The Cyber Security Crisis

Urgent And Critical Protections We Are Urging All Medical Practices To Have In Place NOW To Protect Their Bank Accounts, Client Data, And Reputation From The Tsunami Of Ransomware

The growth and sophistication of cybercriminals, ransomware and hacker attacks has reached epic levels, and NEW protections are now required. We have created this report to inform medical practice managers about what's going on and educate them on new protections we are urging all businesses to put in place NOW.

Provided By: America One Tech
Author: Ed Jones
25 Braintree Hill Park, Ste 200, Braintree, MA 02184
www.americatech.com 781-356-3535 info@americatech.com

Notice: This publication is intended to provide accurate and authoritative information in regard to the subject matter covered. However, no warranties are made. It is provided with the understanding that the author and the publisher are NOT engaged in rendering legal, accounting or related professional services or advice and that this publication contains opinions of its author. This publication is NOT intended as a substitute for specific legal or accounting advice for any particular institution or individual. The publisher accepts NO responsibility or liability for any individual's decisions or actions made as a result of information or opinion contained herein.

America One Technologies, Inc.
Swift Answers. Personal Attention.

When You Fall Victim To A Cyber Security Breach Due To No Fault Of Your Own, Will They Call You

Stupid Or Irresponsible?

Yes, this is harsh.

And WE don't believe you are either of those things.

But if you don't put in place certain the protections we are recommending in this report and allow hackers gain access to any form of client, patient and employee data via your organization, you will get NO sympathy and will be found "at fault" for not taking the protection of patient and employee data seriously.

You will be labeled stupid and irresponsible by others who are impacted by the breach, such as clients, vendors, government officials, competitors and possibly even some of your employees.

According to a report by Gartner titled, "8 Reasons More CEOs Will Be Fired Over Cybersecurity Incidents," twice as many CEOs are getting fired over cyber security incidents than the CIOs or CISO (Chief Information Security Officer) they employ.

You might think this is crazy, or that it won't happen to you. But it IS happening in record numbers to millions of organizations, large and small. And WHEN your organization gets hacked (not IF), this giant, expensive, reputation-destroying nightmare will land squarely on YOUR shoulders.

But it doesn't end there…

According to the laws here in Massachusetts, you will be required to tell your patients that YOU exposed them to cybercriminals.

Depending on the data you host, you may even be investigated and questioned by authorities and patients alike about what you did to prevent this from happening. If you have not implemented the protections we are outlining in this report, you can be found negligent and may be facing fines and lawsuits. Claiming ignorance is not an acceptable defense.

If it becomes public, your competition will have a heyday over this. Patients will be IRATE and will take their business elsewhere. Morale will tank and employees may even 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 for these matters, any financial losses will be denied coverage by your general business liability insurance.

Please do NOT underestimate the importance and likelihood of these threats.

Why We Wrote This Report For Our Clients

Over the last year, there has been a significant increase in the sophistication, frequency and severity of cybercrime attacks. The cost per attack has been steadily on the rise and lawmakers have been implementing new and more comprehensive regulations requiring ALL businesses become more diligent about securing and protecting data they host on their network or face stiff fines.

To make matters worse, COVID-19 forced businesses to hastily send their employees to work from home without a plan, which has led to many working in unsecured environments. This has also energized the efforts of this attackers who are rapidly increasing their efforts to take advantage of the situation.

In fact, the FBI reported a fourfold increase in cybercrime during the COVID-19 outbreak and malicious e-mails are up 600%. This is NOT just "big" companies, but small businesses like yours who are getting attacked.

An Important Notice To Our Clients About A Change In Our Service To Respond To This Crisis

We've been watching these trends and have been designing new solutions and services to protect our clients – specifically our managed services offering for clients who are not currenting on a retainer with us to monitor, maintain and protect their computer networks and data.

For those clients on our managed services retainers, we've been able to simply include them without an added cost – but some are newer, more effective and would be an add-on or replacement for what you have now, which requires us to take a closer look at your current protections and make specific recommendations based on your specific situation.

To prepare you for our discussion, we've compiled this report to educate you and provide details on why we are making these recommendations.

Do You <u>REALLY</u> Need Ongoing Monitoring, Maintenance And Cyber Security Protections?

The biggest challenge we face in protecting our clients is that many stubbornly believe "that won't happen to me" because they're "too small" or "don't have anything a cybercriminal would want." Or they simply think that if it happens, the damages won't be that significant. That may have held true 10 to 20 years ago, <u>BUT NOT TODAY</u>.

- You are correct that most cybercriminals who use ransomware to lock your files do NOT want your files – <u>but they know that YOU DO</u>. Just like a kidnapper, they don't want the

hostage; they know the family does and will pay to get them back safe.

- SMALL businesses are the #1 target for hackers because they often lack sophisticated cyber security protections.

- According to a report by CNBC, the average cyber incident costs a small business **$200,000**. Maybe that's not a lot of money to you. Maybe you can afford a $200,000 hit. But that's only the cost of getting the data back and restoring the network and doesn't take into considering the reputational damages or lost business.

"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 Cyber Security 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.

But make no mistake – small, "average" businesses are being compromised daily, and clinging to the 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 small businesses have been victims of cybercrime in the last year** – and that number includes only the ones 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?

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 you aren't even aware they were using.

  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.

  But 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 some 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 we don't put in place web security filtering to limit 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. **(IMPORTANT: We now have solutions to prevent this that we are rolling out to clients who want to stop this from happening to them.)**

- **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 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, is a far greater cost than what you *might* get awarded, *might* collect in damages. **(IMPORTANT: For our managed IT clients who have one of our backup solutions, we are confident we could get the data back; but for clients who don't, you are vulnerable to this.)**

Do you *really* think you are immune to any or all of *this happening* 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.

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

IMPORTANT: Clients who are on our Platinum Managed Services plan DO have protections in place to greatly reduce the chances of these things happening, and the severity and impact if they get compromised. You should also know there is absolutely no way we, or anyone else, can 100% guarantee you won't get compromised – you can only put smart protections in place to greatly reduce the chances of this happening, to protect data so it IS recoverable and to demonstrate to your employees, clients and the lawyers that you WERE responsible and not careless.

You should also know we are actively reviewing ALL clients' networks and specific situations to recommend NEW protections we feel you should have in place.

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 patients 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." That will not 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 applies only to big corporations: ANY medical practice that collects patient information also has important obligations to its patients 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.

One of the things we want to discuss with you is how to ensure you are and stay compliant.

3. **Cost, After Cost, After Cost:** ONE breach, one ransomware attack, one rogue employee you are not protected against, 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 patients. 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.

   It's estimated that the cost per lost or stolen record is between **$150 to $225 per record compromised, after factoring in IT recovery costs, lost revenue, downtime, fines, legal fees, etc**. How many patient records do you have? Employees? Multiply that by $150 on the conservative side 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 *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?*

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.)

   To be clear, clients under our Platinum Managed Services plan would be protected against THIS from happening.

Here Is Our Current List Of Recommended Solutions We Feel ALL Medical Practices Should Have In Place

Below is a list of things we recommend all medical practices have in place ASAP. We are also working to implement better tools, protocols and documentation, and will be sharing these updates with you as they come available, and in our regular Managed Service - Technology Business Reviews.

☐ **TBRs Or Technology Business Reviews And Security Risk Assessments:** We will be more persistent in scheduling and holding these meetings with [all clients]. During these consultations, we will conduct a security risk assessment and provide you with a score. We will also brief you on current projects, review your IT plan and budgets, discuss NEW tools and solutions we feel you may need and make recommendations. We will also answer any questions you have and make sure you are satisfied with our services.

☐ **Proactive Monitoring, Patching, Security Updates:** This is what we deliver in all our Managed IT Services Plans. Specifically, we:

- **Boost productivity** - with technology that makes doing business simpler
- **Focus on business** - with a team of experts to shoulder the burden of technology
- **Predict your IT costs** - with an all-inclusive fixed monthly rate
- **Protect all you've worked for** - with world-class security for your data and network

☐ **[NEW!] Data Breach And Cyber-Attack Response Plan:** This is a time- and-cost-saving tool as well as a stress-reduction plan. We will be working with medical practices to create and maintain a cyber-response plan so that IF a breach happens, we could minimize the damages, downtime and losses, and properly respond to avoid missteps.

☐ **Ransomware-Proof Backup And Disaster Recovery Plan:** Hackers know you have backups in place, so they construct their attacks to corrupt and lock BACKUP files as well. That's why we are insisting clients upgrade to our Datto backup solution, which is included in our Platinum Managed Services Plan.

- ☐ **A Mobile And Remote Device Security Policy:** All remote devices – from laptops to cell phones – need to be backed up, encrypted and have a remote "kill" switch that would wipe the data from a lost or stolen device. You also need to have a policy in place for what employees can and cannot do with company-owned devices, how they are to responsibly use them and what to do if the device is lost or stolen.

- ☐ **More Aggressive Password Protocols:** Employees choosing weak passwords are STILL one of the biggest threats to organizations. To protect against this, we will require a regular password changes for all employees and put in place controls to ensure weak, easy-to-crack passwords are never used. We will also have checklists for employees who are fired or quit to shut down their access to critical company data and operations.

- ☐ **[NEW!] 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. That's why we are recommending all clients UPGRADE to Sentinel One and ThreatLocker.

- ☐ **Multi-Factor Authentication:** Depending on your situation, we will be recommending multi-factor authentication for access to critical data and applications.

- ☐ **Web-Filtering Protection:** Porn and adult content is still the #1 thing searched for online, and online gaming, gambling and file-sharing sites for movies and music are sites you do NOT want your employees visiting during work hours on company-owned devices. If your employees are going to infected websites, or websites you DON'T want them accessing at work, they can not only expose you to viruses and hackers, but they can also get you nailed for sexual harassment and child pornography lawsuits – not to mention the distraction and time wasted on YOUR payroll, with YOUR company-owned equipment.

- ☐ **[NEW!] Cyber Security Awareness Training:** Employees accidentally clicking on a phishing e-mail, downloading an infected file or malicious application is still the #1 way cybercriminals hack into systems. Training your employees FREQUENTLY is one of the most important protections you can put in place. Seriously. We have several new solutions we can discuss with you to inform and remind your employees to be on high alert and reduce their likelihood of clicking on the wrong e-mail or succumbing to other scams.

- ☐ **Protections For Sending/Receiving Confidential Information Via E-mail:** Employees have access to a wide variety of information that is both confidential and important. We have options to ensure e-mail systems prevent the sending and receiving of protected data.

- ☐ **Secure Remote Access Protocols:** You and your employees should never connect remotely to your server or work PC using GoToMyPC, LogMeIn or TeamViewer. Remote access should strictly be via a secure VPN (Virtual Private Network). For our clients who need this type of access, we will be implementing proper technologies that are secure.

- ☐ **[NEW!] Dark Web/Deep Web ID Monitoring:** There are new tools available that monitor cybercrime websites for YOUR specific credentials being sold or traded. Once such breaches are detected, it notifies you immediately so you can change your password.

America One Technologies, Inc.
Swift Answers. Personal Attention.

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

Over the next couple of months, we will be conducting FREE Cyber Security Risk Assessments for all of our clients.

Here's How It Works: We will conduct a thorough, CONFIDENTIAL investigation of your computer network, backups and security protocols as outlined in this report. Your time investment is minimal: 25 minutes for the initial meeting and 1hour in the second to go over the results.

When this Risk Assessment is complete, we will give you a Risk Assessment Health Score and provide you a recommended IT maintenance plan to put protections in place and then maintain them to avoid you being a "sitting duck" for cybercriminals.

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

If you already have an appointment scheduled right now, you don't have to do anything but be sure you show up.

If you have NOT scheduled a Risk Assessment, call us at 781-356-3535 or send me an e-mail to info@americatech.com. You can also go online to https://www.americatech.com/about-us/security-assessment/ **and book online.**

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," be it an employee issue, serious virus or ransomware attack.

We want to make sure you are brilliantly prepared for it and experience only a minor inconvenience at most. But if you wait and do nothing and ignore our advice, I can practically guarantee this will be a far more costly, disruptive and devastating disaster.

You've spent a lifetime working hard to get where you are today. Let us help you protect and preserve it. Give you complete peace of mind.

Dedicated to serving you,

Ed Jones
Web: www.americatech.com
E-mail: edjones@americatech.com
Phone: 781-356-3535

America One Technologies, Inc.
Swift Answers. Personal Attention.

Here's What Our Clients Are Saying:

"IMMEDIATE RESPONSE FROM AMERICA ONE!

Heather Lancaster
Practice Manager,
New England Eye Centers,
Framingham, MA

America One has always given our practice assurance that our computer issues are their top priority until resolution. When calling, you always speak to a live person. ***You don't have to wait on a ticket process*** *or recorded voicemail. When we have a problem, hearing a voice on the other end assuring us that progress is being made ASAP is paramount to a medical practice. America One also does not have a simple "cookie cutter" service level plan of choices. They will work with you to customize a support structure to your needs. Contact them and see great service is their number one priority!"*

"ALWAYS ACCOMMODATE OUR QUESTIONS WITH GREAT PATIENCE

Gina Corrado
Practice Manager,
Plymouth Carver Primary Care,
Plymouth, MA

Our practice values America One's knowledge, availability and promptness to our IT needs and concerns. I would tell any potential client that they always accommodate our questions with great patience, ***no matter how simple.*** *We also benefit from America One's willingness to help us understand and communicate with our EMR vendor; eClinicalworks."*

"NO CONDESCENDING TREATMENT OF PEOPLE WITHOUT IT SKILLS

Kathy Devlin
Healthcare Administrator,
Primary Care Medical Associates,
Norwood, MA

I would urge any company to use America One because of their personal service. They know our company's employees individually and ***treat everyone with kindness and consideration.*** *There isn't any condescending treatment of people who may not have IT skills."*

"BIGGEST BENEFIT IS IMMEDIATE SERVICE!

Maria Joseph
Practice Manager,
Tufts Floating Specialty Center,
Brockton, MA

The biggest benefit from America One is being able to reach them quickly and their promptness to resolve our computer issues, either remotely or onsite. We appreciate their professionalism, dedication, concern and knowledge. We also appreciate that their ***techs are patient and understanding*** *when we try to explain our computer issues in our own words (not knowing the tech words). I would recommend America One because of all the things they do for us. They make sure our office runs well every day without interference from computer issues."*