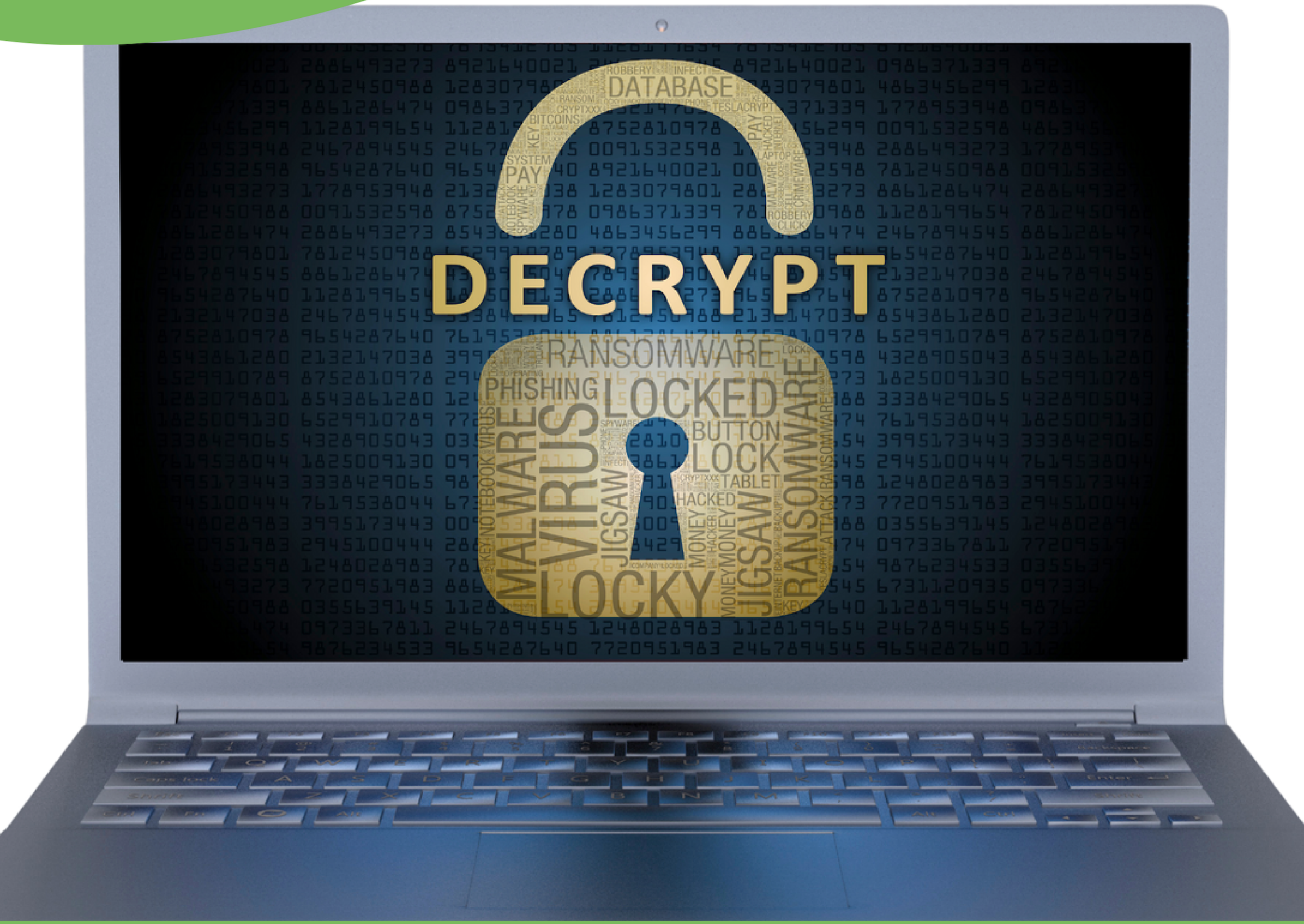
CORPORATE TECHNOLOGIES GROUP

UNMASKING IT SECURITY GAPS:

3 Signs of Ransomware Risks In Your Cybersecurity Strategy

Essential Updates In Cybersecurity And Insurance That Could Seriously Impact Your Business If Not Addressed Promptly



5344 Darrow Road | Hudson, Ohio 44236 | 330-655-8448 | ctgusa.net | info@ctgusa.net

ABOUT OUR COMPANY

For over 24 years, Corporate Technologies Group Inc. has ensured that our clients achieve long-term success by investing the time to understand how they do business and provide them with the right solution to fit their needs.

We are an Ohio-based company with national and international reach that employs a motivated team of highly experienced, customer-focused professionals. We have relationships with 200+ IT product and service providers that enable us to offer our clients a complete portfolio of best-in-class solutions.

Our extensive industry experience combined with a vendor-agnostic approach and knowledge of your business allows us to develop impactful solutions that will enable you to effectively outsource the management of your voice, data, security, premise-based phone systems, and cloud-based services.

Businesses choose Corporate Technologies Group because we provide solutions that enable you to focus on what matters most — your business.

UNMASKING IT SECURITY GAPS:

3 Signs of Ransomware Risks In Your Cybersecurity Strategy

Essential Updates In Cybersecurity And Insurance That Could Seriously Impact Your Business If Not Addressed Promptly

Table of Contents

The Truth Nobody Is Telling You About IT Security

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

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

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

And if you're still operating on any of these "good thoughts," you are putting everything you've worked so hard to earn at risk of serious financial damages with far-reaching negative implications. Consider this report as your wake-up call.

There have been significant changes over the last few years in cyber-attacks, what insurance will cover (and what's necessary to make sure your claim is not denied), and IT protections required. The plan you put in place a year or two ago to deal with all of this is no longer viable.

QUESTION: When was the last time your current IT company had THIS conversation with you? What HAVE they told you about these new threats? If they have been silent, then I would urge you to read this report in full and act on the information urgently.

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

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

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

That's why I wrote this report. Over the last few years, we've discovered that 80% of the businesses we've assessed before becoming clients are even close to being prepared for a cybersecurity incident.

Not a single one.

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

This means if you experience a breach (and it's getting more and more likely you will), your staff would instantly be hit with a crushing workload of cleanup to recover from the breach and to deal with the auditors, the FBI, and the attorneys who will overwhelm them with their demands. You would also be financially devastated by the destruction and the emergency IT services and legal fees you would be forced to pay just to get back up and running.

Worse yet, there is a very good chance your insurance claim will be denied or not fully paid out due to your failure to follow the recommendations in this report.

This is not a subject you want to take lightly or "assume" you have handled. Your cyber security program should not be entirely left to your IT director, IT department, or company.

It should not be assumed that because you are investing tens of thousands of dollars in cyber security, you are actually protected from a cyber-attack. You need to get the facts about what it means to be secure and make choices about what risks, if any, you are willing to take because it will be your company's reputation at stake and your financial responsibility should a breach happen.

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

"Hackers Won't Break Into 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 email or make a mistake? That it won't happen to you?

<u>That's exactly what cybercriminals are counting on you to believe.</u>

It makes you easy prey because you put zero protections in place or simply inadequate ones. Small organizations like yours are the target because you're much easier to compromise. Hackers are unethical - but not stupid.

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

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

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

Are you sure you're too small to worry about hackers? According to Osterman Research, the average ransomware demand is $84,000, not including fines, lawsuits, emergency IT services, or lost business (source: MSSP Alert). You might think you can go out of business and start over, but hackers often know exactly how much you can pay. They set ransoms at an amount you can't refuse and leave back doors to attack again once you recover.

How Bad Can It Be?

("My Insurance Will Cover Me, Won't It?")

Insurance companies aim to make money, not pay out claims. A few years ago, cyber insurance carriers kept 70% of premiums as profit, only paying out 30% in claims. Today, the situation has reversed, leading to significant changes in acquiring and paying out cyber liability insurance.

Getting even a basic cyber liability policy now requires attesting to security measures like multifactor authentication, password management, endpoint protection, third-party penetration testing, and tested data backup solutions. Insurers also look for phishing and cybersecurity awareness training, a Written Information Security Program (WISP), or a Business Continuity Plan. The requirements can vary depending on the carrier and coverage sought.

The biggest overlooked risk is the enforcement of required security protocols. Insurance carriers will deny claims if you fail to implement these measures. During a breach investigation, they will determine if negligence played a role before paying out. You can't defend yourself by saying, "I thought my IT company was handling this!" Your IT company will argue they were not involved in the policy procurement and did not guarantee your security. They might even show evidence that you refused advanced security services, distancing themselves from responsibility.

Exactly How Can Your Business Be Damaged By Cybercrime?

If you haven't documented the steps taken to secure sensitive information and prove you weren't "willfully negligent," you will bear the full cost of a breach.

Loss of Clients and Revenue A breach forces you to notify clients and employees that their private information was exposed. Do you think they'll rally around you? News spreads fast on social media. They'll demand answers: Were you responsible in securing their data, or will you admit you didn't think it would happen to you or didn't want to invest in protection? This will not pacify them, and the trust you've built will be destroyed. Some clients and employees might be understanding, but many will be irate and could even report you to the news. It only takes one lawsuit to create a massive headache. Even without a strong case, the stress and costs of a legal battle are significant.

Legal Fees and Lawsuits. A breach incurs emergency IT support and services costing thousands. Your busy staff will need to respond, and you'll likely need an attorney to represent you or negotiate with hackers. This is costly and has a lasting, negative effect on your business.

Ongoing Costs. According to Cyber Security Magazine, 61% of small and medium-sized businesses reported at least one cyber-attack in the past year. When your organization gets hacked, the expensive, reputation-destroying nightmare falls on you. It doesn't end there. Depending on your data, authorities and clients may investigate your preventive measures. Without the protections outlined in this report, you can be found negligent and face fines and lawsuits.

Claiming ignorance is not a valid defense. If a breach becomes public, your competition will exploit it, clients will leave, morale will plummet, and employees may blame you. Your bank won't replace stolen funds, and without specific cyber insurance, general liability coverage won't cover the losses.

You might think this won't happen to you, but it's happening to millions of organizations. The FCC reports digital information theft is now the most common fraud. Cyber-attack costs are rising due to extended downtime and sophisticated attacks, with additional concerns over Russian hackers targeting Americans due to the Russia-Ukraine war. Don't underestimate these threats.

According to the IBM Cost of a Data Breach Report, the cost for lost or stolen records ranges from $150 to $225 per record, considering IT recovery costs, lost revenue, downtime, fines, and legal fees. Calculate the number of clients and employees you have, multiply by $150, and you'll see the potential costs to your business.

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

- Paying the ransom to get your data back: According to Palo Alto, the average ransomware payment is just over $920,000 nowadays.
- Credit and ID theft monitoring for every person impacted: This can cost between $10 to $30 per record.
- Staff dealing with the aftermath: Your staff will have to handle a flood of paperwork, phone calls, tasks, and projects to clean up the mess and deal with recovery, taking them away from the productive work you hired them to do.
- IT and remediation costs: You will need to cover the fees and IT costs to address your insurance company's forensic findings and re-establish working agreements within your supply chain.
- If the breach involves a computer that transmits or hosts credit card data:
    - Fees of $500,000 per incident for being PCI non-compliant
    - Increased audit requirements
    - Potentially increased credit card processing fees
    - Potential for a company-wide shutdown of credit card activity by your merchant bank, requiring you to find another processor

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

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

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

- **Have they met with you recently – in the last three months – to specifically review and discuss what they are doing NOW to protect you?** Have they told you about new and inexpensive tools such as two-factor authentication or advanced endpoint security to protect you from attacks that antivirus is unable to detect and prevent? If you are outsourcing your IT support, they should, at a MINIMUM, provide you with a quarterly review and report of what they've done – and are doing – to protect you AND to discuss new threats and areas you will need to address.

- **Do they proactively monitor, patch, and update your computer network's critical security settings daily?** Weekly? At all? Are they reviewing your firewall's event logs for suspicious activity? How do you know for sure? Are they providing ANY kind of verification to you or your team?

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

- **Do THEY have adequate insurance to cover YOU if they make a mistake and your business is compromised?** Do you have a copy of THEIR CURRENT policy? Does it specifically cover YOU for losses and damages? Does it name you as a client?

- **Have you been fully and frankly briefed on what to do IF you get compromised? Have they provided you with a response plan?** If not, WHY?

- **Have they told you if they are outsourcing your support to a third-party organization? DO YOU KNOW WHO HAS ACCESS TO YOUR BUSINESS AND THE DATA IT HOLDS?** If they are outsourcing, have they shown you what security controls they have in place to ensure that a rogue technician, living in another country, would be prevented from using their free and full access to your network to do harm?

- **Have they provided you evidence that they have a third party that audits their network?** Did you know that if their network gets hacked, the hackers will have access to your network too? If you haven't seen evidence of their third-party audits, request it immediately.

- **Have they kept their technicians trained on new cybersecurity threats and technologies, rather than just winging it?** If they don't have a way to show you that their team is learning about threats hitting your industry and to validate that their team is up-to-date on current security protocols, how can they guarantee providing you with secure solutions?

- **Do they have a ransomware-proof backup system in place?** One of the reasons the WannaCry virus was so devastating was because it was designed to find, corrupt and lock BACKUP files as well. ASK THEM TO VERIFY THIS. You might *think* you have it because that's what your IT vendor is telling you.

- **Do they have controls in place to force your employees to use strong passwords? Do they require a PASSWORD management system to prevent employees from using weak passwords?** If an employee is fired or quits, do they have a process in place to make sure ALL passwords are changed? Can you see it?

- **Have they talked to you about replacing your old antivirus with advanced endpoint security?** Anti-virus tools from two or three years ago are useless against today's threats. If that's what they have protecting you, it's urgent you get it resolved ASAP.

- **Have they implemented "multifactor authentication," also called 2FA or "two-factor authentication," for access to highly sensitive data? Do you even know what that is?** If not, you don't have it.

- **Have they implemented web-filtering technology to prevent your employees from going to infected websites, or websites you DON'T want them accessing at work?** I know no one in YOUR office would do this, but why risk it? Adult content is still the #1 thing searched for online. Then there's gambling, shopping, social media and a host of other sites that are portals for hackers. Allowing your employees to use unprotected devices (phones, laptops, tablets) to access these sites is not only a security risk but a distraction where they are wasting time on YOUR payroll, with YOUR company-owned equipment.

- **Have they given you and your employees ANY kind of cybersecurity awareness training?** This is now required for insurance providers to cover breaches. Employees accidentally clicking on a phishing e-mail or downloading an infected file or malicious application is still the #1 way 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 e-mail system to prevent the sending/receiving of confidential or sensitive data?** Properly configured e-mail systems can automatically prevent e-mails containing specified data, like social security numbers, credit cards, and other sensitive data from being sent or received.

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

- **Have they had a third-party analyze your network to validate their work?** You would never attempt to proofread your own work. Why would you expect your IT person to? Many regulatory bodies require at a minimum an annual third-party assessment for this reason.

Security Is NOT Compliance – Here are 3 Signs of Ransomware Risks In Your Cybersecurity Strategy

As mentioned earlier, many organizations mistakenly believe that being compliant means being secure. This is not true. You can be compliant and still completely insecure. To ensure you are actually secure, your IT company needs to take three key steps.

Most IT companies are only doing one or two of these steps. You need to ensure they are checking ALL the boxes. This way, if and when a breach occurs and you get audited, you are well-prepared and the damages are minimized. Here are the three crucial steps:

1. Not Performing Regular Third-Party Security Assessments with a Remediation Plan

Hackers are always finding new ways to breach systems. Security tools that worked two years ago may no longer be effective. If your IT company isn't conducting third-party security assessments at least quarterly, they are missing significant vulnerabilities that hackers can exploit. Unfortunately, this is where most businesses stop and don't move on to the next crucial steps.

2. No Full and True Implementation of the Plan Set In Place

Even the best plans are useless if not implemented. You can give a patient a treatment plan, but if they refuse to follow it or cherry-pick advice, they cannot expect to recover. The same goes for security. Your IT consultant should provide options, timelines, and an assessment of pros and cons for choices based on your risk tolerance, situation, budget, and resources. A good IT company or consultant will guide you through this process.

The most important aspect is ensuring that the IT team or company you trust to implement the remediation plan is actually doing it. Based on our experience, 90% of companies offering outsourced IT services are not diligent about fully implementing a security and compliance plan.

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

3. No Documentation Requirements For Security Policies

This is often overlooked by IT companies and medical practices. Behind every security compliance measure is a documentation requirement.

If you have a breach and get audited, you will need to produce documentation of your security activities and policies. Without these documents, your business may not survive a major attack or breach. If you lack documented plans for addressing a ransomware attack, data breach, or disclosure and clear instructions on who needs to do what and when, you are putting yourself and your business at significant risk.

Will You Wait Until You Have a Breach or Violation Before Taking Action?

More than half of home security systems are bought after a burglary. This behavior highlights a common mistake: waiting for a crisis before taking action. Preventative measures are far cheaper, less stressful, and more effective than reacting to a crisis. The best time to assess your security is now, with an unbiased partner—not during a crisis.

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

We will conduct free Security Assessments for businesses to uncover vulnerabilities before a cyber event happens. We will assess one of your networks to look for:

- **Security Implementation:** Is your current IT team implementing critical protections and protocols? These measures minimize breach risks and ensure insurance claims are not denied due to non-compliance.
- **Cost-Effective Security Measures:** What are the most cost-effective actions to secure your network and avoid being accused of "Willful Neglect" if a breach occurs?
- **Penetration Testing:** Is your security robust enough to pass a penetration test? We will conduct one and show whether your IT company is effective or failing you.

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

https://ctgusa.net/discovery-call/

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

Government auditors and insurance providers are thorough and unforgiving. They know where to look for weaknesses and are skilled at finding them.

When audits reveal problems, it creates immense stress on your staff and you. Blame gets passed around, and tensions rise. The best way to prevent this is through a proactive, independent, and confidential compliance assessment. This helps you identify and fix issues now.

It's difficult to review your own work objectively. If you have an IT company, this assessment offers a free, no-risk way to verify their effectiveness.

Take Action Now

If you've scheduled an appointment, simply show up prepared with questions. If you prefer to talk first, call us at **330-655-8144** or **info@ctgusa.net** to schedule an appointment.

It's easy to put this off, but that's rarely the right choice. You will eventually face a cybersecurity event, whether it's an employee mistake, malware, or a ransomware attack.

We want you to be prepared and experience only minor inconveniences. Ignoring this advice will likely result in a more costly and disruptive outcome.

You've worked hard to get where you are. Let us help you protect it.

Brett Harney, President
E-mail: bharney@ctgusa.net
Direct: 330-655-8121
Web: www.ctgusa.net/contact-us