UK Business Cyber Security Crisis

New and Critical Protections Every Business Must Have in Place NOW to Protect Their Client Data Confidential Information and Reputation From the Ever Increasing Threat of Cyber Crime and Ransomware.

munio

Protect Your Business and Your Reputation From The Dangers of Cyber Crime

The UK Business Cybersecurity Crisis

New And Critical Protections Every UK Business Must Have In Place NOW To Protect Their Accounts, Client Data, Confidential Information And Reputation From The Tsunami Of Cybercrime And Ransomware

The growth and sophistication of cybercriminals, ransomware and hacker attacks has reached epic levels. CEOs can no longer ignore it or carelessly think, "That won't happen to us."

It is becoming increasingly clear that your business – large OR small – will be targeted and will be vulnerable UNLESS you take action on the information contained in this important new executive report.

Provided By: Munio | Fortified IT Support & Cyber Security
Author: Jason Lydford | CEO
Saphir House, 5 Jubilee Way, Faversham, Kent ME19 8GD
www.munio-it.co.uk | hello@munio-it.co.uk

When You Fall Victim To A Cyber-Attack By No Fault Of Your Own, Will They Call You Irresponsible or Negligent?

It's EXTREMELY unfair, isn't it? Victims of most other crimes – burglary, mugging, theft – get sympathy from others. They are called "victims" and support comes flooding in, as it should.

But if your business is the victim of a cybercrime attack where client or personal data is compromised, you will NOT get such sympathy. You will be instantly labeled as "irresponsible", or deemed negligent for not providing adequate security for your systems and network. **You may be investigated and clients will question you about what you did to prevent this from happening** – and if the answer is not satisfactory, you can be found liable, facing serious fines and lawsuits EVEN IF you trusted an outsourced IT support company to protect you. Claiming ignorance is not an acceptable defence, and this giant, expensive and reputation-destroying nightmare will land squarely on YOUR shoulders.

But it doesn't end there…

According to the ICO, you may well be required to tell your clients that your systems have been exposed to cybercriminals and as a result their data, or the data that you hold on their behalf, is compromised. Unfortunately, your competition will likely have a heyday over this. Clients will be understandably unhappy and could potentially leave. It could also cause a real upset in regards to your staff morale.

Please do NOT underestimate the importance and likelihood of these threats. It is really not safe to assume your IT company is doing everything they should be doing to protect you; in fact, there is a high probability they are not, which we can demonstrate with your permission.

But first, please allow me to introduce myself and give you a little background on why I created this report.

Why We Are So Concerned About Informing And Protecting YOU

My name is Jason Lydford, CEO of Munio. We specialise in being the outsourced IT company for businesses throughout Kent and London.

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

When they call, they're understandably desperate, scrambling for anyone who can help them put the pieces back together again. Often their business is completely on lockdown. Most if not all

of their data has been corrupted or held for ransom, preventing them from fulfilling obligations they have to their clients, this is often years of work and critical data**.**

They're also scared and *intensely* angry. They feel violated and helpless. Embarrassed. Why didn't their IT company or IT team prevent this from happening? *How are they going to tell their clients that they've exposed them to cybercriminals*? They're in complete disbelief that they actually fell victim – after all, they "didn't think we had anything a cybercriminal would want!"

What makes this unforgivable is that ALL of the CEOs coming to us for help after a serious attack had an IT company they trusted with the responsibility of protecting the business, but found out all too late the company wasn't doing the job it was PAID to do.

As a business owner, that built my own company from the ground up. I know how hard you work to make your company succeed. I understand the risks you've taken, the personal sacrifices you've made. To me, it's an insult to have it all taken away by some cybercriminal, often from another country, who will NOT be held accountable for their actions.

To make matters worse, so many so-called "IT experts" out there aren't doing the job they were hired to do. Sometimes this is simply because they lack the knowledge and skills to ensure the security and protection of your data and networks. As the CEO of a company, you're forced to trust that your IT company or IT team is doing the right things to protect your organisation, and have the right tools and services at their disposal– and when they fail to do their job, this expensive, business-interrupting disaster lands squarely on your shoulders to deal with.

That's why we've started a "one-company revolution" to educate and help as MANY business owners as we can so they never have to deal with the stress, anxiety and loss caused by a cyber-attack, and help you understand just how serious this is so you can be prepared instead of caught completely off guard.

Yes, It CAN Happen To YOU
And The Damages Are VERY Real

You might already know about the escalating threats, from ransomware to hackers, but it's very possible you are underestimating the risk to you. It's also possible you're NOT fully protected and are operating under a false sense of security, ill-advised and underserved by your outsourced IT company.

In fact, if your current IT company has not talked to you about the protections outlined in this report, or about putting a cyber "disaster recovery" plan in place, you are at risk and you are not being advised properly.

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

munio®

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.

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

Don't think you're in danger because you're "small" and not a big organisation like the NHS, Easyjet or Talk-Talk. Or that you have "good" people and protections in place? And especially don't be naive to think that it simply won't happen to you.

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

Right now, there are over 980 million malware programs out there and growing (source: AV-Test Institute), and 40% of the cyber-attacks occurring are aimed at small businesses (source: National Cybersecurity Centre); you just don't hear about it because the news wants to report on BIG breaches OR it's kept quiet by the company for fear of attracting bad PR, lawsuits and data-breach fines, and out of sheer embarrassment.

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

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

Are you "too small" to deal with a hacker using your company's server as **ground zero** to infect all of your clients, vendors, employees and contacts with malware? Are you "too small" to worry about someone taking changing payroll information for your bank account? According to Osterman Research, the AVERAGE ransomware demand is now between £8000 and £13500 (source: National Cyber Security Centre). It's also estimated that small business lost over £10000 per ransomware incident and over 25 hours of downtime.

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 paid.

For starters, getting even get a basic cyber liability or crime policy today may require you to prove you have certain security measures in place, such as multi-factor authentication, password management, endpoint protection, 24/7 managed security protection and tested and proved data backup solutions.

Insurance companies want to see regular phishing training and cyber security awareness training in place, and most will want to see a Disaster Recovery and/or a Business Continuity Plan from your organisation. Depending on the company, 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 with data protection laws. 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 was doing this!" as a defence. Your IT 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. And if you haven't been documenting the steps you've taken to secure your network and prove that you were not "willfully negligent," **this gigantic expensive nightmare will land squarely at your door**.

It's NOT Just Cybercriminals Who Are The Problem

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

- **They leave with your company's files, client data and confidential information stored on personal devices**, as well as retaining access to cloud applications, such as social media sites and file-sharing sites (Dropbox or OneDrive, for example), that your IT department doesn't know about or forgets to change the password to.

In fact, according to an in-depth study conducted by Osterman Research, **69% of businesses experience data loss due to employee turnover and 87% of employees who leave take data with them**. What do they do with that information? Sell it to competitors? actually become a competitor themselves, or retain it to use at their next job.

- **Funds, inventory, trade secrets, client lists and hours stolen.** There are dozens of sneaky ways employees steal, and it's happening a LOT more than businesses care to admit. According to the website StatisticBrain, 75% of all employees have stolen from their employers at some point. From stealing inventory to credit card fraud.

- **They DELETE everything. A common scenario:** An employee is fired or quits because they are unhappy with how they are being treated – but before they leave, they permanently delete all of their e-mails and any critical files they can get their hands on. If you don't have that data backed up, or the office 365 account put into litigation hold, you will most likely lose it all. Even if you took legal action and won, the legal costs, time wasted on the lawsuit and on recovering the data, not to mention the aggravation and distraction of dealing with it all, are all greater costs than what you *might* get awarded if you win the lawsuit and *might* collect in damages.

- **They become a whistleblower.** For example, complaints filed for GDPR and ICO violations primarily come from two sources: 1. An actual cyberattack happening, or 2. Whistleblowers *inside* the organisation. **More specifically, disgruntled employees**.

  Employees, vendors and even clients are protected through UK law for reporting you and your organisation. (https://www.gov.uk/whistleblowing).

Take a look at the above list. Do you *really* think *this can't* happen to you?

Then there's the threat of vendor/supplier theft. Your payroll, HR and accounting firm have direct access to highly confidential information and a unique ability to commit fraud. THEIR employees, not just the leadership team, could steal, data and confidential information. All it takes is a part-time employee – perhaps hired to assist in data entry during a VAT quarter or your end of year accounts, and who is not being closely supervised or is working from home on routine tasks with your account.

Now it is assumed that we do trust our vendors and the majority of those that we work with are as trustworthy as the day is long. But they are not the ones we are talking about, are they?

What Do Other Businesses in Kent Say About the Need to Have Solid Cyber Security in Place?

"Although cyber security is essential for all businesses, I found understanding what was required and how to implement it quite daunting. Munio supported us by assessing exactly what our needs were and explained everything in no-nonsense terms. Not only with the overall security but also on an individual basis with the weekly online training sessions for all staff which are quick, relevant and easy to understand.

I have peace of mind knowing that if any data breaches are detected, they are dealt with quickly to ensure we are not compromised. As our cyber security needs will no doubt continue to change I'm confident in the advice and services we receive from all the team at Munio."

Victoria Highfield – Nellsar

"With the Global increase in cyber-attacks it is crucial to maintain business continuity and protect data and IT infrastructure in today's world. We have total confidence in the fact that our Cyber Security requirements are exceeded by the team at Munio and that our networks and data are protected 24/7/365"

Karla Robinson – Farmwood

We believe that dealing with Cybersecurity in business is key to survival of that business. One slip up by a staff member or owner can allow a catastrophic breach of security which is why we believe that this is a matter which should be taken extremely.

We had a breach years ago through remote desktop which was identified and shut down straight away, the backup systems in place meant that our business could carry on.

We also believe that finding the right Cybersecurity for our business can't be left to chance, it takes good quality professional advice, monitoring and proper training.

Sue Rabbit - Andersonphillips

Exactly How Can Your Company Be Damaged By Cybercrime? Let Us Count The Ways:

1. **Reputational Damages:** What's worse than a data breach? Trying to cover it up. Companies like Yahoo! are learning that lesson the hard way, facing multiple class-action lawsuits for NOT telling their users immediately when they discovered they were hacked. Using dark-web monitoring and forensics tools, where data gets breached is easily traced back to the company and website, so you cannot hide it.

   When it happens, do you think your clients will rally around you? Have sympathy? News like this travels fast – especially on social media. They will demand answers: Has your company been responsible in putting in place the protections outlined in this report, or will you have to tell your clients, "Sorry, we got hacked because we didn't think it would happen to us," or "We didn't want to spend the money." Is *that* going to be sufficient to pacify them?

2. **Government Fines, Legal Fees, Lawsuits:** Breach notification statutes remain one of the most active areas of the law. Every day the ICO and other Government organisations are lobbying for "massive and mandatory" fines and more aggressive legislation pertaining to data breaches and data privacy. The courts are NOT in your favour if you expose client data to cybercriminals.

   Don't think for a minute that this only applies to big corporations: ANY small business that collects customer information (personal or otherwise) also has important obligations to its customers to tell them if they experience a breach.

   "If a security breach has a 'significant impact' you must notify the ICO within 24 hours. You must also notify your users if they are likely to be affected. In some circumstances you or the ICO may also need to inform the wider public about a breach". (Source: https://ico.org.uk/for-organisations/guide-to-eidas/breach-reporting/

3. **Cost, After Cost, After Cost:** One breach, one ransomware attack, one rogue employee can create hours of extra work for staff who are already maxed out when things are going well. Then there's business interruption and downtime, backlogged work delivery for your current clients. Loss of sales. Forensics costs to determine what kind of hack attack occurred, what part of the network is/was affected and what data was compromised. Emergency IT restoration costs for getting you back up, *if* that's even possible. In some cases, you'll consider paying the ransom (DON'T!). Then there are legal fees and the cost of legal counsel to help you respond to your clients and the media. Cash flow could be significantly disrupted.

   According to the Cost of Data Breach Study conducted by Ponemon Institute, organisations spent £2.9 Million recovering from data incidents**, after factoring in IT recovery costs, lost revenue, downtime, fines, legal fees, etc**.

4. **Using You As The Means To Infect Your Clients:** Some hackers don't lock your data for ransom or steal money. Often they use your server, email, website or profile to spread viruses and/or compromise other PCs. If they hack your website, they can use it to relay spam, run malware, build SEO pages or promote their religious or political ideals. (Side note: This is why you also need advanced endpoint security, spam filtering, web gateway security, SIEM and a 24/7/365 Security Operations Centre (SOC) together with the other items detailed in this report, but more on those in a minute.)

munio®

You May Want To Believe You're "Safe"

But Are You Sure?

It's very possible that you are being ill-advised by your current IT company. What have they recently told you about the rising tsunami of cybercrime? Have they recently met with you to discuss new protocols, new protections and new systems you need in place TODAY to stop the NEW threats that have developed over the last few months?

If not, there could be several reasons for this. First, and most common, they might not know HOW to advise you, or even that they should. Many IT companies know how to keep a computer network running **but are completely out of their league when it comes to dealing with the advanced cybersecurity threats we are seeing recently**.

Second, they may be "too busy" themselves to truly be proactive with your account – or maybe they don't want to admit the service package they sold you has become OUTDATED and inadequate compared to far superior solutions available today. At industry events, I'm shocked to hear other IT companies say, "We don't want to incur that expense," when talking about new and critical cybersecurity tools available. Without the right tools/software, how can they possibly offer you the best protection?

And finally, NOBODY (particularly IT people) like to admit they are out of their depth. They feel compelled to exaggerate their ability to avoid looking unskilled. On the other hand, they might actually have you completely covered and be on top of it all. But how do you know?

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.

Further, it's important that you get verification on the items listed. Simply asking, "Do you have insurance to cover us 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 they told you.

- ☐ **Have they met/spoken with you recently – in the last 3 months – to specifically review and discuss what they are doing NOW to protect you?** Have they told you about software updates and tools such as 2FA 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.

munio®

- ☐ **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 urged you to talk to your insurance company** to make sure you have the right kind of insurance to protect against fraud? Cyber-liability? MORE IMPORTANT: Have they reviewed your insurance policy with your agent to ensure they were implementing the cyber protections required under that policy to avoid having a claim denied, coverage not paid?

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

- ☐ **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?

- ☐ **DO YOU KNOW WHO HAS ACCESS TO YOUR PERSONAL COMPUTER AND NETWORK?** 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 dedicated to Cyber Security? Are they running a 24/7/365 Managed Security Centre (SOC)? Do they have anyone on staff experienced in conducting security risk assessments?

- ☐ **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.

- ☐ **Have they put in place a WRITTEN mobile and remote device security policy, and distributed it to you and your employees?** Is the data encrypted on these devices? Do you have a remote "kill" switch that would wipe the data from a lost or stolen device, and is that data backed up so you CAN wipe the device and not lose files?

- ☐ **Do they have controls in place to force your employees to use strong passwords?** Do they require a regular password update for all employees? 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?** There has been considerable talk in the IT industry that antivirus is dead, unable to prevent the sophisticated attacks we're seeing today.

- ☐ **Have they discussed and/or implemented "multifactor authentication" for access to highly sensitive data?** Do you even know what that is? If not, you don't have it.

- ☐ **Have they recommended or conducted a comprehensive risk assessment every single year?** Many insurance policies require it to cover you in the event of a breach. If you handle "sensitive data" such as medical records, credit card or financial information, you may have a legal requirement to do this.

- ☐ **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?** Porn and adult content is still the #1 thing searched for online.

- ☐ **Have they given you and your employees ANY kind of cybersecurity awareness training?** Have they offered to help you create an AUP (acceptable use policy)? Do they offer you regular Cyber Security Awareness Training and run regular Phishing Simulations? 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 secured your e-mail system to prevent the sending/receiving of confidential or protected data?** Properly configured e-mail systems can automatically prevent e-mails containing specified 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 to 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 tools available that monitor cybercrime websites and data for YOUR specific credentials being sold or traded. Once detected, it notifies you immediately so you can change your password and be on high alert.

- ☐ **Do they have a fully 24/7/365 Managed Security Operations Centre (SOC) in place?** A managed SOC is a manned service that leverages threat monitoring to detect malicious and suspicious activity across three critical attack vectors: Endpoint | Network | Cloud.

A Preemptive Independent Risk Assessment:
The ONLY Way You Can Really Be Sure

A security assessment is exactly what it sounds like – it's a process to review, evaluate and "stress test" your company's network to uncover loopholes and vulnerabilities BEFORE a cyber-event happens.

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

An assessment should always be done by a qualified 3rd party, NOT your current IT team or company; fresh eyes see things hidden, even in plain sight, from those looking at it daily.

You want an expert investigating on YOUR behalf who is not trying to cover up inadequacies or make excuses, bringing to you a confidential report you can use to either find vulnerabilities and issues – or to be reassured that your network is being looked after correctly.

Our Free Cybersecurity Risk Assessment Will Give You The Answers You Want, The Certainty You Need

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

This assessment will provide verification from a **qualified 3rd party** on whether or not your current IT company is doing everything they should to keep your computer network not only up and running, but SAFE from cybercrime.

Here's How It Works: After an initial meeting with myself to discuss your company's current IT and cyber security situation, at no cost or obligation, one of my lead security consultants will visit your office and conduct a non-invasive, CONFIDENTIAL investigation of your computer network, backups and security protocols. Your current IT company or guy DOES NOT NEED TO KNOW we are conducting this assessment (although they are welcome if they wish). Your time investment is minimal: about an hour for the entire process.

When this Risk Assessment is complete, you will know:

- **If you and your employees' login credentials are being sold on the dark web.** We will run a scan on your company. It's RARE that we don't find compromised credentials – and I can guarantee what we find will shock and alarm you.

- IF your IT systems and data are **truly secured** from hackers, cybercriminals, viruses, worms and even sabotage by rogue employees.

- IF your **current backup would allow you to be back up and running again <u>fast</u>** if ransomware locked all your files. *In 99% of the computer networks we've reviewed over the years, the owners were shocked to learn the backup they had would NOT fully survive a ransomware attack*.

- IF employees truly know how to spot a phishing e-mail. We will actually put them to the test. *We've never seen a company pass 100%.* Not once.

If we DO find problems…overlooked security loopholes, inadequate backups, credentials that have been compromised, out-of-date firewall and antivirus software and (often) active malware…on one or more of the PCs in your office, we will propose an Action Plan to remediate the situation that you can have us implement for you if you choose.

Again, I want to stress that EVERYTHING WE DISCUSS AND DISCOVER WILL BE <u>STRICTLY CONFIDENTIAL</u>.

Why Free?

Frankly, we want the opportunity to be your Fortified IT & Cyber Security company. We know we are a multi-award winning, extremely competent, responsive and trusted IT & Cyber services provider for small and medium sized businesses across Kent.

However, I also realise **there's a good chance you've had your fingers burned, been disappointed and frustrated by the complete lack of service and the questionable advice** you've previously had from other IT companies in the past. In fact, you might be so fed up and annoyed at being "sold" and underserved that you don't trust anyone. *I don't blame you*.

That's why this assessment is completely and entirely free. Let us earn your trust by demonstrating our expertise. While we would love the opportunity to be your IT company, we will come in with no expectations and only look to provide you with fact-based information so you can make a quality, informed decision – and we'll ONLY discuss the option of becoming your IT company if the information we share makes sense and you want to move forward. Absolutely No hard sell. No gimmicks and no tricks.

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

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. **<u>This I can guarantee</u>:** At some point, you WILL HAVE TO DEAL WITH A CYBERSECURITY EVENT.

Hopefully you'll be brilliantly prepared for it and experience only a minor inconvenience at most. But if you wait and do NOTHING, I can practically guarantee this will be a far more costly, disruptive and devastating attack that will happen to your business.

Don't just "hope" that your IT person has you covered. Get the facts and be certain you are protected.

Contact us and schedule your Free, CONFIDENTIAL Cybersecurity Risk Assessment today: https://www.munio-it.co.uk/it-network-and-cyber-security-assessment/

Feel free to also reach out to me direct at the phone number or e-mail address below.

Looking forward to helping you protect your company,

Jason Lydford | CEO
Munio | Fortified IT Support & Cyber Security Specialists
Web: www.munio-it.co.uk
E-mail: j.lydford@munio-it.co.uk
Tel: 01795 383 383

P.S. – When I talked to other IT professionals like myself and the CEOs who have been hacked or compromised, almost all of them told me they thought their IT team "had things covered."

I'm also very connected with other IT firms across the country to "talk shop" and can tell you most IT guys have never had to deal with the enormity and severity of attacks happening in the last few months. That's why it's VERY likely your IT team does NOT have you "covered" and you need a preemptive, independent risk assessment like the one I'm offering in this letter.

As a CEO myself, I understand that you have to delegate and trust, at some level, that your employees and vendors are doing the right thing – but it never hurts to validate that they are. Remember, it's YOUR reputation, YOUR money, YOUR business that's on the line.