ItCon
IT & Cybersecurity Managed Services

FROM THE DESK OF
Leah Freiman
CEO, ItCon

With Ransomware At An All-Time High, Maybe It's Time You Took A CLOSER LOOK At What Your Current IT Company Is Doing To Secure You From An Expensive, Devastating Cyber-Attack

Dear Colleague,

As you can see, I've sent you a tiny magnifying glass. Why have I done this?

Simply as a way to catch your attention and offer you a **FREE IT Security Risk Assessment** so you can take a "closer look" at whether or not your current IT company is keeping you secure from ransomware, downtime, data loss and cyber-attacks.

My name is **Leah Freiman, CEO** of **ItCon**. On the surface, we appear to be "just another" IT firm, but our approach is unique: We are one of the only outsourced IT services firms in **the New York Metro Area** that truly knows how to secure IT systems for small and midsize businesses, not just make your computers work.

Here's a very scary but 100% real fact: Better than 97% of the IT networks we conduct this free Risk Assessment for are NOT secure from ransomware or cyber-attacks, putting the owner at underappreciated risk for the losses and financial devastation a cyber-attack would cause.

I do realize this may seem "sensational" and that you'd be tempted to throw this letter away thinking I'm just another crackpot consultant looking for a paycheck. Maybe you think, "We're fine." It's natural to insist, "Not in MY company," or to think your IT team or company has you covered.

But I can assure you of this: Like Sherlock Holmes, our IT team has never failed to find significant and preventable security loopholes that were occurring in the companies we've audited – and it's my firm belief that right now, this very minute, YOUR organization has unforgivable gaps in your IT security and your backup and recovery of data.

I'm So Confident In Our Ability To Demonstrate How You're Being Underserved That I'll Guarantee It

Because I'm so confident in what we do,
I'm willing to make you the following good-natured bet…

If we are unable to satisfactorily demonstrate big holes in your IT security, backup and data recovery systems, and you feel as though we've wasted your time, then I'll personally donate $200 to the charity of your choice. *It's that simple.*

Why would I do this?

Two reasons:

First, I know your time is extremely valuable and you don't have time to mess around with companies that don't have anything of value to offer. I'm putting my money on the line so you can see how serious I am about not wasting your time.

Second, with ransomware attacks at an all-time high and the associated costs escalating, it's more critical than ever to make sure you are doing everything you can to minimize that risk and the financial losses a breach would create.

**To schedule a quick 10-minute call
to discuss this Free IT Security Assessment,
go to our website: https://www.itconinc.com/discoverycall**

Here Are A Few Of The Ways Your Current IT Company Is Putting You At Underappreciated Risk

1. Grossly Inadequate Cyber Security Controls

When a cyber-attack happens, the losses stack up and multiply. First, there's an instant loss of productivity. At best, your operations are crippled. Worst case, you're completely shut down, unable to transact, unable to deliver promised products and services to clients and unable to operate. In other cases, thousands – if not millions – of dollars are drained directly from your accounts without any chance of recovery.

Then you have the loss of critical data, as well as reputational damages, potential lawsuits and government fines. **The epicentre of this disaster lands DIRECTLY on YOUR desk for YOU to deal with** – a problem that WILL significantly undo your best-laid plans for growth and progress.

Yet despite this, we have found that 99% of the companies we've audited are GROSSLY unprepared for and unprotected from a cyber-attack event, EVEN THOUGH they have invested heavily in cyber security. Before we showed them irrefutable evidence of these inadequacies, the CEO of one company was convinced his "team had it handled." A ticking time bomb they didn't know was "live" under their seat.

2. Insurance Claim Denials

If your IT company has NOT met with your insurance provider to review the coverages you have for a cyber-attack (crime, cyber-liability, etc.) to ENSURE you have the right IT security protections implemented – which YOU have personally agreed to implement in order to get coverage in your policy – YOU are at risk of having your claim denied when you need it the most.

What has your IT company told you about this? A ransomware attack could stack up losses and costs into the hundreds of thousands or even millions of dollars, from emergency IT restoration to lost sales. If you don't have proper insurance – or if you DO have insurance but aren't adhering to the security protocols required by your policy – these costs will come directly out of your pocket, directly from your bottom line.

Insurance claims can (and will) be denied if your current IT company has not implemented certain cyber security controls mandated by the policy you signed.

3. Chronic IT "Glitches" And Downtime

As the saying goes, "Overhead walks on two legs." Any CEO knows that unproductive, distracted workers not only kill profitability but increase the chances of mistakes, missed deadlines, sloppy work and low morale. *A frustrated team is not a productive one.*

Yet we find that most CEOs don't realize just how often their employees are being interrupted and distracted due to recurring IT failures because it's "hidden" from them. Many are shocked to discover their employees are dealing with chronic IT problems that constantly get in the way of serving clients, closing sales and doing their job, forcing them to stop what they are doing, redo the work they just spent hours doing or possibly NOT do what they are supposed to do.

We will fix ALL of this.

Worst of all? One out of five employees fall victim to phishing campaigns and it's still the #1 way you will get hacked. What is your current IT company doing to stop this?

Curious? Let's Schedule A Brief 10-Minute Call To Discuss

The next step is simple: go online to book a brief 10-minute call with me: https://www.itconinc.com/discoverycall

You can also call my office at 845-222-1120 to schedule your Free Cyber Security Risk Assessment. My personal assistant has been notified to look for your call and will put you through immediately. You may also send me an e-mail to lfreiman@itconinc.com.

On this call we can discuss your unique situation and any concerns you have and, of course, answer any questions you have about us. If you feel comfortable moving ahead, we'll schedule a convenient time for our team to evaluate the health of your business's data security.

During this assessment, the third party we use to audit our networks would analyze your entire security system, inside and out. These assessments normally cost thousands of dollars. (If you google "how much does a penetration test cost?" you'll see one of the first hits indicates between $10,000 and $30,000. We purchase these in bulk for our clients, and I have a few left over this month.)

This assessment can be conducted 100% remotely, with or without your current IT company or department knowing. **At the end of the assessment, you'll know:**

- How to address easily fixable problems with the way your team may be handling sensitive data within your network.
- Whether or not your systems and data are truly secured from hackers and ransomware, and where you are partially or totally exposed.
- If your data is actually being backed up in a manner that would allow you to recover it quickly in the event of an emergency or a ransomware attack.

We will even provide you with a report that will be proof of a third-party analysis of your network – something required right now in many cyber and crime insurance renewal forms.

Fresh eyes see things that others cannot – so at a minimum, this assessment is a completely costand risk-free way to get a credible third-party validation of the security and stability of your network and should give you peace of mind that your data is being protected.

Don't Blindly Trust That Your Current IT Company "Has It Handled"

As Mark Twain once said, supposing is good, but KNOWING is better. As the CEO, you need to know for sure that your IT company is not failing to protect you.

Think about it: the "worst" that can happen is you get $200 to your favorite charity for having an independent, credible third party validate the security, efficiency and stability of your IT systems. **To get started, please call or e-mail me to schedule a quick initial phone consultation**. I will have my assistant follow up to ensure you've received this letter and to discuss how (if?) you'd like to proceed.

Awaiting your response,

Leah Freiman, CEO
ITCon, Inc.
Phone: 845-222-1120
E-mail: lfreiman@itconinc.com

ItCon
TECHNOLOGY AND BUSINESS TOGETHER

3 Surefire Signs
Your IT Company
Is Failing To Protect You
From Ransomware

NEW And Critical Changes To Cybersecurity,
Insurance Coverage And Threats That Will Put Your Business
At Serious Risk If Not Addressed Immediately

www.itconinc.com
https://www.itconinc.com/discoverycall/

P.S. Not ready to meet yet? Then at least go online and download our FREE report, "3 Surefire Signs Your IT Company Is Failing To Protect You From Ransomware." I've had numerous CEOs use this as a "pop quiz" to see IF their IT team could say "yes" to even half of what we've outlined here. Be prepared to be shocked. You can download it instantly at: **www.itconinc.com/cyberreport**