SECURED CYBER SERVICES

When You Fall Victim To A Cyber-Attack Through No Fault Of Your Own, Will They Call You

Stupid…Or Just Irresponsible?

An Important New Report Regarding The Dangers Of Cybercrime On Small Businesses In Northern Virginia and DC And What Small Business Owners Must Do To Protect Themselves

© Technology Marketing Toolkit, Inc.

SECURED CYBER SERVICES

An URGENT Notice To All Small Business Owners And CEOs In Northern Virginia and DC: We have entirely FREE and time-sensitive information that is critical for you as a CEO to know regarding growing cyber security threats AND your company's credentials being sold on the "Dark Web." **Please respond ASAP**.

August 2026
From The Desk of: William Price, CEO
President, Secured Cyber Services

Dear Small Business Owner,

It's EXTREMELY unfair, isn't it? Victims of all other crimes – burglary, rape, mugging, carjacking, theft – get sympathy from others. They are called "victims" and support comes flooding in, as it should.

But if your business is the victim of a cybercrime attack where client or patient data is compromised, you will NOT get such sympathy. You will be instantly labeled as stupid or irresponsible. **You will be investigated and questioned about what you did to prevent this from happening** – and if the answer is not adequate, you can be found liable, facing serious fines and lawsuits EVEN IF you trusted an outsourced IT support company to protect you. Claiming ignorance is not an acceptable defense, and this giant, expensive and reputation-destroying nightmare will land squarely on YOUR shoulders. *But it doesn't end there…*

According to [STATE] laws, you will be required to tell your clients and/or patients that YOU exposed them to cybercriminals. Your competition will have a heyday over this. Clients will be IRATE and leave in droves. Morale will TANK and employees will BLAME YOU. Your bank is NOT required to replace funds stolen due to cybercrime (*go ask them*), and unless you have a very specific type of insurance policy, any financial losses will be denied coverage.

Please do NOT underestimate the importance and likelihood of these threats. It is NOT safe to assume your IT company (or guy) is doing everything they should be doing to protect you; in fact, there is a high probability they are NOT, which we can demonstrate with your permission.

Who Am I And Why You Should Listen To Me About This

My name is William Price, CEO of Secured Cyber Services. We specialize in making technology productive and easy for small business owners in the northern Virginia and DC area and have a stellar reputation for fast, proactive service built over many years.

I do realize that the above statements and this letter may come across as "fearmongering." It may even upset you. That is *not* my intent. I truly only seek to help. In fact, I'm writing to offer you

© Technology Marketing Toolkit, Inc.

a **Free Cyber Security Risk Assessment** for your company to introduce our services to you AND to help you determine if your business could truly survive a cybercrime attack.

To help you understand why I'm so passionate about this topic, let me share with you just ONE cybercrime horror story that may help you understand why I'm so passionate about this.

It started out like any other Monday morning. Someone had come into the office early to get a head start on a client project when an unexpected email appeared. It was from a medical billing company—not a current client, but one that had previously explored services a few months back. They had just discovered that a hacker had infiltrated their systems, gaining access to sensitive patient files, and was now demanding a ransom of $XX,XXX to prevent the data from being exposed.

Their current IT provider's response was grim and dismissive: "There's nothing you can do. Pay the ransom and hope for the best."

Unwilling to accept that as their only option, the company reached out in desperation, seeking a second opinion. A thorough investigation was launched, and while it was possible to recover most of their data, the breach itself couldn't be undone. The incident had to be reported—to their clients, to the patients, and to the FBI.

The fallout was swift. Regulatory agencies investigated and found the company liable, issuing fines totaling $X,XXX. Furious patients filed lawsuits. The physicians who relied on the billing service were forced to take legal action themselves, only to discover the company's insurance provider denied the claim due to the absence of a cyber liability policy.

Despite the efforts made to assist, the damage was irreparable. The business ultimately shut down and filed for bankruptcy. The owner was held personally accountable for all legal expenses, technology recovery costs, and fines.

In a conversation that left a lasting impression, the owner shared his devastation: *"I don't know how this happened. I'm a good business owner, doing right by our clients. I've worked my whole life to build this company—and now it's gone. Everything is gone. The money, the clients, my reputation—it's all been destroyed. I have no idea what to do now. I can't just pay off the fines and walk away. But who's going to hire me? I feel like I'm stuck in a nightmare, just waiting to wake up. I might even lose my home… everything I've worked for. And I didn't even commit a crime."*

That incident made me want to do something. I was SO ANGRY that this happened to a good guy like this! It was unbelievable! He was a hardworking business owner just like you and me. He didn't deserve to be punished for a crime he didn't even commit! Nobody does! His only "guilt" was ignorance. He trusted the wrong IT company to protect him, which is *hardly* a crime. That's why I decided to start a personal mission to help – and at least EDUCATE – as many business owners as I could about the dangers of cybercrime and how they can protect themselves from losing everything.

That's why I'm writing **YOU TODAY**.

Obviously I don't know you or your situation. Your IT guy might be brilliantly ahead of all of this for you, doing all the right things to protect you. However, it's also VERY possible you're being underserved and ill-advised by your IT company.

I frequently get calls from business owners desperate for help after a ransomware attack or devastating virus, or even to clean up the aftermath of a disgruntled employee, **who HAD an IT company that they trusted with the responsibility of protecting the business, but realized all too late they weren't doing the job they were hired to do**.

© Technology Marketing Toolkit, Inc.

SECURED CYBER SERVICES

There are many reasons for this. First, it could be that they simply don't know *how* to advise you, or even that they *should*. Many IT guys know how to keep a computer network running but are completely out of their league when it comes to dealing with the advanced cyber security threats we are RECENTLY seeing.

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

And finally, NOBODY (particularly IT guys) likes to admit they are out of their depth. They feel compelled to exaggerate their ability to avoid being fired. To be fair, they might actually have you covered and be on top of it all. *However…*

In my admittedly informal survey, talking to CEOs who have been hacked or compromised, almost all of them told me they thought their IT guy "had things covered." **That's why it's VERY likely your IT guy does NOT have you "covered" and you need a pre-emptive, independent risk assessment like the one I'm offering in this letter.**

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 business that's on the line. THEIR mistake is YOUR nightmare.

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

For a limited time, we are offering to give away a Free Cyber Security Risk Assessment to a select group of businesses. This is entirely free and without obligation. EVERYTHING WE FIND AND DISCUSS WILL BE STRICTLY CONFIDENTIAL.

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 computer network not only up and running, but SAFE from cybercrime.

Here's How It Works: At no cost or obligation, one of my lead consultants and I will come to your office and conduct a non-invasive, CONFIDENTIAL investigation of your computer network, backups and security protocols. Your current IT company or guy DOES NOT NEED TO KNOW we are conducting this assessment. Your time investment is minimal: one hour for the initial meeting and one hour in the second meeting to go over our Report Of Findings.

When this Risk Assessment is complete, you will know:

- **If you and your employees' login credentials are being sold on the Dark Web** (I can practically guarantee one or more are… THIS will shock you). Thanks to a new threat intelligence and ID-monitoring service we subscribe to, we can run a report on YOUR company and see what credentials are actively being sold on the Dark Web, which is a part

© Technology Marketing Toolkit, Inc.

of the World Wide Web accessible only by means of special software, allowing operators to remain completely and totally anonymous and untraceable, used by the most notorious cybercrime rings around the world.

- IF your IT systems and data are **truly secured** from hackers, cybercriminals, viruses, worms and even sabotage by rogue employees. *If you're not getting weekly security updates from your current IT person, your systems probably aren't secure.* You should also know that antivirus software and most firewalls are grossly inadequate against the sophisticated attacks now happening.

- IF your **current backup would allow you to be back up and running again fast** if ransomware locked all your files. *In 99% of the computer networks we've reviewed over the years, the owners were shocked to learn the backup they had would NOT survive a ransomware attack*. Ransomware is **designed to infect your backups as well**, leaving you defenseless. There are only a handful of backup systems that will prevent this from happening.

- DO your employees truly know how to spot a phishing e-mail? We will actually put them to the test. *We've never seen a company pass 100%. Never.*

- Are your IT systems and backups in sync with compliance requirements for HIPAA, GLBA and SOX, and using best practices?

If we DO find problems…overlooked security loopholes, inadequate backups, credentials that have been compromised, out-of-date firewall and antivirus software and (often) active malware…on one or more of the PCs in your office, we will propose an Action Plan to remediate the situation that you can have us implement for you if you choose. **Again, I want to stress that EVERYTHING WE DISCUSS AND DISCOVER WILL BE STRICTLY CONFIDENTIAL.**

Why Free?

Frankly, we want the opportunity to be your IT company. We know we are the most competent, responsive and trusted IT services provider to small businesses in Northern VA and DC.

However, I also realize **there's a good chance you've been burned, disappointed and frustrated by the complete lack of service and the questionable advice** you've gotten from other IT companies in the past. In fact, you might be so fed up and disgusted with being "sold" and underserved that you don't trust anyone. *I don't blame you*.

That's why this assessment is completely and entirely free. Let us earn your trust by demonstrating our expertise. While we would love the opportunity to be your IT company, we will come in with no expectations and only look to provide you with fact-based information so you can make a quality, informed decision – and we'll ONLY discuss the option of becoming your IT company if the information we share makes sense and you want to move forward. No hard sell. No gimmicks and no tricks.

© Technology Marketing Toolkit, Inc.

SECURED CYBER
SERVICES

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

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. **This I can guarantee:** At some point, you WILL HAVE TO DEAL WITH A CYBER SECURITY EVENT.

Hopefully you'll be brilliantly prepared for it and experience only a minor inconvenience at most. But if you wait and do NOTHING, I can practically guarantee this will be a far more costly, disruptive and devastating attack that will happen to your business.

You've spent a lifetime working hard to get where you are today. Don't let some lowlife thief operating outside the law in another country get away with taking that from you. And certainly don't "hope" your IT guy has you covered.

Get the facts and be certain you are protected.

Contact us and schedule your Free, CONFIDENTIAL Cyber Security Risk Assessment today: www.secured-cyber.com. Feel free to also reach out to me direct at the phone number and e-mail address below.

Dedicated to serving you,

William Price
Web: www.secured-cyber.com
E-mail: info@secured-cyber.com
Direct: 703-520-2355

© Technology Marketing Toolkit, Inc.

Here Is Just One of the Other CEO's We've Helped:

Dr. Peter Cocolis, Owner at Peter Cocolis, DMD

"I've worked with Secured Cyber Solutions for over 2 decades — and I wouldn't trust anyone else with our technology. Whether it's protecting sensitive data or keeping our systems running smoothly, their team has always been knowledgeable, dependable, and proactive. They've supported us through growth, change, and every challenge in between — and we're still going strong."

© Technology Marketing Toolkit, Inc.