BLUENET

The Cyber Security Crisis For Twin Cities Businesses

Critical Protections We Are Urging All Clients 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 our clients about what's going on and educate them on new protections we are urging all clients to put in place NOW.

When You Fall Victim To Ransomware Due To No Fault Of Your Own, Will They Call You STUPID OR IRRESPONSIBLE?

Yes, this is harsh.

And WE don't believe you are either of those things.

If you FAIL to put in place the protections we are recommending in this report and ignore the warnings, then get hit with ransomware or some other form of cyber-attack, you will get no sympathy and will be found "at fault," all fingers pointing at you, for NOT taking the protection of your client's (or patients') data seriously.

You may be investigated and questioned by both authorities and clients about what you did to prevent this from happening. If you have not implemented the protections we are outlining in this report, you can be found liable, facing serious fines and lawsuits. Claiming ignorance is not an acceptable defence, and this giant, expensive, reputation-destroying nightmare will land squarely on YOUR shoulders.

But it doesn't end there…

Minnesota law requires you to disclose the breach of client or vendor data to the party affected by the breach (Minnesota statute 325E.61) and the company could be subject to civil proceedings and penalties. When it becomes public, your competition will have a heyday over this. Clients will be IRATE and will take their business elsewhere. Morale will tank and employees may even blame YOU. 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.

Don't think you have insurance and therefore are "good." There's been a sharp increase in cyber policy claims and payouts being DENIED because it was discovered that the insured did NOT have the IT security measures in place they agreed to when they bought the policy – and trust me when I say the insurance company is going to investigate whether you did before they will pay you a nickel.

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

Why We Wrote This Report for Our Clients

Over the last several years, there has been a significant increase in the sophistication, frequency, and severity of cybercrime attacks. The cost per attack has been steadily on the rise and lawmakers have been implementing new and more comprehensive regulations requiring ALL businesses become more diligent about securing and protecting data they host on their network or face stiff fines.

To make matters worse, COVID-19 forced businesses to hastily send their employees to work from home without a plan, which has led to many working in unsecured environments. Many workers are now choosing to stay home. This has energized the efforts to take advantage of businesses with employees working remote from unsecured locations.

In fact, the FBI reported a fourfold increase in cybercrime during the COVID-19 outbreak – a trend that has not lessened.

We've been watching these trends and putting in place our Security as a Service bundle to increase the level of protection available to our clients. These capabilities are in addition to the core protections in our managed service plans, and they provide additional tools to increase the strength of your defence posture.

To prepare you for our discussion, we've compiled this report to educate you and provide details on why we are making these recommendations.

Yes, It Can Happen to You And The Damages Are Very Real

The biggest challenge we face in protecting YOU and our other clients is that many believe "that won't happen to me" because they're "too small" or "don't have anything a cybercriminal would want." Or they simply think that if it happens, the damages won't be that significant. That may have held true 10 to 20 years ago, BUT NOT TODAY.

Many business owners are operating at under-appreciated, grossly misunderstood risk.

All it takes is a simple, innocent mistake made by an employee to open a cyber-attack on your organization. It's only just one click on the wrong e-mail or one file downloaded by mistake. Can you honestly say ALL of your employees are flawless and faultless? They are above being duped or making a mistake?

Then there's the clean up after the incident. Government auditors will wear you out demanding you file THOUSANDS of pages of documents and reports. Legal fees will stack. Your staff will be grossly distracted from getting any work done as they try and help you with the investigation and recovery. Your insurance company won't pay out right away, and that money you desperately need may be MONTHS out from coming in, all while you're burning money to pay your employees, rent, utilities, etc.

Then there's the time period when you are unable to work. IF your backups and disaster recovery systems aren't ready, cybercriminal will lock it all up, preventing you from working, transacting, meeting client deadlines and processing orders. How long can you go without being able to transact? Covid shutdowns revealed how quickly a business can go under when prevented from transacting.

"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 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.

Right now, there are over 980 million malware programs out there and growing (source: AV-Test Institute), and 70% of the cyber-attacks occurring are aimed at small businesses (source: National Cyber Security Alliance); 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 National Cyber Security Alliance reports that **one in five small businesses have been victims of cybercrime in the last year** – and that number includes only the ones that were reported. In total, small businesses now account for 43% of cyber-attacks annually.

Are you "too small" to be significantly damaged by a ransomware attack that locks all 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 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 ransomware demand is now $84,000 (source: MSSP Alert) with 55% of ransomware attacks are against companies with less than 100 employees. It's also estimated that small business suffers total losses 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 disgruntle employees 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.

- **They take funds, inventory, trade secrets, client lists and HOURS.** There are dozens of sneaky ways employees steal, and it's happening a LOT more than businesses care to admit.

  But here's the most COMMON way they cost you money: We've all heard of quiet quitting. This is the most extreme example, but the more subtle and dangerous scenario are the non-work activities they pursue during work hours. It's far more likely that they will become a vector for a security breach by the sites and applications they use while not doing work. Ads on a gambling site are far more likely to have trojans and viruses than LinkedIn will.

- **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.

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

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. With Dark Web monitoring and forensics tools, data breaches are easily traced back to the company and website, so you cannot hide it.

   When it happens, do you think your customers will have sympathy and rally around you? News like these travels fast on social media. They will demand answers: HAVE YOU ACTED RESPONSIBLY by 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. Right now, several senators are lobbying for "massive and mandatory" fines and more aggressive legislation pertaining to data breaches and data privacy. 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: ANY small business that collects customer information also has important obligations to its customers to tell them if they experience a breach. In fact, 47 states and the District of Columbia each have their own data breach laws – and they are getting tougher by the minute.

   If you're in health care or financial services, you have additional notification requirements under the Health Insurance Portability and Accountability Act (HIPAA), the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA). Among other things, HIPAA stipulates that if a health care business experiences a breach involving more than 500 customers, **it must notify a prominent media outlet about the incident**. The SEC and FINRA also require financial services businesses to contact them about

breaches, as well as any state regulating bodies.

One of the things we want to discuss with you is how to ensure you are and stay compliant.

3. **Cost After Cost After Cost:** A SINGLE breach, ransomware attack, or 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, and loss of sales. You'll incur forensics costs to determine what kind of hack attack occurred, what part of the network is/was affected and what data was compromised. There will also be 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 with the hope that they'll give you your data back. You'll have legal fees and the cost of legal counsel to help you respond to your clients and the media. In summary, your cash flow will be significantly disrupted, and budgets blown up.

   It's estimated that the cost per lost or stolen record is between **$150 to $225 per record compromised, after factoring in IT recovery costs, lost revenue, downtime, fines, legal fees, etc**. How many client records do you have? Employees? Multiply that by $150 on the conservative side and you'll start to get a sense of the costs to your organization.

4. **Bank Fraud:** If your bank account is accessed and funds stolen, the bank is NOT responsible for replacing those funds. Take the true story of Verne Harnish, CEO of Gazelles, Inc., a very successful and well-known consulting firm, and author of the best-selling book *The Rockefeller Habits*.

   Harnish had $400,000 taken from his bank account when hackers were able to access his PC and intercept e-mails between him and his assistant. The hackers, who are believed to be based in China, sent an e-mail to his assistant asking her to wire funds to 3 different locations. It didn't seem strange to the assistant because Harnish was then involved with funding several real estate and investment ventures. The assistant responded in the affirmative, and the hackers, posing as Harnish, assured her that it was to be done. The hackers also deleted his daily bank alerts, which he didn't notice because he was busy running the company, traveling, and meeting with clients. That money was never recovered, and the bank is not responsible.

   Everyone wants to believe "Not MY assistant, not MY employees, not MY company" – but do you honestly believe that your staff is incapable of making a

single mistake? A poor judgment? **Nobody believes they will be in a car accident 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 as a transmission vector to spread viruses and 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 the other items detailed in this report, but more on those in a minute.)

Here Is Our List Of Recommended Solutions We Feel All Clients Should Have In Place

Below is a list of items we recommend all clients have in place to maintain a good defensive posture. We continue to look for opportunities to increase the sophistication of our tools, protocols, and documentation, and will be sharing these updates with you as they come available.

- **Business Reviews And Security Risk Assessments:** We will continue to schedule and hold these meetings periodically. During these meetings, we will provide an assessment of your current security posture. We will also brief you on current projects, review plans, and discuss NEW tools and solutions. 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 Blue Assure Managed IT Services Plans.
- **Review of Cyber Insurance Requirements:** We would work with you to review the requirements for coverage to ensure that you are meeting the requirements and commitments for coverage as outlined by your carrier.

- **Security Breach Response Plan:** During an incident is not the best time to come up with a plan for responding to a security event. We will be working with our clients to create and maintain a cyber-response plan so that should a breach occur, damages, downtime and losses are minimized and addressed quickly.

- **Ransomware-Proof Backup And Disaster Recovery Plan:** Hackers know you have backups, so they construct their attacks to corrupt and lock BACKUP files if those are accessible. Your BDR plan needs to account for this contingency.

- **Security Policies for Mobile And Remote Devices:** 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.

- **Aggressive Password Protocols:** Employees choosing weak passwords are STILL one of the biggest threats to organizations. Choosing and managing complex passwords is difficult. A robust password policy requires a enterprise-grade password manager to support employees in their use of more complex passwords.

- **Advanced Endpoint Security:** Anti-virus software on laptops is no longer sufficient to protect your company against attacks. Your security solution should include the advanced capabilities available today.

- **Multi-Factor Authentication:** Multi-factor authentication for access to critical data and applications.

- **Web-Filtering Protection:** If your employees are going to visit inappropriate websites, not only are you exposed to viruses and hackers, but your company can be implicated for sexual harassment and hostile work environment.

- **Cyber Security Awareness Training:** Employees are still the #1 way cybercriminals hack into systems. Training your employees FREQUENTLY is one of the most important protections you can put in place. We have several new solutions to reduce the likelihood of someone 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. Employees need a tool to support secure sharing of

private information.

- **Secure Remote Access Protocols:** Consumer grade tools for remote access provide minimal protections for data. Remote access should strictly be via a secure VPN using enterprise tools.

- **Dark Web Breach Monitoring:** We leverage a dark web monitoring tool to identify compromised credentials and alert users that an account is vulnerable before those credentials might be used against you.

Our Preemptive Cyber Security Risk Assessment Will Give You The Answers You Want, The Certainty You Need

Over the next couple of months, we will be conducting FREE Cyber Security Risk Consultation for our clients.

Here's How It Works: We will conduct a thorough, CONFIDENTIAL assessment of your computer network, backups and security protocols as outlined in this report. Your time investment is minimal: one to two hours for the initial meeting and a second meeting of an hour to go over our report.

When this Risk Assessment is complete, we will provide you a list of recommendations and an Action Plan to remediate any vulnerabilities we uncover.

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

If you already have an appointment scheduled right now, you don't have to do anything more than meet with us.

If you have NOT scheduled a Risk Assessment, [call us at (952) 900-3832 or send me an e-mail to info@bluenetinc.com. You can also go online to www.bluenetinc.com/riskassessment and book online.]

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 issue, serious virus, or ransomware attack.

We want to make sure you are prepared for an event and experience only a minor inconvenience. Should 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,

Adam Wittke

Web: **www.bluenetinc.com**
E-mail: **info@bluenetinc.com**
Direct: **(952) 900-3832**