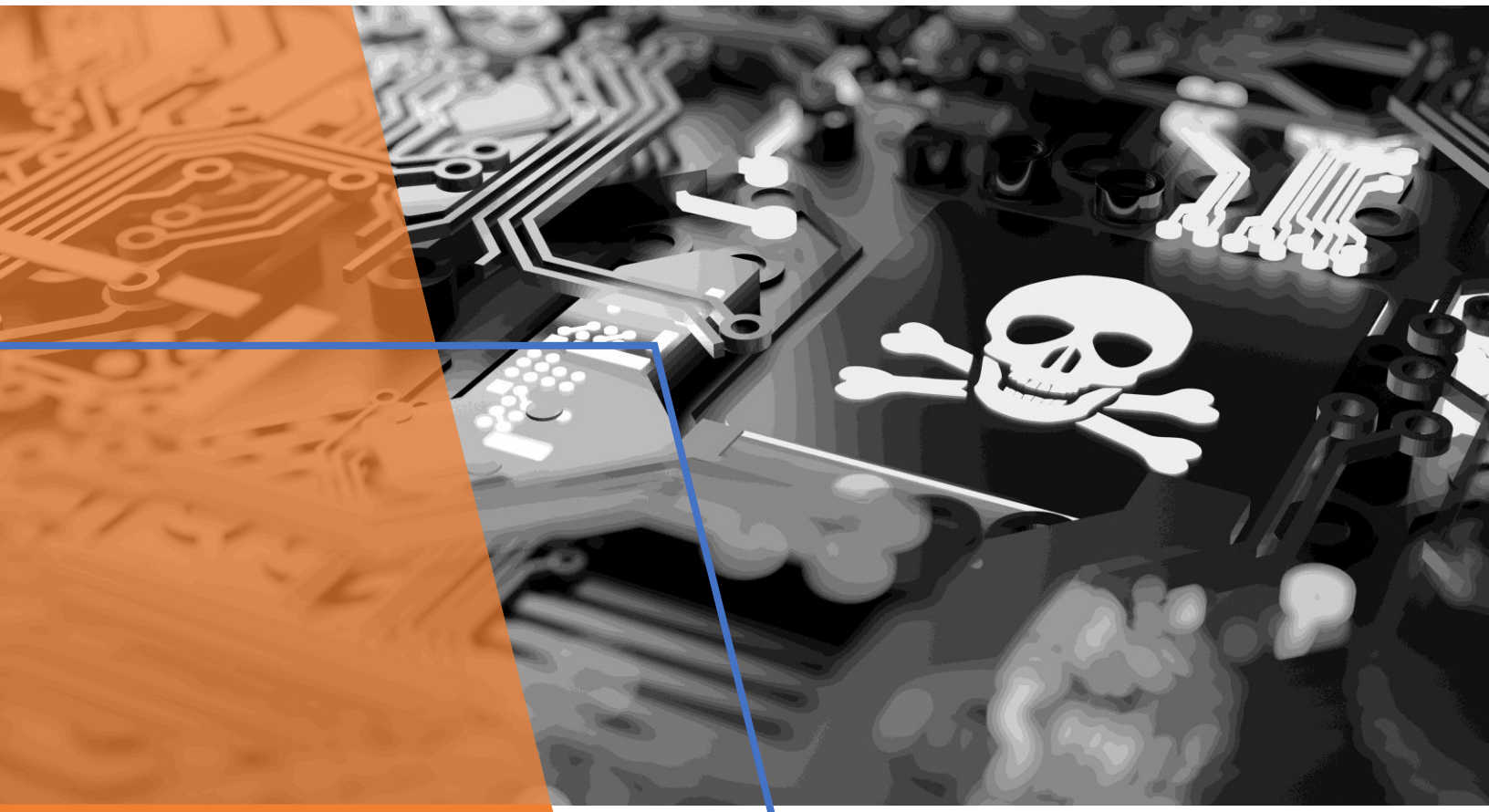
3 Surefire Signs

Your IT Company Is Failing To Protect Your Firm From Ransomware

NEW And **Critical Changes** To Cybersecurity, Insurance Coverage And Threats That Will Put Your Firm At Serious Risk If Not Addressed Immediately



CIO LANDING℠

3 Surefire Signs

Your IT Company Is Failing To Protect Your Firm From Ransomware

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

Discover what most law firms don't know and haven't been told about changes to cybersecurity risks, insurance requirements and threats that are allowing them to operate at **UNDERAPPRECIATED RISK** for a crippling cyberattack and subsequent costs, lawsuits and fines – and what to do about it now.

Provided By: CIO Landing
Author: Juan Carlos Bosacoma
1 Northfield Plaza, Suite 300, Northfield IL 60093
www.ciolanding.com
847-868-9253

About The Author

Juan Carlos Bosacoma, a distinguished figure in the IT industry with over 30 years of experience co-founded CIO Landing to deliver enterprise-grade technology solutions to small and medium-sized businesses. As a visionary and technical mastermind, Juan Carlos has steered CIO Landing from its inception to its current status as a beacon of innovation and cybersecurity excellence. His academic background, with a B.A. in Computer Science from the University of Buffalo and an MBA from the University of Chicago, laid a strong foundation for his illustrious career. Before founding CIO Landing, Juan Carlos hones his expertise at notable companies like Sami Burke, CAP Gemini, and Quaker Oats, and established one of Chicago's first Internet Service Providers, USHost.com, in 1995.

Under Juan Carlos's leadership, CIO Landing, originally known as IT Consulting Associates, has grown into a trusted partner for businesses in the Chicagoland and Miami, FL areas since 2012. The company offers a comprehensive suite of IT services, including outsourced CIO oversight, professional IT services, and technical support. CIO Landing is dedicated to making IT an asset for businesses, offering solutions like onsite IT service, network security, IT infrastructure management, cloud integration, and virtualization.

In addition to his professional achievements, Juan Carlos is a co-author, alongside Hernan Silva, of the Amazon best-selling book, "Sitting Duck: Why Your Business Is a Cybercriminal's Ideal Target." This work underscores his commitment to raising awareness about cybersecurity threats and protecting businesses from digital dangers. He is also a frequently requested speaker, providing educational sessions to small and medium-sized business owners about cybersecurity best practices, practical security advice, and the current cyber threat landscape.

Juan Carlos's certifications include Microsoft Certified Professional Specialist (MCPS), Microsoft Certified Networking Professional Specialist (MCNPS), and Microsoft Small Business Specialist (MSBS), which are a testament to his deep knowledge and skills in technology solutions. Outside of his professional life, he finds joy in paddle tennis, soccer, and spending quality time with his two children, friends, and family. He contributes to his community as a member of the Chicago CEO Roundtable, the Illinois Hispanic Chamber of Commerce, the University of Chicago Investment Club, and a board member of the Greater River North Business Association. Additionally, he serves as an ex-oficio for the Honorary Vice-Council of Bolivia, further demonstrating his diverse interests and commitment to civic engagement.

CIO Landing's success is also reflected in its recognition within the IT industry, including awards like the 2023 and 2024 CRN MSP 500 in the Security 100 category, and accolades from Channel Futures' NexGen 101 and as a Next-Gen Solution Provider Leader. These achievements highlight CIO Landing's role as a cybersecurity guardian and a pathfinder for strategic technology alignment for businesses aiming for growth and sustainability.

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 cyberattacks, 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 guarantee that 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 cyberattack, IT failure or employee mistake and the costs, consequences and damage to your business that will result.

To Reserve Your FREE IT Security Assessment,
please visit **www.ciolanding.com/discoverycall/**
or call our office at 847-868-9253.

That's why I wrote this report. Over the last few years, we've discovered that ZERO of the law firms we've assessed before becoming clients are even close to being prepared for a cybersecurity 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 if you 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 they'd have 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 cybersecurity 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 cybersecurity you are protected from a cyberattack. 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 your firm's reputation at stake and your financial responsibility should a breach happen.

Bottom line, small and mid-sized law firms are the #1 target for cybercriminals 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.

To Reserve Your FREE IT Security Assessment,
please visit **www.ciolanding.com/discoverycall/**
or call our office at 847-868-9253.

"Hackers Won't Break Into My Firm… 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" firm and 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, legal firms 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 law firms 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, legal practices DO get targeted and DO get breached every day – **and the attacks are escalating**.

Make no mistake – small, "average" firms are being compromised daily, and clinging to the smug ignorance of "That won't happen to me" is a 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.

To Reserve Your FREE IT Security Assessment,
please visit **www.ciolanding.com/discoverycall/**
or call our office at 847-868-9253.

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

But the biggest area of RISK that is likely being overlooked in your firm is the actual enforcement of critical security protocols required for insurance coverage. Insurance carriers can (and will) deny payment of your claim if you fail to implement the security measures required to secure coverage. When a breach happens, they will investigate how it happened and whether 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**.

To Reserve Your FREE IT Security Assessment,
please visit **www.ciolanding.com/discoverycall/**
or call our office at 847-868-9253.

Exactly How Can Your Firm Be Damaged By Cybercrime?

Let Us Count The Ways:

1. Loss Of Clients And 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 some of your clients, employees and business associates will be understanding. Some won't even care. But you can bet there will be a small 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 Lawsuits:

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.

To Reserve Your FREE IT Security Assessment,
please visit **www.ciolanding.com/discoverycall/**
or call our office at 847-868-9253.

3. Cost After Cost:

According to the American Bar Association, 25% of law firms reported a cyberattack in 2022, and that percentage is continuing to rise as data is collected for 2023. Additionally, 2023 saw numerous class actions filed against law firms citing they "failed to adequately protect the confidential information of clients" before the cyberattack. So, WHEN your firm 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 (*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.

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 law firms, large and small. The FCC reported that theft of digital information has become the most reported fraud, surpassing physical theft. Costs and losses from cyberattacks 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.

To Reserve Your FREE IT Security Assessment,
please visit **www.ciolanding.com/discoverycall/**
or call our office at 847-868-9253.

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 Networks, the average ransomware payment is just north of $920,000 nowadays.
- Credit and ID theft monitoring for EVERY person impacted, at $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 up and 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 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 a company-wide shutdown 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 regularly 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.

To Reserve Your FREE IT Security Assessment,
please visit **www.ciolanding.com/discoverycall/**
or call our office at 847-868-9253.

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 withstand 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.

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 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.

To Reserve Your FREE IT Security Assessment,
please visit **www.ciolanding.com/discoverycall**
or call our office at 847-868-9253.

Here they are in order:

1. A regular third-party security assessment with a remediation plan.

Hackers are constantly producing new ways to get in. Security tools that worked just two years ago are no longer 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 certain that the IT team or company you put in charge to implement the remediation plan is 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? It is your responsibility to ensure they are doing what they said they would. 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 some IT companies 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 and when you are putting yourself and your business at risk of not surviving the consequences.

To Reserve Your FREE IT Security Assessment,
please visit **www.ciolanding.com/discoverycall**
or call our office at 847-868-9253.

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– 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 law firms 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 your IT company or person is 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.**

To Reserve Your FREE IT Security Assessment,
please visit **www.ciolanding.com/discoverycall**
or call our office at 847-868-9253.

Here's How It Works: We will conduct a thorough, CONFIDENTIAL investigation of your IT network, 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 a one-hour meeting to 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 **implementing critical security protections**, protocols, and systems that would minimize and protect your firm from the chances of a breach?
- 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 vulnerability test? We'll issue one and be able to demonstrate, in a matter of hours, if your IT company is doing its job or completely failing you.

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 you. 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 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.

To Reserve Your FREE IT Security Assessment,
please visit **www.ciolanding.com/discoverycall**
or call our office at 847-868-9253.

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 847-868-9253 or send an e-mail to me at jc@ciolanding.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 cybersecurity "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 your security,

Juan Carlos Bosacoma
Web: www.ciolanding.com
E-mail: jc@ciolanding.com
Direct: 847-868-9253

Why CIO Landing Is Uniquely Qualified To Advise You In This Matter

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

But how do you know someone has the depth of experience to handle this hyper-critical part of your practice? For 12 years my organization has excelled at cybersecurity for legal firms.

Here are just a few of the things that make us uniquely qualified to handle your IT security needs:

- **Comprehensive Cybersecurity Approach:** We employ cutting-edge technology and deep expertise, tailored to meet the specific needs of law firms.
- **Proactive Protection with Advanced Tools:** Utilization of advanced endpoint protection software, incorporating AI technology, protects devices against a wide range of cyber threats. Continuous remote monitoring identifies potential malicious activity early.
- **24/7 Security Operations Center (SOC):** Offers real-time alerts on suspicious activities, ensuring quick incident response and minimizing damage to client environments.
- **Regular Reporting on Security Posture:** Through Technology Business Reviews, our clients are kept informed about emerging threats and the effectiveness of cybersecurity services.
- **Transparency and Trust:** Immediate action and clear communication with clients when threats are detected, building a trust-based relationship.
- **Customized Compliance Strategies:** Tailored cybersecurity frameworks, policies, and procedures ensure compliance with industry-specific regulations like HIPAA, GDPR, and SOC2.
- **Continuous Compliance Efforts:** Regular audits, employee training, and updates to security measures guarantee ongoing adherence to regulatory standards.
- **Data Privacy Assurance:** Strict adherence to U.S. data privacy standards, employing best practices and advanced data solutions for comprehensive data protection.
- **Extensive Training Approach:** Continuous education, practical experience, and vendor-specific training keep the team at the forefront of cybersecurity advancements.
- **Certifications:** The team holds prestigious certifications such as Fortinet NSE, CompTIA Security+, and ISC² Certified Cybersecurity, demonstrating their expertise and commitment to excellence.
- **Employee Cybersecurity Awareness Training:** We boost security by educating your employees to recognize and thwart cyber threats through weekly training videos.
- **ABA Tech Show 2024:** Juan Carlos Bosacoma was a featured speaker, leading two sessions on cybersecurity best practices for law firms.

To Reserve Your FREE IT Security Assessment,
please visit **www.ciolanding.com/discoverycall**
or call our office at 847-868-9253.

Here's What Our Legal Clients Have To Say

Tailored Solutions to Our Firm, Indispensable Partner

Their team of IT professionals is highly skilled, responsive, and proactive. They work to ensure that our systems are always up and running, which has helped to minimize disruptions to our organization. In addition, they have implemented robust cybersecurity measures that have significantly reduced the risk of data breaches, thereby protecting our sensitive client information.

– Edward J Vrdolyak, Managing Partner, Vrdolyak Law Group

Excellent and Reliable Business Partner

When we were searching for an IT company for our law firm, we chose CIO Landing because they were by far the ones who took the most time to understand our needs, answered our detailed questions, and recommended the best solutions.

– Debbie Herst, Business Manager, Law Office of Robert L Herst

Solved IT Problems Others Could Not

We hired CIO Landing, and we are very happy with the work they have done and resolved the problems our other IT company couldn't. We are confident they can handle any problem we have.

– Karen Conti, Founder, Conti Law

IT Security, Cost Effective

Avoiding data breaches and cyber-attacks requires vigilance. If you don't have the right systems in place, you can have major problems. We have worked with CIO Landing for more than 15 years to provide us with full IT support, which includes maintaining our system security and network monitoring. CIO Landing is very cost-effective.

– Marc J Siegel, Managing Partner, Siegel & Dolan

Here's What Our Legal Clients Have To Say

Never Worry About IT Problems, Bi-Lingual

I can testify that when it comes to handling IT situations or problems, CIO Landing has your back. It is so nice to never have to worry about ANY IT problems. The response time is on point and they are always working proactively and never reactively. They are a very well-managed company, and I would recommend them to anyone looking to secure their network. An added plus for us is that they are bi-lingual and that makes a lot of people feel very comfortable.

– Dalia Martinez, Former HR Manager, Vrdolyak Law Group

Quick and Responsive

CIO Landing is awesome! They are quick and responsive. Get the job done and a pleasure to speak with.

– Mary Del Rio, Vrdolyak Law Group

CIO Landing Spoils Us!

There are no technology obstacles CIO Landing can't overcome. We are spoiled! No matter what we throw at them, they solve the problem. They are our business partner as we think of them as an extension of our firm. We focus on our business and CIO Landing gives us peace of mind knowing our technology works!

– Mark Hearsh Esq., Castle Law Group

Responsive and Helpful

They migrated me from Google to Outlook, a monstrous task, and have remained fully engaged during the transition. Very responsive and helpful.

– Jordan Marsh, Trial Attorney, Law Office of Jordan Marsh LLC