The Cyber Security Crisis

Urgent And Critical Protections We Are Urging All Businesses To Have In Place NOW To Protect Their Bank Accounts, Client Data, Confidential Information And Reputation From The Tsunami Of Cybercrime

The growth and sophistication of cybercriminals, ransomware and hacker attacks has reached epic levels, and NEW protections are now required. We have created this report to inform all businesses about what's going on and educate them on new protections we are urging them to put in place.

Cornwallit

KEEPING YOUR BUSINESS PRODUCTIVE

Provided By: Cornwall IT Limited
Author: Aaron Nihat
Tremough Innovation Centre, Penryn, Cornwall, TR10 9TA
Website: www.cornwallit.com
Main Office: 01326 336 332
Email: info@cornwallit.com

If You Fall Victim To A Cyber-Attack By No Fault Of Your Own, Will They Call You Careless…Or Just Irresponsible?

It's EXTREMELY unfair, isn't it? Victims of all other crimes – burglary, mugging, car theft, etc – 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 YOUR client or patient data is compromised, you will NOT get such sympathy. You will be labeled careless and irresponsible. **You may even be investigated and questioned about what you did to prevent this from happening** – and if the answer is not adequate, you can be found liable, facing serious fines and legal action EVEN IF you have protections in place. Claiming ignorance is not an acceptable defense, and this giant, expensive and potentially reputation-destroying nightmare will land squarely on YOUR shoulders.

But it doesn't end there…

According to the GDPR laws here in the United Kingdom, you will be required to notify the Information Commissioner's Office of a data breach and inform your clients that you exposed them to cybercriminals. If it becomes public, your competition will have a heyday over this. Clients will be IRATE and will take their business elsewhere. Your bank is NOT required to replace funds stolen due to cybercrime (*go ask them*), and unless you have a very specific type of insurance policy, any financial losses will be denied coverage.

Please do NOT underestimate the importance and likelihood of these threats.

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

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

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

Look: 82,000 NEW malware threats are being released every single day, and HALF of the cyber-attacks occurring are aimed at small businesses; 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. But make no mistake – small, "average" businesses are being compromised daily, and clinging to the

smug ignorance of "that won't happen to me" is an absolute surefire way to leave yourself wide open to these attacks.

In fact, the **UK's National Cyber Security Centre** reports that in 2018, **43% of small businesses were victims of cybercrime that year** – and that number includes only the ones that were reported. Most small businesses are too embarrassed or afraid to report breaches, so it's safe to assume that the 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 to infect all your clients, vendors, employees and contacts with malware? Are you "too small" to worry about someone taking your payroll out of your bank account? According to Osterman Research, the AVERAGE small business lost over £100,000 per ransomware incident and over 25 hours of downtime. Of course, £100,000 isn't the end of the world, is it? But are you okay to shrug this off? To take the chance?!

It's NOT Just Cybercriminals Who Are The Problem

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

- **They leave with YOUR company's files, client data and confidential information stored on personal devices**, as well as retaining access to cloud applications, such as social media sites and file-sharing sites (Dropbox or OneDrive, for example) that you aren't even aware they were using.

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

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

  But here's the most COMMON way they steal: They waste HOURS of time to do personal errands, shop, play games, check social media feeds, gamble, read the news and a LONG list of non-work-related activities. Of course, YOU are paying them for a 40-hour week, but you might only be getting some of that. Then they complain about being "overwhelmed" and "overworked." They tell you, "You need to hire more people!"

so you do. All of this is a giant suck on profits if you allow it. Further, if we don't put in place web security filtering to limit what sites they can visit (and we certainly do have this for many clients), they could do things that put you in legal jeopardy, like downloading illegal music and video files, visiting adult-content websites, gaming and gambling – all of these sites fall under HIGH RISK for viruses and phishing scams. (IMPORTANT: We now have solutions to prevent this that we are rolling out to clients who want to stop this from happening to them.)

- **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 their e-mails and any critical files they can get their hands on. If you don't have that data backed up, you lose it ALL. Even if you sue them and win, the legal costs, time wasted on the lawsuit and on recovering the data, not to mention the aggravation and distraction of dealing with it all, involve a far greater cost than what you *might* get awarded, *might* collect in damages. IMPORTANT: For all managed IT clients, we are confident we could get the data back; but for clients who are not under that plan, or who do not have our email backup solution, you are vulnerable to this.

Do you *really* think you are immune to any or all of *this happening* to you?

Then there's the threat of vendor theft. Your payroll, HR and accounting firm have direct access to highly confidential information and a unique ability to commit fraud. THEIR employees, not just the leadership team, can steal money, data and confidential information. All it takes is a part-time employee – perhaps hired to assist in data entry during tax season, and who is not being closely supervised or is working from home on routine tasks with your account – to decide to make a little money on the side by selling data or siphoning funds from your account.

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

IMPORTANT: Clients who are on our Cyber Security plan DO have protections in place to greatly reduce the chances of these things happening, and the severity and impact if they get compromised. You should also know there is absolutely no way we, or anyone else, can 100% guarantee you won't get compromised – you can only put smart protections in place to greatly reduce the chances of this happening, to protect data so it IS recoverable and to demonstrate to your employees, clients and the lawyers that you WERE responsible and not careless.

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

   When it happens, do you think your clients will rally around you? Have sympathy? News like this travels fast on social media. They will demand answers: HAVE YOU BEEN RESPONSIBLE 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." That will not be sufficient to pacify them.

2. **Government Fines, Legal Fees, Lawsuits:** Breach-notification statutes remain one of the most active areas of the law. The courts are NOT in your favor if you expose client data to cybercriminals.

   Don't think for a minute that this applies only to big corporations: With GDPR in operation, ANY small business that collects customer information also has important obligations to its customers to tell them if they experience a breach. In fact the Information Commissioner's Office state that a business that suffers a breach has to report this breach to them within 72 hours of finding out. One of the things we want to discuss with you is how to ensure you are compliant and you stay compliant.

3. **Cost, After Cost, After Cost:** ONE breach, one ransomware attack, one rogue employee you are not protected against, 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 be forced to pay the ransom and maybe – *just maybe* – they'll give you your data back. Cash flow will be significantly disrupted, budgets blown up.

4. **Bank Fraud:** If your bank account is accessed and funds stolen, the bank is NOT responsible for replacing those funds. Please check with them to find out.

   Everyone wants to believe "not MY assistant, not MY employees, not MY company" – but do you honestly believe your staff is incapable of making a single mistake? A poor judgment? **Nobody believes they will be in a car wreck when they leave the house every day, but you still put the seat belt on.** You don't expect a life-threatening crash, but that's not a reason to not buckle up. *What if?*

5. **Using YOU As The Means To Infect Your Clients:** Some hackers don't lock your data for ransom or steal money. Often they use your server, website or profile to spread viruses and/or compromise other PCs. If they hack your website, they can use it to relay spam, run malware, build SEO pages or promote their religious or political

ideals. (Side note: This is why you also need advanced endpoint security, spam filtering, web gateway security, and the other items detailed in this report, but more on those in a minute.)

To be clear, clients under our Cyber Security plan would be protected against THIS happening.

Here Is Our Current List Of Protections You Should Have In Place Now

Below is a list of things we recommend all businesses should have in place ASAP. **Some you may already have, and some may be lacking. Here is what our clients currently have in place and what you would receive if you were our client:**

- ☐ **QBRs Or Quarterly Business Reviews And Security Risk Assessments:** We will hold these QBR meetings with all clients. During these consultations, we will conduct a security risk assessment and provide you with a score. We will also brief you on current projects, review your IT plan and budgets, discuss NEW tools and solutions we feel you may need, and make recommendations. We will also answer any questions you have and make sure you are satisfied with our services.

- ☐ **Proactive Monitoring, Patching, Security Updates:** This is what we deliver in our Cyber Security Plan. Specifically, we will monitor all your devices for health, security and performance. We will be able to report on any devices that may need upgrading due to poor performance. We will be able to monitor all devices for known and unknown malware including ransomware attacks. We will monitor all devices to make sure they have the latest critical security updates installed.

- ☐ **[NEW!] Data Breach And Cyber-Attack Response Plan:** This is a time- and-cost-saving tool as well as a stress-reduction plan. We will be working with our clients to create and maintain a cyber-response plan so that IF a breach happens, we could minimize the damages, downtime and losses, and properly respond to avoid missteps.

- ☐ **Ransomware Backup And Disaster Recovery Plan:** One of the reasons the WannaCry virus was so devastating was because it was designed to find, corrupt and lock BACKUP files as well. That's why we are insisting clients upgrade to our advanced backup solution, which is included in our Managed IT Services Plan.

- ☐ **Advanced Email Filtering:** We offer advanced email filtering to greatly reduce the risk of employees click onto phishing emails or malicious links. Any suspicious link or email will be reported as such to immediately alert the employee. 90% of all successful cyber attacks occur from human error so this is a must for all businesses who take cyber security seriously.

- ☐ **A Mobile And Remote Device Security Policy:** All remote devices – from laptops to cell phones – need to be backed up, encrypted and have a remote "kill" switch that

would wipe the data from a lost or stolen device. You also need to have a policy in place for what employees can and cannot do with company-owned devices, how they are to responsibly use them and what to do if the device is lost or stolen.

☐ **More Aggressive Password Protocols:** Employees choosing weak passwords are STILL one of the biggest threats to organizations. To protect against this, we will require a regular password update for all employees and put in place controls to ensure weak, easy-to-crack passwords are never used. We will also have checklists for employees who are fired or quit to shut down their access to critical company data and operations.

☐ **[NEW!] 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. That's why we are recommending all clients UPGRADE to Thor Premium Advanced Security which sites alongside common anti-malware software.

☐ **Multi-Factor Authentication:** Depending on your situation, we will be recommending multi-factor authentication for access to critical data and applications. This is an extra layer of security that can greatly reduce certain cyber attacks.

☐ **Web-Filtering Protection:** Porn and adult content is the #1 thing searched for online, most often during the 9-to-5 workday. Online gaming, gambling and file-sharing sites for movies and music are also ranked in the top searches and are "click bait" hunting grounds for hackers. These are sites you do NOT want your employees visiting during work hours on company-owned devices. If your employees are going to infected websites, or websites you DON'T want them accessing at work, they can not only expose you to viruses and hackers, but they can also get you nailed for sexual harassment and child pornography lawsuits – not to mention the distraction and time wasted on YOUR payroll, with YOUR company-owned equipment. All of this can (and should) be blocked from company-owned Internet and devices.

☐ **[NEW!] Cyber Security Awareness Training:** 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. We have several new solutions we can discuss with you to inform and remind your employees to be on high alert and reduce their likelihood of clicking on the wrong e-mail or succumbing to other scams.

☐ **Protections For Sending/Receiving Confidential Information Via E-mail:** Employees have access to a wide variety of electronic information that is both confidential and important. That's why we'll be ensuring all clients' e-mail systems are properly configured to prevent the sending and receiving of protected data.

☐ **Secure Remote Access Protocols:** You and your employees should never connect remotely to your server or work PC using GoToMyPC, LogMeIn or TeamViewer. Remote access should strictly be via a secure VPN (virtual private network). For our

clients who need this type of access, we will be implementing proper technologies that are secure.

☐ **[NEW!] 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 such breaches are detected, these tools notify you immediately so you can change your password and be on high alert.

Please…Do NOT Just Shrug This Off

We know all business owners are extremely busy but if you need help with your cyber security, we would urge you to get in touch as soon as possible. If you have any questions, **call us at 01326 336332 or send an email, Aaron@cornwallit.com.**

I know you are *extremely busy* and there is enormous temptation to discard the warnings around cyber security, 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 issue, serious virus or ransomware attack.

The purpose of a meeting with us about cyber security is 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 this will be a far more costly, disruptive and devastating disaster.

You've spent a lifetime working hard to get where you are today. Let us help you protect and preserve it. Give you complete peace of mind.

Dedicated to serving you,

Aaron Nihat
Director
Cornwall IT Ltd