The Cyber Security Crisis

CIO LANDING℠

www.ciolanding.com
888-308-8879

The Small Business Cyber Security Crisis

Urgent And Critical Protections Every Small Business 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. Businesses can no longer ignore it or foolishly think, "That won't happen to us."

Your business – large OR small – is at risk of being targeted and compromised.

Provided as an educational service by:

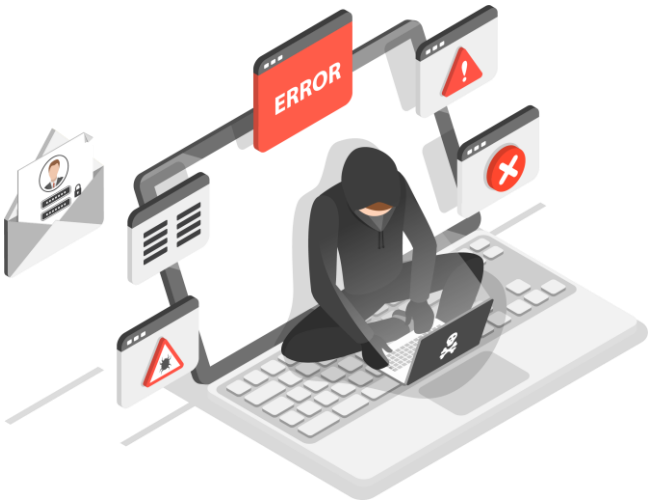
CIO Landing

888.308.8879 | www.ciolanding.com

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, mugging, carjacking, theft – get sympathy from others. They are called "victims" and support comes flooding in, as it should.



But if your business is the victim of a cybercrime attack where client or patient data is compromised, you will NOT get such sympathy. You will be instantly labeled as "stupid" or "irresponsible." **You may be investigated, and clients will question you 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 I.T. support company to protect you. Claiming ignorance is not an acceptable defense, and this giant, expensive and reputation-destroying nightmare will land squarely on YOUR shoulders.

But it doesn't end there…

According to national laws, you will be required to tell your clients and/or patients that YOU exposed them to cybercriminals. Your competition will have a heyday over this. Clients will be IRATE and leave in droves. Morale will TANK and employees will BLAME YOU. Your bank is NOT required to replace funds stolen due to cybercrime (*go ask them*), and unless you have a very specific type of insurance policy, any financial losses will be denied coverage.

Please do NOT underestimate the importance and likelihood of these threats. It is NOT safe to assume your I.T. 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.

Why We Are So PASSIONATE About Informing And Protecting YOU

At CIO Landing, we specialize in being the I.T. department for small to mid-sized businesses nationwide. Our team has a security-centric approach to managing your I.T. because we have seen far too many businesses victimized by cyberattacks.

Our world runs on data and the integrity of our systems relies on strong cybersecurity measures to protect them. Weak cybersecurity measures can have a massive impact, but strong cybersecurity tactics can keep your data safe.

By assessing your business's cybersecurity risk, making companywide changes, and improving data protection, it's possible to guard your business against most data breaches.

Over the last couple of years, we have seen a significant increase in calls from business owners desperate for help after a ransomware attack, data breach event or other cybercrime incident.

When they call, they're desperate, scrambling for anyone who can help them put the pieces back together again. Often their business is completely on lockdown. ALL their data has been corrupted or held for ransom, preventing them from fulfilling obligations they have to their clients. **YEARS of work and critical data – *all gone*.**

They're also scared and *intensely* angry. They feel violated and helpless. Embarrassed. How can money be taken from their bank account WITHOUT their permission or knowledge? Why didn't their I.T. company or I.T. team prevent this from happening? *How are they going to tell their clients/patients that they've exposed them to cybercriminals*? They're in complete disbelief that they fell victim – after all, they "didn't think we had anything a cybercriminal would want!"

We know how hard you work to make your company succeed. We understand the risks you've taken, and the personal sacrifices you've made. To us, it's a GROSS insult to have it all taken away by some cyber-scumbag who will NOT be held accountable for their actions.

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 current I.T. company or team.

This is not a topic to be casual about. Should a breach occur, your reputation, your money, your company, and your neck will be on the line, which is why you must get involved and make sure your company is prepared and adequately protected, not just pass this off to someone else.

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 I.T. department.

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

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

He HAD an I.T. team in place that he believed was protecting them from a data breach – yet the manager of his billing department was able to download a file-sharing program to the company's network to listen to music and unknowingly left her documents folder (which contained over 9,000 patient files) open for sharing with other users of the peer-to-peer network.

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

After filing some 5,000 pages of documents to Washington, he was told the information he had 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 business elsewhere. His insurance providers refused to renew their policies.

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

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

Don't think you're in danger because you're "small" and not a big company like Experian, J.P. Morgan or Target? That you have "good" people and protections in place? That it won't happen to you?

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

Right now, there are over 980 million malware programs out there and growing (source: AV-Test Institute), and 70% of the cyber-attacks occurring are aimed at small businesses (source: National Cyber Security Alliance); you just don't hear about it because the news wants to report on BIG breaches OR it's kept quiet by the company for fear of attracting bad PR, lawsuits and data-breach fines, and out of sheer embarrassment.

Schedule Your Free Cyber Security Risk Assessment Today!
Visit www.ciolanding.com/csa/ or call our office at 888-308-8879.

In fact, the National Cyber Security Alliance reports that **one in five small businesses have been victims of cybercrime in the last year** – and that number includes only the crimes that were reported. Most small businesses are too embarrassed or afraid to report breaches, so it's safe to assume that number is much, much higher.

Are you "too small" to be significantly damaged by a ransomware attack that locks all your files for several days or more?

Are you "too small" to deal with a hacker using your company's server as **ground zero** to infect all your clients, vendors, employees and contacts with malware? Are you "too small" to worry about someone taking your payroll out of your bank account? According to Osterman Research, the AVERAGE ransomware demand is now $84,000 (source: MSSP Alert). It's also estimated that small business lost over $100,000 per ransomware incident and over 25 hours of downtime. Of course, $100,000 may not sink your business, but are you okay to shrug this off? To take the chance?

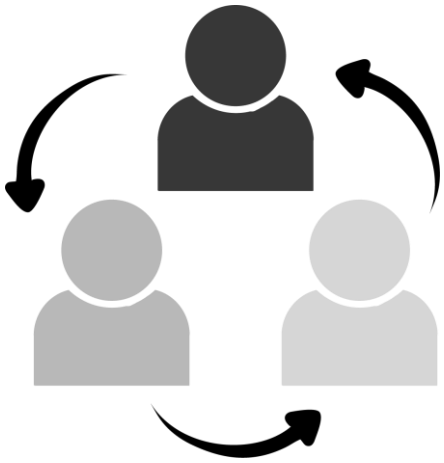
It's NOT Just Cybercriminals Who Are The Problem

Most business owners erroneously think cybercrime is limited to hackers based in China or Russia, but the evidence is overwhelming that disgruntled employees, both of your company and your vendors, can cause significant losses due to their knowledge of your organization and access to your data and systems. What damage can they do?

- **They leave with YOUR company's files, client data and confidential information stored on personal devices**, as well as retaining access to cloud applications, such as social media sites and file-sharing sites (Dropbox or OneDrive, for example), that your I.T. 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 businesses experience data loss due to employee turnover and 87% of employees who leave take data with them.** What do they do with that information? Sell it to competitors, BECOME a competitor or retain it to use at their next job.

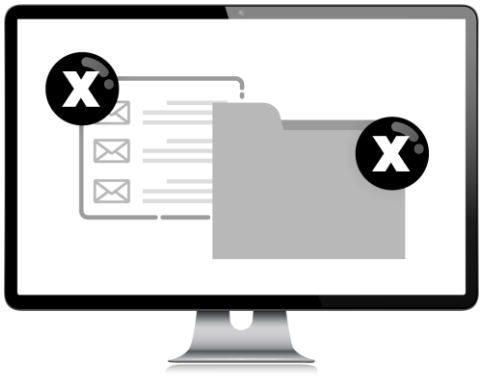
- **Funds, inventory, trade secrets, client lists and HOURS stolen.** There are dozens of sneaky ways employees steal, and it's happening a LOT more than businesses care to admit. According to the website StatisticBrain, 75% of all employees have stolen from their employers at some point. From stealing inventory to check and credit card fraud, your hard-earned money can easily be stolen over time in small amounts that you never catch.



Schedule Your Free Cyber Security Risk Assessment Today!
Visit www.ciolanding.com/csa/ or call our office at 888-308-8879

- **Here's the most COMMON way they steal:** They waste HOURS of time on your dime to do personal errands, shop, play games, check social media feeds, gamble, read the news, and a LONG list of non-work-related activities. Of course, YOU are paying them for a 40-hour week, but you might only be getting 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 I.T. company is not monitoring what employees do and limiting what sites they can visit, they could do things that put you in legal jeopardies, like downloading illegal music and video files, visiting adult content websites, gaming and gambling – all these sites fall under HIGH RISK for viruses and phishing scams.

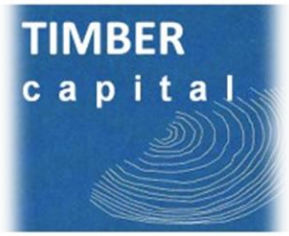
- **They DELETE everything. A common scenario:** An employee is fired or quits because they are unhappy with how they are being treated – but before they leave, they permanently delete ALL of their e-mails and any critical files they can get their hands on. If you don't have that data backed up, you 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, are all greater costs than what you *might* get awarded if you win the lawsuit, *might* collect in damages.



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

Then there's the threat of vendor theft. Your payroll, HR and accounting firm have direct access to highly confidential information and a unique ability to commit fraud. THEIR employees, not just the leadership team, can steal money, data and 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.

What Do Other Businesses Say?



"Security is a primary concern for all businesses and when looking for an IT company, we knew we needed a partner with strong security knowledge. Since working with CIO Landing, we have gained peace of mind about the protection of our data and emails. Their security solutions were installed quickly and have been very effective."

– GBC, Executive, Timber Capital Limited

"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 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."

– MJS, Managing Partner, Siegel & Dolan

"It's important when selecting an IT provider to look at the depth of services offered. CIO Landing handles everything. Other firms wanted to cherry pick our systems and would not provide service in all areas where we needed it. CIO Landing looks at the big picture and is pro-active in finding long-term solutions as opposed to just resolving today's crisis. As a result, our business systems are much more reliable, with almost no downtime."

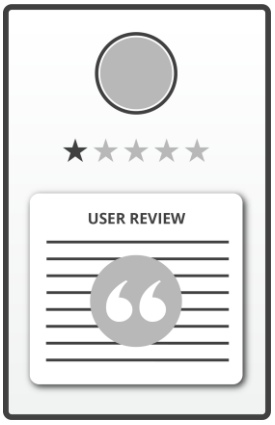
– PH, Executive, Diamond Residential Mortgage Corp

Schedule Your Free Cyber Security Risk Assessment Today!
Visit www.ciolanding.com/csa/ or call our office at 888-308-8879.

Exactly How Can Your Company 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 Yahoo! are learning that lesson the hard way, facing multiple class-action lawsuits for NOT telling their users immediately when they discovered they were hacked. With dark-web monitoring and forensics tools, WHERE data gets breached is easily traced back to the company and website, so you cannot hide it.



When it happens, do you think your clients will rally around you? Have sympathy? News like this travels fast on social media. They will demand answers: HAVE YOU BEEN RESPONSIBLE for 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:

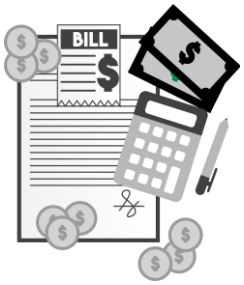
Breach notification statutes remain one of the most active areas of the law. Right now, several senators are lobbying for "massive and mandatory" fines and more aggressive legislation pertaining to data breaches and data privacy. The courts are NOT in your favor if you expose client data to cybercriminals.

Don't think for a minute that this only applies to big corporations: ANY small business that collects customer information also has important obligations to its customers to tell them if they experience a breach. In fact, 47 states and the District of Columbia each have their own data breach laws – and they are getting tougher by the minute.

If you're in health care or financial services, you have additional notification requirements under the Health Insurance Portability and Accountability Act (HIPAA), the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA). Among other things, HIPAA stipulates that if a health care business experiences a breach involving more than 500 customers, **it must notify a prominent media outlet about the incident.** The SEC and FINRA also require financial services businesses to contact them about breaches, as well as any state regulating bodies.

With all the new laws being passed, there is a very good chance you are NOT compliant – **what HAS your I.T. 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 business 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 I.T. 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 I.T. 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 organization. [NOTE: Health care data breach costs are the highest among all sectors.]

4. Bank Fraud:

If your bank account is accessed and funds stolen, the bank is NOT responsible for replacing those funds. Take the true story of Verne Harnish, CEO of Gazelles, Inc., a very successful and well-known consulting firm, and author of the best-selling book *The Rockefeller Habits*.

Harnish had $400,000 taken from his bank account when hackers were able to access his PC and intercept e-mails between him and his assistant. The hackers, who are believed to be based in China, sent an e-mail to his assistant asking her to wire funds to 3 different locations. It didn't seem strange to the assistant because Harnish was then involved with funding several real estate and investment ventures. The assistant responded in the affirmative, and the hackers, posing as Harnish, assured her that it was to be done. The hackers also deleted his daily bank alerts, which he didn't notice because he was busy running the company, traveling and meeting with clients. That money was never recovered, and the bank is not responsible.

Everyone wants to believe "Not MY assistant, not MY employees, not MY company" – but do you honestly believe that your staff is incapable of making a single mistake? A poor judgment? **Nobody believes they will be in a car wreck when they leave the house every day, but you still put your 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 defense, nor is pointing to your I.T. company to blame them. YOU will be responsible, and YOUR company 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: Therefore, 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?

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 company's network to uncover loopholes and vulnerabilities BEFORE a cyber-event happens.

Just like a cancer screening, a good assessment can catch problems while they're small, which means they will be a LOT less expensive to fix, less disruptive to your organization AND give you a better chance of surviving a cyber-attack.

An assessment should always be done by a qualified third party, NOT your current I.T. team or company; fresh eyes see things hidden, even in plain sight, from those looking at it daily.

You want a qualified "Sherlock Holmes" investigating 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

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

This assessment will provide verification from a **qualified third party** on whether your current I.T. 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, we will come to your office and conduct a non-invasive, CONFIDENTIAL investigation of your computer network, backups and security protocols. Your current I.T. 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.

Schedule Your Free Cyber Security Risk Assessment Today!

Visit www.ciolanding.com/csa/ or call our office at 888-308-8879.

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 company, 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 I.T. 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 owners were shocked to learn the backup they had would NOT survive a ransomware attack.*

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 I.T. company. We know we are the most competent, responsive and trusted I.T. services provider to small and mid-sized businesses.

However, we also realize **there's a good chance you've been burned, disappointed and frustrated by the complete lack of service and the questionable advice** you've gotten from other I.T. 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. *We don't blame you.*

That's why this assessment is completely and entirely free. Let us earn your trust by demonstrating our expertise. While we would love the opportunity to be your I.T. company, we will come in with no expectations and only look to provide you with fact-based information so you can make a quality, informed decision – and we'll ONLY discuss the option of becoming your I.T. company if the information we share makes sense and you want to move forward. No hard sell. No gimmicks and no tricks.

Schedule Your Free Cyber Security Risk Assessment Today!
Visit www.ciolanding.com/csa or call our office at 888-308-8879.

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

We 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 we 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, we can practically guarantee this will be a far more costly, disruptive and devastating attack that will happen to your business.

You've spent a lifetime working hard to get where you are today. Don't let some lowlife thief operating outside the law in another country get away with taking that from you. And certainly don't "hope" your I.T. 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!

Visit www.ciolanding.com/csa/

Or call us at 888-308-8879

Dedicated to keeping you protected!

CIO LANDING℠

P.S. – When we've talked to other businesses who have been hacked or compromised, almost all of them told us they thought their I.T. guy "had things covered." We're very connected with other I.T. firms across the country to "talk shop" and can tell you most I.T. 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 I.T. guy does NOT have you "covered" and you need a preemptive, independent risk assessment like the one we're offering in this letter.

A third-party assessment never hurts. Remember, it's YOUR reputation, YOUR money, YOUR business that's on the line. THEIR mistake is YOUR nightmare.