The Cyber Security Crisis for Florida Businesses.

Urgent And Critical Protections We Are Urging All Clients To Have In Place 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 private clients about what's going on and educate them on new protections we are urging all clients to put in place NOW.

Provided **By: Simple Solution Tech**
Author: **Christopher Rodriguez | CEO**
Mailing Address: **13876 SW 37 Street, Suite 255**, **Miami, FL 33175**
Website: **https://www.SimpleSolutionTech.com**
Office Phone: **(786) 233-2002**

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.

But 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/customer's (*or 'patient's -referring to business owners who operate a Hospital, doctor' office or Healthcare business*) data seriously.

You may be investigated and questioned by authorities and clients alike 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 defense, and this giant, expensive, reputation-destroying nightmare will land squarely on YOUR shoulders.

But it doesn't end there…

According to the laws here in Florida, you will be required to report under the **Florida Information Protection Act** (*FIPA*), businesses must notify affected individuals, and businesses without reasonable delay, but no later than 30 days after determining a breach has occurred. If the breach affects more than **1,000 individuals**, consumer reporting agencies must be informed. Failure to comply with these notification requirements can result in administrative fines, with **penalties up to $500,000** depending on the duration of the delay. The **Florida Cybersecurity Standards** offer a framework that private businesses can reference to enhance their cybersecurity measures. These standards are based on the **National Institute of Standards and Technology** (*NIST*). Keep in mind in 2022, Florida enacted legislation prohibiting state and local government entities from paying ransom in the event of a ransomware attack, state's commitment to combating cyber threats and may influence future regulations impacting private businesses.

If 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.

And 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 or not 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.

These laws in Florida, businesses that experience a data breach involving personal information are subject to the Florida Information Protection Act (*FIPA*). This law outlines specific obligations to protect affected individuals and ensure compliance. Key requirements include:

Notification to Affected Individuals: Businesses must inform each Florida resident whose personal information was accessed without authorization. This notification should be made as expeditiously as possible, but no later than 30 days after determining that a breach occurred. The notice should include:

- The date or estimated date of the breach.
- A description of the personal information accessed.
- Your contact information for further inquiries.

Notification to the Florida Department of Legal Affairs: If the breach affects 500 or more Florida residents, you are required to notify the Department of Legal Affairs within 30 days of the breach determination. The notice must include:

- A synopsis of the events surrounding the breach.
- The number of individuals affected.
- Services being offered to affected individuals, if any.
- A copy of the notice sent to individuals or an explanation of other actions taken.
- Contact information for further details.

Notification to Consumer Reporting Agencies: If more than 1,000 individuals are notified at a single time, you must also inform all nationwide consumer reporting agencies of the timing, distribution, and content of the notices.

Third-Party Data Notification: If a third-party agent maintains, stores, or processes personal information on your behalf and experiences a breach, they must notify you within 10 days of the breach determination. Upon receiving such notice, you are responsible for notifying the affected individuals and relevant authorities.

It's important to note that FIPA defines "personal information" as an individual's first name or first initial and last name in combination with any one or more of the following data elements:

- Social Security number.
- Driver's license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity.
- Financial account number, credit card number, or debit card number, in combination with any required security code, access code, or password necessary to permit access to an individual's financial account.
- Information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
- Health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
- A username or email address, in combination with a password or security question and answer that would permit access to an online account.

Failure to comply with these requirements can result in civil penalties, once again including fines up to $500,000, depending on the duration and severity of the non-compliance.

Resource provided from The Florida Bar - For comprehensive guidance, refer to the full text of the Florida Information Protection Act.

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. Now many are staying at home. This has energized the efforts of this attackers who are rapidly increasing their 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 the following new technologies, protocols and services to protect our clients.

Network Security

- **Firewall Management**: Deploy and manage enterprise-grade firewalls to filter and monitor traffic.
- **Intrusion Detection and Prevention Systems (IDPS)**: Detect and block malicious traffic.
- **VPN Services**: Secure remote access to client networks with encrypted Virtual Private Networks.
- **Network Segmentation**: Limit access within networks to minimize breach impact.

Endpoint Protection

- **Antivirus/Antimalware Software**: Deploy solutions with real-time threat detection.
- **Endpoint Detection and Response (EDR)**: Monitor and respond to advanced endpoint threats.
- **Device Management**: Implement Mobile Device Management (MDM) for securing portable devices.

Identity and Access Management (*IAM*)

- **Multi-Factor Authentication (MFA)**: Require additional verification for access.
- **Single Sign-On (SSO)**: Simplify authentication while ensuring secure access.
- **Role-Based Access Control (RBAC)**: Limit permissions based on job roles.

Data Security

- **Data Encryption**: Encrypt data in transit and at rest to prevent unauthorized access.
- **Secure Backup Solutions**: Implement encrypted, offsite, and cloud backups.
- **Data Loss Prevention (DLP)**: Monitor and prevent sensitive data leaks.

Email Security

- **Spam Filtering**: Block phishing emails and malware attachments.
- **Email Encryption**: Secure communications with end-to-end encryption.
- **Phishing Simulations and Awareness Training**: Educate users to spot phishing attempts.

Threat Intelligence

- **Security Information and Event Management (SIEM)**: Aggregate and analyze security events in real time.
- **Threat Hunting Services**: Proactively identify and mitigate advanced threats.
- **Dark Web Monitoring**: Identify compromised credentials on the dark web.

Security Policies and Audits

- **Regular Vulnerability Scanning**: Identify and address security gaps.
- **Penetration Testing**: Simulate attacks to test defenses.
- **Compliance Audits**: Ensure adherence to regulations (*e.g.*, *HIPAA*, *GDPR*).

Incident Response

- **Incident Response Plan**: Develop a detailed protocol for managing and mitigating breaches.
- **Managed Detection and Response (MDR)**: Provide 24/7 monitoring and active response to incidents.

User Training and Awareness

- **Cybersecurity Awareness Training**: Educate users on best practices.
- **Simulated Attacks**: Test user readiness with mock phishing or ransomware scenarios.

Advanced Protections

- **Zero Trust Architecture**: Verify all devices and users continuously.
- **Behavioral Analytics**: Monitor for anomalies in user behavior.
- **AI-Based Threat Detection**: Leverage machine learning for advanced threat identification.

Managed Services

- **Patch Management**: Regularly update software and firmware to close vulnerabilities.
- **Log Management**: Monitor and retain logs for forensic analysis.
- **Disaster Recovery as a Service (DRaaS)**: Provide failover systems to ensure business continuity.

Cloud Security

- **Cloud Access Security Broker (CASB)**: Monitor and secure cloud-based resources.
- **Cloud Backup and Disaster Recovery**: Protect data stored in cloud environments.

Compliance Support

- **Policy Documentation**: Assist clients in developing security policies.
- **Audit Prep Services**: Ensure readiness for regulatory audits.

Some we've been able to include in our normal fees and services to you during a "*break-fix support*" – but some are newer, more effective and would be an add-on or replacement for what you have now, which requires us to take a closer look at your current protections and make specific recommendations based on your specific situation in order move forward from "*break-fix support*" to "*Manager Service Support*".

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 stubbornly 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 up a cyber-attack on your organization. One click on the wrong e-mail. One file downloaded by mistake. Do you honestly believe ALL of your employees are flawless and faultless? 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 are 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. 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 your payroll out of your bank account? According to Osterman Research, the AVERAGE ransomware demand is now $84,000 (*source: MSSP Alert)*. It's also estimated that small businesses 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 on your dime 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, 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.

- **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, is 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 Data Disaster Reovery and 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.

What Do Other CEOs In Florida Say?

The question we asked our clients with "Why do you think other CEOs should take cybercrime seriously like you do?"

Here the other CEO's responded back that we provider services:
"*Cybercrime is no longer just an IT issue—it's a business risk that can impact every part of an organization, from operations to reputation and finances. I believe other CEOs should take it seriously because the cost of not doing so can be catastrophic. Beyond financial loss, a single breach can erode trust with customers, disrupt business continuity, and even bring legal liabilities. Investing in cybersecurity isn't just protecting data—it's safeguarding the future of the business. In today's environment, where attacks are becoming more sophisticated, CEOs have a responsibility to lead by prioritizing a culture of security at every level of their organization.*"

"*Cybercrime isn't something that happens to 'other companies' anymore—it's a universal threat that targets businesses of all sizes. CEOs need to understand that it's not just about protecting data; it's about protecting the trust and loyalty of their clients, partners, and employees. Ignoring cybersecurity is like leaving the doors to your business wide open. By taking it seriously, we not only protect what we've built but also show our team and customers that we're committed to their security and well-being. It's a leadership decision that speaks volumes about the integrity and resilience of an organization.*"

"*Cybercrime is a silent disruptor that can strike at any time, often with devastating consequences. For me, it's about staying ahead of the game—protecting my company's assets, ensuring compliance, and maintaining operational stability. CEOs need to recognize that cybersecurity isn't just a cost; it's an investment in the longevity and competitiveness of their business. The risks of downtime, data loss, or reputation damage are far greater than the effort it takes to implement strong defenses. Taking cybercrime seriously is simply smart business strategy.*"

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

IMPORTANT: Clients who are on our **Managed IT and Cybersecurity 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.

You should also know we are actively reviewing ALL clients' networks and specific situations to recommend NEW protections we feel you should have in place.

1. **Reputational Damages:**
   What's worse than a data breach? **Trying to cover it up**. Companies like Yahoo!, and AT&T 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/patients] 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. 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, financial services, hospitality, construction and engineering, government and public sector, real estate, legal, education, reatail and e-commerce, 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:**
   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. Then there are legal fees and the cost of legal counsel to help you respond to your clients and the media. Cash flow will be significantly disrupted, budgets blown up. Some states require companies to provide one year of credit-monitoring services to consumers affected by a data breach and more are following suit.

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. [**NOTE: Health care data breach costs are the highest among all sectors.**]

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 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, SIEM and the other items detailed in this report, but more on those in a minute.*)

To be clear, clients under our Manage IT and Cybersecurity Plan would be protected against THIS from happening.

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

Below is a list of things we recommend all clients have in place **ASAP**. We are also working to implement better tools, protocols and documentation, and will be sharing these updates with you as they come available, and in our Quarterly Technology Reviews for clients on our Manage IT Service and Cybersecurity Plan.

- ☐ **QBRs Or Quarterly Business Reviews And Security Risk Assessments:** We will be more persistent in scheduling and holding these 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 Managed IT and Cybersecurity Plan. Specifically, we ensure your systems remain secure, reliable, and up-to-date. By continuously monitoring your IT environment, potential issues are identified and resolved before they cause disruptions. Regular patching and updates close security vulnerabilities, protect against emerging threats, and enhance system performance, giving you peace of mind and allowing you to focus on your business operations.

- ☐ **Insurance Review:** At least once a year, we will provide you with a copy of our policies and protections for **YOU**. We can also work with your insurance agent to review your cyber liability, crime and other relevant policies to ensure we, as your IT company, and you as a company are fulfilling their requirements for coverage.

- ☐ **[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-Proof Backup And Disaster Recovery Plan:** Hackers know you have backups in place, so they construct their attacks to corrupt and lock **BACKUP** files as well. That's why we are insisting clients upgrade to our Disaster Recovery and Backup solution,

which is included in our Managed IT and Cybersecurity Plan.

- ☐ **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 monthly 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 Managed IT Service and Cybersecurity Plan.

- ☐ **Multi-Factor Authentication:** Depending on your situation, we will be recommending multi-factor authentication for access to critical data and applications.

- ☐ **Web-Filtering Protection:** Porn and adult content is still the #1 thing searched for online, and online gaming, gambling and file-sharing sites for movies and music 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.

- ☐ **[NEW!] Cyber Security Awareness Training:** Employees accidentally clicking on a phishing e-mail, 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 *Screen Connect*, *AnyDesk*, *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, it notifies you immediately so you can change your password and be on high alert.

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 Assessments for all of our clients.

Here's How It Works: We will conduct a thorough, CONFIDENTIAL investigation of your computer network, backups and security protocols as outlined in this report. Your time investment is minimal: **1 hour** for the initial meeting and **1 hour** in the second meeting to go over our Report of Findings.

When this Risk Assessment is complete, we will give you a Risk Assessment Health Score and 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 but be sure you show up.

If you have NOT scheduled a Risk Assessment, Call us at 786-233-2002 or send us an e-mail to mailto:info@simplesolutiontech.com

You can also go online to https://www.SimpleSolutionTech.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 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,

Christopher Rodriguez | CEO
Web: https://www.SimpleSolutionTech.com
E-mail: Christopher@simplesolutiontech.com
Office: 786-233-2002

Here's A Few Testimonials What Our Clients Are Saying

Please find below the testimonial we have on record from the projects we've completed for our clients. If you don't see your feedback listed, it means we'd love to hear about your experience with the services we've provided so far!

Daisy Rodriguez – Premier Mitigation

"We have used Simple Solution Tech since 2015, and the first time we used Simple Solution Tech was to back up the work we needed in the new system. After that, the technician came in and did several weeks of installing the computer programs we required for the insurance companies. They ensure everything is updated and our computers are running smoothly. Christopher sometimes uses remote access software when there's something he doesn't think he has to drive into our office; he's been able to fix it through the system. We haven't had an issue, and he always answers our call."

Isabel Ibañez. – Central Veterinary Export, Inc.

"Simple Solution Tech has been an absolute game-changer for our business. Their proactive monitoring and quick support have saved us from countless headaches. We can't imagine running our business without them."

Roy V. Prieto – M.D.P.D

"I feel a sense of relief knowing that I don't have to worry about technical issues because I trust anything that goes wrong will be addressed promptly and resolved correctly by Simple Solution Tech. Whenever I request or need assistance, the team quickly follows up and immediately provides a solution, ensuring my concerns are addressed promptly. If someone is considering their services, I would wholeheartedly

recommend trying Simple Solution Tech. I am confident they'll be more than satisfied with the professionalism, expertise, and results delivered."

Ricardo Uii Aquino – 911 Dry Solutions, Inc.

"We need a new IT company to service our emails and IT issues, and so we hired them for support. They've fixed our email automation issues. Their team also has helped set up our network and IT infrastructure. Whenever we need assistance or improvements, I can approach them for support and changes. They work until the problem is resolved, no matter what time it is. Christopher's very knowledgeable and offers his services at reasonable prices. He goes out of his way to resolve any issue."

Antonio Glustak – New Life Tires and Auto Repair.

"Simple Solution Tech started to work on our IT issues in 2010 and as the primary IT Support company. Their work is of high quality, and they are sincere. The new method works well, and there are no issues with the office. Suppose there are any issues with the network or computer. I call them. Everything always"

Rick Modero – Bunker 360

"We did a trial run with Simple Solution Tech, and I was satisfied with their work. We wanted support with implementing projects we were doing with our clients. They assist with the physical installation, programming of devices, and backend development. Their team handles gateways and safety button installations at our hotels and provides technical support for those devices. They provide peace of mind. We started with them at the beginning of 2019, and our work is ongoing. I've been in this business for over 30 years and worked with numerous vendors. With them, I can leave them in charge of a project and trust that they'll get the job done. They're knowledgeable and informed. I wish I could clone them so we could use them at all our locations. They provide a peace of mind. I've never had an issue with them."

Additional Client Testimonials web links provided below:
https://www.simplesolutiontech.com
https://clutch.co/profile/simple-solution-tech#highlights
https://maps.app.goo.gl/W8xpQ5F7EmdGodGV8

