motiva

Are You Taking An Expensive Gamble With your Agency's IT Security?

Take This Quick Quiz To Find Out:

1. Are you *just* using a username and password to log in to your Agency Management Software? When companies like First American Financial, RMS, First Unum Life Insurance, and Paul Reve life Insurance (all NY Based Agencies) were breached, all their customer's information went directly to the dark web and was sold to cybercriminals, they had to pay DFS **over $6 million in settlements**.

2. Every quarter when you sit down with your IT company/team to review your Penetration Test Results do they tell you how vulnerable your network is? Do they produce a formal, written, multistep process for securing your network and RECOVERING from a ransomware attack? *Ask to see it; even if you don't fully understand it, the "tell" is if they can't produce it or make excuses and try to dismiss your request.*

3. Do you have VERIFIED daily backups of your data? Does your IT team conduct regular "fire drill" test restores to see if the backups are actually working? *Do you even know if this is being done? Or are you still using the "I am on the cloud excuse" did you know that Microsoft Office 365 doesn't have a backup for your emails.*

4. Are your employees' workstations and devices' Hard Drives Encrypted (it's part of the DFS Cybersecurity Law) To prevent them from downloading files and accessing applications that can compromise your network? If not, you're in direct violation of the DFS Cybersecurity Regulation NYCRR500.

5. Do you have a qualified third party auditing your IT company or team's security protocols and systems? No one should proofread their own work – and you as the CEO should insist on this instead of just taking them at their word that everything is "fine."

If you cannot confidently say "Yes" to these questions, or if you don't know the answers, this letter is of critical importance to you.

From the Desk of:
Walter Contreras
Founder / CEO Motiva

1400 Old Country Road Westbury, NY 11590 · 646-374-1820 · www.motiva.net

motiva

Dear Fellow CEO,

As you can see, I've enclosed a poker chip with this letter. Why have I done that? Actually, there are two very important reasons:

1. I have something **extremely important** to tell you and I wanted to make sure this letter would catch your attention.

2. Since what I'm writing you about pertains to a "gamble" you're taking with your Agency's technology security, I thought this would be an appropriate "eye-catcher." **Here's what this is about**…

My name is Walter Contreras, CEO of Motiva. We're an IT support company located here in New York that provides outsourced IT services to "ONLY" INSURANCE AGENCIES, WE KNOW YOUR BUSINESS AND HOW YOU OPERATE.

In the past few months, we've seen the most aggressive uptick in ransomware attacks on Insurance Agencies in our lifetime. I'm sure you've already heard the recent news stories about First American getting hit – but what you might not know is that smaller agencies are getting ransomed more frequently, and the attacks are getting more aggressive and costly.

Based on what we're seeing, it's not a matter of "if" but WHEN you'll experience a cyber-attack.

I don't mean to frighten you, but to EDUCATE you and **offer help** so you are able to minimize the cost, downtime and damages rather than be caught completely unprepared and suffer substantial losses – which is why I'm writing you today and extending this offer…

Our Free And Confidential Cyber Security Risk Assessment Will Give You The Answers You Want, The Certainty You Need

For a limited time, we are giving away a Free Cyber Security Risk Assessment. This is confidential, entirely free and without obligation.

↠ This assessment will provide verification from a **qualified third party** on whether or not your current IT company is doing everything they should to keep your data and computer network SAFE from ransomware, hackers and cyber-attacks.

Here's How It Works: We will have a brief, nontechnical conversation about your company's IT security. We'll ask you a few questions that you should easily be able to answer. Depending on what we discover, we can move to the next step, which is to conduct a quick, non-invasive, CONFIDENTIAL investigation of your computer network, backups and security protocols.

motiva

Your current IT company or team DOES NOT NEED TO KNOW we are conducting this assessment, or we can involve them. (The choice is yours, but we recommend NOT letting them know this inspection is happening so we can get a truer read of how secure you are. After all, the cybercriminals won't tip you off that they're about to hack you).

Your time investment is minimal: 30 minutes for the initial consultation and one hour in the second meeting to go over what we discover. **When this Risk Assessment is complete, here's what you will know:**

- If your IT systems and data are **truly secured** from hackers, cybercriminals, ransomware and even sabotage by rogue employees.
- If your **current backup would allow you to be up and running again fast if ransomware locked all your files** – *99% of the computer networks we've reviewed failed this test.*

If you and your employees' login credentials are being sold on the dark web right now and what to do about it (I can practically guarantee they are due to a recent 8.4 billion credentials being sold on the dark web. What we find will shock you).

If we find problems, we will tell you what they are and prepare a Security Action Plan, for free, on how to remediate the situation; and if you choose, we can assist you in its implementation.

After doing this for 17 years for agencies in NY, I can practically guarantee I will find significant and preventable security loopholes in your network and problems with your backups. Like Sherlock Holmes, we never fail. If nothing else, our Risk Assessment is an easy and cheap (free) way to get a valid third party to verify your security and give you peace of mind.

"We're Fine…"

"Nobody Wants To Hack US…"

It's natural to want to insist, "Not in MY AGENCY," or think, "That won't happen to us." You may think because you're small or don't have "anything a hacker would want," you're immune to these attacks – but ransomware attacks are growing at an alarming rate, and it's happening to small businesses that INSISTED it wouldn't happen to them.

According to Cloudwards.net, **51% of businesses surveyed reported being hit by ransomware in 2020**, and this year the number is *growing*. Maybe you have already been hit and survived, which has left you feeling "safe." But what you don't realize is that you have identified yourself as a target THAT WILL PAY. It's very likely they will come back to you, because to the hackers, you are a paying client – **68% of companies that have been hit WILL BE TARGETED AGAIN!**

PenTest Magazine reported that the average business had to shell out **$178,000 to a hacker group** to get their data back – and that's just for the ransom, NOT for the cost of downtime, emergency IT restoration costs, lost business, reputational damage and lost revenue from clients leaving and the enormous time and emotional toll it puts on you and your employees.

motiva

Yes, I'm Sure You Have An IT Company, But Here's How They Could Be Failing You

As a CEO myself, I understand that you have to delegate and trust, at some level, that your 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 agency that's on the line. One mistake, one slip-up, even from a loyal and well-intentioned person, becomes YOUR nightmare.

How could they be failing to protect you?

The biggest reason is that they might not possess the expertise needed. Many IT pros know how to keep a computer network running **but are completely out of their depth** when it comes to dealing with the advanced cyber security threats we are RECENTLY seeing.

IMPORTANT: A little-known "secret" in the outsourced IT world is that many smaller IT shops don't have the expertise or head count on staff to handle the sophisticated attacks going on. They won't admit that to you, because NOBODY (particularly IT guys) likes to admit they are out of their depth.

Second, they may be "too busy" themselves to truly be proactive with your account – or maybe they don't want to admit the security solutions they sold you have become OUTDATED and inadequate compared to far superior solutions available today.

If you talk to CEOs who have been hacked or compromised, all of them say they *thought* their IT team "had things covered." That's why you need a preemptive, independent risk assessment like the one I'm offering in this letter.

Why Free?

Two reasons. First, we want to do everything we can to protect Insurance Brokers in our area against these cyber-scumbags who steal from honest, hardworking business owners like us without repercussions. WE have to stand together as Americans to stop this from happening.

Second, we would prize the opportunity to be your IT company. But we want to EARN your trust by demonstrating our expertise and providing value in advance. Again, I want to stress that this free Risk Assessment comes with no strings attached, no "hard sell" and no tricks.

Please…Do NOT Just Shrug This Off
(What To Do Now)

1400 Old Country Road Westbury, NY 11590 · 646-374-1820 · www.motiva.net

I know you are *extremely busy* and there is enormous temptation to discard this, shrug it off, worry about it "later" or dismiss it altogether. That is, undoubtedly, the easy choice…but the easy choice is rarely the RIGHT choice. **Here's how to request your FREE Cyber Security Risk Assessment:**

- Go online to: **https://motiva.net/risk/**
- Call me direct at (646) 374-1820
- E-mail me direct with questions: walter@motiva.net

Dedicated to your peace of mind,

Walter Contreras
CEO, Motiva

Not Ready To Meet Just Yet?

Then at least download our new Executive Report titled **"7 Urgent Security Protections Every Business Should Have In Place Now."** It's a completely free resource containing insider information and facts that every CEO and business owner should read ASAP. You can instantly download this report for free at our website: https://motiva.net/specialreport/

motiva

Thinking About Taking A Pass?
Have A Look At What Our Clients Are Saying:

" Working with Motiva makes me feel safe. I know all of my customers' information is protected from cyberthreats. The entire team has been amazing at handling our calls and issues. Their customer service is second to none. Motiva's team is so patient, there's always someone who answers the call live. I know Motiva has my back, I highly recommend them. "
Tricia Baratta - Comp Matters Inc

"The single most important benefit to using Motiva is peace of mind. I know we have our great Motiva Team providing vital system security, and they are always ready to answer questions or provide technical support.
Motiva came to us highly recommended by the Big I and by several other local agents. Motiva's staff are knowledgeable and efficient. They are very familiar with insurance agency operations, the NYS DFS security requirements, Microsoft products, and the Applied TAM system. Motiva is always available and always a pleasure to deal with."
Joseph Grasso – Hartt Insurance Agency Inc

"The reliability and knowledge of the Insurance Industry that Motiva brings to the table is invaluable to me. They are always consistent, they know who we are, and understand the DFS Law better than we do. I highly recommend them to any Insurance Broker not matter what size. "
Carol DePinto - Kron Associates, Inc.