The Cybersecurity Crisis

The Small & Medium Sized Business Cybersecurity Crisis

New And Critical Protections Every Small & Medium Size Business Must Have In Place NOW To Protect Their Bank Accounts, Client Data, Confidential Information And Reputation From The Tsunami Of Cybercrime And Ransomware

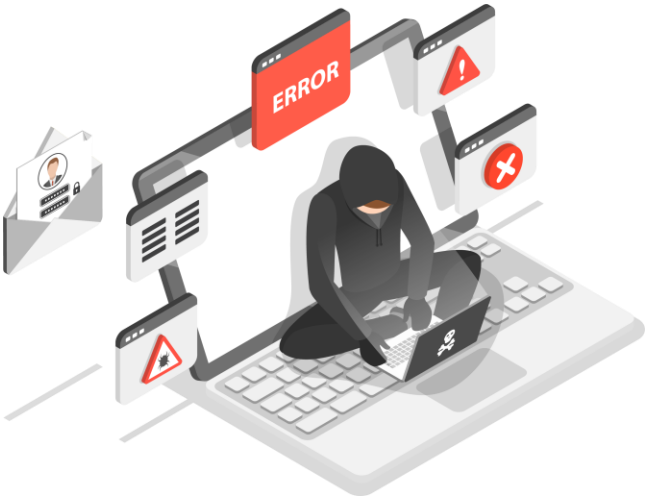
The growth and sophistication of cybercriminals, ransomware and hacker attacks has reached epic levels. CEOs can no longer ignore it or foolishly think, "That won't happen to us."

Your business – large OR small – will be targeted and will be compromised UNLESS you take action on the information revealed in this shocking new executive report.

Provided as an educational service by:
Paul Marchese, CEO
Marchese Computer Products, Inc.
www.mcpinc.com

When You Fall Victim To A Cyber-Attack By No Fault Of Your Own, Will They Call You Stupid…Or Just Irresponsible?

It's EXTREMELY unfair, isn't it? Victims of all other crimes – burglary, 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 may be <u>investigated and clients will question you</u> 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 New York 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, <u>any financial losses will be denied coverage</u>.

<u>Please do NOT underestimate</u> 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.

But first, please allow me to introduce myself and give you a little background on why I created this report.

Why We Are So PASSIONATE About Informing And Protecting <u>YOU</u>

My name is Paul Marchese, CEO of Marchese Computer Products, Inc. We specialize in being the outsourced IT department for small to medium sized businesses in the Western New York and Central New York areas. Maybe you've read my book, Business Owner's Guide to Cyber Security, which is a CEO's guide to cybercrime. Or maybe you saw me with Mr. Wonderful, Kevin O'Leary, from Shark Tank discussing cyber security in our Small Business Tech day from back in December of 2022. I and my company is committed to removing the burden of IT from our client plate so they can spend their time growing their business.

Over the last couple of years, my team and I have seen a significant increase in calls from business owners desperate for help after a ransomware attack, data breach event or other cybercrime incident.

When they call, they're desperate, scrambling for anyone who can help them put the pieces back together again. Often their business is completely on lockdown. ALL their data has been corrupted or held for ransom, preventing them from fulfilling obligations they have to their clients. **YEARS of work and critical data – *all gone*.**

They're also scared and *intensely* angry. They feel violated and helpless. Embarrassed. How can money be taken from their bank account WITHOUT their permission or knowledge? Why didn't their IT company or IT team prevent this from happening? *How are they going to tell their clients/patients that they've exposed them to cybercriminals*? They're in complete disbelief that they actually fell victim – after all, they "didn't think we had anything a cybercriminal would want!"

What makes this unforgivable is that ALL of the CEOs coming to us for help after a serious attack had an IT company they trusted with the responsibility of protecting the business, but realized all too late the company wasn't doing the job it was PAID to do.

As a business owner, that boot-strapped my own company from the ground up. I know how hard you work to make your company succeed. I understand the risks you've taken, the personal sacrifices you've made. To me, it's a GROSS insult to have it all taken away by some cyber-scumbag in a Third World country who will NOT be held accountable for his actions.

To make matters worse, so many so-called "IT experts" out there aren't doing the job they were hired to do – and that truly angers me. As the CEO of a company, you're FORCED to trust that your IT company or team is doing the right things to protect your organization – and when they fail to do their job, this expensive, devastating, business-interrupting disaster lands squarely on YOUR desk to deal with.

That's why we've started a "one-company revolution" to educate and help as MANY business owners as we can so they never have to deal with the stress, anxiety and loss caused by a cyber-attack, and help you understand just how serious this is so you can be brilliantly prepared instead of caught completely off guard.

Yes, It CAN Happen To YOU And The Damages Are VERY Real

You might already know about the escalating threats, from ransomware to hackers, but it's very possible you are underestimating the risk to you. It's also possible you're NOT fully protected and are operating under a false sense of security, ill-advised and underserved by your outsourced IT company.

Schedule Your Free, Cybersecurity Risk Assessment Today!

Visit **www.mcpinc.com/risk** or call our office at 585-343-2713**.**

In fact, if they have not talked to you about the protections outlined in this report, or about putting a cyber "disaster recovery" plan in place, you are at risk and you are not being advised properly.

This is not a topic to be casual about. Should a breach occur, your reputation, your money, your company and your neck will be on the line, which is why you must get involved and make sure your company is prepared and adequately protected, not just pass this off to someone else.

QUESTION: When was the last time your current IT company had THIS conversation with you? What HAVE they told you about these new threats? If they have been silent, then I would urge you to read this report in full and act on the information urgently.

"Not My Company…Not My People…We're Too Small," You Say?

Don't think you're in danger because you're "small" and not a big company like Experian, J.P. Morgan or Target? That you have "good" people and protections in place? That it won't happen to you?

That's EXACTLY what cybercriminals are counting on you to believe. It makes you easy prey because you put ZERO protections in place, or grossly inadequate ones.

Right now, there are over 980 million malware programs out there and growing (source: AV-Test Institute), and 70% of the cyber-attacks occurring are aimed at small businesses (source: National Cybersecurity Alliance); you just don't hear about it because the news wants to report on BIG breaches OR it's kept quiet by the company for fear of attracting bad PR, lawsuits and data-breach fines, and out of sheer embarrassment.

In fact, the National Cybersecurity Alliance reports that **one in five small businesses have been victims of cybercrime in the last year** – and that number includes only the crimes that were reported. Most small businesses are too embarrassed or afraid to report breaches, so it's safe to assume that number is much, much higher.

Are you "too small" to be significantly damaged by a ransomware attack that locks all of your files for several days or more?

Are you "too small" to deal with a hacker using your company's server as **ground zero** to infect all of your clients, vendors, employees and contacts with malware? Are you "too small" to worry about someone taking your payroll out of your bank account? According to Osterman Research, the AVERAGE ransomware demand is now $84,000 (source: MSSP Alert). It's also estimated that small business lost over $100,000 per ransomware incident and over 25 hours of downtime. Of course, $100,000 isn't the end of the world, is it? But are you okay to shrug this off? To take the chance?

How Bad Can It Be?
My Insurance Will Cover Me, Won't It?

Insurance companies are in the business to make money, NOT pay out policy claims.

A few years ago, cyber insurance carriers were keeping 70% of premiums as profit and only paying out 30% in claims. Fast forward to today and those figures are turned upside-down, causing carriers to make drastic changes in how cyber-liability insurance is acquired and coverages paid.

For starters, even getting a basic cyber-liability or crime policy today may require you to prove you have certain security measures in place, such as multi-factor authentication, password management, endpoint protection and tested and proved data backup solutions.

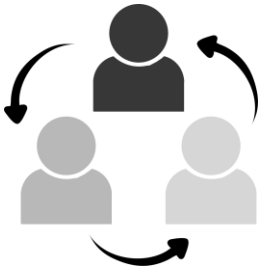
Insurance carriers want to see phishing training and cybersecurity awareness training in place, and some will want to see a WISP and/or a Business Continuity Plan from your organization. Depending on the carrier, your specific situation and the coverage you're seeking, the list can be longer.

But the biggest area of RISK that is likely being overlooked in your business is the actual enforcement of critical security protocols required for insurance coverage and compliance with data protection laws. Insurance carriers can (and will) deny payment of your claim if you failed to actually implement the security measures required to secure coverage. When a breach happens, they will investigate how it happened and whether or not you were negligent before paying out.

You cannot say, "I thought my IT company was doing this!" as a defense. Your IT company will argue they were not involved in the procurement of the policy and did not warranty your security (none will; check out your contract with them). They might show evidence of you refusing to purchase advanced security services from them to further distance them from any responsibility. And if you haven't been documenting the steps you've taken to secure your network and prove that you were not "willfully negligent," **this gigantic expensive nightmare will land squarely on your shoulders to pay**.

It's NOT Just Cybercriminals Who Are The Problem

Most business owners erroneously think cybercrime is limited to hackers based in China or Russia, but the evidence is overwhelming that disgruntled employees, both of your company and your vendors, can cause significant losses due to their knowledge of your organization and access to your data and systems. What damage can they do?



- **They leave with YOUR company's files, client data and confidential information stored on personal devices**, as well as retaining access to cloud applications, such as social media sites and file-sharing sites (Dropbox or OneDrive, for example), that your IT department doesn't know about or forgets to change the password to.

  In fact, according to an in-depth study conducted by Osterman Research, **69% of businesses experience data loss due to employee turnover and 87% of employees who leave take data with them**. What do they do with that information? Sell it to competitors, BECOME a competitor or retain it to use at their next job.

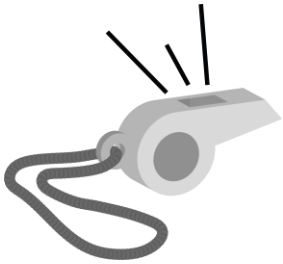
- **Funds, inventory, trade secrets, client lists and HOURS stolen.** There are dozens of sneaky ways employees steal, and it's happening a LOT more than businesses care to admit. According to the website StatisticBrain, 75% of all employees have stolen from their employers at some point. From stealing inventory to check and credit card fraud, your hard-earned money can easily be stolen over time in small amounts that you never catch.

  Here's the most COMMON way they steal: They waste HOURS of time on your dime to do personal errands, shop, play games, check social media feeds, gamble, read the news and a LONG list of non-work-related activities. Of course, YOU are paying them for a 40-hour week, but you might only be getting half of that. Then they complain about being "overwhelmed" and "overworked." They tell you, "You need to hire more people!" so you do. All of this is a giant suck on profits if you allow it. Further, if your IT company is not monitoring what employees do and limiting what sites they can visit, they could do things that put you in legal jeopardy, like downloading illegal music and video files, visiting adult content websites, gaming and gambling – all of these sites fall under HIGH RISK for viruses and phishing scams.

- **They DELETE everything. A common scenario:** An employee is fired or quits because they are unhappy with how they are being treated – but before they leave, they permanently delete ALL of their e-mails and any critical files they can get their hands on. If you don't have that data backed up, you lose it ALL. Even if you sue them and win, the legal costs, time wasted on the lawsuit and on recovering the data, not to mention the aggravation and distraction of dealing with it all, are all greater costs than what you *might* get awarded if you win the lawsuit, *might* collect in damages.

- **They become a PAID whistleblower for the government.** For example, complaints filed for HIPAA violations on medical practices primarily come from two sources: 1. An actual cyber-attack happening, or 2. Whistleblowers *inside* the organization. **More specifically, disgruntled patients and employees**, not government auditors.

  Employees, vendors and even patients/clients can be financially rewarded for reporting YOU and be protected under a Safe Harbor law. Ambulance chasing attorneys know this and are advertising to take whistleblower cases on Google (just do a quick search for "Medicaid fraud whistleblower reward" and look at the ads that come up from law firms). There's even a website, www.CorporateWhistleBlower.com that promotes, "Get Rewarded For What You Know," encouraging people to come forward for Medicare fraud or companies over-billing or defrauding the government. This is just the tip of the iceberg coming for ALL industries as state and federal governments enact more cybersecurity protection laws.



Take a look at the above list. Do you *really* think *this can't* happen to you?

Then there's the threat of vendor theft. Your payroll, HR and accounting firm have direct access to highly confidential information and a unique ability to commit fraud. THEIR employees, not just the leadership team, can steal money, data and confidential information. All it takes is a part-time employee – perhaps hired to assist in data entry during tax season, and who is not being closely supervised or is working from home on routine tasks with your account – to decide to make a little money on the side by selling data or siphoning funds from your account.

Schedule Your Free, Cybersecurity Risk Assessment Today!
Visit **www.mcpinc.com/risk** or call our office at 585-343-2713.

What Do Others In Western New York Say?

"Marchese Computer not only rescued our law firm's critical data from a failing machine but also provided unparalleled protection and cybersecurity measures that have proven invaluable. Their local presence made all the difference, responding swiftly to our urgent situation. Their dependability and reliability have set a new standard for us when it comes to IT services. With Marchese Computer, it's not just about fixing issues; it's about comprehensive solutions that prevent future problems. Their expertise in cybersecurity gave us peace of mind, knowing our sensitive legal information is safeguarded. Marchese Computer is more than a service; they're a dedicated partner who genuinely cares about our firm's security. If you're seeking top-tier protection, promptness, and a true local ally in the digital realm, we wholeheartedly recommend Marchese Computer. They've earned our trust and gratitude."

– Thomas A. Burns, Attorney at Law, Criminal Defense Attorney

"Since teaming up with Marchese Computer Products, Inc., **I don't have to worry about client information security.** They've become our trusted SAFETY NET, taking the weight of IT matters off my shoulders. Their team is **always quick to answer my questions** and to help me understand our system better. With their support, **I have more time to work on my business**. I can't recommend Marchese Computer Products, Inc. enough!"

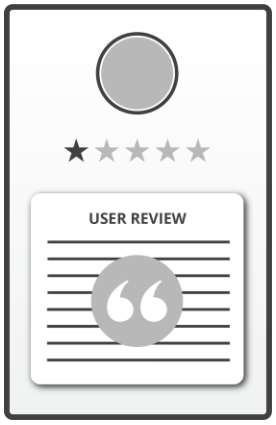
– Jennifer Thom

Schedule Your Free Cybersecurity Risk Assessment Today!

Visit **www.mcpinc.com/risk** or call our office at 585-343-2713.

Exactly How Can Your Company Be Damaged By Cybercrime? Let Us Count The Ways:

1. Reputational Damages:



What's worse than a data breach? Trying to cover it up. Companies like Yahoo! are learning that lesson the hard way, facing multiple class-action lawsuits for NOT telling their users immediately when they discovered they were hacked. With dark-web monitoring and forensics tools, WHERE data gets breached is easily traced back to the company and website, so you cannot hide it.

When it happens, do you think your clients will rally around you? Have sympathy? News like this travels fast on social media. They will demand answers: HAVE YOU BEEN RESPONSIBLE in putting in place the protections outlined in this report, or will you have to tell your clients, "Sorry, we got hacked because we didn't think it would happen to us," or "We didn't want to spend the money"? Is *that* going to be sufficient to pacify them?

2. Government Fines, Legal Fees, Lawsuits:

Breach notification statutes remain one of the most active areas of the law. Right now, several senators are lobbying for "massive and mandatory" fines and more aggressive legislation pertaining to data breaches and data privacy. The courts are NOT in your favor if you expose client data to cybercriminals.

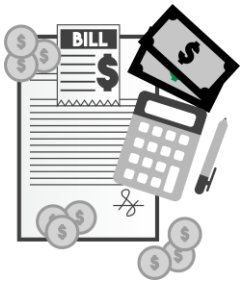
Don't think for a minute that this only applies to big corporations: ANY small business that collects customer information also has important obligations to its customers to tell them if they experience a breach. In fact, 47 states and the District of Columbia each have their own data breach laws – and they are getting tougher by the minute.

If you're in health care or financial services, you have additional notification requirements under the Health Insurance Portability and Accountability Act (HIPAA), the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA). Among other things, HIPAA stipulates that if a health care business experiences a breach involving more than 500 customers, **it must notify a prominent media outlet about the incident**. The SEC and FINRA also require financial services businesses to contact them about breaches, as well as any state regulating bodies.

With all the new laws being passed, there is a very good chance you are NOT compliant – **what HAS your IT company told you about this?**

Schedule Your Free Cybersecurity Risk Assessment Today!
Visit **www.mcpinc.com/risk** or call our office at 585-343-2713.

3. Cost, After Cost, After Cost:



ONE breach, one ransomware attack, one rogue employee can create HOURS of extra work for staff who are already maxed out when things are going well. Then there's business interruption and downtime, backlogged work delivery for your current clients. Loss of sales. Forensics costs to determine what kind of hack attack occurred, what part of the network is/was affected and what data was compromised. Emergency IT restoration costs for getting you back up, *if* that's even possible. In some cases, you'll be forced to pay the ransom and maybe – *just maybe* – they'll give you your data back. Then there are legal fees and the cost of legal counsel to help you respond to your clients and the media. Cash flow will be significantly disrupted, budgets blown up. Some states require companies to provide one year of credit-monitoring services to consumers affected by a data breach, and more are following suit.

According to the Cost of Data Breach Study conducted by Ponemon Institute, the **average cost of a data breach is $225 per record compromised, after factoring in IT recovery costs, lost revenue, downtime, fines, legal fees, etc**. How many client records do you have? Employees? Multiply that by $225 and you'll start to get a sense of the costs to your organization. [NOTE: Health care data breach costs are the highest among all sectors.]

4. Bank Fraud:

If your bank account is accessed and funds stolen, the bank is NOT responsible for replacing those funds. Take the true story of Verne Harnish, CEO of Gazelles, Inc., a very successful and well-known consulting firm, and author of the best-selling book *Mastering The Rockefeller Habits*.

Harnish had $400,000 taken from his bank account when hackers were able to access his PC and intercept e-mails between him and his assistant. The hackers, who are believed to be based in China, sent an e-mail to his assistant asking her to wire funds to 3 different locations. It didn't seem strange to the assistant because Harnish was then involved with funding several real estate and investment ventures. The assistant responded in the affirmative, and the hackers, posing as Harnish, assured her that it was to be done. The hackers also deleted his daily bank alerts, which he didn't notice because he was busy running the company, traveling and meeting with clients. That money was never recovered and the bank is not responsible.

Everyone wants to believe "Not MY assistant, not MY employees, not MY company" – but do you honestly believe that your staff is incapable of making a single mistake? A poor judgment? **Nobody believes they will be in a car wreck when they leave the house every day, but you still put the seat belt on.** You don't expect a life-threatening crash, but that's not a reason to not buckle up. *What if?*

Claiming ignorance is not a viable defense, nor is pointing to your outsourced IT company to blame them. YOU will be responsible and YOUR company will bear the brunt.

5. Using YOU As The Means To Infect Your Clients:

Some hackers don't lock your data for ransom or steal money. Often they use your server, website or profile to spread viruses and/or compromise other PCs. If they hack your website, they can use it to relay spam, run malware, build SEO pages or promote their religious or political ideals. (Side note: This is why you also need advanced endpoint security, spam filtering, web gateway security, SIEM and the other items detailed in this report, but more on those in a minute.) Are you okay with that happening?

You May Want To Believe You're "Safe"
But Are You Sure?

It's very possible that you are being ill-advised by your current IT company. What have they recently told you about the rising tsunami of cybercrime? Have they recently met with you to discuss new protocols, new protections and new systems you need in place TODAY to stop the NEW threats that have developed over the last few months?

If not, there could be several reasons for this. First, and most common, they might not know HOW to advise you, or even that they should. Many IT companies know how to keep a computer network running **but are completely out of their league when it comes to dealing with the advanced cybersecurity threats we are seeing recently**.

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. At industry events, I'm shocked to hear other IT companies say, "We don't want to incur that expense," when talking about new and critical cybersecurity tools available. Their cheapness CAN be your demise. Did you know that the average is 217 days that a hacker is on a network today before they attack, why? Simply to obtain all your info and then ask for money!

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. So how do you know?

Is Your Current IT Company Doing Their Job?
Take The Quiz On The Next Page To Find Out

If your current IT company does not score a "Yes" on every point, they are NOT adequately protecting you. Don't let them "convince" you otherwise and DO NOT give them a free pass on any one of these critical points.

Further, it's important that you get verification on the items listed. Simply asking, "Do you have insurance to cover us if you make a mistake?" is good, but getting a copy of the policy or other verification is critical. When push comes to shove, they can deny they told you.

Schedule Your Free Cybersecurity Risk Assessment Today!

Visit **www.mcpinc.com/risk** or call our office at 585-343-2713

If your current IT company does not score a "YES" on every point, they are NOT adequately protecting you.

- ❑ **Have they met with you recently – in the last 3 months – to specifically review and discuss what they are doing NOW to protect you?** Have they told you about new and inexpensive tools such as 2FA or advanced endpoint security to protect you from attacks that antivirus is unable to detect and prevent? If you are outsourcing your IT support, they should, at a MINIMUM, provide you with a quarterly review and report of what they've done – and are doing – to protect you AND to discuss new threats and areas you will need to address.

- ❑ **Do they proactively monitor, patch and update your computer network's critical security settings daily? Weekly? At all? Are they reviewing your firewall's event logs for suspicious activity?** How do you know for sure? Are they providing ANY kind of verification to you or your team?

- ❑ **Have they EVER urged you to talk to your insurance company** to make sure you have the right kind of insurance to protect against fraud? Cyber-liability? MORE IMPORTANT: Have they reviewed your insurance policy with your agent to ensure they were implementing the cyber protections required under that policy to avoid having a claim denied, coverage not paid?

- ❑ **Do THEY have adequate insurance to cover YOU if they make a mistake and your network is compromised?** Do you have a copy of THEIR CURRENT policy? Does it specifically cover YOU for losses and damages?

- ❑ **Have you been fully and frankly briefed on what to do IF you get compromised?** Have they provided you with a response plan? If not, WHY?

- ❑ **Have they told you if they are outsourcing your support to a third-party organization? Do you know who has access to your personal computer and network?** If they are outsourcing, have they shown you what security controls they have in place to ensure a rogue technician, living in another country, would be prevented from using their free and full access to your network to do harm?

- ❑ **Have they kept their technicians trained on new cybersecurity threats and technologies, rather than just winging it?** Do they have at least ONE person on staff with CISSP (Certified Information Systems Security Professional) or CISM (Certified Information Security Manager) certification? Do they have anyone on staff experienced in conducting security risk assessments?

- ❑ **Do they have a ransomware-proof backup system in place?** One of the reasons the WannaCry virus was so devastating was because it was designed to find, corrupt and lock BACKUP files as well. ASK THEM TO VERIFY THIS. You might *think* you have it because that's what your IT vendor is telling you.

- ❑ **Have they put in place a WRITTEN mobile and remote device security policy and distributed it to you and your employees**? Is the data encrypted on these devices? Do you have a remote "kill" switch that would wipe the data from a lost or stolen device, and is that data backed up so you CAN wipe the device and not lose files?

- ❑ **Do they have controls in place to force your employees to use strong passwords?** Do they require a monthly password update for all employees? If an employee is fired or quits, do they have a process in place to make sure ALL passwords are changed? Can you see it?

- ❑ **Have they talked to you about replacing your old antivirus with advanced endpoint security?** There has been considerable talk in the IT industry that antivirus is dead, unable to prevent the sophisticated attacks we're seeing today.

- ❑ **Have they discussed and/or implemented "multifactor authentication" for access to highly sensitive data?** Do you even know what that is? If not, you don't have it.

- ❑ **Have they recommended or conducted a comprehensive risk assessment every single year?** Many insurance policies require it to cover you in the event of a breach. If you handle sensitive data, such as medical records, credit card and financial information, Social Security numbers, etc., you may be required by law to do this .

- ❑ **Have they implemented web-filtering technology to prevent your employees from going to infected websites, or websites you DON'T want them accessing at work?** Porn and adult content is still the number one thing searched for online. This can expose you to sexual harassment and child pornography lawsuits, not to mention the distraction and time wasted on YOUR payroll, with YOUR company-owned equipment .

- ❑ **Have they given you and your employees ANY kind of cybersecurity awareness training?** Have they offered to help you create an AUP (acceptable use policy)? Employees accidentally clicking on a phishing e-mail or downloading an infected file or malicious application is still the number one way cybercriminals hack into systems. Training your employees FREQUENTLY is one of the most important protections you can put in place. Seriously.

- ❑ **Have they properly configured your e-mail system to prevent the sending/receiving of confidential or protected data?** Properly configured e-mail systems can automatically prevent e-mails containing specified data, like Social Security numbers, from being sent or received.

- ❑ **Do they allow your employees to connect remotely using GoToMyPC, LogMeIn or TeamViewer?** If they do, this is a sure sign to be concerned! Remote access should strictly be via a secure VPN (virtual private network).

- ❑ **Do they offer, or have they at least talked to you about, dark web/deep web ID monitoring?** There are new tools available that monitor cybercrime websites and data for YOUR specific credentials being sold or traded. Once detected, it notifies you immediately so you can change your password and be on high alert.

A Preemptive Independent Risk Assessment: The ONLY Way You Can Really Be Sure

A security assessment is exactly what it sounds like – it's a process to review, evaluate and "stress test" your company's network to uncover loopholes and vulnerabilities BEFORE a cyber-event happens.

Just like a cancer screening, a good assessment can catch problems while they're small, which means they will be a LOT less expensive to fix, less disruptive to your organization AND give you a better chance of surviving a cyber-attack.

An assessment should always be done by a qualified third party, NOT your current IT team or company; fresh eyes see things hidden, even in plain sight, from those looking at it daily.

You want a qualified "Sherlock Holmes" investing on YOUR behalf who is not trying to cover up inadequacies or make excuses, bringing to you a confidential report you can use before others find dirty laundry and air it in harmful ways.

Our Free Cybersecurity 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 Cybersecurity 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: an hour for the initial meeting and an hour in the second meeting to go over our Report Of Findings.

Schedule Your Free Cybersecurity Risk Assessment Today!

Visit **www.mcpinc.com/risk** or call our office at 585-343-2713.

When This Risk Assessment IS Complete, You Will Know:

- ✓ **If you and your employees' login credentials are being sold on the dark web.** We will run a scan on your company, right in front of you, in the privacy of your office if you prefer (results will NOT be e-mailed or otherwise shared with anyone but you). It's RARE that we don't find compromised credentials – and I can guarantee what we find will shock and alarm you.
- ✓ If your IT systems and data are **truly secured** from hackers, cybercriminals, viruses, worms and even sabotage by rogue employees.
- ✓ 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*.
- ✓ If 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%.* Not once.
- ✓ If your IT systems, backups and Security are in sync with compliance requirements for HIPAA, GLBA and SOX, and using best practices to ensure your company is fully protected.

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 Western New York.

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.

Schedule Your Free Cybersecurity Risk Assessment Today!

Visit **www.mcpinc.com/risk** or call our office at 585-343-2713**.**

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 CYBERSECURITY 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 there 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

Cybersecurity Risk Assessment Today!

Visit **www.mcpinc.com/risk**.
Or feel free to also reach out to me direct at **585-343-2713**

Dedicated to serving you,

Paul Marchese, President
E-mail: paul@mcpinc.com
Direct: 585-343-2713

P.S. – When I talked to other IT professionals like myself and the CEOs who have been hacked or compromised, almost all of them told me they thought their IT guy "had things covered."

I'm also very connected with other IT firms across the country to "talk shop" and can tell you most IT guys have never had to deal with the enormity and severity of attacks happening in the last few months. That's why it's VERY likely your IT guy does NOT have you "covered" and you need a preemptive, 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.