The Professional Services Cyber Crisis

Urgent And Critical Protections Every Practice Must Have In Place NOW To Protect Their Bank Accounts, Client Data, Confidential Information And Reputation From The Tsunami Of Cybercrime

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

Your practice – 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 By: My Info Tech Partner
Author: Aaron Fisher, CISSP
PO Box 317 Bentley WA 6102
https://www.myinfotechpartner.com.au 08 6244 2556

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 practice is the victim of a cybercrime attack where client data is compromised, you will NOT get such sympathy. You will be instantly labelled 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 firm to protect you. Claiming ignorance is not an acceptable defence, and this giant, expensive and reputation-destroying nightmare will land squarely on YOUR shoulders. *But it doesn't end there...*

According to Australian Mandatory Breach laws, you will be required to tell your clients 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 underserved 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 firm and your neck will be on the line, which is why you must get involved and make sure your firm is prepared and adequately protected, not just pass this off to someone else.

PO Box 317, Bentley, WA, 6102
Tel. 08 6244 2556 www.myinfotechpartner.com.au info@myinfotechpartner.com.au
ABN: 40 607 937 879

This Is Too Serious A Matter To Entrust To Others And Completely Delegate Without Your Involvement

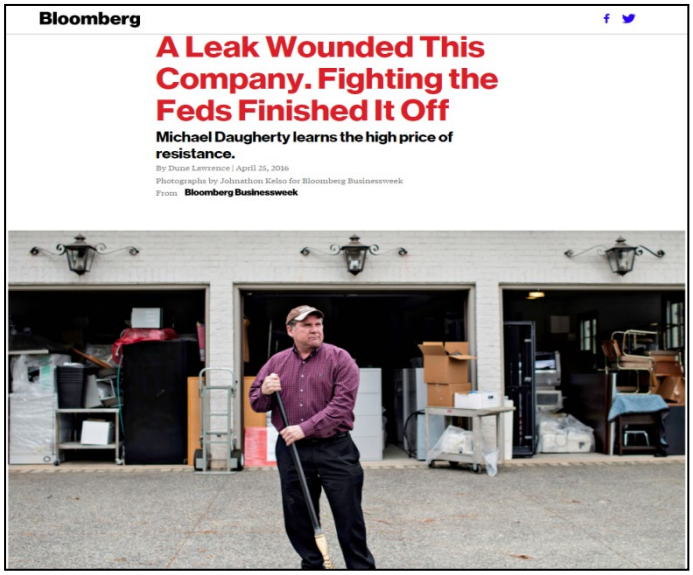
This is no longer an issue that can simply be delegated to the IT department.

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 firm tested blood, urine and tissue samples for urologists – a practice that was required to comply 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 firm'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 firm 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 firm reported him to the Federal Trade Commission, who then came knocking.


Bloomberg

A Leak Wounded This Company. Fighting the Feds Finished It Off

Michael Daugherty learns the high price of resistance.

By Dune Lawrence | April 25, 2016

Photographs by Johnathon Kelso for Bloomberg Businessweek

From Bloomberg Businessweek

After filing some 5,000 pages of documents to Washington, he was told the information he shared on the situation was "inadequate"; in-person testimony by the staff regarding the breach was requested, as well as more details on what training manuals he had provided to his employees regarding cyber security, 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 practice 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 practice, storing what was left of the medical equipment he owned into his garage, where it remains today.

PO Box 317, Bentley, WA, 6102
Tel. 08 6244 2556 www.myinfotechpartner.com.au info@myinfotechpartner.com.au
ABN: 40 607 937 879

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

Don't think you're in danger because you're "small" and not a big firm like DLA Piper, Deloitte or Mossack Fonseca? 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.

Look: 82,000 NEW malware threats are being released every single day, and HALF of the cyber-attacks occurring are aimed at practices; you just don't hear about it because the news wants to report on BIG breaches OR it's kept quiet by the firm for fear of attracting bad PR, lawsuits and data-breach fines, and out of sheer embarrassment. But make no mistake – small, "average" practices 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 practices have been victims of cybercrime in the last year** – and that number includes only the ones that were reported. Most practices 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, weeks or more? Are you "too small" to deal with a hacker using your firm's server as "ground zero" to infect all of your clients, suppliers, 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 practice 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 practice managers and/or directors erroneously think cybercrime is limited to hackers based in China or Russia; but the evidence is overwhelming that disgruntled employees, both of your firm and your suppliers, can cause significant losses due to their knowledge of your firm and access to your data and systems. What damage can they do?

- **They leave with YOUR firm'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, 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 practices 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 or retain it to use at their next job.

PO Box 317, Bentley, WA, 6102
Tel. 08 6244 2556 www.myinfotechpartner.com.au info@myinfotechpartner.com.au
ABN: 40 607 937 879

- **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 practices care to admit. According to the website StatisticBrain, 75% of all employees have stolen from their employers at some point. From stealing inventory to cheque 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 dollar 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 they 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 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.

Do you *really* think *this can't* happen to you?

Then there's the threat of supplier 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 Firm 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 Mossack Fonseca 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 firm 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

PO Box 317, Bentley, WA, 6102
Tel. 08 6244 2556 www.myinfotechpartner.com.au info@myinfotechpartner.com.au
ABN: 40 607 937 879

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 favour if you expose client data to cybercriminals.

   Don't think for a minute that this only applies to big corporations: ANY practice that collects customer information also has important obligations to its clients to tell them if they experience a breach. In fact, if your practice turns over more the $3 million in revenue a year and you don't notify people that you encountered a breach you may be liable up to $2 100 000 in fines from the Office of the Australian Privacy Commissioner.

   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?**

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 practice 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 firm.

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 firm, 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 firm" – 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 defence, nor is pointing to your outsourced IT firm to blame them. YOU will be responsible and YOUR firm 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 cyber security 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 cyber security tools available. Their cheapness CAN be your demise.

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 Firm Doing Their Job?
Take This Quiz To Find Out

PO Box 317, Bentley, WA, 6102
Tel. 08 6244 2556 www.myinfotechpartner.com.au info@myinfotechpartner.com.au
ABN: 40 607 937 879

If your current IT firm 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.

- ☐ **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 Dark Web monitoring for your firm's credentials 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 firm** to make sure you have the right kind of insurance to protect against fraud? Cyberliability?

- ☐ **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 policy?

- ☐ **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 3rd-party firm? **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 cyber security 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 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.

- ☐ **Have they put in place a mobile and remote device security policy?** 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 3 monthly password update for all employees? If an employee is fired

PO Box 317, Bentley, WA, 6102
Tel. 08 6244 2556 www.myinfotechpartner.com.au info@myinfotechpartner.com.au
ABN: 40 607 937 879

or quits, do they have a process in place to make sure ALL passwords are changed?

- ☐ **Have they talked to you about replacing your old antivirus with advanced endpoint security backed by a SOC?** 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 implemented "multi-factor authentication" for access to highly sensitive data?** Do you even know what that is?

- ☐ **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 #1 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 firm-owned equipment.

- ☐ **Have they given you and your employees ANY kind of cyber security awareness training?** Have they offered to help you create an AUP (acceptable use policy)? Employees accidentally clicking on a phishing e-mail, downloading an infected file or malicious application is still the #1 way cybercriminals hack into systems.

- ☐ **Do they offer, or have they at least talked to you about, Dark Web 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 firm'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 firm 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; 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 Cyber Security Risk Assessment Will Give You The Answers You Want, The Certainty You Need

PO Box 317, Bentley, WA, 6102
Tel. 08 6244 2556 www.myinfotechpartner.com.au info@myinfotechpartner.com.au
ABN: 40 607 937 879

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

This assessment will provide verification from a **qualified 3rd 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.** We will run a scan on your firm, 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 practice managers and directors 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 firm pass 100%.* Not once.

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 practices in Perth.

However, I also realise **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.*

PO Box 317, Bentley, WA, 6102
Tel. 08 6244 2556 www.myinfotechpartner.com.au info@myinfotechpartner.com.au
ABN: 40 607 937 879

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 firm, 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 firm if the information we share makes sense and you want to move forward. No hard sell. No gimmicks and no tricks.

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 practice.

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: https://www.myinfotechpartner.com.au/ps-cyber-risk/. Feel free to also reach out to me direct at the phone number and e-mail address below.

Dedicated to serving you,

Aaron Fisher
Web: https://www.myinfotechpartner.com.au/
E-mail: aaron.fisher@myinfotechpartner.com.au
Direct: 08 6244 2556

P.S. – When I talked to other IT professionals like myself and the Practice Directors 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 suppliers are doing the right thing – but it never hurts to validate that they are. Remember, it's YOUR reputation, YOUR money, YOUR practice that's on the line. THEIR mistake is YOUR nightmare.

PO Box 317, Bentley, WA, 6102
Tel. 08 6244 2556 www.myinfotechpartner.com.au info@myinfotechpartner.com.au
ABN: 40 607 937 879

Here Are Just A Few Other Clients We've Helped:

Proactive Advice, Peace Of Mind And Genuinely Good Service

The biggest benefit with working with My Info Tech Partner is the peace of mind that a third party is thinking about our IT Requirements and Cyber Security Issues. This combined with their **proactive advice, promptly resolving our issues and offering a genuinely good service gives me the peace of mind to focus on my practice.**

I would recommend them to anyone suffering from a lack of peace of mind with their current IT firm and worried about the potential damage a cyber attack could cause to their practice.

Cameron Gruber, Director, Red Fox Business Solutions

Gives Me Peace of Mind with Personalised Services and Always Accessible

The biggest benefit we've had since working with My Info Tech Partner is the **Peace of Mind that someone is managing our IT, keeping us safe leaving us problem free.** This combined with their calm and professional approach lets us know everything is in hand and I can concentrate on running my business.

If you're are sitting on the fence and wondering why should I choose My Info Tech Partner? It's simple, they offer personalised services and are always accessible.

Dani Van Schelven, Director, Hot Books 2.0

Reliable, Saves Us Money And Takes All Your IT Worries Away

The biggest benefit we've had since working with My Info Tech Partner is they are reliable in delivering the services we need. This combined with their **proactive approach helps resolve small issues before they turn into big expensive problems,** saving us money.

If you're are sitting on the fence and wondering why should I choose My Info Tech Partner? It's simple, they take all your IT worries away.

Marius Wieczorek, General Manager, PFWA

Quick Resolution and Unheard of Customer Service!

PO Box 317, Bentley, WA, 6102
Tel. 08 6244 2556 www.myinfotechpartner.com.au info@myinfotechpartner.com.au
ABN: 40 607 937 879

my InfoTech partner

After two attempts from other providers we called in My Info Tech Partner. [They] quickly identified and resolved the problems, installed the new modem. [They] **also looked for and resolved a number of other errors and an industry first – [they] followed up to ensure everything was operational** after 48 hours.

Clyde Hudson, Director, Clyde Hudson and Associates

Saves us Time and Money, Unheard-of Communication for an IT Firm and Highly Recommended

Operating a Real Estate office, **this system has saved us time and money on countless occasions.** We rely on having access to historical records to help resolve disputes and the day to day operation of the practice. My Info Tech Partner are extremely prompt and thorough with their services as well as being friendly, approachable and very communicative – not something that you find often with IT companies! I would highly recommend My Info Tech Partner and an email archiving solution to any practice.

Chelsea Bruhn, Director/Licensee, Peter Bruhn and Associates

Punctual, Resolved Quickly and Highly Recommended

My Info Tech Partner were very good, [they] arrived at the specified time and **took no time at all to analyse the problem and rectify it. I would highly recommend [them]** for your computing problems.

Lynton Vivian, Owner, Hearth House Midland

DESTEC ENGINEERING PTY LTD

Gives Me Peace Of Mind And Extremely Responsive

The biggest benefit to working with My Info Tech Partner is the peace of mind that our data is backed up and can be recovered in real time and remotely with our multiple locations. This **compounded with their knowledge of our needs and their quick response time gives us great confidence moving forward.**

I would recommend them to anyone that is unsure of what their options are and what the best way is to solve their unique challenges.

Colin Bloomfield J.P., Director – Destec Engineering

PO Box 317, Bentley, WA, 6102
Tel. 08 6244 2556 www.myinfotechpartner.com.au info@myinfotechpartner.com.au
ABN: 40 607 937 879

Excellent Communication And Follow Up

The biggest benefit I have received since working with My Info Tech Partner is their **communication and follow up. They constantly keep me up to date** with progress of jobs and projects, so I know where things are at and what the fix was to the problem.

I would recommend them to anyone looking for an IT firm that is frustrated by a lack of communication and follow up.

Sarah Maguire, System Administrator – Australian Marine Complex Common User Facility

PO Box 317, Bentley, WA, 6102
Tel. 08 6244 2556 www.myinfotechpartner.com.au info@myinfotechpartner.com.au
ABN: 40 607 937 879