses, ALL of your work files and other data, then ask you to pay to get them back. If you don't pay, they delete your files. If you DO pay, they delete your files anyway OR come back and demand MORE money because you've indicated you're willing to pay. They're called cybercriminals for a reason: **they're lawless scumbags who don't follow the rules**.

Can you honestly say your client records and ALL of the history, data and work files on your server are something *not* worth protecting?!?!

And finally, just like a real virus (common cold), malware spreads without anyone *intentionally* giving it to you. They are designed to be self-propagating, so claiming “nobody would want to attack us” is akin to saying, “I won’t catch a cold because nobody wants to give me one.” **It doesn’t work that way.**

Most of the attacks are 100% automated, using software programs designed to hammer millions of computers at once, working 24 hours a day, 365 days a week, to find security loopholes on ALL computers connected to the Internet. You’re under attack by highly organized, highly motivated TEAMS of sophisticated coders who attack en masse – not some lone hacker sitting at home selecting his victims. All it takes is to miss ONE critical software update and you’re toast. ONE employee clicking on the wrong link. ONE client or trusted vendor sending you an infected file.

Have A Question That Was Not Answered Here?

If you have any other questions you need answered, please call the office direct at **508-205-1114** or send an e- mail to **Rob@clearcomit.com**

Rob Cleary

Rob Cleary
President/CEO
ClearCom IT Solutions, Inc.
Web: www.ClearComIT.com