CETech | Sales: (585) 441-0055| Email: info@cetechno.com | 3144 S Winton Rd, Suite 300, Rochester, NY 14623

FREE Special New CFO Report
And IT Risk Assessment

5 Significant Financial Risks

CFOs Aren't Being Warned About By Their IT Department

The IT Security And Compliance Crisis For CFOs

NEW And Critical Changes To IT Security, Insurance Coverage And FTC Safeguards That Will Put Your Company At Serious Financial Risk If Not Addressed This Year

Discover what the vast majority of CFOs don't know and haven't been told about significant changes to cyber security risks, insurance coverage and regulatory compliance laws that are putting them at **UNDERAPPRECIATED RISK** for a crippling cyber-attack and subsequent costs, lawsuits and fines – and what to do about it now.

Provided By: CETech| IT Services & IT Support for Rochester, Syracuse, and Buffalo
Author: Sue & Fred Brumm
3144 S Winton Rd Suite 300 Rochester, NY 14623
www.cetechno.com | (585) 441-0055| info@cetechno.com

CETech Is Uniquely Qualified To Advise You in This Matter

Regulatory compliance and IT security have brought high-fee “experts” out of the woodwork who are, quite honestly, woefully inexperienced and uninformed. Software and IT companies, business consultants and even insurance agencies see this as their golden opportunity – and are therefore rushing to present themselves as saviors.

But how do you know someone actually has the depth of experience to handle this hypercritical part of your business? For 17 years, my organization has excelled at cyber security for manufacturing, tech, and other businesses.

12 Things We Do Differently

IT Hassle Free!
We “wow” clients with the ultimate customer experience. We are easy to deal with, eliminate downtime, and provide multiple ways to contact us (email, phone, chat). We get it right the first time. We will do whatever it takes to make you happy. No hassles, No problems.

Cybersecurity Experts
Security is paramount and we implement and monitor security best practices for all our clients. We continuously educate our team and our clients on the latest methods to keep them safe. Our cybersecurity experts can help protect your company against the latest threats to your business.

A Proactive Approach
Our philosophy is proactive, not reactive. With state-of- the-art network monitoring and management, we manage your network 24/7 to identify issues and address them BEFORE they become problems, rather than putting out fires.

A Partnership
We believe our customer challenges are our own. We work with you to provide technology solutions for any business problems you may have. We design, evaluate and justify technology solutions from a thorough understanding of the business needs of your company.

Quick Live Local Response 24x7
We provide immediate 24x7 emergency response. A live local (not outsourced) person will answer your call day or night. Your employees can request help via chat, email or by phone.

All-Inclusive: No Hidden Fees!
No need to track block hours or fear going over budget. One flat fee for support. We do NOT charge fees for after-hours or emergency support, travel or on-site visits. We provide fixed fee pricing for both support and projects. We stick to your budget!

A Proven Track Record
Credible reputation in the industry since 2006. Our proudest accomplishment is the large number of long-term clients who year after year put their trust in us. Check out our 5-star reviews, numerous testimonials, and over 5000 client satisfaction surveys.

No Finger Pointing
Start with us and we handle it from there. We handle all aspects of your IT including hardware and software management, vendor relationships, website management, maintenance renewals, and any other related technology needs. We will interface with any vendors on your behalf. You will never have to work with any other vendor to fix your IT needs. We focus on your IT so you can focus on your business.

Depth of Knowledge & Experience
We hire only seasoned, professional technicians with at least 5 -10 years' experience from a vast array of backgrounds and industries. All our employees are background checked and vetted. We provide our technicians with continuing education opportunities on a regular basis to allow them to stay current with the latest technology.

Compliance, No Problem
We understand the complexities of compliance, we can work with you to meet your company's compliance requirements, such as NY SHIELD, HIPAA, NIST, PCI, ISO and others.

No Geek Speak
You deserve to understand what we are doing under the hood and have your questions answered in plain English. Our technicians will clearly explain what is happening, so you understand.

100% Satisfaction Guarantee
We want you to be completely satisfied with our services. If you don't like it or it doesn't work for you - return it at no cost. No questions asked. Zero risk, if you are not satisfied, we will refund your money

The Truth Nobody Is Telling You
That Is Exposing You To Underappreciated Risk

There's a giant threat looming over your organization that is "hiding" in the wings, waiting to wreak havoc, that you are woefully unprepared for due to the negligence and possibly ignorance of your outsourced IT company, insurance provider and possibly even your internal IT team.

You *think* your IT company or person has your company protected. You *think* you're compliant with the new NY SHIELD, HIPAA, NIST, PCI, ISO and other requirements (or at least good enough). You *think* your insurance company will cover your losses and expenses if a ransomware attack or breach occurs. You *think* your staff is being smart and not putting you at risk because they "know better" than to fall for a phishing attack or click on a strange e-mail. You *think* your bank, credit card processing company or software vendor assumes all the risk for the payments you take and credit card processing. And you *think* that because you're small, nobody wants to target you.

Worst of all, you *think* a ransomware attack or data breach would be a minor inconvenience with very few negative effects or costs because you *think* you're prepared. And a few 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 assumptions, you are putting your business at risk for serious financial damages with far-reaching negative implications.

Consider this report is your wake-up call. There have been significant changes over the last few years in the severity and sophistication of cyber-attacks. In response, the government has issued more aggressive regulatory compliance protocols that you are legally required to adhere to. Insurance companies have drastically changed their policies, not only making it far more difficult to get coverage, but also making the cyber security requirements you must have in place for coverage far more stringent and comprehensive.

Bottom line: the plan you put in place a couple of years 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 "compliant" 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 ransomware attack, discover all of the legal and financial consequences and then say, "Why wasn't I told THAT?"

To be clear, this is not just about meeting the FTC Safeguards Rule or your insurance company's requirements for coverage. This is about making sure you completely understand the risks associated with a cyber-attack, IT failure or employee mistake – and the costs, consequences and damage it will do to your business.

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

Not a single one.

All of them were operating under the incorrect assumption that they were "secure enough" and *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 ransomware attack (and it's getting more and more likely you will), your staff would be instantly hit with a crushing workload of cleanup to recover from the breach, dealing with auditors, the FBI and attorneys who will overwhelm them with requests and demands. You would also be financially devastated by the fines, emergency IT services and 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. Regulatory compliance and IT systems security should NOT be entirely abdicated to your office manager, IT department or outsourced IT company. It should not be assumed that because your software company is "compliant" 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: it's almost certain you have 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 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.

Why You As CFO Must Get Directly Involved With IT Security And Compliance

One of the most important roles a CFO fills is to evaluate and mitigate financial risks to the organization that your IT leader, or CIO, may not be able to do:

- Identify, analyze and quantify risks to financial performance.
- Determine which risks should be reduced with safety measures (and how to right size/prioritize resource allocation accordingly).
- Determine which risks should be transferred to an insurer and what coverages, conditions and premium costs are appropriate for those risks.
- Advise CEOs and boards about the current risk state and make recommendations.
- Advise CEOs and boards about the risks associated with any decisions currently under consideration, so that those decisions can be made with their risk factors and risk management costs “baked in.”
- Continuously track risk over time to respond to changes in the magnitude, nature and manageability of risks – as well as to drive continuous improvement in risk management tactics and processes.

Unfortunately, CFOs tend to do very little of this when it comes to cyber security risks and regulatory compliance specific to the protection of data and systems. According to the Deloitte Center for Controllership, only about 20% of organizations do CFOs work closely with IT to understand and take a central role in the management of cyber risks.

This lack of involvement is especially remarkable given that 34.5% of these exact same organizations have experienced at least one attack on their financial data.

Several factors may contribute to this, but one main reason is that cyber security and the handling of data protection have traditionally been viewed as purely technical issues for the IT department to manage. Many CFOs feel that their lack of technical knowledge renders them unqualified to understand and participate in the discussion of what to do to mitigate the risks associated with their organizations' ever-expanding digital environment.

Another factor may be that CFOs and their functional equivalents already have their hands full with other major issues. Rapidly rising interest rates, lingering issues related to the Covid pandemic, supply chain shortages, remote workforces, the labor shortage and other financially impactful developments have made the past few years quite challenging for CFOs, so it stands to reason that they would defer deeper engagement with technology-related risks that, at least theoretically, are already under the care of the IT department.

But this delegation has become abdication for 3 reasons:

1. The magnitude of cyber risk is too great to escape the essential involvement of the CFO to not only evaluate and understand the costs and ramifications associated with a cyber event, but also to make decisions about compliance and risk tolerance that cannot possibly be left to the IT department.

2. Your IT department is not equipped to address risk from a true financial and business perspective. Technologists approach issues such as hacking and insider threats as technical issues with technical solutions. They are neither positioned nor qualified to assess the potential adverse financial impact of a cyber-attack or compliance violation without the heavy involvement of you, the CFO.

3. IT now touches every aspect of your organization's ability to transact, thereby making it intimately connected to all other financial risk. If you're mitigating supply-chain risk by increasing your inventories, you're using technology to maintain those new inventory targets. If you're mitigating your exposure to the risk of business fraud with appropriate process controls, you're using technology to implement and enforce those controls. Technology touches every aspect of financial risk – and every aspect of the business is touched by technological risk.

"A Breach Won't Happen To My Business…We're Not A Target. My Staff Is Too Smart. We're *Good*," You Say?

Don't think you're in danger because you're "too small" or 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 are trusting your IT department to put protections in place without ever verifying their strength and completeness. Hackers are unethical but ***not*** stupid.

We have found that even many larger businesses with IT departments and significant IT investments have a bread-bag twist tie locking the gate to a veritable gold mine of prize data (client data and financial 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 IT teams working for large organizations and government entities. You and your staff are NOT above making a mistake or being duped.

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

According to the ***ThreatLabz*** State Of Ransomware report, ransomware attacks have increased by over 37% this year, with the average enterprise ransom payment exceeding $100,000, with an average demand of $5.3 million.

Of course, $100,000 isn't the end of the world, is it? But that's not where it ends. Even if you can recover your data, a hacker has access to all of it…e-mails, financial reports, payroll information, your client list, employee data. You will be legally required to notify your customers. Do you think they'll be "understanding"? Sympathetic that you exposed them? How will your employees feel about all of this?

But are you okay to shrug this off? *To take a chance?*

If a really small business gets hacked and sued for exposing sensitive data, they can argue they didn't know or didn't have the financial resources to implement good cyber security. But a larger organization like the one you're running, with IT resources, trying to make that argument won't win. Saying you "didn't know" is not even a reasonable excuse, given the extensive information that is available about cyber security protections.

No government agency, attorney, insurance company or even clients are going to buy that excuse. You HAVE been warned. You HAVE been told and you should know better.

If you get breached, you WILL be fined and questioned about what you did to protect your employees' and client data. You have a legal obligation to protect this information, and you will face financial consequences IF you shrugged this off, made an assumption you are "good" or abdicated this entirely to your IT staff.

How Bad Can It Be?
My Insurance Will Cover Me, Won't It?

Insurance companies are in business to make money, NOT to 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 paid.

For starters, getting a basic cyber liability policy today requires you to prove you have certain security measures in place, such as multi factor authentication, password management, endpoint protection and immutable backup of data. Insurance carriers want to see phishing training and cyber security awareness training in place, and some will want to see a WISP (written information security program) and/or a business continuity plan from your organization. Depending on the insurance 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, they will investigate how it happened and whether or not you were negligent before paying out.

You cannot say, "I thought my IT company/department was doing this!" as a defense. If you outsource some aspect of your IT, that company will argue 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.

Your IT leader will argue they've been asking you for more budget and denied the resources in tools and people to truly secure your environment. Finger-pointing will ensue, and regardless of whose fault it is, it will be up to YOU to prove that you were not "willfully negligent," and this gigantic expensive nightmare will land squarely on your shoulders to deal with.

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 required to notify your clients 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 customers, "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 into security and compliance because we needed to bolster our bottom line." 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 the FTC, FBI or other regulatory agencies – *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. Even if they don't have a case and cannot prove damages, do you really need that headache?

2. At the very least, they will find another vendor and will be sure to tell their friends and family how you exposed their private information and financials to cybercriminals. Let's say it's only 20% – can you afford to lose 20% of your revenue overnight, along with their friends and family members who are (or could be) potential clients?

3. **Reduction Of Enterprise Value (EV):**

It's well-known that a cyber incident can sink an organization's stock price and valuation because of the substantial damage to brand value and loss of goodwill and customer trust.

When the MGM Grand was his with a very public cyberattack, they not only incurred a cool $80 million in immediate losses in revenue but also a half-billion drop in its stock price. When Capital One disclosed a data breach, its share price immediately dropped nearly 6% in after hours trading. Two weeks later, the share price dropped nearly 14%. ©

You might argue that you're not as large as Capital One or MGM Grand, but if you are looking for investors, initiating a merger or acquisition or attempting any significant financial transaction, a breach WILL instantly change the game, lowering your valuation and financial strength, raising questions and creating delays.

4. **Legal Fees, Regulatory Fines, Lawsuits:**

When a breach happens, you will incur emergency IT support and services that can quickly run into thousands of dollars. It's also very likely you'll want to retain an attorney who specializes in these matters. Even if you somehow avoid a fine for noncompliance, 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 overburdened staff will be forced to take time to respond. You will be questioned and investigated. None of this will be cheap, and it will have a lasting, negative effect on your business.

We also live in a litigious society where anyone who feels "harmed" can lawyer up and come after you. Everyone has "disgruntled" clients and employees. A hack can give them the simple reason they want to exact vengeance upon your organization.

The financial judgements resulting from these lawsuits are sobering. Consider the judgements against Equifax ($380 million), Home Depot ($200 million), CapitalOne ($190 million), and Uber ($148 million). Smaller companies aren't immune; their losses will simply be proportional to their size and the number of customers involved.

5. **Insurance Costs:**

As we've already highlighted, insurance carriers can and WILL deny a claim if they discover your IT department was negligent in fully enforcing the stringent requirements they set for providing the policy that you agreed to. When was the last time you had an independent third party audit your current IT systems to ensure you are fully compliant with that policy to avoid getting your coverage denied?

Sure, they *say* they are enforcing good cybersecurity protocols, but have they actually seen the insurance application? Are you sure they have fully implemented the specific items detailed on that document? If not, there's a risk that needs to be addressed.

Another unexpected cost is that when a breach occurs, you might find yourself unable to get coverage (worst case) or having to pay exorbitant fees (best case) for cyber liability, crime and ransomware insurance in the future.

Cyber insurance rates are surging and won't come down anytime soon.The chief executive of one of the world's biggest insurance companies has warned that cyber attacks will become "uninsurable" as the disruption from hacks, along with the costs incurred and likelihood of experiencing a ransomware attack, continue to grow.

6. **Ransomware, Emergency IT Costs And Clean Up:**

Hopefully your current IT staff or company is prepared for such an attack – but often they aren't, you are forced to bring in ransomware recovery experts who don't come cheap. That's just one of a litany of costs that you might not have considered, or might not be sufficiently covered by your current insurance policy:

• Paying the ransom to get your data back and/or for it NOT to be publicly released. Right now, the average "ask" is over $5 million. Hackers use the data they collect from you to set the ransom price. They know if you have the financial means to pay – and it's not just to get your data back, but also to NOT release your data to your competitors and the general population at large. Remember the Ashley Madison breach? Millions of records of people who were paying to cheat on their spouses were publicly released. Think about the data you have – contracts, confidential details of business dealings, salary details, YOUR personal emails and the emails of your entire executive team. What would you pay to prevent that from getting out?

• The cost of providing 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 letters to your clients (or patients) about the breach.

• Costs of your staff having to deal with a 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 IT costs to remediate your insurance company's forensic findings, as well as an increase in insurance for cyber liability and crime – possibly even getting your coverage dropped.

If the breach involves a computer that transmits or hosts credit card data:

✓ Fines of $500,000 per incident for being PCI noncompliant.
✓ Increased audit requirements and the costs associated with them.
✓ Increased credit card processing fees.
✓ Company wide shutdown of credit card activity by your merchant bank, requiring you to find another processor.
✓ Cost of printing and postage for a breach notification mailing to all clients and individuals impacted.

✓ Company wide shutdown of credit card activity by your merchant bank, requiring you to find another processor.
✓ Cost of printing and postage for a breach notification mailing to all clients and individuals impacted.

If You Won't Secure Your Data For *You*, Then At Least Consider Your Clients, Investors, Employees And All Key Stakeholders Of The Organization

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."

Hopefully you (and your executive team) aren't as arrogant as this particular doctor. However, you might not be taking this 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 being exposed? What about investors and shareholders? How do THEY feel about all of this?

Do THEY feel as though a ransomware attack would be something to shrug off?

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

It's very possible that you are being ill-advised by your current IT company or your internal IT team. What have they recently told you about the new threats emerging over the last year? About the rapid changes in cyber liability, crime and ransomware insurance? About the new FTC Safeguard and PCI compliance laws pertaining to credit cards and financial payments?

Have they discussed what your risk tolerance is and put together a plan and budget to ensure you're not at undue risk? How about a disaster recovery plan in the event of a ransomware attack or other data-erasing disaster?

Situations can change in an instant – if they are not truly monitoring your environment daily, scanning quarterly for compliance and in constant communication with you (or a key person on your staff) about your security and risk, they are NOT doing their job.

There could be several reasons they are failing you.

First, and most common: they might not know HOW to advise you, or even that they should. Many IT companies or CIOs know how to keep IT up and running but are completely out of their league when it comes to dealing with the advanced cyber security threats we are seeing today and are NOT experts in the legal requirements of compliance or the insurance policies you are buying.

At a recent conference of my IT peers, I was shocked to learn many haven't even read the NIST framework (which is the National Institute of Standards and Technology) and are unfamiliar with the actual FTC Safeguard, PCI laws and guidelines, and the NYS Shield Act.

They're utterly clueless about compliance. That doesn't stop them from selling you IT services. They might even tell you that they're keeping you secure, but when you get breached, they'll point their finger at you, saying 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 your IT department or outsourced IT firm and ask them, point-blank, "Can you assure me you are doing everything we should to guarantee we are compliant with the FTC Safeguards, PCI compliance and other laws in our state?" 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 or team doing the RIGHT things.

Second, they may be "too busy" themselves or not have sufficient staff to be truly proactive with cyber security protocols and compliance – which means they are NOT doing the ongoing work that needs to be done (and they might still be charging you as if they were).

Third, if you're outsourcing some aspect of your IT needs, the company you've hired might just be cheap and unwilling to make a significant investment in the tools, people and training they need to not only secure THEIR company, but also yours. Maybe they don't want to admit the service package they sold you has become OUTDATED and inadequate. Their cheapness CAN be your demise.

CETech | Sales: (585) 441-0055| Email: info@cetechno.com | 3144 S Winton Rd, Suite 300, Rochester, NY 14623

Is Your Current IT Company Or Department Doing Their Job?
Take This Quiz To Find Out

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

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

□ Have they met with you recently – in the last 3 months – to specifically review and discuss areas of RISK (security and compliance) and what they are doing NOW to protect you? Have they fully implemented basic and critical security protocols such as 2-factor authentication or advanced endpoint security to protect you from attacks that antivirus is unable to prevent? DO YOU HAVE A RANSOMWARE RESPONSE PLAN?

□ Have they ever asked to see your cyber liability insurance application? Have they verified they are doing everything your policy REQUIRES to avoid having a claim denied in the event of a cyber-attack? Insurance companies don't make money paying claims; if you are breached, there will be an investigation to prove you weren't negligent and that you were actually doing the things you've outlined on your policy.

□ If you outsource some of your IT support, does the company you're outsourcing to 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? Has your IT lead provided you with a response plan? If not, WHY?

□ Have you assessed any key vendors who host or have access to your sensitive data to ensure THEIR security is up to par, not putting you at risk by association? Who is doing this? How are they assessing those risks?

□ Has your IT team been trained on new cyber security threats and technologies, rather than just winging it? Do you have at least ONE person on staff with CISSP (Certified Information Systems Security Professional) or CISM (Certified Information Security Manager) certification? Does your outsourced IT company have such a person helping to plan and manage your IT and security?

□ Do you have a ransomware-proof backup system in place? This is called an “immutable backup,” and you should have this in place.

CETech | Sales: (585) 441-0055| Email: info@cetechno.com | 3144 S Winton Rd, Suite 300, Rochester, NY 14623

Ransomware is designed to corrupt not only your network but also your backups. Therefore, you must ensure you have backups in place that cannot be corrupted or changed – that’s what an *immutable* backup is.

□ Does your IT team have controls in place to force your employees to use strong passwords? Have they implemented a password manager to store login credentials and prevent employees from using weak passwords or reusing the same passwords again and again? 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?

□ Has your IT team talked to you about replacing your old antivirus with advanced endpoint security? Antivirus tools from 2 or 3 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 MFA or “2-factor authentication,” for access to highly sensitive data? Do you even know what that is? If not, you don’t have it and you absolutely need this in place for all employees.

□ Have they recommended or conducted a comprehensive risk assessment every single year? Some industries are required to do this by law. Are you one of them? Do you even know? Your IT company or department shouldn’t be left to do this on their own. YOU, the CFO, should be involved with getting an independent third-party audit by someone who sits on your side of the table to ensure you are getting the security you expect.

□ 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 most searched-for thing 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.

□ Have they given you and your employees ANY kind of cyber security awareness training? This is now required for 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.

□ Have they properly configured your email system to prevent the sending/receiving of confidential or protected data? Properly configured email systems can automatically prevent emails containing specified data, like Social Security numbers, credit cards,

patient files and other sensitive data from being sent or received.

CETech | Sales: (585) 441-0055| Email: info@cetechno.com | 3144 S Winton Rd, Suite 300, Rochester, NY 14623

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

□ 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 your info is detected, they notify you immediately so you can change your password and be on high alert.

Our Free Preemptive Cyber Security Risk Assessment Will Instantly Reveal Risks In Your IT Security

Over the next couple of months, we will be conducting free Cyber Security Risk Assessments for CFOs in our area to find and expose vulnerabilities and failings in your security, which equates to financial risk, BEFORE a cyber event happens.

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

You get a highly trained, qualified "Sherlock Holmes" investigating on your behalf.

Here's How It Works: We will start with a confidential discovery phone consultation so you can get to know us and we can better understand your current concerns. Your time investment is minimal: 30 minutes] for the initial meeting and 90 minutes in the second meeting to go over our Report Of Findings and recommendations.

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.

• Has your current IT company or team actually implemented sufficient security protections, protocols and systems to protect you? As Mark Twain famously said, "Supposing is good, but *knowing* is better." We'll conduct an incredibly simple, confidential test that will give you irrefutable proof of the security of your IT environment. Be prepared to be shocked at what we'll show you.

• Whether or not you would be able to say "Yes" to 20 basic IT security and compliance questions any insurance company, government auditor or opposing counsel (attorney) will ask you to determine if you've been "willfully negligent" if a breach happened. If you cannot confidently confirm these questions, your IT company (or whoever is advising

you on security, compliance and legal risk) is failing you by either NOT implementing these security measures or NOT giving you the confidence to know you are doing them.

CETech | Sales: (585) 441-0055| Email: info@cetechno.com | 3144 S Winton Rd, Suite 300, Rochester, NY 14623

- Whether your IT budget is being used prudently and where it will have the greatest impact. We often find companies are spending sufficiently on IT in general, but are *overspending* on things they don't need and are grossly underfunded on other tools and strategies that will have a much greater impact and ROI.

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:

https://www.cetechno.com/is-this-you/

Please…Do NOT Just Shrug This Off

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 have not booked this free Cyber Security Risk Assessment, please go online and do it now:

https://www.cetechno.com/securityaudit/

I know you are *extremely busy* and there is enormous temptation to discard this, shrug it off, worry about it "later" or dismiss it altogether. That is, undoubtedly, the easy choice…but the easy choice is rarely the RIGHT choice.

This I can guarantee: At some point, you will have to deal with a cyber security "event," be it an employee mistake, 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,

Sue Brumm

Web: http://www.cetechno.com
E-mail: sbrumm@cetechno.com
Direct: (585) 617-0317

