3 SUREFIRE SIGNS

Your IT Company Is Failing To Protect You From Ransomware

NEW And Critical Changes To Cyber Security, Insurance Coverage And Threats That Will Put Your Business At Serious Risk If Not Addressed Immediately

IT PROS
MANAGEMENT
AN IT PROS HOLDING COMPANY

Discover what the vast majority of businesses don't know and haven't been told about changes to cyber security risks, insurance requirements and threats that are allowing them to operate at UNDER APPRECIATED RISK for a crippling cyberattack and subsequent costs, lawsuits and fines – and what to do about it now.

IT PROS
MANAGEMENT
AN IT PROS HOLDING COMPANY

Provided By:

IT Pros Management

Author: Randy Martinez

303 N. Glenoaks Blvd Suite 200 Burbank, CA 91502

www.itprosmanagement.com **(866) 487-7671**

ABOUT THE AUTHOR

Randy Martinez

Vice President Technical Services

IT Pros Management

Randy's Top Areas of Expertise:

- Cybersecurity
- Microsoft 365 Implementations
- Microsoft Silver Partner
- Virtual Chief Information Officer (vCIO)
- Virtual Chief Security Officer (vCSO)
- Cloud Computing Infrastructure
- Published Author
- Business Start Up Consultant

As a Virtual Chief Information Officer (vCIO)and Virtual Chief Security Officer (vCSO) for several businesses and non-profits he's helped hundreds of organizations experience explosive growth while guiding them down the complicated technology path in a secure manner by implementing customized technology solutions to allow for scaling as well as future proofing the technical investments his clients make. He's a highly sought-after speaker and the co-author of the Amazon Best Seller "On Thin Ice" a comprehensive guide on cybersecurity and "RELAX" I.T. is Covered".

The Truth Nobody Is Telling You

About IT Security

All of the hard work, investments and time you've put into growing your business is at HIGH risk due to the false information and half-truths you've been told by cybersecurity experts, IT companies and even your insurance provider.

You think your IT company or person has your network protected. You think you're doing everything right (or at least well enough). You think your insurance company will cover your losses and expenses if a breach occurs. You think your staff is being smart and not putting you at risk because you're already paying for security tools. You think your bank, credit card processing company or software vendor assumes all the risk for the payments you take and for credit card processing. And you think that because you're small, nobody wants to target you.

Worst of all, you think a data breach would be a minor inconvenience with very few negative effects or costs. And two years ago, you might have been right…

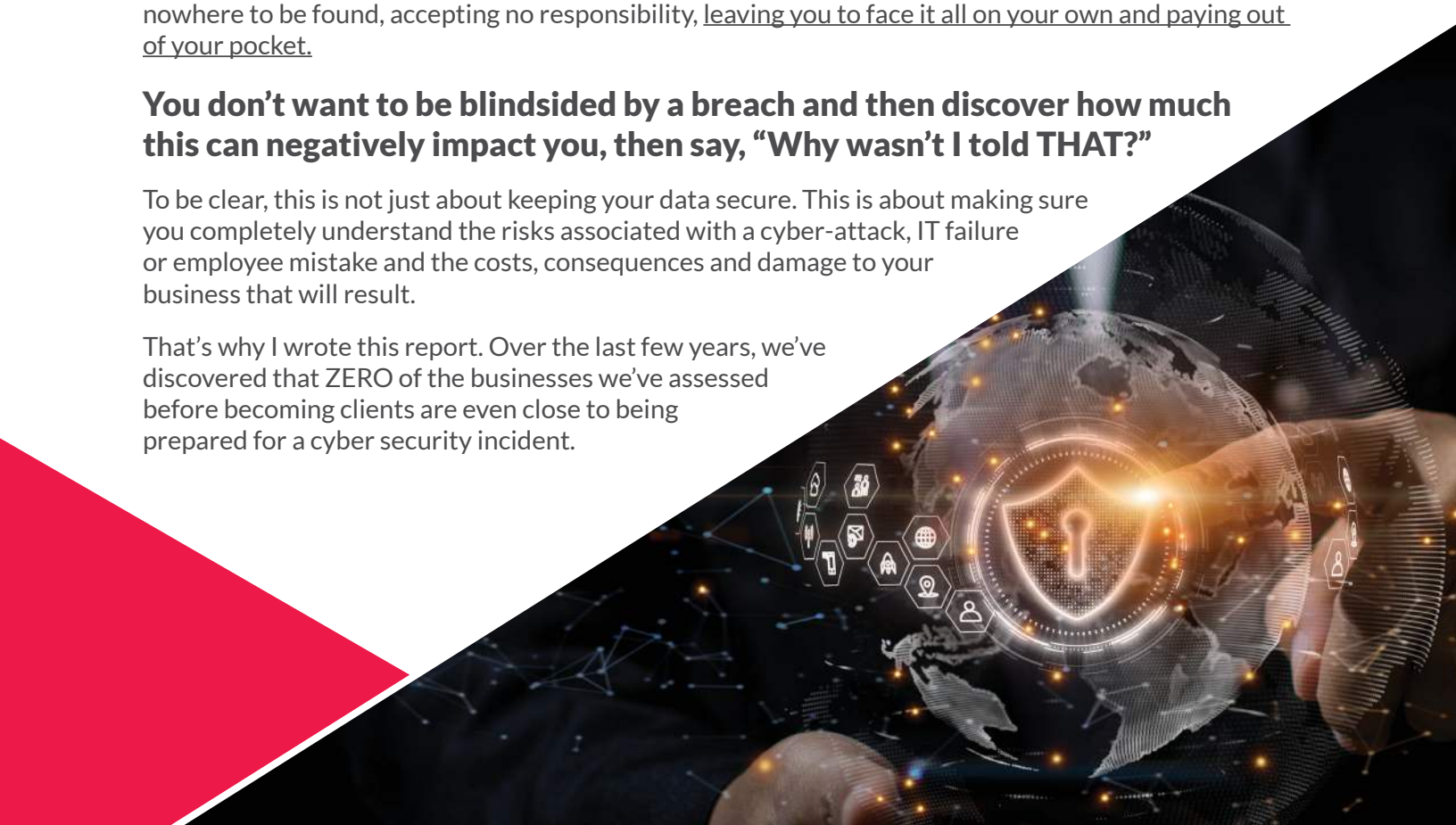
But today, ALL of these assumptions are wildly inaccurate – and if you're still operating on any of them, you are putting everything you've worked so hard to earn at risk of serious financial damages with far-reaching negative implications. Consider this report as your wake-up call. There have been significant changes over the last few years in cyber-attacks, what insurance will cover (and what's necessary to make sure your claim is not denied) and IT protections. The plan you put in place a year or two ago to deal with all of this is no longer viable.

We can practically guaranteethat what you've been told about keeping your business secure from hackers is either wildly inaccurate or insufficient and incomplete, putting you in a situation of underappreciated risk,and when a breach happens, those who sold you their secure solution will be nowhere to be found, accepting no responsibility, leaving you to face it all on your own and paying out of your pocket.

You don't want to be blindsided by a breach and then discover how much this can negatively impact you, then say, "Why wasn't I told THAT?"

To be clear, this is not just about keeping your data secure. This is about making sure you completely understand the risks associated with a cyber-attack, IT failure or employee mistake and the costs, consequences and damage to your business that will result.

That's why I wrote this report. Over the last few years, we've discovered that ZERO of the businesses we've assessed before becoming clients are even close to being prepared for a cyber security incident.



Not a single one

All of them were operating under the incorrect assumption that they were "secure enough," and they grossly underestimated the costs and wide-reaching negative impact a breach would have. Their trusted team of "experts," who are supposed to be informing them and protecting them, are FAILING to do their job. You are very likely in the same situation.

This means ifyou were to experience a breach (and it's getting more and more likely you will), your staff would instantly be hit with a crushing workload of cleanup to recover from the breach and to deal with the auditors, the FBI and the attorneys who will overwhelm them with things they demand. You would also be financially devastated by the destruction, as well as the emergency IT services and legal fees and services you would be forced to pay for just to get back up and running. Worse yet, there is a very good chance your insurance claim could be denied or not fully paid out due to your failure to do the things we've outlined in this report.

This is NOT a subject you want to take lightly or "assume" you have handled. Your cyber security program should NOT be entirely abdicated to your IT director, IT department or company. It should not be assumed that because you are investing tens of thousands of dollars in cyber security that you are actually protected from a cyber-attack. YOU need to get the facts about what it means to be secure and make choices about what risks, if any, you are willing to take, because it will be yourcompany's reputation at stake and your financial responsibility should a breach happen.

Bottom line, small and mid-sized businesses are the #1 target for cyber criminals for reasons we'll discuss in this report – and you have almost certainly NOT been given a plan that is 1) complete, 2) practical, and 3) affordable. Your parachute is full of holes, and you are completely without a backup chute that will deploy.

QUESTION: When was the last time your current IT company had THIS conversation with you?

What HAVE they told you about these new threats? If they have been silent, then I would urge you to read this report in full and act on the information urgently.

Hackers Won't Break Into To My Business… We're Too Small. My Staff Is Too Smart. We're Good,

You Say?

Don't think you're in danger because you're a "small" businessand don't have anything a hacker would want? That you have "good" people who know better than to click on a bad e-mail or make a mistake? 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 simply inadequate ones. In fact, SMALL organizations like yours are the target because you're infinitely easier to compromise. Hackers are unethical, but not stupid.

You have a twist tie locking the gate to a veritable goldmine of prize data that can be sold for millions of dollars on the dark web. Let's be clear: You are dealing with highly sophisticated cyber criminals who can outsmart -and have outsmarted - extremely competent IT teams working for large organizations and government entities. You and your staff are NOT above making a mistake or being duped.

Further, most of the businesses that get breached are not "handpicked" by hackers – that's not how they operate. They run grand-scale operations using automated software that works 24/7/365 to scan the web and indiscriminately target as many victims as they can. Like commercial fishing boats, they cast wide nets and set baited traps – and yes, small medical practices DO get targeted and DO get breached every day – and the attacks are escalating.

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 absolutely surefire way to leave yourself wide-open to these attacks.

Are you 100% sure you're "too small" to deal with a hacker who exposes your sensitive data? Are you "too small" to worry about paying the ransoms and costs that you will incur? According to Osterman Research, the AVERAGE ransomware demand is now $84,000 (source: MSSP Alert) – and that does not include fines, lawsuits, emergency IT services or lost business.

You may think to yourself, I will just go out of business. I could just start over. Here's the thing: the hackers often figure out exactly how much money you have so they can make sure to ask for just enough that you will pay it rather than go out of business. They also leave back doors so they can pop back in and "harvest" your network again in a couple of years when you recover.

How Bad Can It Be?

My Insurance Will Cover Me, Won't It?

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

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

For starters, getting even a basic cyber liability policy today may require you to attest that you have certain security measures in place, such as multifactor authentication, password management, endpoint protection, third-party penetration testing and tested data backup solutions. These carriers want to see phishing training and cyber security awareness training in place, and some will want to see a WISP and/or a Business Continuity Plan from your organization. Depending on the carrier, your specific situation and the coverage you're seeking, the list can be even longer.

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

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

Exactly How Can Your Business Be Damaged By Cybercrime?

Let Us Count The Ways

1. Loss Of ClientsAnd Revenue

If you are breached, you will be forced to notify your clients and employees that you exposed their private information to hackers.

Do you think all your clients will rally around you? Offer 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 them, "Sorry, we exposed your sensitive information and financial data to criminals because we didn't think it would happen to us," or "We didn't want to invest in protecting your data because we're small." That will not be sufficient to pacify them and the trust you've worked so hard to build will be destroyed.

It's true that someof your clients, employees and business associates will be understanding. Some won't even care. But you can bet there will be asmall percentage of your clients or employees who become irate and maybe even report you to the local news – and it only takes ONE lawsuit to make your life miserable. Worst case, they find an attorney who will take their case for invasion of privacy. Even if they don't have a case and cannot prove damages, do you really need that headache?

At the very least, they will cancel their contracts with you and be sure to tell their friends and family how you put their personal, business and financial data at risk of exposure to criminals. Let's say it's only 20% - can you really afford to lose 20% of your clients overnight, along with their friends and family members who are (or could be) potential clients?

2. Legal Fees And Law suits

When a breach happens, you will incur emergency IT support and services that can quickly run into thousands of dollars. You and your already busy, overburdened staff will be forced to take time to respond. You will be questioned and investigated and will likely want to retain the services of an attorney to represent you or negotiate with the hackers. None of this will be cheap and it will have a lasting, negative effect on your business.

3. Cost After Cost

According to Cyber Security Magazine, 61% of all SMBs have reported at least one cyber-attack during the previous year. So, 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…

Depending on the data you host, you may even be investigated and questioned by authorities and clients 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.

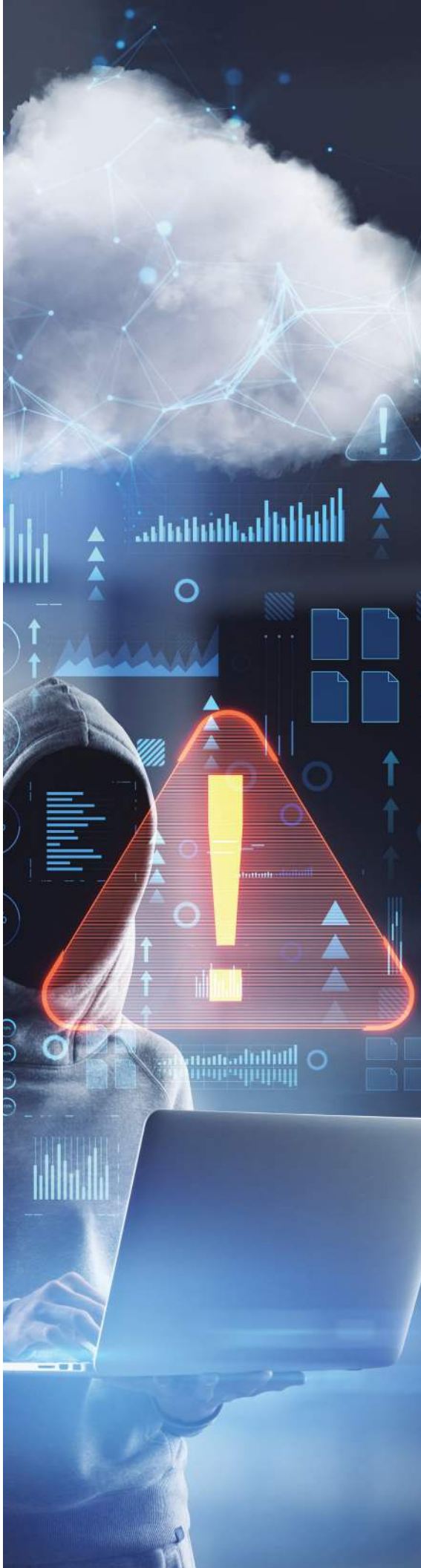
If the breach becomes public, your competition will have a heyday over this. Clients will be IRATE and will take their business elsewhere. Morale will tank and employees may even blame YOU. Your bank is NOT required to replace funds stolen due to cybercrime (goask them), and unless you have a very specific type of insurance policy for these matters, any financial losses will be denied coverage by your general business liability insurance.

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.

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. The FCC reported that theft of digital information has become the most commonly reported fraud, surpassing physical theft. Costs and losses from cyber-attacks are rising due to extended downtime and the sophistication of attacks. And now the Russia-Ukraine war is creating great concern over Russian hackers taking aim at Americans in retaliation for tough sanctions put in place.

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

According to the IBM Cost Of Data Breach Report, the cost for lost or stolen records is between $150 to $225 per record compromised, after factoring in IT recovery costs, lost revenue, downtime, fines, legal fees, etc. How much sensitive data do you have? How many employees? Multiply the number of clients you support, and the number of employees' data you have by $150 on the conservative side, and you'll start to get a sense of the costs to your business.



Here are just a few of the costs you might not have considered

- Paying the ransom to get your data back. According to Palo Alto, the average ransomware payment is just north of $920,000 nowadays.
- Credit and ID theft monitoring for EVERY person impacted, at a cost of $10 to $30 per record.
- Costs of your staff having to deal with a tsunami of paperwork, phone calls, tasks and projects to clean this mess upand deal with the recovery, which takes them away from the productive work you hired them to do.
- The fees and IT costs to remediate all of your insurance company's forensic findings and re-establishing working agreements within your supply chain.
    - If the breach involves a computer that transmits or hosts credit card data:
    - Fees of $500,000 per incident for being PCI non-compliant
    - Increased audit requirements
    - Potentially increased credit card processing fees
    - Potential for company-wide shut down of credit card activity by your merchant bank, requiring you to find another processor

In A World Full Of Marketing Promises, How Do You Know Your Current IT Company Is ACTUALLY Doing A Great Job?

It's very possible that you are being ill-advised by your current IT company. What have they recently told you about the new threats emerging over the last 3 to 6 months? Are they meeting with you on a quarterly basis to go over a recent third-party analysis of your environment to ensure you are still secure? Situations can change in an instant – if they are not truly monitoring your environment daily, scanning quarterly and in constant communication with you (or a key person on your staff) about security, they are NOT doing their job.

There could be several reasons for their failing you.

First, and most common, they might not know HOW to advise you, or even that they should. Many IT companies know how to keep a computer network running but are completely out of their league when it comes to dealing with the advanced cybersecurity threats we are seeing today. Many of these IT firms will tell you to your face that they are doing everything to protect you, but upon simple inspection, they prove grossly negligent in making sure your (let alone their) systems are secure and able to with stand current cyber threats.

That doesn't stop them from selling you IT services. They might even tell you they're keeping you secure, but when you get breached, they'll point the finger at you saying YOU didn't want to spend the money on security, and they didn't warranty that you wouldn't get a breach or that they were keeping you compliant, leaving you to completely handle this on your own and carry the damages and cost.

Here's a test: E-mail them and ask them, point-blank, "Can you assure me you are doing everything we need to ensure we're secure?" If they say yes, ask them to demonstrate it. You might find out that their story falls apart like a cheap suit. NOBODY (particularly IT guys) likes to admit they are out of their depth. They feel compelled to exaggerate their ability to avoid being fired and replaced – but it falls upon YOU to make sure you have the RIGHT company doing the RIGHT things.

Second, they may be "too busy" themselves or not have sufficient staff to truly be proactive with your account – which means they aren't doing the ongoing work that needs to be done (and they might still be charging you as if they were).

Third, they might just be cheap and unwilling to make the significant investment in the tools, people and training they need. Maybe they don't want to admit the service package they sold you has become OUTDATED and inadequate. Their cheapness CAN be your demise.

Is Your Current IT Company Doing Their Job?

Take This Quiz To Find Out

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

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

- ☐ **Have they met with you recently – in the last three 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 two-factor authentication 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 asked to see your cyber liability insurance policy?** Have they verified they are doing everything your policy REQUIRES to avoid having a claim denied in the event of a cyber-attack? Insurance companies don't make money paying claims; if you are breached, there will be an investigation to prove you weren't negligent and that you were actually doing the things you've outlined in your policy.
- ☐ **Do THEY have adequate insurance to cover YOU if they make a mistake and your business is compromised?** Do you have a copy of THEIR CURRENT policy? Does it specifically cover YOU for losses and damages? Does it name you as a client?
- ☐ **Have you been fully and frankly briefed on what to do IF you get compromised?** Have they provided you with a response plan? If not, WHY?
- ☐ Have they told you if they are outsourcing your support to a third-party organization? **DO YOU KNOW WHO HAS ACCESS TO YOUR BUSINESS AND THE DATA IT HOLDS?** If they are outsourcing, have they shown you what security controls they have in place to ensure that 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 provided you evidence that they have a third-party that audits their network?** Did you know that if their network gets hacked, the hackers will have access to your network too? If you haven't seen evidence of their third-party audits, request it immediately.
- ☐ **Have they kept their technicians trained on new cybersecurity threats and technologies, rather than just winging it? I**f they don't have a way to show you that their team is learning about threats hitting your industry and to validate that their team is up-to-dateon current security protocols, how can they guarantee providing you with secure solutions?
- ☐ **Do they have a ransomware-proof backup system in place?** One of the reasons the Wanna Cry virus was so devastating was because it was designed to find, corrupt and lock BACKUP files as well. ASK THEM TO VERIFY THIS. You might *think* you have it because that's what your IT vendor is telling you.
- ☐ **Do they have controls in place to force your employees to use strong passwords?** Do they require a PASSWORD management system to prevent employees from using weak passwords? If an employee is fired or quits, do they have a process in place to make sure ALL passwords are changed? Can you see it?
- ☐ **Have they talked to you about replacing your old antivirus with advanced endpoint security?** Anti-virus tools from two or three years ago are useless against today's threats. If that's what they have protecting you, it's urgent you get it resolved ASAP.
- ☐ **Have they implemented "multifactor authentication," also called 2FA or "two-factor authentication," for access to highly sensitive data?** Do you even know what that is? If not, you don't have it.
- ☐ **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?** I know no one in YOUR office would do this, but why risk it? Adult content is still the #1 thing searched for online. Then there's gambling, shopping, social media and a host of other sites that are portals for hackers. Allowing your employees to use unprotected devices (phones, laptops, tablets) to access these sites is not only a security risk but a distraction where they are wasting time on YOUR payroll, with YOUR company-owned equipment.
- ☐ **Have they given you and your employees ANY kind of cybersecurity awareness training?** This is now required for insurance providers to cover breaches. Employees accidentally clicking on a phishing e-mail or downloading an infected file or malicious application is still the #1 way cyber criminals hack into systems. Training your employees FREQUENTLY is one of the most important protections you can put in place. Seriously.
- ☐ **Have they properly configured your e-mail system to prevent the sending/receiving of confidential or sensitive data?** Properly configured e-mail systems can automatically prevent e-mails containing specified data, like social security numbers, credit cards, and other sensitive data from being sent or received.
- ☐ **Do they allow your employees to connect remotely using GoToMyPC, LogMeIn or TeamViewer?** If they do, this is a sure sign you should be concerned! Remote access should strictly be via a secure VPN (virtual private network).
- ☐ **Have they had a third-party analyze your network to validate their work?** You would never attempt to proofread your own work. Why would you expect your IT person to? Many regulatory bodies require at a minimum an annual third-party assessment for this reason.

Security Is NOT Compliance –

Make Sure Your IT Company Is Taking These 3 Steps

As previously discussed in this report, a mistake many organizations make is thinking that because they're compliant, they are automatically secure. Sorry. Not so. You can be compliant and completely insecure, but there are three key steps to ensure you are actually secure.

Most IT companies are only doing one or two of the three. You want to make sure they are checking ALL the boxes so if and/or when a breach occurs and you get audited, you are brilliantly prepared, and the damages are minimized. Here they are in order:

1. A regularthird-party security assessmentwith a remediation plan.

Hackers are constantly coming up with new ways in. Security tools that worked just two years ago are no longer are sufficient today. If they aren't having a third-party security assessment performed at least every quarter like clockwork, they are missing gaping holes that are actively being exploited by hackers. Problem is, this is where most businesses stop and don't go on to steps 2 and 3 below.

2. Full and true IMPLEMENTATION of their plan.

Best-laid plans are worthless if not implemented. You can give a patient a treatment plan – but if they refuse to follow it, or skip steps and cherry-pick your advice, they cannot expect to get well.

Same goes for security – your IT consultant should be giving you options, timelines and a weighing of pros and cons for choices you make about how to implement a plan to become compliant based on your risk tolerance, situation, budgets, resources, etc. A good IT company or consultant will guide you through this.

But the most important aspect is to make absolutely certain that the IT team or company you put in charge to implement the remediation plan is actually doing it. Based on our personal experience, 90% of the companies selling outsourced IT services and support are NOT being diligent about the full and complete implementation of a security and compliance plan.

In a world of marketing promises, how do you know your IT and security partner is delivering as promised? Please see the previous section of this report to know if they are truly implementing the plan. Further, we are offering a free, independent Security Assessment to audit your current IT company and tell you the truth about what they are (or aren't) doing for you.

3. Documentation

This is the part most IT companies and medical practices skip. Behind every security compliance measure is a documentation requirement.

If you have a breach and subsequently get audited, you will be required to produce documentation of your security activities and policies. If you do not have those documents, your business will not be able to sustain a major attack or breach. If you do not have documented plans for how to address a ransomware attack, data breach, or disclosure and clear instructions on who needs to do what when, you are putting yourself and your business at risk of not surviving the consequences.

Will You Wait Until You Actually Have A Breach Or Report Filed Against You Before Doing Something About It?

Over half of all home security systems and cameras are bought (or beefed up) by homeowners after a burglary or home invasion. Across the country, warnings of bad storms drive hordes of people to the store to stock up on water, food and other supplies – and anyone who hesitates or waits to hit the store AFTER work or WHEN they have the time often arrives to find the store shelves empty, and the remaining picked-over supplies at jacked-up prices.

We are strongly cautioning against any assumption that you are truly protected and prepared should a breach occur, or should you get reported for a violation. Fire prevention is infinitely cheaper, less stressful and more orderly than having to call the fire trucks and work the hose when your house is ablaze. Cancer is BEST treated when found EARLY and aggressively treated, not left to get worse until the point of no return.

The time to have an in-depth, fresh look at the state of your security program is right now, with a friend who has your best interests in mind

- NOT an insurance agent or an attorney
- when there is no crisis happening, no auditors calling, no security breach occurring.

Our Free Preemptive IT Security Analysis Will Reveal If Your Current IT Company Is Doing What They Should

Over the next couple of months, we will be conducting free Security Assessments for CEO(s), CFO(s) and COO(s) to find and expose vulnerabilities and failings in your security BEFORE a cyber event happens.

Fresh eyes see things – so the biggest value of our Assessment is getting us to sit on YOUR side of the table and give you straight answers to whether or not your IT company or person is actually doing what they should to minimize your chances of experiencing a breach and minimize the losses that can occur. You get a "Sherlock Holmes" investigating on your behalf.

Here's How It Works: We will conduct a thorough, CONFIDENTIAL investigation of your IT network, backups and security protocols through the lens of not only an IT company, but also from the perspective of a hacker and an insurance provider. Your time investment is minimal: 30 minutes for the initial meeting and one hour for the second meetingto go over our Report of Findings.

When this Assessment is complete, here are just a few of the most frequently discovered problems we are likely to uncover and the answers we'll be able to provide you.

- Is your current IT company or team actually implementing critical security protections, protocols and systems that would not only minimize the chances of a breach, but also ensure your insurance claims would not be denied due to not following through on something YOU agreed to do on your insurance policy's declarations contingent for coverage?
- What are the least expensive, most impactful things you can do to secure your network and avoid getting slapped with "Willful Neglect" should a breach happen?
- Is your security configured well enough that you can pass a simple cybersecurity analysis called a penetration test? We'll issue one and be able to demonstrate, in a matter of hours, if your IT company is doing their job or completely failing you.

All of these are tiny "ticking bombs" in your security, waiting to go off at precisely the wrong time. We urge you to go to the URL below and book your

FREE Cyber Security Analysis

https://www.cybersecanalysis.com/

When Others Audit – Insurance Companies, Government Regulators – There Is No Kindness

Government auditors and insurance providers won't give you the benefit of the doubt. They know what to look for and where the failings typically occur. They are experienced in finding lax protocols and know what stones to turn over.

When such audits reveal problems, there is serious stress and strain placed on your staff and on you personally. Tensions rise, fingers get pointed and resentment can build. Your own preventive, independently conducted, completely confidential compliance assessment is the ONLY practical way to prevent embarrassment or worse consequences. It's also the smart way to unearth problems you can fix now.

Candidly, no one should proofread their own work – so if you do have an IT company you are paying, this will give you a free, no-risk way to tell for sure if they are doing the job you're paying them to do.

Please…Do NOT Just Shrug This Off

(What To Do Now)

If you have scheduled an appointment, you don't have to do anything but be sure to show up, ready with any questions you might have.

If you prefer to talk to us first, call us at **(866) 487-7671** or
send me an e-mail at **randy@itprosmanagement.com.**

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 mistake, malware infestation or even a 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.

Dedicated to serving you,

Randy Martinez

www.itrposmanagement.com **randy@itprosmanagement.com** **(818) 519-9866**

Why IT Pros Management Is Uniquely Qualified

To Advise You In This Matter

IT security has brought high-fee “experts” out of the wood work who are, quite honestly, woefully inexperienced and uninformed. Software and IT companies, medical practice consultants and even insurance agencies see this as their golden opportunity, rushing to present themselves as saviors.

But how do you know someone actually has the depth of experience to handle this hyper critical part of your practice? For 12 years my organization has excelled at cybersecurity for small/medium size businesses and non-profits Here are just a few of the things that make us uniquely qualified to handle your IT security needs:

Complete Visibility

An organization cannot defend assets it does not know about. This is increasingly becoming. important as the workplace expands outside of the office to remote work situations and bring your-own-device policies that give employees more flexibility to do their work.

IT Pros Management can provide a comprehensive prevention strategy provides solutions to combat threats outside of the physical security that an organization would traditionally have.

Reduce the Attack Surface

Often times, hardware and software come preconfigured with unnecessary applications and insecure default settings for ease of use. This adds complexity to the threat landscape and enriches the attack surface of an organization. IT Pros Management prevention-centric solutions reduces the number of items that are insecure by design, removing threat vectors that an attacker could use to compromise a system.

Stop KnownThreats

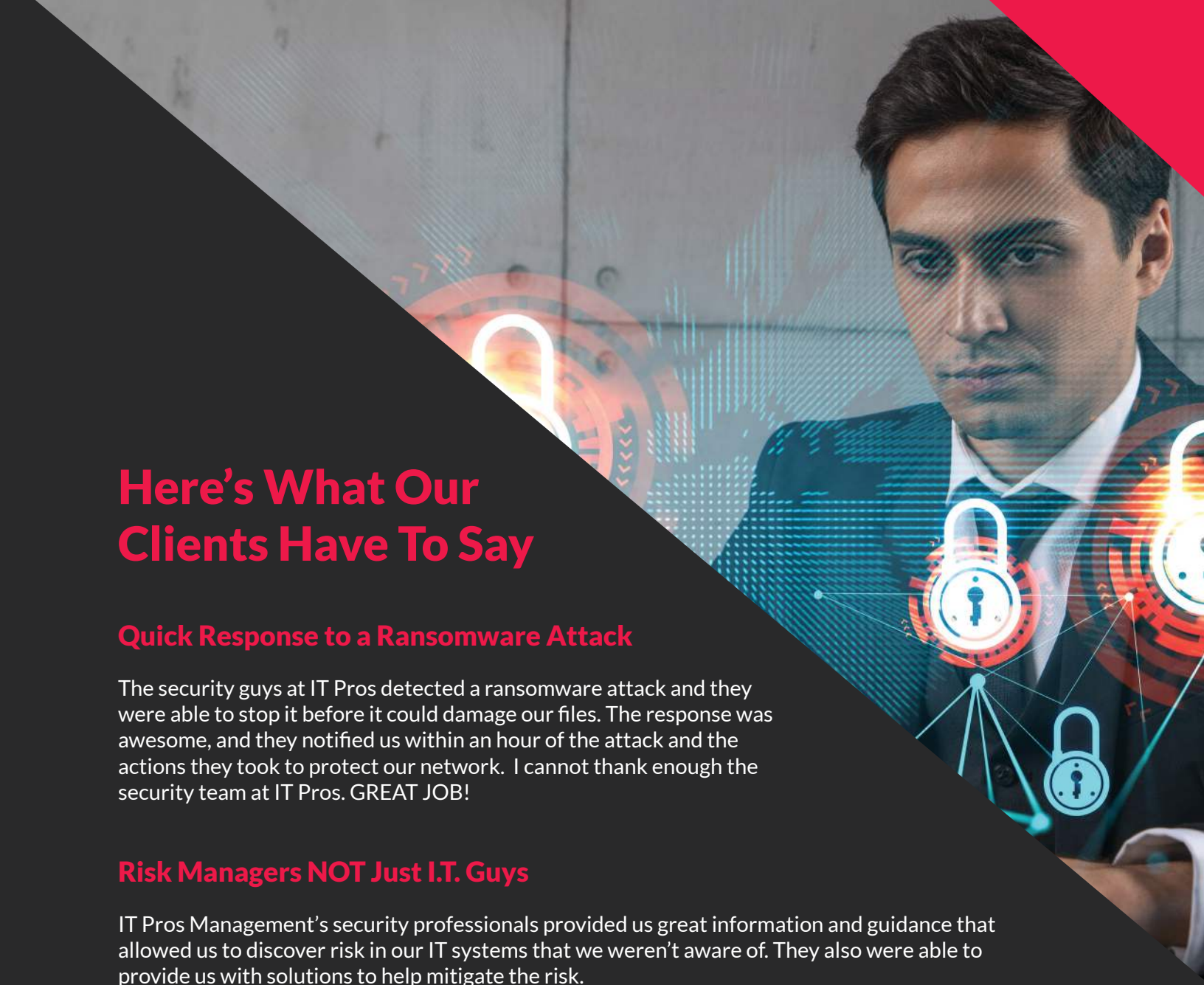
There is a wealth of intelligence regarding known malicious files and threat vectors that have been used by threat actors to compromise an organization. IT Pros Management's Security Operation Center (SOC) compile this informationand use it to protect anorganization's assets isone of the easiest ways to implementing a prevention centric approach to secure an organization's assets.

Prevent UnknownThreats

Traditional antivirus solutions rely on malware signatures— unique fingerprints that represent a specific, known threat. In today's sophisticated threat landscape, this approachis no longer adequate. IT Pros Management uses a comprehensive protection suite coupling machine learning and artificial intelligence to catch unknown and evolving threats to stay ahead of attackers.

Automation with Human Validation

The increasing use of security tools using AI and machine learning to prevent threats is a double-edged sword. While the protection is superb, no solution is perfect. There is the slim chance that a threat will go undetected by the AI, while legitimate files may be incorrectly flagged as malicious. This is where IT Pros Management's trained security professionals come into play— remediating threats that fly under the radar while validating benign files that are classified as a threat.



Here's What Our Clients Have To Say

Quick Response to a Ransomware Attack

The security guys at IT Pros detected a ransomware attack and they were able to stop it before it could damage our files. The response was awesome, and they notified us within an hour of the attack and the actions they took to protect our network. I cannot thank enough the security team at IT Pros. GREAT JOB!

Risk Managers NOT Just I.T. Guys

IT Pros Management's security professionals provided us great information and guidance that allowed us to discover risk in our IT systems that we weren't aware of. They also were able to provide us with solutions to help mitigate the risk.

Stop Social Engineering in its Tracks

We looked around for a solution to social engineering that (a) worked, and (b) made things easy on our clients and end users. ID 20/20 checked all our boxes. There have been multiple social engineering attempts on our staff businesses since we adopted ID 20/20 software — but not a single one has been successful.

Stay a Step Ahead of Threat Actors

The difference between the legacy solutions that we used to rely on and the next generation tools that make up IT Pros Management's cyber security stack — it's like night and day. The advanced AI and machine learning have been particularly eye-opening. Threats to our network that we used to have no way of seeing are now easy catches.