The Financial Industry Cybersecurity Crisis

NEW And **CRITICAL** Changes To I.T. Security, Insurance Coverage And Data Protection Laws That Will Put Your Business At Serious Financial Risk If Not Addressed This Year

The [Small Business] Cybersecurity Crisis

NEW And **CRITICAL** Changes To I.T. Security, Insurance Coverage And Data Protection Laws That Will Put Your Business At Serious Financial Risk If Not Addressed This Year

Discover what the vast majority of CEOs don't know and haven't been told by their I.T. company or team about changes to cybersecurity risks, insurance and growing data protection laws that put them at **UNDERAPPRECIATED RISK** of a crippling cyber-attack and subsequent costs, lawsuits and fines – and what to do about it now.

Provided By:
Cecile Mengue
Cybercile LLC
1300 Summit Ave #520 Fort Worth, TX 76102
Phone: 817-941-3575 Email:support@cybercile.com Web: www.Cybercile.com

About The Author

Cecile Mengue is the founder and CEO of Cybercile, a cybersecurity company specializing in penetration testing, compliance readiness, and ongoing security advisory for financial institutions, fintechs, and SMBs in the money transfer industry. With years of experience in cybersecurity as an Ethical Hacker, Cecile has helped organizations protect sensitive financial data, achieve compliance with regulations such as PCI, GLBA, SOC 2, and FFIEC, and reduce the risk of wire fraud, ransomware, and insider threats.

Under Cecile's leadership, Cybercile has become a trusted security partner to financial SMBs and institutions that require enterprise-grade cybersecurity but lack the in-house expertise to manage it. Cybercile's Managed Penetration Testing and Advisory Program has enabled clients to uncover hidden vulnerabilities, improve their security posture, and confidently pass regulatory audits.

In addition to client work, [Your Name] is a frequent speaker on cybersecurity risk management and compliance in financial services, helping business leaders understand how to align security investments with business outcomes. She is passionate about educating executives, boards, and staff on real-world cyber risks and how to defend against them.

When not advising clients, Cecile enjoys traveling and mentoring future cybersecurity professionals .

Cybercile serves financial services firms and SMBs nationwide, with a focus on companies in the money transfer and fintech sectors. Cybercile | support@cybercile.com

The Truth Nobody Is Telling You About I.T. Security And The Risk You're Exposed To

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 high-paid I.T. companies and your insurance provider.

You *think* your I.T. company or person has your network protected. You *think* you're compliant with a growing number of new data protection and I.T. security laws (or at least good enough, close enough to being compliant and secure). You *think* your insurance company will cover your losses and expenses if a breach occurs and your business is significantly impacted. You *think* your staff is being smart and not putting you at risk because they "know" not to be stupid or click on strange e-mails. You *think* your bank, credit card processing company or software vendor assumes all the risk for the payments you take and the 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 these, you are putting your business at risk of serious financial damages with long-reaching negative implications. Consider this report your wake-up call. There have been significant changes over the last few years in the impact of cyber-attacks, new regulatory compliance law about what YOU as a business owner are responsible for, what insurance will cover (and what's necessary to make sure your claim is not denied) and I.T. protections.

With all the changes, I can assure you of this: the plan you put in place a year or two ago to deal with I.T. security and risk 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 position of underappreciated risk, and when a breach happens, those who sold you their "I.T. compliant" solution or I.T. security services 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 cyber-attack 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 meeting government standards around HIPAA, GLBA, PCI compliance, etc. This is about making sure you completely understand the risks associated with a cyber-attack, I.T. failure or employee mistake and the costs, consequences and damage that will result for your business.

That's why we wrote this report. Over the last few years, we've discovered that ZERO of the businesses and medical entities we've assessed before becoming clients are even close to being prepared for a security incident, much less able to pass a compliance audit.

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 incur. 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, dealing with auditors, the FBI and attorneys who will overwhelm you with things they need. You would also be financially devastated by the fines, emergency I.T. services, legal fees and services you would be forced to buy 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. I.T. compliance and I.T. systems security should NOT be entirely abdicated to your business administrator, I.T. department or company. It should not be assumed that because your software company is "HIPAA compliant" or hosted on an online portal that you are – and that you are protected from a cyber-attack. YOU need to get the facts about what it means to be "willfully neglectful" and make choices about what risks you are willing to take, if any, because it will be your business's reputation and your financial responsibility should a breach happen.

Bottom line: small businesses and medical practices 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 I.T. company or CIO had THIS conversation with you? What HAVE they told you about these new threats? If they have been silent, then I would encourage you to read this report in full and act on the information with urgency.

"A Breach Won't Happen 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" business 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 grossly inadequate ones. In fact, SMALL businesses are the target because you're infinitely easier to compromise. Hackers are unethical but *not* stupid.

You have a bread-bag twist tie locking the gate to a veritable gold mine of prize data (medical records, credit cards, financial records and personal information) that can be sold for millions of dollars on the dark web. Let's be clear: you are dealing with highly sophisticated cybercriminals who can and have outsmarted extremely competent I.T. 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 small 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 to indiscriminately target as many victims as they can. Like commercial fishing boats, they cast wide nets and set baited traps. And yes, small businesses DO get targeted and DO get breached every day – **and the attacks are escalating**.

According to the "State of Cybersecurity Report", in 2024 there were on average 1,876 attacks per organization per week (≈ 97,552 per year), an increase of 75% compared with the year before**. Several industry sources point to the fact that 83% of small and medium-sized businesses are not financially prepared to recover from a cyberattack, yet it's getting more difficult by the day to get insurance coverage for such incidents. Further, insurance claims are being denied.**

Why? Because the businesses who bought the insurance policies agreed to adhere to and implement critical protections in the application, but then didn't follow through on ensuring they were. They ASSUMED their I.T. company "had it covered," but they didn't.

You just don't hear about these breaches because the news wants to report on BIG attacks, or it's kept quiet by the business for fear of attracting bad PR, lawsuits and data-breach fines out of sheer embarrassment.

But make no mistake – small, "average" businesses are being compromised daily, and clinging to the smug ignorance of "That won't happen to me" is an absolutely surefire way to leave yourself wide open to these attacks.

And if you get breached, you WILL be fined and questioned about what you did to protect patient and client data. Unlike other small businesses, you have a legal obligation to protect that information, and you would face financial consequences IF you shrugged this off, made an assumption you are "good" or abdicated this entirely to your staff.

You can't argue, "I didn't know." Cyber-attacks have been happening for years now – and ignorance is not an acceptable excuse to a judge or government regulator. You HAVE been warned. You HAVE been told and you should know better.

Are you 100% sure you're "too small" to deal with a hacker who exposes your clients' financials, credit cards, personal data or medical records? Are you "too small" to worry about paying the fines and costs that you will incur?

The AVERAGE ransomware demand is now between $2 million and $5.2 million – and is on the rise. And that does not include legal fines, lawsuits, emergency I.T. support services for recovery of your systems and clients and revenue lost.

It's also estimated that small businesses lose about $100,000 per ransomware incident and over 25 hours of downtime – add that to the minimum fine for willful violations of compliance laws such as HIPAA, which is <<$50,000 for the first violation and up to $250,000 or more for repeat violations. Or PCI fines that can vary from $5,000 to $100,000 a month. Of course, $150,000>> isn't the end of the world, is it? **Are you okay to shrug this off? To take the chance?**

Larger companies have extensive staff and the ability to invest in sophisticated technology to protect them, as well as lawyers and I.T. personnel on call to prevent and respond should an incident occur. **That's NOT the case for you, the small business.** You don't have such resources or the funding to afford them; therefore, the LAST thing you need is to be woefully unprepared for an inevitable breach or compliance violation, which will undoubtedly be made worse by some ambulance-chasing attorney who convinces even one of your clients they've been significantly harmed by your lack of compliance.

Schedule Your Free Cybersecurity Risk Assessment Today!

Visit **www.cybercile.com/riskassessment** or call our office at 817-941-3575.

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 coverages are paid.

For starters, getting even a basic cyber-liability policy today may require you to prove you have certain security measures in place, such as multifactor authentication, password management, anti-phishing technology, employee awareness training and immutable data backup in place. 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 longer.

But the biggest area of RISK that is likely being overlooked in your business is the actual enforcement of critical security protocols required for insurance coverage and compliance. 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, before paying out, they will investigate how it happened and whether or not you were negligent.

You cannot say, "I thought my I.T. company was doing this!" as a defense. Your IT company will argue that they were not involved in the procurement of the insurance 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 personally identifiable information (PII) to prove that you were not "willfully negligent," **this gigantic, expensive nightmare will land squarely on your shoulders to be paid for out of your pocket**.

Schedule Your Free Cybersecurity Risk Assessment Today!

Visit **www.cybercile.com/riskassessment** or call our office at 817-941-3575.

Exactly How Can Your Business Be Damaged By Cybercrime And A Known Data Breach Of Sensitive Data?

Let Us Count The Ways:

1. Loss Of Clients And Revenue:

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

Do you think all your clients will rally around you? Have sympathy? News like this travels fast on social media. They will demand answers: HAVE YOU BEEN RESPONSIBLE in putting in place the protections outlined in this report, or will you have to tell your clients, "Sorry, we exposed your private information and financial data to criminals because we didn't think it would happen to us," or "We didn't want to invest in compliance and I.T. security because we're small"? That will not be sufficient to pacify your clients, and the trust you've worked so hard to build will be destroyed.

It's true that some of your clients will be understanding. Some won't even care. But you can bet there will be some small percentage of your clients who become irate, reporting you to any government entity that will listen – *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 or for negligence on your part to follow "best practices" for data security. Even if they don't have a case and cannot prove damages, do you really need that headache?

At the very least they will find a competitor of yours to do business with and will be sure to tell their friends and family how you exposed their private information and financials to criminals. Let's say it's only 20% – but can you afford to lose 20% of your clients overnight, along with their friends, associates and colleagues who are (or could be) potential clients?

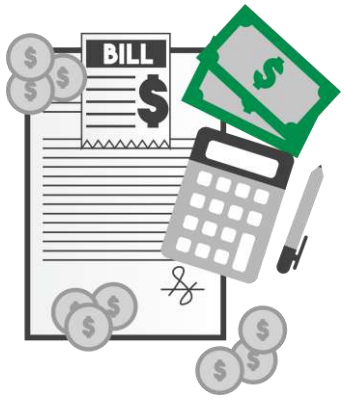
Word of mouth is GREAT for referrals, not so great when it's spreading the truth of you being hacked.

2. Legal Fees, Compliance Fines, Lawsuits:

When a breach happens, you will incur emergency I.T. support and services that can quickly run into thousands of dollars. It's also very likely you'll want to retain an attorney. Even if you somehow avoid a fine for noncompliance to any number of cybersecurity standards (and there are a growing number of them, many of which you might not even realize you are supposed to comply with), there will be costs and hours upon hours of time invested into gathering the mountain of data the auditors will want to see.

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 against the auditors. None of this will be cheap, and it'll have a lasting, negative effect on your business.

3. Cost After Cost:



It's estimated that the cost per lost or stolen record is between $150 to $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 $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.** This year, the average ransom payment increased to over <<$1 million dollars>> on average, a significant increase from previous years. Maybe that's not a lot of money? Maybe that won't hurt your business to pay?

  Don't mind if you lose ALL of your data? What if they threaten to e-mail your employees your payroll? Or post your entire inbox for the world to see? You don't have anything SECRET you don't want revealed publicly, do you? Or what if they use your clients' data to embarrass you or help a competitor? But that's just the tip of the iceberg…

- If you have medical records of ANY kind, or process, interact with or have access to them, you'll pay **MORE**. Sophos, a well-known, leading cybersecurity company, recently published the "State Of Ransomware In Healthcare" report. This report revealed that health care was the most likely sector to pay a ransom, with just over <<60% of respondents who experienced encryption admitting to paying the ransom, compared to a cross-sector average of 46%.>>

- Credit and ID theft monitoring for EVERY client impacted, at a cost of <<$10 to $30>> per record.

- Notification costs of having to print and mail clients about the breach (this is required by law in many states and industries).

- Costs of your staff having to deal with the tsunami of paperwork, phone calls, tasks and projects to clean up this mess and deal with the auditors that takes them away from productive work you hired them to do.

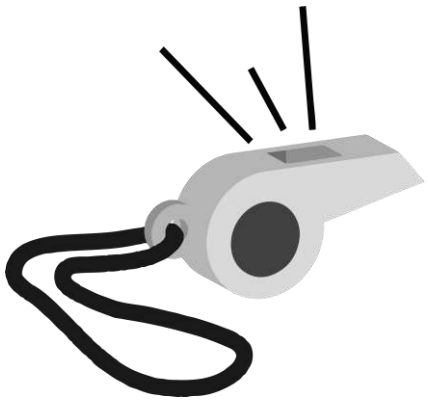
- The fees and I.T. costs to remediate all of your insurance company's forensic findings and reestablishing contracts with vendors who may have been impacted by association and cancelled their agreements with you.

- If the breach involves a computer that transmits or hosts credit card data:
  - ✓ Fees of <<$5,000 to $100,000 per month>> for a PCI violation
  - ✓ Increased audit requirements
  - ✓ Potentially increased credit card processing fees
  - ✓ Potential for company-wide shutdown of credit card activity by your merchant bank, requiring you to find another processor
  - ✓ Cost of printing and postage for notification mailing that is separate from the medical record notification

Schedule Your Free Cybersecurity Risk Assessment Today!

Visit **www.Cybercile.com/riskassessment** or call our office at 817-941-3575.

It's Not The Government Auditors You Have To Worry About, But This…



Complaints filed for compliance violations primarily come from two sources: 1) an actual cyber-attack happening, and 2) whistleblowers *inside* the organization. NOT government auditors.

More specifically, disgruntled clients and employees.

They can be financially rewarded for reporting YOU and be protected under a safe harbor law. Ambulance-chasing attorneys know this and are advertising on Google to take whistleblower cases (just do a quick search for "Medicaid fraud whistleblower reward" and look at the ads that come up from law firms). There's even a website, www.CorporateWhistleBlower.com, that promotes "Get Rewarded For What You Know," encouraging people to come forward for Medicare fraud. There are other sites as well. Just search online for "Corporate Whistleblower" and you'll see PAID ADS for companies and law firms that are encouraging people to report you for payment.

It's not a stretch to imagine an unhappy patient, employee or ex-business associate lodging a HIPAA, PCI or other data-privacy complaint against you or your organization as a way of getting revenge out of jealousy, for what they feel is unfair treatment or simply because you're "rich" and they're not.

Because they are the "enemy within," they are savvy enough to know (or at least suggest) that you have engaged in willful neglect because they know you have no policies and procedures, risk assessments, workforce training standards or documentation of compliance.

Their report triggers a mandatory investigation where you could be slapped with a huge fine, not to mention the massive distraction it becomes for you and your staff. Of course, all of this could be avoided, or at least minimized, with some basic legwork before the complaint and minimal changes to procedure following it.

If You Won't Secure Your Data For You, Then At Least Consider Your Clients

Recently I had a doctor running a noncompliant, nonsecure small medical business say to me, "HIPAA compliance is a joke. I'm not going to get audited or breached. Who's going to come and get me anyway…the HIPAA police? I'm not spending another dime on compliance or security." If you knew your doctor had THIS attitude with YOUR medical records, how would you feel about it?

Hopefully, you aren't as arrogant as this particular doctor. However, you might not be taking compliance as seriously as you could. Maybe you don't care if *you* get audited or fined. Maybe you

feel comfortable with your current security protocols and are willing to take the risks. But what about your clients? Do you believe they would have the same tolerance for risk when it comes to their private information, credit cards, Social Security number, cellphone, e-mail, etc.?

Hackers are running a business, and the people buying those records are going to use your client's identity to purchase prescriptions and drugs, file false tax returns and take out bank loans. They are going to create bills that are then handed to your clients to deal with.

Birthdays, Social Security numbers, credit card data and full contact information give hackers the ability to conduct malicious schemes and theft under your client's identity.

As another doctor pointed out to us, they feel the Hippocratic Oath of "do no harm" extends beyond medicine and applies to all things a patient entrusts in your care. Doctors know prevention is the BEST medicine – and that's why you need to do everything within your power to prevent a cyber-attack that will expose your clients' medical records.

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

It's very possible that you are being ill-advised by your current I.T. company. What have they recently told you about the new threats emerging over the last three to six months? Are they meeting with you on a quarterly basis to go over a recent scan 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 them failing you.

First, and most common, they might not know HOW to advise you, or even that they should. Many I.T. 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**.

Schedule Your Free Cybersecurity Risk Assessment Today!

Visit **www.cybercile.com/riskassessment** or call our office at 817-941-3575.

At a recent conference of my peers, I was shocked to learn that many haven't even read the NIST framework and are unfamiliar with the actual HIPAA, PCI or GLBA laws and guidelines. They're utterly clueless about compliance. That doesn't stop them from selling you I.T. services. They might even tell you that they're keeping you secure, but when you get breached, they'll point the finger at you, saying that YOU didn't want to spend the money on security, and they didn't warranty 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 quick test for your I.T. person or company. E-mail them and ask them, point blank, "Can you assure me you are doing everything we should to ensure we are compliant and secure from a data breach?" If they say yes, ask them to demonstrate it.

You might find out that their story falls apart like a cheap suit. NOBODY (particularly I.T. 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 a 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 I.T. Company Doing Their Job?
Here Are 5 Signs They're Failing You

There are several things your I.T. company or team should be doing for you; but there are 5 that are supremely critical. If your current I.T. 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.

1 **Have they met with you recently – in the last three months – to specifically review and discuss compliance, your risk tolerance and what they are doing NOW to protect you?**

Cybersecurity threats and laws are constantly changing, which is why they should be meeting with you at least every 3 to 6 months to review your risks. Also, have they told you about new and inexpensive tools, such as two-factor authentication or CDR (cloud detection and response), to protect you from attacks that antivirus cannot prevent? If you are outsourcing your I.T. support, they should, at a MINIMUM, provide you with a report of what they've done – and are doing – to protect you AND to discuss new threats and areas you will need to address.

2 Do they proactively monitor, manage and update your computer network's critical security, backups and overall stability?

This is called a "managed service" offering and EVERY ethical I.T. company should insist on this for their clients. Not a "call us when something breaks" model that leaves you exposed to a cyber-attack, data loss and/or extended downtime.

3 Do they have an "immutable" backup in place that cannot be corrupted by ransomware?

One of the reasons the WannaCry virus was so devastating was that 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 I.T. vendor is telling you. Make sure your backups are complete, backing up end-user data on the device as well as your server and cloud data (like e-mail) in a manner that cannot be corrupted by a ransomware attack.

4 Have they recommended (or insisted) you and your employees implement some kind of cybersecurity awareness training?

Cybersecurity awareness training is now required to comply with most data protection laws and insurance companies to cover breaches. Employees accidentally clicking on a phishing e-mail or downloading an infected file or malicious application is still the #1 way cybercriminals hack into systems. Training your employees FREQUENTLY is one of the most important protections you can put in place. Seriously.

5 Have they ever asked to see your cyber-liability or crime 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 determine whether you were negligent and whether you were actually doing the things you've outlined on your policy.

Schedule Your Free Cybersecurity Risk Assessment Today!

Visit **www.cybercile.com/riskassessment** or call our office at 817-941-3575.

Here Are Some Additional Things Your I.T. Company Or Person Should Be Doing For You:

- ❑ **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 a rogue technician, living in another country, would be prevented from using their free and full access to your network to do harm?

- ❑ **Have they kept their technicians trained on new cybersecurity threats and technologies rather than just winging it?** Do they have at least ONE person on staff with CISSP (Certified Information Systems Security Professional) or CISM (Certified Information Security Manager) certification? Do they have anyone on staff experienced in conducting security risk assessments?

- ❑ **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?** Antivirus 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 highly sensitive data?** Do you even know what that is? If not, you don't have it and you need to put it in place for critical cloud applications.

- ❑ **Have they recommended or conducted a comprehensive risk assessment every single year?** In many cases, you are required to do this by law, and your IT company should be handling the IT part of that for you.

- ❑ **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, PCs) 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.

- ❑ **Do they allow your employees to connect remotely using GoToMyPC, LogMeIn or TeamViewer?** If they do, this is a sure sign that you should be concerned! Remote access should strictly be via a secure VPN (virtual private network).

- ❑ **Have they properly configured your e-mail systems to prevent the sending/receiving of confidential or protected data?** Properly configured e-mail systems can automatically prevent e-mails containing specified data, like Social Security numbers, credit cards, patient files and other sensitive data from being sent or received.

- ❑ **Do they offer, or have they at least talked to you about, dark web/deep web ID monitoring?** There are new tools available that monitor cybercrime websites and data for YOUR specific credentials being sold or traded. Once it's detected, the tool notifies you immediately so you can change your password and be on high alert.

- ❑ **Do they have CDR (cloud detection and response) technology on your Office 365 and/or Google Workplace apps?** These are the apps you live and work out of daily and are highly vulnerable to a cyber-attack. Ask if they specifically have CDR protections; if not, you need to demand they do.

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 nearly 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 dealt with 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 your I.T. and data security is right now, with a friend who has your best interests in mind when there is no crisis happening, no auditors calling, no security breaches occurring – NOT a government auditor or an attorney seeking damages.

That's why we've reserved initial phone consultations with our I.T. security and leadership team for business owners like you who are looking for a qualified third party to look with "fresh eyes" at your current I.T. security policies and procedures and conduct a free, preemptive independent risk assessment.

Our Free, Preemptive I.T. Security Risk Assessment Will Reveal If Your Current I.T. Company Is Doing What They Should

Over the next couple of months, we will be conducting free I.T. and Cybersecurity Risk Assessments for businesses and small money transfer firms in The Dallas/Fort Worth 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 I.T. company or person is actually doing what they should be doing to minimize your chances of experiencing a breach and minimize the losses that can occur.

You get a "Sherlock Holmes" investigating on <u>your</u> behalf.

<u>Here's How It Works</u>: We will conduct a thorough, CONFIDENTIAL investigation of your I.T. network, backups and security protocols. Your time investment is minimal: **15 minutes** for the initial meeting and **30 minutes** to go over our Report Of Findings.

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

- Whether or not your systems and data are *truly* secured from hackers and ransomware, and where you are partially or totally exposed.
- If your data is *actually* being backed up in a manner that would allow you to recover it quickly in the event of an emergency or ransomware attack.
- Where you are unknowingly violating **data breach, compliance regulations, insurance requirements; etc..**
- Whether you can lower the overall costs of I.T. while improving communication, security and performance, as well as the productivity of your employees.

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 assessment now:

www.cybercile.com/riskassessment

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, 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, on your business administrator 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 I.T. company or compliance auditor 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 already, 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 817-941-3575 or send me an e-mail to support@cybercile.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, a small breach 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 it will be a far more costly, disruptive and devastating disaster.

You've spent a lifetime working hard to get where you are today. Your company DEPENDS on you to manage financial risk. Let us help you protect and preserve it.

Dedicated to serving you,

Cecile Mengue
Web: www.Cybercile.com
E-mail: cecile@cybercile.com
Direct: 817-941-3575