ITCON INC.

The Medical Practice Cyber Crisis

Urgent and Critical Protections

Every Medical Practice

Must Have In Place NOW To Protect Their

Bank Accounts, Client Data, Confidential Information And Reputation From The Tsunami Of Cybercrime

ItCon
TECHNOLOGY AND BUSINESS TOGETHER

Provided By: ItCon Inc.
Author: Leah Freiman
14 N Madison Ave #201 Spring Valley, NY 10952
845.738.1661

The growth and sophistication of cyber criminals,

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 implement the security measures discussed in this executive report.

Putting these protections in place can drastically reduce or eliminate the reputational damages, downtime, data loss, litigation, embarrassment and significant costs of a cyber-attack.

Can This Happen To Me?

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, 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 New York 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.

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 under-served by your outsourced IT company.

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.

Can This Happen To Me?

This Is Too Serious A Matter

To Entrust To Others And Delegate Without Your Involvement

ONE slipup from even a smart, tenured employee clicking on the wrong e-mail, innocently downloading an application, lazily using an easy-to-remember password for ONE application is all it takes to open the door to a hacker or ransomware **and create real damage**.

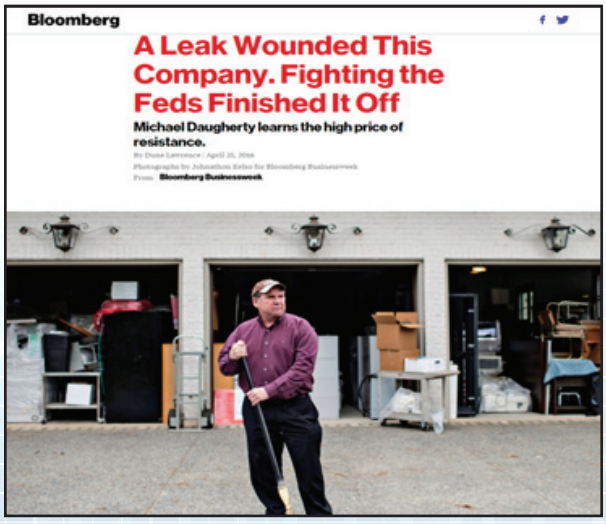
Take the story of Michael Daugherty, former CEO of LabMD. His small, Atlanta-based company tested blood, urine and tissue samples for urologists – a business that was required to company with federal rules on data privacy as outlined in the Health Insurance Portability and Accountability Act, or HIPAA

He HAD an IT team in place that he believed was protecting them from a data breach – yet the manager of his billing department was able to download a file-sharing program to the company's network to listen to music, and unknowingly left her documents folder (which contained over 9,000 patient files) open for sharing with other users of the peer-to-peer network.

This allowed an unscrupulous IT services company to hack in and gain access to the file and use it against them for extortion. When Daugherty refused to pay them for their "services," the company reported him to the Federal Trade Commission, who then came knocking.

After filing some 5,000 pages of documents to Washington, he was told the information he shared on the situation was "inadequate," requesting in-person testimony from the staff regarding the breach, and requesting more details on what training manuals he had provided to his employees regarding cybersecurity, documentation on firewalls and penetration testing. (QUESTION: ARE YOU DOING ANY OF THIS NOW?)

Long story short, his employees blamed HIM and left, looking for more "secure" jobs at companies that weren't under investigation. Sales steeply declined as clients took their business elsewhere. His insurance providers refused to renew their policies.



The FTC relentlessly pursued him with demands for documentation, testimonies and other information he already provided, sucking up countless hours of time. The emotional strain on him – not to mention the financial burden of having to pay attorneys – took its toll, and eventually, he closed the doors to his business, storing what was left of the medical equipment he owned into his garage where it remains today (see image).

ItCon
TECHNOLOGY AND BUSINESS TOGETHER

Can This Happen To Me?

"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 a Experian, J.P. Morgan or Target? That you have "good" people and protections in place? That "won't happen to you?"

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

Look: 82,000 NEW malware threats are being released every single day and HALF of the cyber-attacks occurring are aimed at small businesses; 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, data-breach fines and out of sheer embarrassment. But make no mistake – small, "average" businesses are being compromised daily, and clinging to smug ignorance of "that won't happen to me" is an absolute surefire way to leave yourself wide open to these attacks.

In fact, the National Cyber Security Alliance reports that **one in five Medical Practices have been victims of cybercrime in the last yea**r – and that number is only the ones that were reported. Most medical practices do NOT report such losses.

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, small businesses 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? Take the chance?

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 (Drop Box 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 busi-**

ItCon
TECHNOLOGY AND BUSINESS TOGETHER

Can This Happen To Me?

nesses experience data loss due to employee turnover and 87% of employee who leave take data with them. What do they do with that information? Sell it to competitors or retain it to use at their next job.

- **Funds stolen;** 75%of all employees have stolen from their employers, **with the median amount being $175,000** (according to the website Statistic Brain). From stealing inventory to sell or for personal use to check and payroll fraud, your hard-earned money can easily be stolen in small amounts over time that you never catch.

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

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 sell confidential information. All it takes is a part-time employee hired to assist in data entry during tax season that is not being closely supervised, working from home or routine tasks with your account to decide to make a little money on the side by selling data or siphoning funds from your account.

What Do Other CEOs In [CITY] Say?

[Use this section to put a few comments from your best clients about why they are taking your advice and protecting their organizations. Ask your clients for a few comments to include in a white paper/report you are creating about cybercrime. All they need to do is answer the question, "Why do you think other CEOs should take cybercrime serious like you are?" You can send them an e-mail and ask them to answer that question. Next, edit their answers to read properly and get their permission to publish. IT IS OKAY TO EDIT WHAT THEY SAY TO MAKE THE POINT YOU WANT TO MAKE. That's what reporters do all the time but publish without getting consent. Further, change the headline above and the comments to make the target market you are prospecting. For example, if you are targeting small, privately owned medical companies, the headline above should say, "What Doctors And Office Managers Of Nashville Medical Practices Are Saying."]

[Insert 3-4 comments here.]

7 Types of Damages

Exactly How Can Your Company Be Damaged By A Cybercrime?

Let's 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 its users immediately when they discovered they were hacked. With Dark Web monitoring tools, WHERE data gets breached is easily traced so you cannot hide it anymore.

   Do you think you're [clients/patients] will rally around you? Have sympathy? News like this travel 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. If such laws are passed, it would mean mandatory controls and inspections be put in place for data privacy, with severe fines and penalties to companies that fail to comply, as well as compensation to consumers for stolen data.

3. With new bills and amendments being proposed, discussed and passed practically every month. Right now, two senators are trying to get "massive and mandatory" fines for data breaches passed into law.

   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. (Only Alabama, New Mexico, and South Dakota do not.) [NOTE: You might want to modify this section to your specific niche, like medical or financial institutions, and state.]

   If you're in healthcare and financial services, you have additional notification requirements under the Health Insurance Portability and Accountability Act (HIPPA), the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA). Among other things, HIPPA stipulates that if a healthcare 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.

   One thing is for certain; the government is unpredictable, and they LOVE to impose laws and regulations. This isn't going to get better, easier.

4. **Cost, After Cost, After Cost.** ONE breach, one ransomware attack, one rough employee can product HOURS of extra work for staff that is already maxed out when things are going well. Then there's busi-

ness 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's 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. Connecticut requires companies to provide one year of credit monitoring services to consumers affected by a data breach.

According to the Cost of Data Breach Study conducted by Ponemon Institute, revealed the **average cost of a data breach at $225 per record compromised**. 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: Healthcare data breach costs being the highest among all sectors.]

5. 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 bestselling book, *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 back in the affirmative, and the hackers, posing as Harnish, replied assuring her that it was to be done. The hackers also deleted his daily bank alerts, which he didn't notice because he was buy 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 judgement? **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?*

6. Lawsuits and fines: That means there's a very good chance you are NOT compliant – **what HAS your IT company told you about this**?

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.

7. 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?

Are You Protected?

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

Look at these [15] protections as a "pop quiz" to see if YOUR company is actually implementing ALL of these protocols to protect you – **and if you don't know, WHY NOT? What excuse does your IT provider have for not talking to you about these?**

At a MINIMUM, your IT company should have the following in place:

- Security patches and updates to all applications
- Smart spam filtering that doesn't block wanted e-mails, but keeps malware out
- A properly configured firewall (NOTE: Most are not set up or maintained properly)
- Up-to-date network documentation of hardware and software

3 More Protections You Need, But Probably Don't Have

While many companies will have the above list of protections in place to some degree, here are three more that are necessary both for protecting your company, but also for proving you are doing everything you can to protect your [clients/patients]:

#1: Security Awareness Training

The #1 security threat to any company is... Its own EMPLOYEES! According to the cyber security training company, KnowBe4, **91% of successful data breaches started with a spear phishing attack** – an employee clicking on an infected e-mail.

Spam filters and anti-virus software cannot protect your network from an employee that intentionally clicks on and downloads a virus. That's why it's CRITICAL that you educate all of your employees how to spot an infected e-mail or online scam. All it takes is ONE slip up, and you're foolish if you think your employees know better.

Further, many crime and cyber liability insurance policies will REQUIRE that you have an AUP (acceptable use policy) and cyber security training in order to receive coverage in the event of a breach (see Michael Daugherty's story outlined earlier). If you cannot prove you were providing training, you could be denied coverage. We encourage all of our clients to take a close look at the wording of their insurance policies and make sure they are compliant, so their coverage isn't denied in the event of a breach, ransom attack or financial theft.

Employees can also compromise your company by using weak passwords that are easy for them to remember, downloading infected files or software applications OR accessing company applications from home PCs or mobile phones that are NOT being monitored, patched, updated and protected by your IT department or company.

That's why it's critical to make cyber security awareness training an important, ON-GOING part of your cyber protection, along with an Acceptable Use Policy that is enforced.

For our clients we provide [FILL IN WITH BRIEF DETAILS OF WHAT YOU PROVIDE.]

#2: Mobile And Remote Device Security

If an employee is accessing company data with an unprotected, unmonitored, personal device, such as a cell phone, tablet or home computer, they can easily infect your network with a virus OR give a hacker access to your data.

Often, employees are doing this without the knowledge or consent of their managers and IT team. So the FIRST step is finding out if this is going on (and it most likely is). Then, if you choose to allow employees to use personal mobile devices or home computers, you must protect that device like any other PC on your company network with advanced endpoint security, encryption, backup, etc.

At a minimum, ALL mobile devices should have a PIN code to access. Next they should have a remote "kill" switch that locks the device and wipes the data if lost or stolen. According to Bitglass, over 68% of health care data breaches occur when devices are lost or stolen. You also have to think about employees who quit or who are fired. How will you be able to erase YOUR data if it's on their own personal device?

Further, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, you may not be legally permitted to allow employees to access it on devices that are not secured; but that doesn't mean an employee might not innocently "take work home." If it's a company-owned device, you need to detail what an employee can or cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

#3: Strong Passwords That Are Enforced

Thanks to the power of AI (artificial intelligence), hackers have developed sophisticated software that can check over 100 million combinations of a password per second, also called "brute-force" attacks. Worse of all? This software is available for free online and can run off of any PC.

Today, a complex 8-digit password using mixed case, numbers and symbols has only 1 billion permutations and can be cracked in **16 minutes**. To speed things up, hackers hijack hundreds of thousands of computers to do the work automatically. To say the numbers become enormous at this point would be a gross understatement.

Remember, if your password is readable, a beginner can hack it with free software in seconds. Our advice is to make sure it's complex and at least 12 characters long, with upper and lower case letters, numbers and symbols – particularly for online banking or to password vault applications.

But human beings are NOT foolproof and will default to shorter, easier-to-remember

passwords. That's why you need to enforce good passwords. We recommend a trusted password generator and using a password portal to keep all your passwords safe.

#4: Dark Web ID Monitoring

BECAUSE most people are incredibly lazy about selecting strong passwords and the ease of which hackers can crack one, you also need to add Dark Web monitoring to protect yourself.

The "Dark Web" is a part of the World Wide Web used by all cybercrime rings and hackers that is only accessible using special software. All users and operators are anonymous and untraceable, which is why it's the playground for all cybercriminals.

Dark Web monitoring scans the Dark Web for your specific credentials being sold or traded. Once detected, it notifies you immediately so you can change your password (hopefully to a strong one!) and allows you to be on high alert for strange activity in your applications and online banking.

WARNING: There are several companies who are now offering to do a Dark Web scan for you. Be VERY careful of going online and conducting one if you don't know the company and the people behind it. They could be scams designed to get your password or credentials! Further, Experian and Equifax started offering Dark Web scans; but my concern is that both of these companies has massive data hacks and exposed millions of personal records – definitely not a company I would trust. Further, it was rumored that the terms and conditions you agreed to when requesting these scans by these companies contained language that waived your rights to privacy, protecting THEM if they were hacked again. While we are not a law firm and cannot confirm if this is true, we can tell you it's our opinion that you should be very careful about who you trust to your credentials.

#5: Advanced Endpoint Security, NOT Antivirus

There has been a debate going on in the last year about whether antivirus software is "dead." While once the mainstay of security, many IT professionals argue that it's not enough to defend against the sophisticated attacks happening due to two major reasons.

First, malware can spread at a blindingly fast rate thanks to the growing connectivity of devices and faster internet technology. That means a virus can become widespread before the antivirus vendors even know it exists. Second, hackers produce variants of their malware that are designed to evade antivirus programs, as was seen by the recent ransomware attacks which evaded 100% of antivirus software systems.

Without getting too techie, advanced endpoint security is an approach where each computer or end point (PC, laptop, mobile phone, laptop, etc.) is responsible for its own security. Further, security is based on the behavior of the device, which means when malicious activity is detected, it's stopped. NEED MORE ON THIS FROM JAY.

#6: Multi-Factor Authentication

Have you ever had to enter a pin code sent to your cell phone along with a password to access a website, such as your bank or even your Google profile? That is multi-factor authentication. It's a security feature for certain sites that requires you to enter a passcode or pin that is sent to a cell phone or e-mail address.

While you might not want it for EVERY website, you would want to turn this on for your banking website or other applications, website and devices that hold sensitive information. NEED MORE ON THIS FROM JAY.

7: A Ransomware-Proof, Image Backup

Like anything else, there are good and bad; and a bad

Have An Business-Class, Image Backup. This can foil the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you don't have to pay a crook to get them back. A good backup will also protect you against an employee accidentally (or intentionally!) deleting or overwriting files, natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups should be AUTOMATED and monitored; the worst time to test your backup is when you desperately need it to work!

1. Don't allow employees to access company data with personal devices that aren't monitored and secured by YOUR IT department. The use of personal and mobile devices in the workplace is exploding. Thanks to the convenience of cloud computing, you and your employees can gain access to pretty much any type of company data remotely; all it takes is a known username and password. Employees are now even asking if they can bring their own personal devices to work (BYOD) and use their smartphone for just about everything.

   But this trend has DRASTICALLY increased the complexity of keeping a network – and your company data – secure. In fact, your biggest danger with cloud computing is not that your cloud provider or hosting company will get breached (although that remains a possibility); your biggest threat is that one of your employees accesses a critical cloud application via a personal device that is infected, thereby giving a hacker access to your data and cloud application.

   So if you ARE going to let employees use personal devices and home PCs, you need to make sure those devices are properly secured, monitored and maintained by a security professional. Further, do not allow employees to download unauthorized software or files. One of the fastest ways cybercriminals access networks is by duping unsuspecting users to willfully download malicious software by embedding it within downloadable files, games or other "innocent"-looking apps.

   But here's the rub: Most employees won't want you monitoring and polic-

ing their personal devices; nor will they like that you'll wipe their device of all files if it's lost or stolen. But that's exactly what you'll need to do to protect your company. Our suggestion is that you only allow employees to access work-related files, cloud applications and e-mail via company-owned and monitored devices, and never allow employees to access these items on personal devices or public WiFi.

2. Don't Scrimp On A Good Firewall. A firewall acts as the frontline defense against hackers blocking everything you haven't specifically allowed to enter (or leave) your computer network. But all firewalls need monitoring and maintenance, just like all devices on your network or they are completely useless. This too should be done by your IT person or company as part of their regular, routine maintenance.

3. Protect Your Bank Account. Did you know your COMPANY'S bank account doesn't enjoy the same protections as a personal bank account? For example, if a hacker takes money from your business account, the bank is NOT responsible for getting your money back. (Don't believe me? Go ask your bank what their policy is on refunding you money stolen from your account!) Many people think FDIC protects you from fraud; it doesn't. It protects you from bank insolvency, NOT fraud.

   So here are 3 things you can do to protect your bank account. First, set up e-mail alerts on your account so you are notified any time money is withdrawn. The FASTER you catch fraudulent activity, the better your chances are of keeping your money. In most cases, fraudulent activity caught the DAY it happens can be stopped. If you discover even 24 hours after it's happened, you may be out of luck. That's why it's critical that you monitor it daily and contact the bank IMMEDIATELY if you see any suspicious activity.

   Second, if you do online banking, dedicate ONE computer to that activity and never access social media sites, free e-mail accounts (like Hotmail) and other online games, news sites, etc. with that PC. Remove all bloatware (free programs like QuickTime, Adobe, etc.) and make sure that machine is monitored and maintained behind a strong firewall with up-to-date anti-virus software. And finally, contact your bank about removing the ability for wire transfers out of your account and shut down any debit cards associated with that account. All of these things will greatly improve the security of your accounts.

FREE Assessment

Pre-Emptive 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 3rd party, NOT your current IT team or company; everyone knows you cannot accurately proofread your own work. Our fresh eyes OFTEN uncover problems when conducting assessments.

And although we put "Assessments" last on this list, it truly is the first place you should start to see where you are vulnerable, and to determine the quality of your protection in the other [14] areas outlined in this report.

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

FREE Assessment

Dark Web, which is a part 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, backups and EMR support in sync with compliance requirements for HIPAA, GLBA and SOX, and using best practices to ensure that your business is continuously running smoothly.

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 medical practices in 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.

FREE Assessment

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.itconinc.com/security. Feel free to also reach out to me direct at the phone number and e-mail address below.

Dedicated to serving you,

Leah Freiman

Leah Freiman
Web: www.itconinc.com
E-mail: coach@itconinc.com
Direct: 845-738-1661

Testimonials

Here Are Just A Few Other CEOs We've Helped

THEY'RE NOT JUST A PROVIDER THEY ARE PART OF OUR TEAM!

ItCon set up a functioning worry-free co-managed IT department for us. They are on top of EVERYTHING be it technical, security, personal relationships or miscellaneous tasks. ItCon takes it all upon themselves, they dot all their i's and cross all their t's. Every person at ItCon is vigilant about not letting anything fall through the cracks. Our in-house IT staff has an amazing, transparent, working relationships with them and ItCon created the possibility to get everyone on the same page working as a team, to be as efficient and productive as possible. I am truly happy that I hired ItCon to be part of our team!

Joel Kestenbaum
Chief Operating Officer
ODA Primary Health Care Network

SECURE PROACTIVE IT AND CYBERSECURITY

ItCon has upgraded our company to perform better, they are here for us not only to handle our IT, Cyber Security, and anything related to our data, they are ALWAYS here for us no matter how big or small the task is. with ItCon, EVERYTHING is possible! ItCon are proactive as opposed to reactive and have an excellent personal relationship with everyone in the company from executives to the people behind the phones alike. I can truly rely on them to treat my company with the utmost care while keeping it up to par and secure. If someone is shopping for a solid IT MSSP, I would tell them: Don't waste your time going around trying other firms and wasting money, time, and resources just to realize you would have saved all that and a lot of aggravation by making the right decision. Instead use that wasted money and time to help a brother in need. 😉

Rachamim Hakakian
Director of Operations
Yedei Chesed

ItCon
TECHNOLOGY AND BUSINESS TOGETHER