CYBERSECURITY BACKBONE

What Every Business Owner Needs to Know

BILLY SOLANO

Master Technology Strategist for CMIT Solutions of LA, Irvine, Mexico, and South Africa: Billy Solano

author of
Cybersecurity Backbone
What Business Owners Should Know

Billy Solano
CMIT Solutions of LA, Irvine, Mexico, and South Africa
24007 Ventura Blvd Suite 290
Calabasas CA 91302
www.cmitcybersolutionsla.com

Printed in the USA.

CONTENTS

Chapter 1:
Built by Risk, Driven by Purpose

Roots In Business, Ready For More

I was born into business. Growing up in Mexico City, my family ran restaurants and marketing agencies, and my mother was a powerhouse in sales. I was raised around deals, negotiations, and the kind of work ethic that wins awards. From an early age, I saw what it meant to lead, to sell, and to serve—lessons that shaped me long before I ever held a title.

I earned my degree in business in Mexico and then went on to pursue a master's in marketing in La Jolla, California. That time in the U.S. planted seeds that would matter later. But at first, I returned home, working briefly in the family business before realizing I wanted to chart my own path.

That led me into software. And it wasn't by design. A headhunter reached out about a sales role at JD Edwards. I had no background in technology, but I knew people. I knew how to build trust and move relationships forward. That was enough. I joined the company, and within four years, I was vice president of the Company.

My success came from leveraging those connections and earning new ones. I helped bring in major accounts, including Grupo Modelo, Telmex, and Coca-Cola Bottling. These were household names, and we were delivering enterprise-grade solutions at scale.

It was that project with Modelo that changed everything. We needed to roll out ERP software across five countries. JD Edwards didn't have the bandwidth, so I reached out to a consulting firm that could help: Andersen Consulting, which would soon become Accenture.

The project was a massive success, and Accenture came calling. They offered me a partnership. I took it and spent the next decade providing global consulting services to some of the world's largest companies.

From there, I launched my own SAP channel firm. We landed a $20 million deal out of the gate. Things were booming. But then, life shifted.

A security threat—not digital, but physical—would reroute everything.

Who We Serve And Why

When I left the world of big enterprise to launch CMIT Solutions of LA, Irvine, Mexico, and South Africa, Irvine, Mexico, and South Africa, I didn't just want to build another IT company. I wanted to apply the lessons I'd learned working with Fortune 500 firms and make them accessible to small and mid-sized businesses that truly need protection. We don't serve everyone, and that's intentional.

We focus on companies where data is mission-critical. If losing access to their information would cripple their operations, we're a good fit. If data drives the business, whether it's client files, financial records, or proprietary systems, then it needs to be protected like a vital asset, not an afterthought.

That means we're the right partner for firms like accountants, attorneys, engineers, manufacturers, and healthcare providers. These businesses rely on accurate, accessible, and secure data every single day. One attack, one breach, one crash, and everything can come to a halt. That's not a risk they can afford.

On the other hand, there are industries we don't pursue. Government contracts come with layers of bureaucracy that make it difficult to move quickly or serve effectively. And we typically avoid restaurants. Not because they aren't important, but because their main technology pain points require a level of on-site support that doesn't fit our model of remote-first, scalable service.

We built our business for companies that need consistent uptime, smart planning, and proactive protection. We're not a break-fix shop. We're your IT department, just outsourced and deeply committed.

If the data matters, we're the partner you want. And if the data doesn't matter, frankly, we're not the right fit. That clarity keeps our team focused, our services sharp, and our client relationships strong.

Small Businesses, Big Vulnerabilities

Most small and mid-sized businesses come to us with a common problem: their technology isn't working as it should, or worse, it's leaving them vulnerable.

In many cases, they've tried hiring a single IT person. However, that person is often a junior engineer who costs $50,000 to $60,000 a year and still struggles to keep up with the pace of change. Even if they're smart and hardworking, they simply don't have the depth, certifications, or vendor access to cover everything from backups to cybersecurity.

That's where we come in. Our model provides businesses with access to a comprehensive IT department for a fraction of the cost of building one in-house. We handle everything, divided into eight towers—Email, Devices, Servers, Network, BCDR, Awareness Training, IT Support, and Compliance. Ninety percent of the time, we handle it remotely, so clients get responsive service without having to wait for someone to drive across town.

The issues we solve aren't just technical. They're operational. One of the biggest risks we see is out-of-date systems. Businesses don't realize how vulnerable they

are until something breaks or gets breached. If their machines aren't patched, if the antivirus is outdated, if their data isn't backed up off-site, they're one click away from disaster.

And then there's the software issue. Every platform, from Microsoft to Adobe, is constantly pushing out updates to fix security flaws. If those patches aren't applied correctly—or worse, if they're applied too quickly without testing—things crash. We've seen this play out in real life, like when an untested patch from a major security vendor took down airport systems across the country. Most small companies lack the time and resources to prevent such a catastrophe. We do.

Technology should support your business, not sabotage it. But without the right plan and partner, most small businesses are left guessing and hoping nothing goes wrong. That's not a strategy. That's a risk.

Why Cybersecurity Is Personal

For me, cybersecurity isn't just a business offering. It's deeply personal. My decision to focus on security came not from training or a textbook, but from real-world threats that changed my life.

Years ago, while still living in Mexico, I was running a successful consulting firm. My family and I lived in a beautiful home inside a country club. I played golf regularly, networked with top business leaders, and thought I had it all figured out. We had armored cars. My kids went to school with security escorts. It was the price of success. Or so I thought.

Then a friend of mine disappeared. He missed two Saturday golf games in a row. When we finally got in touch with his wife, the truth came out. He'd been kidnapped and held for ransom. It was a wake-up call. He was only released after agreeing to a $2.5 million payout and after convincing his captors that he could get them more money if they let him go.

The most shocking part? His housekeeper had tipped off the kidnappers. She'd shared his routines, his habits, even where he stored valuables. It wasn't random. It was orchestrated over months.

That incident forced me to re-evaluate everything. My family's safety couldn't be guaranteed, no matter how successful I was. So, we left. I moved my business to the United States and started over.

Years later, I faced a new kind of threat, digital this time. One of my first MSP clients, an accountant who was also my neighbor, had downplayed his data risk. He paid for basic services, nothing more. But behind the scenes, a hacker had been inside his system for six months, quietly watching and learning.

On December 19, the worst possible time for an accountant, the hacker locked everything down. He demanded $1 million in bitcoin. What we discovered was shocking: 325 clients, over a terabyte of sensitive data, and no viable backup. My client told us he had 10 to 15 clients' data. He was off by a factor of twenty.

Just like with the kidnapping, this wasn't random. It was calculated. It was preventable. And it changed me.

Since then, I've committed myself to becoming a cybersecurity expert, not just for my business, but for every client who trusts me to protect theirs.

From Survivor To Specialist

The ransomware attack that hit my client—and hit me personally—was more than just a costly lesson. It was a turning point. I realized that if I wanted to lead in this space, I couldn't just offer technology. I had to offer protection. To achieve this, I needed to become an expert in cybersecurity.

So, I began my journey. I looked for the best vendors, tools, and training. I studied how hackers operate. I already understood how they moved in the physical world because of the kidnapping scare years earlier. Seeing how similar

their tactics were in cyberspace was eye-opening. Both types of attackers hide quietly, gather information, and wait for the perfect moment to strike.

I didn't just skim articles or attend a few webinars. I earned certifications. My team and I completed intensive training programs, including one from Galactic Advisors, a company that specializes in penetration testing and security validation. After completing their program, we became officially certified cybersecurity providers.

But that was only the beginning. Every vendor we work with has its own requirements for certification. Currently, our team holds between 15 and 18 separate credentials that cover a range of areas, including endpoint protection, secure networking, and industry compliance standards.

This isn't a field you master once. It is always evolving. Cybersecurity is a constant race between threats and defenses. The bad actors change their tactics often, and we must adapt just as fast. With AI now in play, attacks are becoming more frequent and more complex. Fortunately, the tools we use have also become more powerful. We apply AI technology to analyze data logs, monitor networks, and detect suspicious behavior before it turns into a crisis.

Becoming a cybersecurity expert wasn't part of my original plan. But when the threats became personal, I knew I had to be the one who could protect others from going through the same thing. Today, that's what drives everything we do.

Saving A Manufacturer From Digital Disaster

Some success stories start quietly, just like the attacks they prevent. That was the case when a U.S.-based manufacturer reached out to us. They specialize in producing cosmetics for global French brands. Their internal IT team had noticed some strange activity. Nothing major, just enough to raise a flag.

They asked us for an assessment. That's something we do often—a deep dive into systems, configurations, vulnerabilities, and warning signs. What we uncovered was shocking.

The attacker was already inside.

Our tools and team found that their environment had been compromised for months. Malware had been deployed quietly. Six ransomware bombs had been planted, all set to detonate on May 19, a day when the company had critical trades scheduled with Europe. If those bombs had gone off, the entire operation would have been paralyzed. The client had no idea they were living on borrowed time.

Thankfully, we caught it. Our cybersecurity agents neutralized each threat, cleaned the environment, and established robust defenses to prevent it from happening again. It was a near-miss and a hard-earned save. But it was also a reminder: modern cyberattacks aren't loud. They're stealthy. They sit and wait. And they strike when your guard is down.

That client is still with us. They've since become a vocal advocate of proactive security, and they've given us permission to share their story as a formal case study.

What mattered most in that moment wasn't just the technology we used, though that was crucial. It was the experience to interpret the signs, the urgency to act, and the systems in place to move fast.

It wasn't luck that saved them. It was preparation. And that's what we bring to every client we serve.

What Sets CMIT Solutions of LA, Irvine, Mexico, and South Africa Apart

At CMIT Solutions of LA, Irvine, Mexico, and South Africa, we're part of something bigger. Our clients benefit from both national strength and local commitment—a rare combination in the IT world.

Nationwide, we operate as a network of more than 280 offices across the U.S. and Mexico. That network includes over a thousand certified engineers and technicians. Our support infrastructure includes Network and Security Operations Centers in Atlanta and Philadelphia, with mirrored capabilities in Mumbai to ensure round-the-clock coverage. If a natural disaster, outage, or emergency were to hit one location, we have built-in continuity to keep our clients protected and supported.

But that's just the technical side. The real differentiator is ownership. Each CMIT Solutions office is independently owned. I'm not a middle manager. I'm your neighbor. My name is on the line, and that personal accountability changes everything. My clients know me not just as a service provider, but as someone invested in their community, their business, and their success.

This model lets us offer the best of both worlds. Our clients get the buying power, vendor access, and proven systems of a national IT firm. However, they also benefit from the consistency and care of a trusted local partner. No faceless help desk. No bouncing from one unfamiliar tech to another. Just reliable service, delivered by someone who's accountable and accessible.

It's not just about fixing computers. It's about building trust. And that starts by showing up consistently, competently, and with a genuine commitment to helping businesses thrive.

First Steps To Secure Your Business

Cybersecurity can feel overwhelming, especially for small business owners who already wear too many hats. But getting started doesn't have to be complicated. In fact, there are a few key steps that every business can take right away to dramatically reduce its risk.

First, make sure all your software is up to date. That means operating systems, antivirus software, productivity tools—everything. Most attacks target known

vulnerabilities, and those gaps are often patched—but only if you apply the updates. Don't assume your systems are current. Verify.

Second, enforce strong password practices and implement multifactor authentication (MFA). MFA is one of the simplest and most effective ways to stop unauthorized access. It adds a second layer, like a code on your phone or an app prompt, so even if someone steals your password, they can't get in.

Third, back up your data. Not just locally, but to a secure offsite or cloud location that is isolated from your primary network. Backups should be automated, encrypted, and tested regularly. It's not enough to have a backup. You need to know it will work when you need it most.

Fourth, train your people. Cybersecurity isn't just about tools. It's about behavior. Most breaches start with a simple mistake—clicking a bad link, opening a suspicious attachment, or responding to a fake email. Regular awareness training can turn your team from a risk into a line of defense.

And finally, have a plan. Know who you'd call in an emergency. Know what systems matter most. Document your critical vendors and access credentials in a secure, centralized place. If something goes wrong, you won't have time to figure it out on the fly.

These aren't just best practices. They're the basics. And they work. Start with these steps, and you'll be ahead of most businesses already. Then, when you're ready to go deeper, partner with someone who can help you build a security strategy that scales with your growth.

Why I Do This Work

This business is personal to me. Not just because of the threats I've seen, but because of the people I serve. I've worked with global companies and managed multi-million-dollar projects. I've sat at boardroom tables and negotiated

international deals. Today, I get the most satisfaction from helping small business owners sleep better at night.

These are people who have built something from the ground up. They've taken risks, made sacrifices, and poured themselves into their work. For them, technology isn't just a tool. It's the backbone of their operations. If their systems fail or their data is compromised, everything they've built is at risk.

That's why I take this role seriously. I'm not just here to fix computers or install software. I'm here to be a trusted advisor, someone they can call when something's wrong or when they want to grow safely and smartly.

I believe every small business deserves the same level of protection as the big guys. They deserve someone who sees around corners, who understands what's coming, and who's already working to protect them from it.

If you're reading this and wondering whether your business is truly protected, don't wait for something to go wrong. Start asking questions. Get clarity. Make a plan.

You don't have to go it alone. And you don't have to settle for reactive, unreliable support. There's a better way to protect your business and your peace of mind.

Keep reading. The other chapters in this book will show you how to make smarter decisions and avoid common pitfalls. Together, we can turn technology from a source of stress into a competitive advantage.

Chapter 2:
Why Cybercrime Today Can't Be Ignored

Your business is growing. Sales are strong. Customers are happy. Operations are a well-oiled machine. Employee morale and productivity are off the charts. Then you start getting whispers from your team about some malware that your marketing guy unintentionally opened. "No worries," you think to yourself. "We should be protected since we bought that virus protection way back when."

You send your best computer guy to remedy the problem. Rebooting the computer does nothing. An assortment of virus removal tools comes up empty. Then he breaks it to you: "This isn't just a virus. It's ransomware. Sir, some hacker has access to all of our customers' files, and he LOCKED them. He won't give us access unless we pay him $7,500…PER ACCOUNT!"

Blood races to your head. You feel your heart pounding. Time stands still. This business you've invested all your time and money in has come to a grinding halt. And all of the customers you have relationships with – their files are at the mercy of an evil hacker who could be halfway around the world.

As a proud businessperson, you refuse to give in to these cybercriminals. You don't pay the ransom because it would bankrupt your business. Over the next few days and weeks, the results of this single event cripple your business. First, production and sales fall off a cliff. Second, since you're required by law to inform your customers their private information and credit cards are now compromised, you make those difficult calls…and consequently lose half of your clients. Next

come the lawsuits and the fines. Finally, the public relations nightmare buries what's left of your business.

I know this probably sounds like hyperbole, like nothing that extreme could happen to a business like yours. Unfortunately, similar cybercrimes are becoming more and more common today. And no matter how protected you think your IT network is, these professional hackers and cybercriminals invest countless hours to always be one step ahead of you.

Cybercrime today can't be ignored. In fact, the more educated you are regarding the many facets of cybercrime today and the cyber security measures you need to implement to keep your network safe, the more confident you'll be to never face a nightmare scenario where you risk losing productivity, sales, customers, money and ultimately your business. So, let's start at the beginning…

What Exactly Is Cybercrime?

Cybercrime is defined as any criminal activity that involves a computer, networked device or network. Cybercriminals, also called hackers, create malware, computer viruses and Trojan programs designed to wreak havoc on computers and networks around the world. At the very least, these cybercrimes can slow the speed of the computers on your network. At the other extreme, their actions can significantly disrupt and even cripple a business.

There are multiple categories of cybercrime, but all of them begin with a computer virus or malware program. These cybercriminals utilize these subversive and often undetected viruses to achieve their specific criminal objectives, which are usually:

- Stealing usernames, passwords, bank accounts or private information
- Accessing and selling personal information or confidential business information
- Advertising products or services on victims' computers

- Infecting computers or a network to run spam campaigns, distributed denial-of-service attacks (DDoS attacks) and/or blackmailing operations to force a substantial payment

While the motive of some cybercriminals is to directly damage or disable computers, devices and entire networks, most cybercriminals are in it for the money. Profit-driven criminal activity can include ransomware attacks, e-mail and Internet fraud, identify theft and attempts to steal financial accounts, credit cards or other payment information. Today, many cybercriminals are targeting corporate data for both theft and resale.

We tend to think of cybercriminals as men cloaked in hoodies conducting their malfeasance on the dark web. That's not always the case. Many are dressed in suits and work in a corporate office, just like well-respected businesspeople. Also, rather than hiding via the dark web, they are doing their damage in more public channels, such as social media.

History Of Cybercrime

While the Internet certainly enabled cybercrime to become more prevalent, the first instances of cybercrime were committed before the Internet as we know it today existed. In the 1970s, before computers were in households, cybercrime occurred over telephones. "Phone phreaking" was the practice of exploiting hardware and frequency vulnerabilities in a telephone network to get free or reduced phone rates.

The advent of e-mail in the late '80s marked the first major wave of cybercrime. Do you remember the Nigerian Prince scam? Of course, phishing scams like those required a total buy-in from the recipient and involved physically sending money. As a result, similar e-mail scams only conned those who were ill-informed and desperate.

With the advancement of web browsers in the 1990s, we saw the proliferation of viruses in this next wave of cybercrime. Back then, viruses lived on questionable

websites. Simply the act of visiting those websites brought about uninvited problems to your computer. Perhaps your computer ran slower. Maybe you had to endure annoying pop-up ads on your screen. Perhaps you were redirected to a porn site or two, which made for some explaining to your colleagues or spouse. All in all, while these viruses seemed serious at the time, they are almost laughable compared to what viruses can do today.

In the year 2000, America first learned of the word "malware." The infamous ILOVEYOU worm infected 50 million computers by accessing their private e-mail contacts and corrupting data. Before the ILOVEYOU worm, viruses and malware were easy to spot: if you don't know the sender or the message looks sketchy, don't open it and certainly don't click on it. That single piece of malware changed the rules. Suddenly, even trusted sources with seemingly innocent messages had to be scrutinized. Fortunately, this sparked a surge of antivirus software.

In the early 2000s, social media came to life. What could possibly go wrong when you have practically the whole world putting their private information online? You guessed it: identity theft and stealing personal information. These online hackers stole personal information to access bank accounts, set up credit cards or commit other financial fraud.

Today, we have crossed the line to a far more aggressive and more damaging brand of cybercrime. One where it's a global criminal industry totaling nearly half a trillion dollars annually. These cybercriminals operate in gangs, use well-established methods and target anyone who is connected to the Internet. And while the tools to detect and divert these cybercrimes are getting far more sophisticated, so are the cybercriminals today.

Sobering Cybercrime Statistics

No matter how many news stories you see about cybercrime attacks, no matter how many businesses you personally know that have been compromised, you can only get a crystal-clear picture of this massive industry (yes, cybercrime is an industry) when you see the statistics.

First, cybercrime represents the fastest-growing types of crime in the world. Cyberattacks are not only growing exponentially in frequency and total dollar theft, but they are also increasing in size, scope and sophistication. Make no mistake, business is booming for cybercriminals.

The Cost Of Cybercrime

- Global cybercrime costs are expected to escalate to $10.5 trillion annually by 2025, underscoring the growing threat and financial burden of cyber threats. (Source: Cybercrime Magazine)
- The United States continues to have the highest average data breach cost at $9.36 million, maintaining its position for the 14th consecutive year. (Source: IBM Cost of a Data Breach Report 2024)
- In 2024, the global average cost of a data breach reached $4.88 million, marking a 10% increase from the previous year. (Source: IBM Cost of a Data Breach Report 2024)
- The average cost of a ransomware attack on a company is $1.85 million, highlighting the significant financial impact of such incidents. (Source: Security Dive)
- Ransomware attacks surged by 73% in 2023, with attackers demanding an average of $1.54 million per incident. (Sophos, State of Ransomware 2024)
- Small businesses were the target of 43% of cyberattacks, yet only 14% were prepared to defend themselves. (Accenture, Cost of Cybercrime Study)

Cybercrime Is Commonplace Today

- 90% of organizations experienced at least one disruptive cyberattack in the past year, highlighting the pervasive nature of cyber threats across industries. (Source: 2023 CISO Report)
- In 2024, the FBI's Internet Crime Complaint Center (IC3) received nearly 860,000 cybercrime complaints, with reported losses exceeding $16 billion—a 33% increase from the previous year. (Source: The Washington Post)
- Phishing attacks remain the most reported cybercrime, accounting for approximately 193,000 complaints in 2024, underscoring the need for increased awareness and preventive measures. (Source: New York Post)
- Ransomware complaints increased by 9% in 2024, totaling 3,156 incidents, highlighting the growing threat to critical infrastructure. (Source: FBI 2024 IC3 Report)

Most Organizations Are Ill-Prepared Against Cyberattacks

- 64% of Americans have never even checked to see if they were affected by a data breach. (Source: Varonis)
- 56% of Americans don't know what steps to take in the event of a data breach.
- Only 31% of Gen Z individuals feel very confident identifying phishing attempts, a decrease from 40% in 2022, highlighting the need for improved cybersecurity education among younger generations. (Source: EY)
- Only 54% of U.S. workers know what phishing even means.
- The average susceptibility rate to phishing attempts across all industries and organizational sizes is 34.3%, indicating that a significant portion of employees are vulnerable to such attacks. (Source: KnowBe4 Phishing By Industry Benchmarking Report, 2024)
- It takes companies an average of 204 days to identify a data breach Additionally, it takes an average of 73 more days to contain the breach, bringing the total breach lifecycle to 277 days. (Source: IBM Cost of a Data

Breach Report 2023)

- 60% of small businesses close within six months after a cyber-attack. (Source: Cybercrime Magazine)

Where Is Cybercrime Headed?

While proactive IT services providers using today's latest software and technologies can keep many of the viruses, malware and ransomware off of networks and computers, cybercriminals and hackers are also becoming increasingly sophisticated. In the next few years, we can expect to experience more aggressive cyberattacks that are far more difficult to detect. What does this mean for you? Without the right IT experts and tools shielding your network, your data, your money and your business are at far greater risk.

While nobody can pinpoint exactly where cybercriminals will hit next, we have a few likely targets.

Internet Of Things Hacking

The Internet is no longer confined to our computers. It's everywhere. From our cars to our smart home devices, like Alexa and Echo, to our security systems and appliances, to our watches and fitness trackers, this proliferation of the Internet is referred to as the Internet of Things (IoT). And as the Internet spreads, so do the cyberattacks and viruses.

These convenient devices are usually wirelessly connected to the Internet, which makes them even more vulnerable. In the near future, hackers will find ways to control entire systems all from a single compromised entry point. Just imagine the widespread ramifications when your wireless camera hacks a thermostat that connects to a power plant. The more smart devices you have in your home or your office, the more gateways you have into your entire network.

Social Engineering

As we become more and more protective of our private information, cybercriminals are becoming smarter and using more sophisticated technologies to make us let our guard down. Social engineering is how they will accomplish this in the future. It will be the new norm in hacking.

Social engineering occurs when organized cybercriminals know every possible detail about their targets. They know when their targets post on Facebook, which colleagues' e-mails they open and which websites they visit. With that critical information, these more advanced hackers can pose as an employee, friend or loved one. When that happens, it's no longer an e-mail from a Nigerian Prince that's easily detected and deleted. Now it's an e-mail from your boss or business partner to get your passwords or financial details. Make no mistake, in the near future, you'll always need to keep your guard up.

Cloud Attacks

Over the last few years, businesses have been racing to the cloud. Using cloud-based solutions, businesses have been able to increase their operational efficiencies while minimizing costs. Operating in the cloud does provide another layer of security. However, since the majority of companies now keep much of their valuable data in the cloud, cybercriminals are working overtime to find a way into these mines of data.

Widespread Ransomware

Just like all of us, cybercriminals want to be paid. They've realized one of today's most lucrative cybercrimes involves stealing and locking down companies' private data for the purpose of collecting a ransom. Ransomware is a form of malicious software that encrypts a company's files, rendering critical systems and data inaccessible until a ransom is paid. This threat has evolved significantly in recent years, with attacks now targeting not just large corporations but also small and mid-sized businesses, public institutions, and even managed service providers (MSPs).

The volume and impact of ransomware attacks have surged dramatically. In 2023 alone, global ransomware damages were estimated to exceed $30 billion, and experts predict that this figure will continue to rise. A recent report from IBM found that the average ransomware payment has reached over $1.5 million, while the overall cost of recovery, including downtime, reputational damage, and legal consequences, is much higher. Alarmingly, a growing number of victims—about 71%—end up paying the ransom, either due to lack of preparedness or the critical nature of the encrypted data. As a result, ransomware remains the fastest-growing form of cybercrime, and businesses of all sizes must take proactive steps to mitigate this threat.

After reviewing how cybercrime could bring your business operations, productivity and sales to a screeching halt; how cyberattacks could cost you considerable money in fines, lawsuits, sales and even ransom; and after reading through the sobering statistics about how cybercrime has impacted businesses around the globe, you will have a clearer picture of the future of cyberattacks and you realize the serious nature of cybercrime and how you must take action now to mitigate your risks.

In the next chapter, you'll get a peek into some of the largest data breaches in the world and how they cost businesses considerably in terms of finances, customers and reputation.

Chapter 3:
The Largest Data Breaches Of The 21st Century

Data breaches happen just about every hour of every day. Far too many fly under the radar because most of them involve small businesses. While they turn business owners' and employees' lives upside down, you'll rarely learn about those cybercrimes on the news or on social media.

The cyberattacks that are in the spotlight involve giant brands we know and cost millions of dollars in theft and damages. The following case studies highlight how large companies were breached, what data was compromised, the financial and customer-loss fallout and how their management teams handled the situation. From these true stories, you can glean lessons of what to do to better protect your business from cybercrime and the steps you should take after a cyberattack.

National Public Data

In 2024, National Public Data, a company specializing in background checks, suffered an enormous data breach that exposed approximately 2.9 billion personal records. This included highly sensitive information such as Social Security numbers, names, addresses, and email addresses. The sheer scale of this breach is staggering and makes it one of the largest data exposures in recent history. The incident highlighted not only the risks inherent in handling sensitive data but also the devastating consequences when cybersecurity measures fail.

The aftermath of this breach was severe. The company faced multiple lawsuits from affected individuals and state regulators and ultimately had to file for bankruptcy. For small and medium-sized businesses, this serves as a stark warning. Even companies with expertise in data management and verification can fall victim to sophisticated cyberattacks if their security posture isn't robust enough. This breach illustrates that cyber risk is not confined to direct targets but can cascade through business ecosystems, affecting vendors, partners, and their customers.

This event should prompt SMB leaders to reevaluate how they protect customer data, especially when working with third-party providers. Comprehensive vendor risk management, continuous security assessments, and investments in advanced cybersecurity controls are essential. Failing to do so could expose your business to significant financial losses, reputational damage, and operational disruption.

Source: https://www.cbsnews.com/news/social-security-number-leak-npd breach-what-to-know/

Facebook

Early in 2025, a hacker under the pseudonym ByteBreaker claimed to have compromised data from 1.2 billion Facebook accounts. The stolen information reportedly included personal details such as names, user IDs, phone numbers, email addresses, birthdates, genders, and location data. Although Facebook itself was the primary target, the breach's implications extend far beyond the platform. For SMBs that depend on Facebook for marketing, customer engagement, or user authentication, this breach poses indirect risks that can impact their own business operations.

One major concern is the increased potential for fraud and identity theft, which can affect your customers and, by extension, your business reputation. Attackers can leverage stolen data to craft highly convincing phishing campaigns or social engineering attacks targeting your employees or clients. This creates

vulnerabilities even for companies with strong internal cybersecurity because the threat now comes from compromised external platforms.

The Facebook breach underscores the importance of a broader cybersecurity strategy that includes evaluating third-party risks. SMBs must stay vigilant not only about their own systems but also about the platforms they rely on. Regular security training, multi-factor authentication, and monitoring for suspicious activity related to external accounts should be part of your ongoing risk mitigation efforts.

Source: https://nypost.com/2024/08/19/business/national-public-data-admits-hackers-stole-social-security-numbers/

MOVEit Transfer

The 2023 MOVEit Transfer breach stands as a critical example of how vulnerabilities in third-party software can ripple through thousands of organizations. MOVEit Transfer, a popular file-sharing tool used across industries, was exploited by the Cl0p ransomware group. This attack affected over 2,700 organizations worldwide and compromised sensitive data belonging to more than 93 million individuals. The breach impacted sectors ranging from healthcare to government agencies, demonstrating that no industry is immune from supply chain cyber risks.

This incident highlights a fundamental shift in the cybersecurity landscape: even if your company has strong internal defenses, third-party software vulnerabilities can create significant exposure. For SMBs, this means that vendor security cannot be an afterthought. Organizations must implement rigorous third-party risk management practices, including vendor audits, timely patch management, and clear incident response protocols involving external partners.

Moreover, the MOVEit breach shows that attackers increasingly focus on supply chain weaknesses as a way to maximize impact. To stay ahead, SMBs need a layered defense strategy that incorporates continuous monitoring and

collaboration with vendors to ensure security standards are met. Failure to address these external risks could leave your business vulnerable to attacks beyond your direct control.

Source: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a?utm_source

Yahoo

Having ONE BILLION of your customers' accounts hacked is historically bad. Finding out years later that it was actually THREE BILLION accounts – every single Yahoo user – is even worse. In 2013, Yahoo suffered an epic data breach when cybercriminals stole names, passwords and e-mail addresses from its massive customer base. Fortunately, financial information was not compromised.

After an investigation with a third-party forensic team in 2017, Yahoo obtained new intelligence and now believes that ALL user accounts were affected. Yes, three billion accounts in all!

Yahoo took action and sent e-mails to everyone affected. They also required password changes and invalidated unencrypted security questions, all in an effort to protect user information.

While it's not clear who was behind Yahoo's cyberattack, security analysts reported that the stolen data was being sold on the dark web, an underground version of the Internet that utilizes specific software and special authorizations to access.

To add fuel to the fire, hackers attacked Yahoo again a year later. This time, the cybercrime affected approximately 500 million customers. Just recently, the Department of Justice indicted two Russian spies and two hackers for that second attack.

Source: https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html

Capital One

How much damage can a single hacker do to a giant financial enterprise? How about $150 million in damages. In 2019, a single cybercriminal was accused of breaking into Capital One's server and accessing more than 100 million customers' accounts and credit card applications.

This young woman, who previously worked as a software engineer for a tech company, gained access to 140,000 Social Security numbers, one million Canadian Social Insurance numbers and 80,000 bank accounts. In addition, she stole many customers' names, addresses, credit scores, credit limits, balances and more. By exploiting a misconfigured web application firewall, she was able to sneak into their network and access these customer records.

Perhaps the only reason Capital One realized they were hacked was because the cybercriminal took to social media and practically bragged about her theft. First, she posted on GitHub, a software development platform, about the information she stole from Capital One, including her full first, middle and last name. Next, she boasted on social media about her illegal score.

Finally, on a Slack chat service channel she explained exactly how she broke into Capital One's data files, claiming to use a special command to extract files in their directory, which was stored on Amazon's servers. She even wrote, "I wanna get it off my server that's why I'm archiving all of it lol." It wasn't long after her posts that the case was in the hands of the FBI.

Capital One notified people affected by the breach. In addition, they will make free credit monitoring and identity protection available to their customers. They expect to incur between $100 million and $150 million in costs related to

the hack, including customer notifications, credit monitoring, technology costs, legal support and lost customers due to this cybercrime.

Source: https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html

Marriott International

Between 2014 and 2020, Marriott International experienced a series of significant data breaches that compromised the personal information of over 344 million guests worldwide. The most substantial breach originated from Marriott's acquisition of Starwood Hotels & Resorts in 2016. Unbeknownst to Marriott at the time, Starwood's reservation system had been infiltrated by attackers as early as July 2014. These intruders remained undetected until September 2018, during which they accessed sensitive data, including names, passport numbers, email addresses, and payment card details of approximately 339 million guests globally, with 131.5 million of those being U.S. customers

The breaches were not isolated incidents. In addition to the prolonged intrusion into the Starwood system, Marriott disclosed another breach in 2020, where hackers accessed the information of 5.2 million guests through the use of login credentials from two employees at a franchise property. These successive breaches highlighted systemic failures in Marriott's cybersecurity infrastructure, including inadequate monitoring of acquired systems and insufficient implementation of security measures such as multi-factor authentication and encryption.

In response to these breaches, Marriott reached a $52 million settlement in October 2024 with the Federal Trade Commission (FTC) and attorneys general from 49 states and the District of Columbia. As part of the settlement, Marriott agreed to implement a comprehensive information security program designed to protect consumer data more effectively. This program includes measures such as regular security assessments, enhanced data encryption, and stricter access controls. Additionally, Marriott committed to providing U.S. customers with options to delete personal information associated with their accounts and to restore any stolen loyalty points .

For small and medium-sized businesses, the Marriott breaches serve as a cautionary tale about the importance of robust cybersecurity practices, especially during mergers and acquisitions. They underscore the necessity of thorough due diligence, continuous monitoring of all systems (including those acquired), and the implementation of comprehensive security protocols to protect sensitive customer information.

Source: https://dailysecurityreview.com/security-spotlight/marriott-agrees-52m-settlement-for-data-breach-a-deep-dive-into-cybersecurity-failures-and-legal-ramifications/?utm_source=chatgpt.com

Source : https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-against-marriott-starwood-over-multiple-data-breaches?utm_source=chatgpt.com

Home Depot

In 2014, home improvement retailer Home Depot faced a massive public relations nightmare when hackers penetrated their network. By utilizing a vendor's stolen login credentials, these cybercriminals were able to install their own malware that stole customers' credit card data and e-mail addresses. Installed on the stores' self-checkout registers, this malware was able to evade even the latest antivirus software. Unfortunately, this data breach went undetected for several months.

All told, this cyber security attack resulted in information from 56 million credit cards and debit cards in the United States and Canada to be stolen. In addition, 53 million e-mail addresses were compromised. Home Depot said that among the private information stolen were the customer's name, credit card number, expiration date and the three- or four-digit verification code on the back of the card.

Aside from costing Home Depot many millions of dollars in bad press and lost customers, the initial breach cost them $62 million. After incurring these costs and customer attrition, the Atlanta-based company agreed to pay $19.5 million to settle a class-action lawsuit brought by shoppers. This lawsuit included a $13 million fund to compensate customers for out-of-pocket expenses.

In addition to the class-action lawsuit, Home Depot gave many customers gift cards in the amount of $50 to show appreciation for being loyal. They also offered customers free identity-protection services, including a year of credit report monitoring. Finally, Home Depot has been forced to adopt new data security measures to protect its customers from future cyberattacks.

Source: https://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/

https://www.cnet.com/news/home-depot-offers-19m-to-settle-customers-hacking-lawsuit/

Uber

If there's ever a lesson into improperly handling a data breach, it's Uber. In November of 2016, the international ride-hailing company, Uber, had private information stolen from both riders and drivers. The hackers stole e-mail addresses, names and cellphone numbers from 50 million riders and 7 million drivers. In addition, they stole about 600,000 driver's license numbers from drivers.

To make matters worse, the hackers demanded a ransom of $100,000 to not go public about the breach. Uber agreed to pay the hackers $100,000 in an effort to keep the incident quiet. In an embarrassing lack of transparency, Uber hid this data breach from its drivers and riders for over a year!

The Uber breach settlement is one of the largest in history for a data privacy case. The company agreed to pay $148 million in total, which will be distributed among all states involved. There are two reasons the penalty was so steep: first,

they failed to provide timely notice of the breach. Each state's individual privacy laws require businesses to quickly disclose any data breach. Second, Uber engaged in deceptive trade practices. The state of Texas claimed that Uber violated their Deceptive Trade Practices Act by failing to provide adequate security after claiming their data was secured.

Source: https://www.cpomagazine.com/cyber-security/lessons-from-the-uber-breach-settlement/

Because these global brands have tens of thousands of employees and hundreds of millions or more in revenue, their security breaches are magnified and made examples of. Their fines are massive and their customer fallout is often irreparable.

But don't rest comfortably just yet. What you're about to read in the next chapter is the truth: small businesses like yours are cybercriminals' #1 target.

Chapter 4:
Why YOU Are Cybercriminals' #1 Target

CEOs and business owners of small businesses share many of the same beliefs about cybercriminals and the odds that their own businesses will be attacked. They have a FALSE sense of security. The reason: many of them buy in to a number of misconceptions.

Misconception #1: Our business is too small. Cybercriminals are mainly targeting major corporations.

On the surface, that brand of thinking seems logical. After all, why would you target small businesses when these global giants have a ton more data and money to steal? Plus, you tend to only see headlines about cyberattacks involving major players like J.P. Morgan, Target, Experian, Home Depot and Yahoo.

That's exactly what cybercriminals are counting on you to believe. It makes small businesses easy prey because they tend to put zero protections in place or grossly inadequate ones.

Why don't you hear about banks being robbed anymore? Because criminals know that banks have incredibly sophisticated security measures in place. Not only is it very difficult to rob a bank, it's nearly impossible to get away with it and not get caught. Therefore, most criminals go after soft targets, such as homes or gas stations. This same logic is the reason most cybercriminals target small

businesses and not the Fortune 500 businesses. They know you're not spending millions on cyber security and you don't have a massive IT team working 24/7 to protect your assets.

According to the 2024 "State of SMB Cybersecurity" report by ConnectWise, a staggering 94% of small and medium-sized businesses (SMBs) experienced at least one cyberattack in the past year, marking a significant increase from 64% in 2019. (Source: Connectwise) Of course, that number includes only the ones that self-reported. Most small businesses are too embarrassed or afraid to report breaches because they don't want the PR nightmare. Also, while many states have adopted the "you must report a security breach" mentality, business owners know there are no penalties or fines if they don't report. Of course, states are now working on legislation to penalize those who do not self-report.

It's safe to assume far more small businesses have been hacked than the statistics show. And if you never implement stronger IT security measures, you are essentially a "sitting duck," just waiting for the inevitable to become another small business statistic.

Misconception #2: We have competent IT people / We have adequate protections in place.

If you have an entire IT department or even one IT person, you may believe you already have a shield of protection around your computers, important files and network. Chances are that your IT team and security tools aren't operating at the same level as those of Facebook, Marriott, Uber, Home Depot, or Google with their vast budgets and dedicated cybersecurity departments."

Perhaps that's why according to the Small Business Administration, 88% of small business owners believe they are vulnerable to a cyber-attack. Also, Corvus Insurance states that 47% of small businesses with fewer than 50 employees have absolutely no cybersecurity budget. And BullGuard says that 40% of attacked small businesses lost critical data.

Cyberthieves stole data from approximately 500 million Marriott International customers. These hackers first entered their network four years before the cyber-attack even took place!

Equifax, one of the largest credit bureaus in the US, had a data breach that exposed 147.9 million customers. Even worse, 209,000 consumers had their credit card data compromised.

Approximately 5 million usernames and passwords of Google Gmail account holders were compromised and leaked on a Russian forum site.

If these titans of industry that have the newest cyber security software and technologies and scores of cyber security experts can get hacked, so can small businesses like yours.

Risks To Your Business

Though you never imagine it could happen to your business, what could you realistically expect if you fall victim to a cybercrime? The fact is, even one event could trigger an avalanche of disruptions, costs and damage to your business that could last months or years, or worse, you may simply never recover and be forced to close your doors. Here's hoping you never have to endure the costly and time-consuming cleanup of a cyberattack. But if it happens to you and your business, the following are the dominos you can expect to fall.

A Mountain Of Costs

Just one breach, one ransomware attack or one rogue employee can create untold hours of extra work from your entire team. Then there's business interruption, downtime and backlogged work delivery for your current clients. Because business productivity slides and attention to prospects and existing clients suffer, it's not uncommon to see a drop in sales for several weeks or months.

Then comes the costs associated with the hack. First, there are forensics costs to determine what kind of hack occurred, which parts of the network were affected

and what data was compromised. Second, you can expect to pay for emergency IT restoration costs for getting back up and running, if that's even possible. Third, if the attack was ransomware, you'll be forced to pay the ransom and hope these criminals who hacked your network honor their word and give you your data back. Hint: Can you really trust criminals to be honest? You may pay and still not get your data back! The price may even go up!

Then you can expect your cash flow will be significantly disrupted and budgets blown up. After all, when your customers' private information is stolen and you're begging them not to leave, do you really think marketing becomes a priority?

According to IBM, the average cost of a data breach today is $165 per compromised record. Think about how many records you have. Clients, employees, prospects. Now multiply that number by $161, and you'll start to get a sense of the costs to your organization. (Note: The healthcare industry incurs the highest average data breach costs at $7.13 million, and doctors can have thousands of patients.)

Think about how many records you have. Clients, employees, prospects. Now multiply that number by $225, 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 industries, and doctors can have thousands of patients.)

Government Fines, Legal Fees, Lawsuits

Beyond the loss of customers and sales, beyond the restoration costs and lack of productivity, if your business is the victim of a cyberattack, there are also massive external expenses you are likely to incur.

The government will be among the first in line with their hands in your pockets. Breach notification statutes remain one of the most active areas of the law. Right now, several senators are lobbying for "massive and mandatory" fines pertaining to data breaches and data privacy. Forty-seven states and the District of Columbia have their own data breach laws, and they are getting tougher. The

government could care less that it was a criminal act and wasn't entirely your fault. They expect you to pay punitive fines.

If you're in the health care or financial services sectors, 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). Beyond simply notifying clients with compromised information, if the breach involves more than 500 clients or patients, you must notify a prominent media outlet about the incident. That's when a public relations firestorm is ignited, and clients leave in droves.

Then there are legal fees and the cost of legal counsel to help you respond to your clients and the media. Speaking of legal, in today's litigious society, you can fully expect some people whose private information was stolen (customers, vendors, employees) to sue your company. Proving your security was sufficient to protect their assets would probably be a losing battle. Therefore, you would most likely lose the lawsuit, costing you tens of thousands, hundreds of thousands or more. It adds up quickly.

Loss Of Reputation And Customers

Your reputation IS your business. If you have a data breach and your customers' private information is stolen – whether it's their credit card numbers, their e-mail addresses or their passwords – it is your responsibility to inform each and every compromised account. Ideally, you should let them know of the data breach through multiple forms of communication (e-mail, phone call, notice on your website) as quickly as possible so they have time to cancel their credit cards and change their passwords.

Nobody likes delivering news that will negatively affect their business, but it must be done. Yes, once your customers are aware their private information was compromised, you can expect some pretty harsh responses. Statistics show that 83% of consumers in the US claim they will stop spending at a business for

several months after a security breach, and 21% will never return to that business. Even worse, lots of your customers will take to social media and review-type websites to express their anger and smear your company. Plus, the customers who believe they lost significant money or time may even consider legal action.

The first wave of business loss comes from these disgruntled customers. The next wave of loss results from your damaged reputation. Once word spreads that you didn't have the security protections in place to keep your customers' private information safe, it's a black eye for your company's trustworthiness. People will steer clear of your business and run toward your competitors.

What's worse than a data breach, losing customers and the reputational fallout that follows? Not telling your customers at all and trying to cover it up. Companies like Yahoo and Uber are learning that lesson the hard way, facing multiple class-action lawsuits for not telling their users immediately when they discovered they were hacked. Nowadays, there are monitoring and forensics tools that can easily trace a data breach right back to the company where and when the breach occurred. In other words, there is nowhere to hide. Delay in reporting a breach snowballs the fines, lawsuits and customer backlash.

While a data breach that exposes your customers' trusted passwords, credit card numbers and personal information is bad, covering it up or simply pretending it never occurred could be the death of your business. Customers may forgive a mistake. They certainly won't forgive lying. And when word gets around that you cared more about protecting your profits than protecting your customers, it will take years to undo that damage.

Bank Fraud

Not all cybercriminals target your customers. Many of them will directly target you and your business. More than stealing information, they'll want to steal your money. There is a false assumption today that any money stolen by a cybercriminal is instantly and easily replaced by your bank or financial institution. This is NOT always the case.

If your bank account is accessed and funds stolen, the bank is not responsible for replacing those funds. Take the true story of successful author and CEO of Gazelles, Inc., Verne Harnish. Verne was using free, public WiFi while outside of the country, which allowed hackers to gain access to his username and password so they could access his e-mail account. The hackers, who are believed to be based in China, reviewed his sent e-mails to mimic the same verbiage Verne used before and then sent an e-mail to his assistant asking her to wire funds to three different locations. Because Harnish was involved with multiple real estate and investment ventures and because it looked just like previous requests to wire money, it didn't strike the assistant as out of the ordinary. Plus, how many people would question what their boss asked them to do?

The assistant responded in the affirmative, and the hackers, posing as her boss, assured her that it was to be done. The cybercriminals also deleted Verne's daily bank alerts so he wouldn't be tipped off when the money was stolen. All told, these cybercriminals stole $400,000. What's worse, the bank was not responsible and the money to this day has never been recovered.

How could you possibly prevent a similar theft or someone trying to access your credit or debit cards? You could set up both e-mail AND text alerts for all financial transactions, including your credit and debit cards. Of course, you would need to thoroughly review each alert to ensure each transaction was legitimate.

False Sense Of Security

Right now, you're probably thinking, "MY assistant would never do that." But that's what EVERYBODY thinks: "Not MY assistant. Not MY employees. Not MY company." Everybody thinks like this until it happens to THEM.

Do you honestly believe that your staff is incapable of making a single mistake or a poor judgment? Nobody believes they will be in a car wreck when they leave the house every day, but you still wear a seat belt. You don't expect a life-threatening crash, but that's not a valid reason to avoid buckling up. Unless

you're equally protected in your business, you are at risk for losing considerable money, lots of customers and mountains of goodwill and reputation.

Now that you know that you and your small business ARE a likely target for a cybercrime and just how much one data breach can cost your company, let's take a closer look at exactly how these cybercriminals can attack your network and destroy your business.

Chapter 5:
How Cybercriminals Attack Your Network

You've just learned how much damage these cybercriminals can do to your finances, customer base, reputation and ultimately your business. But how do they break into your network and cause these massive financial and productivity nightmares? There are literally dozens of ways cybercriminals can hack into your system. The following are several of today's most used methods to wreak havoc on your entire network.

Spamming

Many people think that spam is an acronym. It's not. The name came from an old *Monty Python* episode in which the word "spam" is repeated over and over. In the sketch, by repeating the word at increasing volume, it became both annoying and irrelevant. The nickname "spam" stuck because it perfectly describes the flood of useless, irrelevant and uninvited e-mails that people receive in their e-mail inboxes.

Today, spam is still the #1 entry point into a network simply because people click links that they shouldn't. Spam also becomes a challenge when the sheer volume of unwanted e-mails crowds out your important business and personal messages.

Just a few years ago, spam was easy to detect because of the broken English and funky links. Today's scammers are smarter, use company logos and spell-

check everything so as not to be detected. Accidentally opening and clicking on a spam link could invite threatening malware into your computers and network. Rather than wait for unwanted spam to negatively affect your business, create a proactive plan to address it. This could include software that detects and removes spam or creating anti-spam filters or rules to keep it out of your in-box.

Phishing

While most everyone can spot a spam e-mail at a glance, phishing is much more difficult to discern. The reason is because phishing uses realistic e-mails in an attempt to trick recipients into sharing passwords and other sensitive information.

Cybercriminals who rely on phishing to steal passwords, private information or even money are constantly perfecting their craft to resemble the company they are trying to mimic. One widespread example of phishing mimicked Visa and told recipients that their credit card would be temporarily disabled if they didn't go to a specific website and change their password immediately. Every step of the way, from the e-mail to the website, looked very similar to Visa's branding.

Another phishing example includes a bank e-mail tricking an employee into providing company banking information. By sending threatening messages to specific employees, they are more likely to oblige and act too hastily. Phishing e-mails may also feature attached zip files that, once opened, will spread malicious viruses throughout computers and entire systems in almost no time at all.

While many Americans are now wise to never send personal information and certainly not credit card numbers or passwords via e-mail, phishing is still a very effective entryway into businesses' computers and IT networks. Rather than deal with the embarrassment of asking their manager or boss whether or not an e-mail is legitimate, many employees will take action on a professional-looking e-mail. It takes just seconds to let unwanted hackers into your business network. And once they're in, there's no telling the damage they can do.

Malware

A combination of the words "malicious" and "software," malware is any piece of software or code created with the intent of damaging devices or stealing data. Malware includes all malicious software, including viruses, worms, spyware, ransomware, Trojan viruses and others.

So, why do cybercriminals spend so much time creating and distributing malware? They do so with the intention of selling it online to the highest bidder for use by other criminals. Also, some cybercriminals engage in malware as a tool for protests. Others use it to test cyber security or even as weapons of war between governments.

Malware can also be used to turn a computer into a bot (robot) designed to perform malicious attacks on other computers. Therefore, even if your firewall is set up to block attacks from countries such as China or Russia, it won't block malware attacks from your local computer.

Ransomware

Ransomware is a type of malware that is exactly what it sounds like – a software that holds your computer system and sensitive information hostage until you pay the ransom for the decryption key. Imagine coming into the office and discovering that you can no longer access your customers' files, financial information or all of your research and development records for your upcoming product launch. These cybercriminals know just how important this information is to keeping your revenue stream flowing, which is why they know most businesses will pay.

Ransomware is typically introduced to a system through a single employee who opens something they shouldn't. Because it is often hidden in attachments, such as an "unpaid invoice" in PDF format or a package-tracking document in Word form, ransomware often looks very innocent. However, when it's opened, the malware makes it impossible to open any other documents or applications until the ransom is paid.

Emerging trends include ransomworms, such as the infamous WannaCry and NotPetya attacks. Ransomware attacks are now a part of today's cyberthreat environment, which is getting considerably more sophisticated and costlier. In August 2019, in a coordinated ransomware attack, twenty-two Texan towns had their networks hijacked. A year earlier, Atlanta's IT infrastructure was infected by ransomware. Although the city elected not to pay, they still spent upwards of $18 million to recover.

Because health care businesses must protect their patients at all costs, nearly half of all ransomware attacks target health care companies. And because most hospitals, doctor's offices, clinics and dentists have thousands of patients, paying the hacker per patient record can result in an extraordinary amount of money. The most high-profile attacks today affect large businesses and municipal governments. Even though many target specific industries, hackers are also casting large nets, including small businesses. By infecting hundreds or thousands of businesses just like yours, even if only a small percentage of them pay, they win.

Spyware

Spyware is another type of malware that can be downloaded as easily as ransomware, through the same unassuming kinds of e-mail attachments. However, rather than holding your information hostage for a ransom, it doesn't appear to do much of anything. Behind the scenes, it's actually doing a lot. It could be logging every keystroke in your entire company or copying e-mails and sending all of the gathered data to the spyware's creator. Of course, the only minor indicator that your system has been infected is that it may seem a little slower than usual.

Most spyware is used in conjunction with adware to monitor your Internet and social media habits. But it's a huge privacy and security threat. Spyware can actually be used to gather personal information for the purposes of identity theft and fraud. Because you have no control over what spyware monitors or where the information is sent, it's in your best interests to prevent all spyware in the first place and do everything you can to remove it from your computers.

Adware

Most everybody knows adware when they see it. Adware, comprised of the words "advertising" and "malware," typically creates annoying pop-ups that crowd your computer screen. Now, unlike other malware, adware is not as dangerous as it is merely irritating. However, it does have the capability of undermining your security settings and tracking your activities as it slows down your computer performance.

Adware is mainly used for pinpoint marketing. While spyware watches your web-browsing habits, adware serves up ads based on what you're looking for. It's similar to your grandmother's party line, where you could listen in to your neighbors' conversations. Call the operator and ask for Pizza Hut's phone number. Then, just before you call Pizza Hut, Domino's is calling to tell you about their specials. They know you want pizza so they are getting in front of you with ads to entice you to buy from them.

Worms

Worms are unique in the world of malware because they are "stand-alone." That's because worms don't need interaction to spread to other computers. Once it gains access to a network – like clicking on an innocent-looking attachment in an e-mail – the worm quickly spreads, relying on technical vulnerabilities to infiltrate the network. That's right, an Internet worm is much like a parasite. Like a tapeworm, it duplicates itself across as many computers as possible. While worms themselves are rarely dangerous, they often create backdoors in the system that allow a hacker to launch more serious malware attacks.

Trojan Viruses

Remember the story about the Trojan Horse? In the Trojan War, the Greeks secretly constructed a huge wooden horse that hid a select force of men inside. They rolled this massive horse into Troy, and before they knew what hit them, the Greeks won the war. Because it hides within plain sight (seemingly harmless programs), this form of malware is called a Trojan.

While viruses and worms can self-replicate and infect additional files and computers on your network, a Trojan introduces dangerous malware to a computer or network. These advanced forms of malware survive because they go unnoticed. While there, they can collect information, create holes in your security or take over your computer and lock you out.

Social Engineering

As societies become more educated about how to detect malware and viruses, cybercriminals must become more sophisticated to sneak into your in-box and entice you to click. Similar to phishing, social engineering is far more personal. With social engineering, the attack can range from something as simple and direct as posing as a coworker with a seemingly legitimate e-mail and asking for a password, to developing relationships online or even in person, viewing social media pictures of where a potential victim frequently visits and targeting them outside of work.

Ransomware can be designed to exploit technical vulnerabilities and sneak into your computers and network, but the simplest form of spreading it is by someone opening up the front door. That happens when hackers can outsmart your employees, and they open an e-mail that looks like it's from a friend or colleague. The more advanced the social engineering process, the more likely someone will unknowingly invite malware into your network and business.

Cybercriminals today have an entire arsenal of weapons to attack every computer in your company as well as your network. From simple phishing, spyware and adware software to dangerous malware, costly ransomware and Trojan viruses, it's like your business is a sitting duck just waiting for the inevitable to happen. Thankfully, over the next few chapters, we will give you the strategies, tools and resources to build a formidable wall and defend yourself from these hackers and cybercriminals.

Chapter 6:
What You Can Do NOW To Protect Your Network And Business

After reviewing just how much you and your business stand to lose due to threats by hackers and cybercriminals, and all of the complex and subversive ways into your network, you may wonder if you even have a chance. Absolutely!

In our experience, the business owners who best avoid getting hacked are the ones who are most proactive. The more defenses you put now between your network and cybercriminals, the more likely it is you'll avoid becoming the next small-business statistic.

Taking Responsibility As A Business Owner

As a business owner myself, I understand the massive responsibilities we must assume. You're responsible for increasing revenue and growing the business. That means attracting and closing sales or bringing in new clients or patients. You're responsible for meeting payroll for your employees and ensuring they work for a quality company that provides adequate health care, training and excellent facilities. You're responsible for ensuring operations, marketing, accounting and possibly the warehouse all run smoothly.

Yet I'm shocked at the number of business owners I've met over the years who believe that managing their computers and IT infrastructure – possibly the most important aspect of their business – should be someone else's duty. Of course, nobody expects you to be the one who monitors your network, scans for

viruses and installs software to optimize your system. However, as the owner or manager of your business, at the very least, you should know just how secure your network is … or is not.

I am willing to wager that your computer network and the critical data it holds are not nearly as secure as you think they are. Because after auditing most business networks, I am usually appalled by the incompetence and irresponsibility I discover. In 98% of the computer networks we review, I find faulty or nonexistent backups, security loopholes, shoddy reporting and flawed systems that simply cost more to maintain and don't align with the operations of the business.

If you are exposed and your network gets hacked, news travels fast on social media. Your clients and your community won't be quick to forgive. A response of "Sorry, we got hacked because we didn't think it would happen to us" or "We simply didn't want to spend the money to prevent a cyberattack" will not be sufficient. They will demand answers.

Make no mistake, as a business owner, protecting your IT network and all of the private data and financial information on it is a top priority. And whether you have a computer guy, an in-house IT team or a third-party consultant who oversees all things IT in your business, who do you think your clients, partners and employees will blame if a hacker breaks in? Ultimately, they will blame you. It's your business. It's your responsibility.

Fortunately, this chapter is dedicated to helping you take necessary steps to protect your network and your business so nobody has an opportunity to point fingers, because your system will remain safe and secure.

Keep Spyware, Malware And Viruses Off Your Network

You've just read all of the dangers of spyware, malware and viruses. Once this malicious software gets onto your business computers, it's only a matter of time before it invades your IT network and starts wreaking havoc. Often, it goes unnoticed until long after the damage is done.

Rest assured, you can be vigilant about keeping this malware off your network. That's because in almost every cyberattack case, malware, spyware and viruses were able to infect a network because of some action taken by a user. Cybercriminals are incredibly clever and have figured out ways to access your computer network through some of the most innocent and common daily activities.

For example, many of the clients we see infected with spyware simply downloaded a screen saver, an "enhanced" Web browser, a music file or some other enticing but unnecessary program. By simply taking this unintentional action, they unknowingly downloaded a number of spyware and malware programs.

As a result of their actions, they could no longer use their computer because of its slowness, instability and abundance of pop-ups. Sure, your computer consultant can usually clean up the mess caused by these programs, but it is still your responsibility to become educated about what you and your employees can and cannot download. The following is a short list of program types that nobody in your office should download:

- Screen savers
- "Enhanced" Web browsers like Cool Search
- Emoticons
- Games
- Peer-to-peer file-sharing software (e.g., KaZaa, BitTorrent)
- Music files
- "For fun" surveys
- Banners that challenge you to "punch the monkey," shoot something or answer a trivia question to win a prize
- Sweepstakes or drawings
- Any software that requires you to accept certain conditions. By agreeing to those conditions, usually outlined in small print, you are agreeing to accept third-party software

While each of those program-type files should raise a red flag and immediately be deleted, there are a wide variety of files that may or may not be harmful to your computers and network. That's where it becomes tricky. You certainly don't want to slow down productivity in your office; however, if you let just one piece of malware sneak in, it could bring your entire business to a grinding halt.

As the owner of your business, you should keep a lookout for and keep your guard up for the following types of files delivered by e-mail. While most of these files should be harmless, all it takes is one that's packed with a dangerous payload to infiltrate your network and disrupt your entire business.

Executable Files

This is where all of this mayhem started. If there are any files to avoid like the plague, it's executable files. There are a couple of different types:

- **.exe Files –** The extension .exe marks an executable file that can become active on your computer the second you open it. Over the years, these types of executable files have carried very dangerous payloads that have infected entire networks. These files should NEVER be opened if attached to an e-mail. Thankfully, there are many other less dangerous file formats available today. Plus, most e-mail providers, such as Gmail and Outlook, completely block e-mails containing .exe extensions, so you'll hopefully never see them.
- **HTML Files –** Not too long ago, you would receive multiple HTML e-mails every day. Since it is the standard language used to create web pages, it was very common. However, in the .html format, Trojans and worms can easily hide. To fight the risk of accidentally releasing malware onto your system, many companies no longer allow HTML e-mails to hit their servers.

Text Files, PDFs And Document Files

Any business office is going to constantly send and receive text files, PDFs and document files in order to get work done. The large majority of these are legitimate files; however, all it takes is one that looks like an innocent file before it starts eating away at your network.

- **.txt Files –** These are generally harmless since they represent a standard text document that is recognized by Word or any word-processing program. They can also be opened using Microsoft Notepad and Apple TextEdit. However, in the year 2000, the ILOVEYOU computer worm spread rapidly across the globe. People opened it because it had a .txt.vbs extension, but most e-mail programs didn't display the ".vbs" part. People opened it because they thought it was a simple text document. Instead, it did $10 billion worth of damage.
- **.pdf Files –** Everyone knows PDF files. Most of the time, they are harmless files opened with Adobe Reader. However, there are many security gaps that allow cybercriminals to transport malware onto your computer using PDF files. If you don't recognize who is sending the PDF, think twice before opening it and downloading it. Beware of links within PDF documents that take you to a remote website or download a malicious payload.
- **.doc / .docx / .xls / .xlsx / .ppt / .pptx Files –** These are all Office documents that are commonly e-mailed. The danger in opening these files is that they could contain macro viruses. Starting with Office 2007, Microsoft made a helpful change by alerting you of a file containing potential harmful macros with the extension .docm. However, a .doc file may or may not contain macros. Beware of links within these documents, especially if they take you to a remote site or download dangerous malware.

Certainly, you can't adopt a policy to never accept e-mails with .pdf files or .doc files. That could be a nightmare for your team's productivity. However, you can be proactive in how you handle these files. First, confirm with the sender that they intentionally sent the file you received. If you weren't expecting an e-mail with a file attachment, simply double-check with them. Second, if you receive an e-mail with a .doc attachment, ask the sender if they could resend the file as a .pdf, which could be less of a risk.

Image Files

The extension .jpg represents an image or picture file. If you run an advertising agency, photography studio or architectural firm, you would naturally receive these types of files on a daily basis. However, most businesses have little reason to receive .jpg files, especially when they can easily be turned into less risky .pdf files.

The reason .jpg files could be harmful to your network is that the extension is often used to camouflage an executable program. Make sure your e-mail program displays the complete file extension to lessen the risk of a malicious attachment.

Audio Files

Audio files are typically sent as a recording of a webinar, videoconferencing call or presentation. Therefore, they should not be a regular occurrence in most companies. If your employees tend to send and receive many audio files, you may inquire if they are exchanging songs via your company e-mail. You certainly don't want to put your entire business at risk because employees are violating company e-mail policies.

- **.mp3 Files –** These audio files are generally safe. But always double-check with the sender prior to opening.
- **.wav Files –** Audio data in a WAV file is not compressed. These files tend to be much larger in size than .mp3 files. Because it's not compressed, .wav can be a much easier file type to hide malware. Always be suspicious of any .wav attachments that come across your network.

Video Files

Like audio files, large video files are excellent hiding places for malware. You'll know it's a video file by the extension: .mpg / .mpeg / .avi / .wmv / .mov / .ram. Again, most businesses don't exchange video files on a regular basis. If one of your employees gets bombarded by multiple e-mails with video file attachments on a daily basis, inquire if it's truly necessary or unrelated to business.

Compressed Files

Compressed files, like .zip and .rar files, pose a significant risk for businesses like yours. That's because they can contain viruses that become active as soon as you extract them. Always make sure you trust the origin of the e-mail attachment before opening.

Beware Of Additional Entry Points

If hackers really want into your network, they have more options than hoping your employees click on their e-mail attachment. If you don't have the most up-to-date security patches and virus definitions installed, wrongdoers can access your computer in other ways.

Most spyware and virus attacks are the result of an end user (such as an employee, business owner or partner) downloading a questionable file or program, disabling their antivirus software or somehow circumventing security settings or acceptable-use policies set by your computer guy or IT consultant.

Many businesses have hardware or software inadequacies that may not be able to be controlled or prevented by typical computer consultants. Also, many business owners don't want to pay for their consultants to perform simple preventive maintenance, update security patches and virus definitions or monitor their system's performance. This lack of maintenance is an invitation for problems that could become massive inconveniences that affect your time and wallet.

A Good Firewall Is Essential

Don't scrimp on a good firewall. A firewall acts as the frontline defense against hackers blocking everything you haven't specifically allowed to enter (or leave) your computer network. As with all devices on your network, firewalls need monitoring and maintenance. Your company IT person or consultant should include your firewall as part of their regular maintenance of your network.

There are several reasons why your business will benefit from a strong firewall:

- **Block access to unapproved websites.** You can set up a firewall to block access to social media sites, betting sites, sports sites and other time wasters.
- **Protect your business from malicious code.** Strong firewalls can inspect the traffic going into and out of your network. All day, every day, your firewall can detect and block viruses, worms, spam and other unwanted Internet traffic. Plus, they will log intrusion attempts as well as block malicious applications while allowing access to the good ones.
- **Better control your bandwidth.** Beyond providing security, you can actually meter and limit your network bandwidth. By curtailing non-business traffic, such as videos, music and images, you'll have more bandwidth for essential business applications.
- **Provide VPN services.** Today, firewalls can provide site-to-site connectivity through virtual private networks (VPNs), which allow users at remote sites to securely access your internal network resources. Now, any work-from-home employees, as well as traveling employees and contractors, can increase their productivity and collaboration by securely accessing your network.

Train Your Employees

Because we're talking about safeguarding your computers, network and data, we tend to think that the best defense should also be electronic. While installing virus and malware detection software is critical to keeping your important data out of the wrong hands, your first line of defense should be the people in and around your office. Yes, you and your employees. Training your employees on how to properly use your technology and how to identify potential cyberthreats is essential to staying one step ahead of the cybercriminals.

Tucking this vital information into the back of an employee manual is simply not sufficient. Neither is a one-time staff training that will be ignored and forgotten. You and your entire team should have a basic understanding of the methods of cybercrime, as well as regular updates on computer security protocol and the latest in cybercrime tactics and defenses. Your employees should have

an in-depth understanding and proactive resolve to ensure the best practices toward passwords, keeping a clean space, identifying malicious e-mails, proper communication, social engineering and encrypting e-mails. More information about encrypting e-mails is covered later in this chapter.

Create And Enforce An Acceptable Use Policy (AUP)

Training your employees goes beyond teaching them about being diligent in spotting a malicious e-mail. Everyone on your team needs to be aware of how they can actively protect your business from cybercrime. You can accomplish this by circulating Internet security policies, also known as acceptable use policies (AUP) or fair use policies. These are written documents created by the business owner that clearly state precisely what employees, subcontractors and end users can and can't do in regard to accessing the Internet, company computers and e-mail while working for your business.

You should require everyone who accesses your network in any capacity to sign the acceptable use policy before they are able to access your Internet, computers or e-mail. By requiring an agreement, AUPs ensure your end users are explicitly aware of their rights and responsibilities.

For example, employees should not be allowed to download or access programs, screen savers, pictures, music files or file-sharing networks. Not only will this save precious bandwidth, it also prevents accidentally downloading viruses and spyware. An AUP should also educate employees on the appropriate use of your company's resources.

If you don't want your staff to download pornographic material and send racist jokes through a company e-mail account, for instance, you have to communicate this information to them in an AUP and have them acknowledge in writing that they have read and understood it. Your IT consultant can help you draft this document and enforce the policies outlined in it.

There are multiple reasons why you should consider an AUP for your business:

- **First, it ensures the safety of the users.** By clearly outlining prohibitions and rights, it can help deter illegal or offensive behavior that can damage the reputation of the organization or endanger users. Examples of this include the sale of counterfeit goods or outlining standard practice for commenting on blog posts.
- **Second, AUPs can protect the business from any legal action.** In case of any legal action or cybercrimes associated with your company's website, the acceptable use policy proves the company has taken reasonable measures to protect the interests of users.
- **Third, they can safeguard the organization's reputation.** Any business, especially those that engage with customers online, should make an effort to show due diligence in regard to cyber security and safety.
- **Fourth, AUPs enhance ease of use and productivity.** Business owners and managers don't want to pay for employees who waste company time on Facebook, YouTube and other non-productive sites. An AUP guides end users and customers on acceptable practices.
- **Fifth, AUPs better regulate employees using their own personal devices.** If an employee is checking unregulated, personal e-mail on their own laptop and their laptop gets infected by malware, a hacker now has a gateway to enter YOUR network. Also, what happens if that employee leaves the company?

Create And Enforce A Bring Your Own Device (BYOD) Policy

A BYOD policy allows employees to bring in personal mobile devices and use these devices to access company data, e-mail, etc. While inviting in computers and devices from home may be convenient and a way to curb costs, it also invites new opportunities to breach your network and access your company data.

Questions you should ask: Are you permitted to erase company data from their personal laptop or phone? If not, what happens if those devices get into the wrong hands and hackers suddenly have direct access to your servers? You must

protect your business with an AUP that permits you to remotely wipe any device so your company data isn't compromised.

Further, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, you may not be legally permitted to allow employees to access it on personal devices that are not secured. Of course, this doesn't usually happen in a malicious way. An employee may innocently take work home with them. If it's a company-owned device, you need to detail what an employee can or cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

Creating Better Passwords

Of course, it's much easier to remember the same password you've used a million times before … or one featuring your birthdate or your daughter's name … or simply using "password" (which, even after countless jokes and warnings, is still one of today's most frequently used passwords). And yes, it can be a pain to have to reset your password each time you forget it. But, for the security of your company's network and data, it's well worth the extra time and inconvenience to create very secure passwords.

Generally, the longer the password, the more secure. Ideally, it should include at least one special character, one number and both uppercase and lowercase letters. But once you land on that perfect password, don't use it for multiple applications. Create new passwords for each new application used. Also, two-factor authentication should be in place every time a password is required. Two-factor authentication is an extra layer of protection that ensures only the person who is supposed to access the account can access it. Simply knowing the password would not be sufficient.

Also, it should go without saying that your password should be kept to yourself and not shared with anyone else, including coworkers, partners, friends and family. In addition, if you must terminate an employee, or upon them resigning, make sure their passwords are no longer active.

Many of your employees probably utilize auto-fill passwords. After all, in less than a second, your password is automatically filled in and you're zipping through the Internet without having to remember your password or request a password reset. There are also password-manager applications that make it a cinch to log in. The problem is, hackers know these are a gold mine to all of your private data.

Rather than keeping your passwords on a spreadsheet or a notepad that could easily be compromised, it's better to utilize a password manager. Therefore, you only need to remember one master password and the password manager houses all of your passwords. While a password manager could potentially be hacked, it's far safer than keeping a password file on your computer.

To protect your browsers from password theft, we recommend turning off this auto-fill option. Please note that depending on the browser you are using (Chrome, Firefox or Safari), the directions to turn off password auto-fill will vary.

Keep A Clean Work Space

"How you do anything is how you do everything." – T. Harv Eker, author, businessman and motivational speaker. If your employees have a messy workspace, odds are their computer desktop are also disheveled and unorganized. I bet their cars and homes are equally as cluttered. On the flipside, when you can see the entire desktop, you can bet that person also has a clean computer desktop with files neatly organized.

Both your employees' computer desktops and actual desks should be kept clean, with no material on them that isn't relevant to work function. Also, leaving passwords or other personal material on, in or around one's desk is also a recipe for potential disaster.

Know How To Identify Malicious E-mails

Your entire team must be vigilant to spot, question and delete potential threats delivered via e-mail. When your employees begin from the stance that EVERY e-mail contains possible malware, you have many more defenders who will help protect your computers and network.

It only takes a second to evaluate an incoming e-mail and determine if it's a potential threat. Look for clues that could send up red flags, including:

- Unfamiliar domain names as part of the sender's e-mail address
- Short, vague and irrelevant messages with links attached
- Unexpected links with no explanation
- Innocuous attachments to vague and/or unfamiliar e-mails
- Incorrect spelling or bad grammar
- Asking for personal information
- A threatening or panic-causing message

One recent type of e-mail attack is called a man-in-the-middle attack, where the hacker secretly intercepts communications between two parties. These types of attacks can be identified because when you click on a link in the e-mail, nothing happens. But something IS happening: the hacker may gain remote access to your computer. If you ever click a link and think nothing happened, play it safe and report it to your IT consultant.

Give each employee a tip sheet to keep on their desk regarding these types of suspicious e-mails. In addition, encourage your employees to call the sender if they are ever in doubt. Simply e-mailing the sender to inquire if it's legitimate may not be enough if their e-mail has been compromised. As these phishing e-mails and attempts to break into companies' systems continue to evolve, regular briefings of all employees should be an important part of your business structure.

Keep Communication Open

You've heard the saying "See something, say something." Well, that applies to cyber security as well. If an e-mail, web page or attachment looks or seems suspicious, assume it is. Of course, you should avoid clicking the link or opening the attachment. Beyond that, you should also alert your IT consultant. If your consultant does recognize it as a potential cyberattack, make sure everyone on the team knows what the attempted attack looks like so they can identify possible future attacks.

The fact is, most cybercriminals are trying to infiltrate an entire business, not simply stopping at one person. So, if anyone in your organization spots a potential attack, odds are their colleagues could be hit next. If they are working through your whole team, a heads-up will likely prevent any slips in security.

If anyone on your team is unable to recognize and avert a cyberattack, encourage them not to hide it because of embarrassment. Instead, own it. Let everyone know what the attack looks like, how to either delete it or avoid it and the ways in which it affected your business. Once your employees clearly understand that this is far more dangerous than just nuisance spam, you'll have everyone looking out for it.

Destroy Old Data

People have a tendency to simply "throw away" computers and hardware when they get new technologies. This is a mistake. Obsolete computers should not only be wiped clean before being trashed or donated, their hard drives should be completely destroyed. This proactive measure should also be done to printers or any devices that store data for any length of time.

Just think of everything that's on your computer: passwords, customer files, private and financial data. You may think it's trash, but a cybercriminal sees it as treasure. And rather than having to hack your network, he simply plucks your old computer from the trash or recycle center. Don't make it easy for them!

Protect Your WiFi Network

It seems just a few years ago, free WiFi access was a rarity. Today, most customers and clients expect free access to a guest WiFi network. While you want to better serve those in your office or place of business, you certainly don't want to offer cybercriminals one more access point into your network.

So, to keep customers happy and criminals away, here are a few rules to follow when setting up your WiFi:

- **Don't give guests access to your primary WiFi.** It doesn't take a veteran hacker to break into your company network using your WiFi as an access point. Almost anyone with a slight technical background could do it. And once they're in, all of your confidential data, customer information, credit cards and passwords can be stolen. Make it a point to provide a full security stack solution on all tablets and devices and even your phones. Nobody should be allowed to access the company WiFi unless it is fully protected.
- **Create a separate guest WiFi.** If the router in your office supports a built-in guest WiFi feature, you can create a separate "virtual" network. In other words, your guests and clients can jump online without accessing your company's primary network.
- **Restrict bandwidth and distance.** While you may want to offer Internet access to your customers, you shouldn't do so at the expense of your own business productivity. Therefore, since your guest WiFi still utilizes your ISP connection, you should limit total bandwidth usage on your guest network. Visitors usually engage in higher-bandwidth activities, such as streaming TV shows, watching videos and playing music. In addition to restricting bandwidth, you should ensure your router doesn't allow people outside of your office or building to access the guest WiFi, again eating up valuable bandwidth and also putting your business at more risk for cybercrime.

Encrypt E-mails

By now, you realize that e-mails are one of the most frequently used entry points for delivering malware. Aside from that significant threat, even amateur hackers can easily intercept and steal just about any information you send via e-mail. Thankfully, the large majority of the e-mails people tend to send do not contain financial information or private content you don't want to get into the wrong hands.

\However, on occasion, you or your employee may need to send information that would expose your business if a hacker stole it. Rather than waiting to send via certified mail or another slow method, you can now easily encrypt your e-mail to add another layer of protection. While the most sophisticated cybercriminals may still be able to decrypt it and access your private communications, encrypting is one of today's most secure ways to protect your e-mails.

So, how does e-mail encryption work? You have both a public key and a private key, which is known as public key infrastructure. While your public key is handed out to anyone you choose, such as your entire office, your family and your friends, or even made public, your private key is known only by you.

When someone on your team wants to send you a message that is meant only for you to see, they would encrypt it using your public key. However, your private key is required to decrypt the message. If, at that point, someone intercepted your e-mail, it would look like useless gibberish. Aside from encrypting your message, you can also use your private key to digitally sign the message, so the recipient is confident it came from you.

The best advice is to never send account information, passwords or credit card information via e-mail. However, if there is no other viable method of transferring that private information, make sure you are using encryption software.

Be Aware Of Sneaky Ways Hackers Invade Your Network

While your entire team should be aware of the most common ways cybercriminals can attack your network, they should also know about the lesser-used sneaky ways they can invade. After all, if they're only focused on the most basic ways your system can be compromised, you are not mitigating all of the risks.

Not too long ago, Microsoft released a security bulletin about three newly discovered vulnerabilities that could allow an attacker to gain control of your computer. How? Simply by tricking you into downloading and opening a maliciously crafted picture. Along with the warning, Microsoft released a Windows update to correct these vulnerabilities. Problem was, if you didn't have a process to ensure you were applying critical updates as soon as they became available, you were still completely vulnerable to this attack.

Want another compelling reason to ensure your network stays up-to-date on the latest security patches? Most hackers don't discover these security loopholes on their own. Rather, they learn about them when Microsoft or any other software vendor announces the vulnerability and issues an update. That is the hackers' cue to spring into action. They immediately analyze the update and craft a way to exploit it using malware or a virus. In no time, they have a way to infiltrate any computer or network that has not yet installed the security patch. And the time between the release of the update and the release of the exploit that targets the vulnerability is getting shorter every day.

When the "Nimda" worm was first discovered in 2001, for instance, Microsoft had released the patch that protected against that vulnerability 331 days before. Network administrators had plenty of time to apply the update, yet because so many failed to do so, the Nimda ("admin" spelled backwards) worm caused lots of damage.

Clearly, your IT consultant needs to be paying close attention to your systems to ensure that critical updates are applied as soon as they are announced. That's why we highly recommend that small-business owners without a full-time IT staff allow their consultant to monitor and maintain their network.

Have An Excellent Backup

Ransomware is one of today's most popular and aggressive cybercrime attacks, where a hacker locks up your files and holds them for ransom until you pay a fee to access them. The second you get that notice on your computer screen that you can no longer access your files is the very second you regret not having a backup system in place. Because if your files are backed up, you don't have to pay a crook to get them back.

A good backup will also protect you against an employee accidentally (or intentionally) deleting or overwriting files. Natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters can all be made less horrific if you have a quality backup system in place. While your hardware may be a total loss in some disasters, your important data and private customer information will still be whole and accessible.

Your backups should be automated and monitored. Ensure your IT consultant has a policy in place to test every month. In addition, they should get notifications of data usage so they can monitor fluctuations and oddities. The worst time to test your backup system is when you desperately need it to work!

Check Before You Connect

We live in a world today where speed is essential and portability is expected. It seems everyone has multiple flash drives or thumb drives to plug into a computer's USB port to quickly save and exchange data, images, videos, etc. The problem is, because they are so prevalent, we don't always remember who we got these portable drives from and what information is contained on the drive. There are countless examples of using an innocent USB drive or CD to upload malware

onto a computer or network. Unless you know exactly what's on the device and you trust the person who gave you the device, don't let it onto your system!

Now you have multiple ways to defend your network and protect your data, financial information and ultimately your business. Again, being proactive is key. I also strongly advise implementing as many of these security measures as you can. Simply having a strong firewall and capable backup system may not be enough.

One security measure many business owners are flocking to is the cloud. Along with ease, convenience and cost savings, the cloud offers your business an added layer of security. This next chapter takes us into the cloud.

Chapter 7:
Better Security In The Cloud

While cloud computing has technically been around since the 1960s, the "cloud" as we know it first appeared in 2011 with IBM's SmartCloud and Apple's ICloud. Yet, so many people today are still confused about exactly what the cloud is and how it can enhance their business. In this chapter, we will answer all of your questions about the cloud and how it may even bolster your network security.

What Exactly Is Cloud Computing?

Wikipedia defines cloud computing as "the use and access of multiple server-based computational resources via a digital network (WAN, Internet connection using the World Wide Web, etc.)."

But as a business owner or manager, you simply want to know how the cloud can enhance your productivity and even improve your cyber security. So, to help you better understand how cloud computing can positively impact your business and computer network, let's compare it to the evolution of public utilities and electricity.

Back in the industrial age, in order for factories to produce their sellable goods they had to also produce their own electricity. Whether in the manufacture of textiles or railroad spikes, using machines gave these companies enormous competitive advantages by producing more goods with fewer workers and in less time. For years, the businesses that flourished were those that were capable of producing their own power. As a result, the production of power was every bit as important as the skill of their workers and quality of their products.

Therefore, factories had to master two crafts: producing their goods and producing power. Fortunately, Thomas Edison found a solution to this widespread problem. He developed a commercial-grade replacement for gas lighting and heating that was centrally sourced. Suddenly, electricity could be distributed to the many factories that needed it.

The concept of electric current being generated in central power plants and then delivered to factories caught on fast. At that point, electricity became a utility. No longer did manufacturers have to be in the business of producing their own power with expensive waterwheels. In no time, factories that took advantage of this new lower-cost option offered by public utilities were at a competitive advantage. Almost overnight, thousands of steam engines and electric generators were rendered obsolete in those factories.

While Edison's invention and ingenuity made this possible, what really drove the demand was pure economics. Utility companies were able to leverage economies of scale that single manufacturing plants simply couldn't match in output or in price. Beyond flowing into every factory, the price of power dropped so significantly that it was suddenly being used in just about every household in America.

Today, technological advancements are providing us similar advantages. The only difference is that instead of cheap and plentiful electricity, advancements in technology and Internet connectivity are driving down the costs of computing power. Just like paying for a utility, with cloud computing, businesses can pay for "computing power" without having to absorb the exorbitant costs of installing, hosting and supporting the technology on-premise.

Did you know, you are probably already experiencing the benefits of cloud computing in some capacity? Below are a number of cloud computing applications or "software as a service" (SaaS) you might be using right now:

- Gmail, Hotmail or other free e-mail accounts
- Facebook, Twitter, LinkedIn, Instagram and other social media

- NetSuite, Salesforce and other customer relationship management software
- Constant Contact, Infusionsoft, AWeber or other e-mail broadcasting services
- Zoomerang, SurveyMonkey and other online survey tools
- All things Google (search, AdWords, maps, etc.)

Fact is, almost every application you use today can be (or already is) put "in the cloud," where you can access it and pay for it via your browser for a monthly fee just like utility pricing. You don't purchase and install software but instead access it via an Internet browser.

Office 365 and Google Apps are perfect examples of how people today want and need cloud computing. For a reasonable monthly or annual fee, you get full access and use of Office applications that used to cost a few hundred dollars to purchase. And, since these apps are being powered by the cloud provider, you don't need an expensive computer with lots of power to use them – just a simple Internet connection is all you need on a laptop, desktop or tablet.

Pros And Cons Of Moving To The Cloud

Please keep in mind there is no "perfect" solution. All of your options have upsides and downsides that need to be evaluated on a case-by-case basis. Many "cloud experts" out there will convince you that cloud computing is the only way to go. Sure, it's their expertise, but it's also how they get paid. Expecting otherwise would be like going to a Toyota dealership and waiting for the salesperson to give you an honest opinion about Nissans and Hondas. Their goal is to sell you a Toyota.

It's possible that the best option for you is a hybrid solution where some of your applications and functionality are in the cloud and some are still hosted and maintained from an in-house server. Here are the general pros and cons of cloud computing:

Pros Of Cloud Computing:

- **Lowered IT costs.** This is probably the single most compelling reason why companies choose to move their network to the cloud. Not only do you save money on software licenses, but you also save on hardware (servers and workstations) as well as on IT support and upgrades.

  Rather than constantly writing cash-flow-draining checks for IT upgrades because the technology is constantly improving, you may save quite a bit by considering cloud computing.

- **Freedom and convenience.** One of the major reasons people prefer cloud computing is the ability to access your desktop and/or applications from anywhere and any device. If you travel a lot, have remote workers or prefer to use an iPad while traveling and a laptop at your house, cloud computing will give you the ability to work from any of these devices at any location

  Gone are the days when employees are confined to a desktop. Considering there are over 3.5 billion smartphones in use today, cloud computing ensures everyone is kept in the loop. Through the cloud, you can offer conveniently accessible information to sales staff who travel, freelance employees or remote employees.

- **Flexibility.** The cloud offers businesses like yours more flexibility versus hosting on a local server. Need extra bandwidth? Cloud computing can meet that demand instantly without the massive time and expense of upgrading your IT infrastructure. With a cloud-focused approach to your business, you have far more freedom and flexibility to positively impact your overall efficiency.

- **Use it without "owning" it.** You don't own the responsibility of having to install, update and maintain your IT infrastructure. It's like living in a condo where someone else takes care of the building and landscape maintenance. They handle all plumbing issues and keep up the lawn, but you still have access to all facilities. This "use it without owning it" approach is particularly attractive for companies that are new or expanding, and don't want the heavy outlay of cash for purchasing and supporting an expensive computer network.

- **"Greener" technology.** Yes, switching to cloud-based applications can actually save on power and your electric bill. Of course, smaller businesses may not see much if any savings. However, for larger companies that need to constantly cool a server closet with multiple servers that must run 24/7/365, the savings can be considerable.
- **More robust security.** There's a common fear that security can be an issue when you adopt a cloud-computing solution. That's because people think it's more difficult to protect something that's not physically in their office. When important data is kept securely onsite, you believe that data is better protected. If you're not exactly sure where your files are in the cloud, how can you be sure cybercriminals aren't accessing them remotely? That's the concern, at least.

  Security in a cloud-computing environment is very robust. First, a cloud host's primary job is to carefully monitor security. In a conventional in-house environment, your IT team must divide their time between many IT concerns, including security. Second, one of the biggest sources of cyberattacks includes internal data theft perpetrated by employees. With the threat of internal data theft, it can actually be much safer to keep sensitive information off-site.

  According to RapidScale, 94% of businesses noticed an improvement in IT security after they switched to the cloud. That's because the data is being encrypted and is transmitted over networks and stored in databases. This advanced encryption makes it even more difficult for hackers to access and steal your data. Also, the data centers must follow strict compliance and regulations while being tested each year. In most cases, there's a security camera, keypads and fingerprint scanners just to enter the lobby area of these data centers. Beyond the lobby, devices are protected in cabinets behind locked cages.
- **Disaster recovery is instantaneous.** The server in your office is extremely vulnerable to multiple threats. Viruses, human error, hardware failure, software corruption, and even physical damage due to a fire, flooding or other natural disaster are all very possible. If your server was in the cloud and

your office was flooded, you could simply purchase a new laptop and be back up and running that same day. Of course, if you had a traditional network with tape drives, CDs, USB drives or other physical storage devices to back up your system, it could take weeks to get back up and running. Even then, you may have lost all of your data, including financial information, customers' accounts and private information, as well as all of your employees' work!

- **Loss prevention.** If you are not investing in a cloud-computing solution, all of your valuable data is tied directly to the office computers it resides in. For now, that may not be an issue. However, computers and servers will crash at some point. And when that happens, you just might end up permanently losing all of your critical data. This is far more common than you might imagine, since computers can malfunction for many reasons, from viral infections to hardware deterioration to simple user error. Did you know that 10,000 laptops are reported lost or stolen every week at major airports? If you aren't in the cloud, you risk losing all of the important data and projects that have built your business to what it is today.

  Plus, like a public utility, cloud platforms are far more robust and secure than your average business network because they can utilize economies of scale to invest heavily into security, redundancy and failover systems, making them far less likely to go down.

  Automatic software updates. Cloud-based applications automatically refresh and update themselves, instead of forcing an IT department to perform a manual organization-wide update. Not only can you save critical time with automated software updates, you can save money by not spending more on internal or external IT resources.

Cons Of Cloud Computing:

- **The Internet going down.** While you can mitigate this risk by using a commercial-grade Internet connection and maintaining a second backup connection, there is still a chance you'll lose Internet connectivity, making it impossible to work.

- **Data security.** You've just learned that data in the cloud can be safer than simply storing it on computers and/or a server that resides in your office; however, many people still feel uncomfortable about having their data stored "invisibly" in an off-site location. So, before you choose any cloud provider, you need to find out more information about where they are storing your data, how it is encrypted, who has access and how you can get it back.
- **Compliance issues.** There are a number of laws and regulations, such as Gramm-Leach-Bliley, Sarbanes-Oxley and HIPAA, that require companies to control and protect their data. They also require businesses to certify that they have knowledge and control over who can access the data, who sees it and how and where it is stored. In a public cloud environment, this can be an issue since many cloud providers won't tell you specifically where your data is stored.

  Most cloud providers have SAS 70 certifications, which require them to be able to describe exactly what is happening in their environment, how and where the data comes in, what the provider does with it and what controls are in place over the access to and processing of the data. However, as the business owner, it's your neck on the line if the data is compromised, so it's important that you ask for some type of validation that they are meeting the various compliance regulations on an ongoing basis.

Migration Gotchas! What You Need To Know About Transitioning To A Cloud-Based Network

When done right, a migration to Office 365 or another cloud solution should be like any other migration. There's planning that needs to be done, prerequisites that have to be determined and the inevitable "quirks" that need to be ironed out once you make the move.

Every company has its own unique environment, so it's practically impossible to try and plan for every potential pitfall; however, here are some BIG things you want to ask your IT consultant about before making the leap.

- **Downtime.** Some organizations cannot afford any downtime, while others can do without their network for a day or two. Make sure you communicate your specific needs regarding downtime, and make sure your IT provider has a solid plan to prevent extended downtime.
- **Painfully slow performance.** Ask your IT consultant if there's any way you can run your network in a test environment before making the full migration. Imagine how frustrated you would be if you migrate your network and discover everything is running so slow you can barely work! Again, every environment is slightly different, so it's best to test before you transition.
- **Third-party applications.** If your organization has plug-ins to Exchange for faxing, voice mail or integration into another application, make sure you test to see if it will still work in the new environment.

Different Types Of Cloud Solutions

- **Pure Cloud.** In this solution, all of your applications and data are put on the other side of the firewall (in the cloud) and accessed through various devices (laptops, desktops, iPads, phones) via the Internet. This is the most common type of cloud solution.
- **Hybrid Cloud.** Although "pure" cloud computing has valid applications, for many it's downright scary. And in some cases, it is NOT the smartest move, due to compliance issues, security restrictions, speed and performance.

  A hybrid cloud solution enables you to put certain pieces of existing IT infrastructure (storage and e-mail) in the cloud, and the remainder of the IT infrastructure stays on-premise. This gives you the ability to enjoy the cost savings and benefits of cloud computing where it makes the most sense without risking your entire environment.
- **Single Point Solutions.** Another option would be to simply put certain applications, like SharePoint or Microsoft Exchange, in the cloud while keeping everything else on-site. Since e-mail is usually a critical application that everyone needs and wants access to on the road and on various devices

(iPad, smartphone, etc.), often this is a great way to get advanced features of Microsoft Exchange without the cost of installing and supporting your own in-house Exchange server.

- **Public Cloud Vs. Private Cloud.** A public cloud is a service that anyone can tap into with a network connection and a credit card. They are shared infrastructures that allow you to pay as you go and are managed through a self-service web portal. Private clouds are essentially self-built infrastructures that mimic public cloud services, but are on-premise. Private clouds are often the choice of companies that want the benefits of cloud computing but don't want their data held in a public environment.

Cloud Computing FAQs

Question: Could I keep a local copy of my data in case we lose access to the cloud?

Answer: We resolve this by keeping a synchronized copy of your data on your on-site server as well as in the cloud. Here's how this works: Microsoft offers a feature with Windows called "DFS," which stands for Distributed File Systems. This technology synchronizes documents between cloud servers and local servers in your office. So, instead of getting rid of your old server, we keep it on-site and maintain an up-to-date synched copy of your files, folders and documents on it.

If the Internet goes down or slows to a grind, you simply open a generic folder on your PC and the system will automatically know to pull the documents from the fastest location. Once a file is modified, it syncs it in seconds so you don't have to worry about having multiple versions of the same document. Using this process, you get the benefits of cloud with a backup solution to keep you up and running during slow periods or complete Internet outages.

Question: What about security? Isn't there a big risk of someone accessing my data if it's in the cloud?

Answer: In many cases, cloud computing is a MORE secure way of accessing and storing data. Just because your server is on-site doesn't make it more secure; in fact, most small to medium businesses can't justify the cost of securing their network the way a cloud provider can. And most security breaches occur due to human error – one of your employees downloads a file that contains a virus, they don't use secure passwords or they simply e-mail confidential information out to people who shouldn't see it.

Question: What if you go out of business? How do I get my data back?

Answer: We present network documentation that clearly outlines where your data is and how you could get it back in the event of an emergency. This includes emergency contact numbers, detailed information on how to access your data and infrastructure without needing our assistance, a copy of our insurance policy and information regarding your backups and licensing.

We also give you a copy of our disaster recovery plan, which shows what we've put in place to make sure we stay up and running.

Question: Do I have to purchase new hardware (servers, workstations) to move to the cloud?

Answer: No! That's one of the selling points of cloud computing. It allows you to use older workstations, laptops and servers, because the computing power is in the cloud. Not only does that allow you to keep and use hardware longer, but it allows you to save on workstations and laptops because you don't need the expensive computing power required in the past.

What To Look For When Hiring An IT Consultant To Move Your Network To The Cloud.

Unfortunately, the IT consulting industry has its share of incompetent or unethical people who will try to take advantage of trusting business owners who

simply do not have the ability to determine whether or not they know what they are doing. Sometimes this is out of greed for your money; more often it's simply because they don't have the skills and competency to do the job right but won't tell you that up front because they want to make the sale.

Automotive repair shops, electricians, plumbers, lawyers, realtors, dentists, doctors, accountants, etc., are heavily regulated to protect the consumer from receiving substandard work or getting ripped off. However, the computer industry is still highly unregulated, and there are few laws in existence to protect the consumer – which is why it's so important for you to really research the company or person you are considering, to make sure they have the experience to set up, migrate and support your network in the cloud.

Critical Questions To Ask Your IT Company Or Computer Consultant Before Letting Them Move Your Network To The Cloud:

Question: How many clients have you provided cloud services for to date, and can you provide references?

Answer: Just as you would never hire a plumber who is brand-new to plumbing, the same goes for your network. You don't want someone practicing on your network who could make matters worse. At a minimum, make sure they have have at least 5 years of experience, and successfully completed over 100 cloud migrations across **diverse industries**, and they should be able to provide **verifiable references** in google reviews.

Question: How quickly do they guarantee to have a technician working on an outage or other problem?

Answer: Anyone you pay to support your network should give you a written SLA (service level agreement) that outlines exactly how IT issues get resolved and in what time frame. I would also request that they reveal what their average resolution time has been with current clients over the last three to six months.

They should also answer their phones live from 8:00 a.m. to 5:00 p.m. and provide you with an emergency after-hours number you may call if a problem arises, including on weekends.

If you cannot access your network because the Internet is down or due to some other problem, you can't be waiting around for hours for someone to call you back or start working on resolving the issue. Make sure you get this is writing; often cheaper or less experienced consultants won't have this or will try and convince you it's not important or that they can't do this. Don't buy that excuse! They are in the business of providing IT support, so they should have some guarantees or standards around this that they share with you.

Question: What's your plan for transitioning our network to the cloud to minimize problems and downtime?

Answer: We run a simultaneous cloud environment during the transition and don't "turn off" the old network until everyone is 100% confident that everything has been transitioned and is working effortlessly. You don't want someone to switch overnight without setting up a test environment first.

Question: Do you provide a no-risk trial of our network in the cloud to test the proof of concept BEFORE we commit to a long-term contract?

Answer: Yes. At CMIT Solutions of LA, Irvine, Mexico, and South Africa, we offer all qualified clients a **no-risk, 10-day cloud "test drive"** so you can experience firsthand what it would be like to run your business in the cloud — using **your own applications, data, and workflows.**

This is not a full migration, but rather a **proof-of-concept environment** that allows your team to evaluate performance, accessibility, and user experience before making a long-term commitment. It's an ideal way to identify any potential adjustments, special configurations, or limitations — without disrupting your current infrastructure.

There is no charge for this and no obligation to move forward. At the end of the 10 days, you'll have a clear picture of whether a full cloud migration is the right path for your organization, or whether a hybrid or on-premise model better fits your needs.

Our goal is to provide clarity, not pressure — and to make sure your cloud strategy aligns with your business goals, not just technology trends.

Question: Do they take the time to explain what they are doing and answer your questions in terms that you can understand (not geek-speak) or do they come across as arrogant and make you feel stupid for asking simple questions?

Answer: At CMIT Solutions of LA, Irvine, Mexico, and South Africa, we believe **clear communication is just as important as technical expertise.** Our technicians are trained to have the **"heart of a teacher"** — they are patient, empathetic, and committed to helping clients understand what we're doing and why, using simple, non-technical language.

We invest in regular customer service and communication training, ensuring that our team can break down complex IT topics in a way that's relevant to your business — not filled with jargon or acronyms.

We measure success not just by the number of issues resolved, but by **how our clients feel** about the experience. In fact, our clients consistently rate our service at **9.7 out of 10** for communication and professionalism.

Whether you're the CEO, an office manager, or a team member unfamiliar with IT, we will always treat your questions with **respect and clarity**. No arrogance. No tech snobbery. Just real answers that make sense to you.

Question: Where will your data be stored?

Answer: You should receive full documentation about where your data is, how it's being secured and backed up and how you could get access to it if necessary WITHOUT going through your provider. Essentially, you don't want your cloud provider to be able to hold your data (and your company) hostage.

Question: How will your data be secured and backed up?

Answer: If they tell you that your data will be stored in the back of their office, what happens if THEY get destroyed by a fire, flood or other disaster? What are they doing to secure the office and access? Are they backing it up somewhere else? Make sure they are SAS 70 certified and have a failover plan in place to ensure continuous service in the event that their location goes down. If they are building on another platform, you still want to find out where your data is and how it's being backed up.

Question: What is THEIR disaster recovery plan? What happens if they go out of business?

Answer: At CMIT Solutions of LA, Irvine, Mexico, and South Africa, we believe that **trust and transparency** are essential to any technology partnership — especially when it comes to business continuity.

First, we maintain our **own internal disaster recovery plan** to ensure that our systems, client records, and service infrastructure remain fully operational in the event of a crisis. This includes **redundant cloud backups, offsite data storage**, and a tested business continuity protocol that allows our team to support you even during natural disasters, cyber incidents, or unexpected disruptions.

Second, to protect our clients in the unlikely event that CMIT Solutions of LA, Irvine, Mexico, and South Africa were to go out of business or be acquired, all of our service environments are built on **independent, widely supported platforms** like **Microsoft Azure, Datto, Egnyte**, and others — not proprietary

systems that only we can manage. This means your data remains **fully portable and accessible**, with detailed documentation and administrative access shared transparently.

Lastly, CMIT Solutions of LA, Irvine, Mexico, and South Africa is part of a **national network of independently owned franchises** with over 280 offices across North America. In the rare case that one office closes or transitions ownership, others can step in to **seamlessly continue service**, backed by the same national standards and tools.

Your business continuity is our top priority — even beyond our own.

Do they have adequate errors-and-omissions insurance as well as workers' compensation insurance to protect YOU?

Answer: Absolutely. At CMIT Solutions of LA, Irvine, Mexico and South Africa, we understand that protecting your business means also protecting you from liability and unforeseen incidents.

We carry a comprehensive Technology Services Errors & Omissions (E&O) Professional Liability Insurance policy issued by State Farm under the name IT Solutions of North LA, LLC.

- **Policy Number:** PS0000006806204
- **Coverage Amount:** $1,000,000 (one million dollars)

In addition, we maintain a full **business liability and office insurance policy** covering:

- **Medical expenses and general business liability** up to $2 million
- **Aggregate product/completed operations and general aggregate coverage** up to $4 million

This means that if an unforeseen incident occurs — whether a technician accidentally causes downtime, data loss, or even suffers an injury while on your premises — you are fully protected. We also comply with all state and federal

workers' compensation requirements, further shielding you from potential legal exposure.

In today's litigious world, this type of protection isn't optional — and we encourage all clients to request and review the insurance policies of any IT provider they're considering.

At CMIT Solutions of LA, Irvine, Mexico, and South Africa, we don't just protect your systems — we protect **your peace of mind**.

Question: Is it standard procedure for them to provide you with written network documentation detailing what software licenses you own, your critical passwords, user information, hardware inventory, etc., or are they the only person with the "keys to the kingdom"?

Answer: All clients receive this in written and electronic form at no additional cost. We also perform a quarterly update on this material and make sure certain key people from your organization have this information and know how to use it, giving you complete control over your network.

Side Note: You should NEVER allow an IT person to have that much control over you and your company. If you get the sneaking suspicion that your current IT person is keeping this under their control as a means of job security, get rid of them (and we can help to make sure you don't suffer ANY ill effects). This is downright unethical and dangerous to your organization, so don't tolerate it.

Question: Do they have other technicians on staff who are familiar with your network in case your regular technician goes on vacation or gets sick?

Answer: Yes, and since we keep detailed network documentation (basically a blueprint of your computer network) and updates on every client's account, any of our technicians can pick up where another left off.

Question: Do they INSIST on doing periodical test restores of your backups to make sure the data is not corrupt and could be restored in the event of a disaster?

Answer: We perform a monthly "fire drill" and perform a test restore from backup for our clients to make sure their data CAN be recovered in the event of an emergency. Upon completion, we then give our clients a report showing that this test restore was conducted and all systems are running as they should.

If there's a problem, we notify our clients immediately and start working to resolve it the same day. After all, the WORST time to "test" a backup is when you desperately need it.

Question: Is their help desk US-based or outsourced to an overseas company or third party?

Answer: At CMIT Solutions of LA, Irvine, Mexico, and South Africa, we proudly provide a **U.S.-based, in-house help desk** staffed by experienced, full-time technicians who are dedicated to resolving your issues quickly, professionally, and securely.

We consider this one of the most important aspects of delivering excellent customer service. Our help desk team is trained not just in technical problem-solving, but also in communication, empathy, and professionalism — so you'll always speak with someone who is both **friendly and knowledgeable**.

Equally important, by keeping our help desk operations within the United States and under our own direct management, we help ensure that your **data remains protected under strict U.S. privacy and compliance standards**. We do not outsource support to third-party providers overseas, as that introduces potential risks to data security and accountability.

Whether your issue is urgent or routine, our support team is just a call or ticket away — and we treat every interaction as an opportunity to reinforce your trust in our service.

Question: Do their technicians maintain current vendor certifications and participate in ongoing training – or are they learning on your dime?

Answer: At CMIT Solutions of LA, Irvine, Mexico, and South Africa, we take training and certification **very seriously** — because your business should never be the testing ground for inexperienced technicians.

All of our techs are required to maintain **up-to-date certifications** with the platforms and tools we support. We currently work with more than **25 industry-leading vendors**, including:

Microsoft, ConnectWise, Nodeware, Huntress, RocketCyber, Barracuda XDR, Datto, Timus, Augmentt, Egnyte, Conceal, CyberQP, IT Glue, Liongard, ScalePad, Kaseya, Autotask, BullPhish, Backup Radar, and others.

This ensures that our team is always current on the **latest features, security protocols, and best practices** across every platform we use — which translates to better protection, faster resolutions, and greater reliability for you.

In fact, our **hiring process is so selective that 99% of applicants don't make it through**. (Fun fact: many of them end up working for less demanding competitors.) Only the most qualified, service-driven professionals make it onto our team — because we believe our clients deserve nothing less.

With CMIT Solutions of LA, Irvine, Mexico, and South Africa, you can rest assured that your IT systems are supported by people who are already certified, trained, and battle-tested — **not learning at your expense.**

Question: Are they familiar with (and can they support) your unique line-of-business applications?

Answer: We own the problems with all line-of-business applications for our clients. That doesn't mean we can fix faulty software – but we WILL be the liaison between you and your vendor to resolve problems you are having and make sure these applications work smoothly for you instead of pointing fingers and putting you in the middle.

Question: When something goes wrong with your Internet service, phone systems, printers or other IT services, do they own the problem or excuse it away by saying, "That's not our problem to fix"?

Answer: We feel WE should own the problem for our clients so they don't have to try and resolve any of these issues on their own – that's just plain old good service and something many other computer guys won't do.

Chapter 8:
Preventing Identity Theft

What Exactly Is Identity Theft?

Most everybody has had at least one fraudulent charge appear on their credit card statement. While it wasn't your purchase, you still had to jump through several hoops to get it removed from your account. That's considerable time, energy and frustration for something you didn't even do! Or when you go to file your taxes and realize someone else has already received YOUR refund by using your information. We all know how difficult it is to deal with the simplest of IRS issues, much less proving you didn't file already.

Now imagine having your entire identity stolen. Now you're not just facing one fraudulent charge, but EVERYTHING. Your social security number, business ID number, access to your personal and business bank accounts, retirement accounts – all swiped out from under you. Your personal and business credit cards can be maxed out too. And if they have your debit card information, your checking account could fall to ZERO in no time. What's even worse, you could lose your client database, financial records and all of the work files your company has ever produced or compiled. That's identity theft.

Think back to all of the time you invested to get one or two fraudulent charges taken care of. Now imagine what would happen if you had to invest an enormous amount of time, money and energy to try to restore your credit and good reputation. Think about how much your business would suffer if one day your payroll money or the money you use to pay vendors was stolen.

Even worse, what if a cybercriminal stole your identity for the purpose of pulling off other criminal acts? Yes, that happens. Could your business survive a front-page news story about how you or your company ripped off hundreds of people? Think you're "innocent until proven guilty"? Not when it comes to the eyes of the media, your customers and your competitors!

But That Could Never Happen To Me!

No business owner thinks it could happen to them. Those are just stories you hear about from other businesses that have much looser IT security measures. Maybe you believe that your business isn't a target because it's too small or not the right industry. I'm here to tell you, sticking your head in the sand and convincing yourself you aren't a target is one of the very reasons there's a giant red target on your back.

While it may be difficult to determine the actual financial impact identity theft would have on your business, you can't deny the fact that it would have a negative effect. Cash most definitely is king. And if yours is stolen and used by a cybercriminal, the emotional toll such an event would take on you personally would certainly impact your business, even if you haven't put a pencil to figuring out the exact cost.

Here are some sobering statistics:

- In 2023, the Federal Trade Commission (FTC) received over 1 million reports of identity theft, accounting for approximately 17% of all consumer complaints. (Source: Federal Trade Commission)
- Americans lost an estimated $47 billion to identity fraud and scams in 2024, an increase of $4 billion from the previous year. (Source: Reuters)
- Victims spent an average of 10 hours resolving identity fraud issues in 2023, up from six hours in 2022. (Source: AARP)

Aside from the money and financial information and customer data potentially stolen, it's your time that you're truly being robbed of. Think about

all of your time involved in clearing your name. Discovering and reporting the identity theft. Requesting reports from the credit bureaus. Putting a fraud alert in place. Reviewing your credit reports. Removing fraudulent activity from your credit history. Altogether, this massive time commitment could cost you anywhere from six to 18 months to clean up!

Can you afford to drop what you're doing and spend up to a year-and-a-half cleaning up this mess, getting your money back and defending your soiled name? Absolutely not. Nobody has that kind of time.

Why Small Businesses Are More Vulnerable To Identity Theft

With the constant changes to technology and the daily development of new threats, it takes a highly trained technician to secure even a basic 5- to 10-person computer network. However, in an attempt to save money, many businesses try to do their own in-house IT support and designate the person with the most technical expertise as the part-time IT manager. This never works out because this makeshift IT person has another full-time job to do and is usually not skilled enough to properly support an entire computer network anyway.

This inevitably results in a network that is ill-maintained and unstable. It also means that the backups, virus updates and security patches are not getting timely updates, giving a false sense of security.

It's only a matter of time before an online hacker finds his way into your network and steals your information. If you're lucky, it will only cost you a little downtime, but there's always a chance you could end up like the companies affected by these criminals …

$764,000 Stolen from Insurance Company

A man was indicted, pleaded guilty to federal charges and was sentenced to 27 months' imprisonment for obtaining private bank account information about an insurance company's policyholders and using that information to deposit $764,000 in counterfeit checks into a bank account he established.

Social Security Number Swiped from a Website

A defendant has been indicted on bank fraud charges for obtaining names, addresses and social security numbers from a website and using the data to apply for a series of car loans over the Internet.

$13,000 Drained from This Business Owner's Account

A woman was indicted and pleaded guilty to federal charges involving her obtaining a fraudulent driver's license in the name of the victim, using the license to withdraw more than $13,000 from the victim's bank account and obtaining five department store credit cards in the victim's name and charging approximately $4,000 on those cards.

So, once these thieves steal your identity, what can they do with it? Well, in 2018, a Georgia man booked a three-night stay at a luxury Disney World hotel for $1,042. Next, he was very generous and bought 11 tickets to a Disney park at the hotel gift shop for a total of $1,582 (Mickey ain't cheap). On day two, he bought 11 more Disney tickets for nearly $2,000. Suspicious of the charges, officers detained the man and discovered he was carrying an Illinois driver's license and four credit cards that he purchased on the dark web! He attempted to give his family and friends a grand vacation on someone else's dime!

How Online Identity Thieves Get Hold Of Your Information

Some identity theft does occur through more "old school" methods such as stealing your wallet, overhearing you give a credit card or social security number over the phone or even raiding your business filing cabinet or trash. However, common-sense tactics such as avoiding public conversations that involve your personal or business financial information or putting locks on your file cabinets can be used to combat those threats.

Internet threats to your identity, on the other hand, are much more sophisticated and involve greater "know-how" in order to prevent them.

There are four basic ways cybercriminals gain access to your personal information over the Internet. They are:

1. **Phishing –** Phishing is where online scammers send spam or pop-up messages to your computer and try to get you to provide personal or sensitive business information over the Internet. Online criminals will typically send messages that look like legitimate messages from your bank, credit card company or other financial institution. In the message, there is usually a website link where it asks you to update your contact information.

   Many of these websites look like exact replicas of your bank or credit card website. However, entering your information into one of these sneaky portals means you are handing over the keys to the kingdom to a complete "evildoer."

   The Internet thief can now use your personal information to gain access to other private accounts, raid your business and rack up thousands of dollars in faulty charges.

2. **Tech Support Scams –** Scam artists are using the phone to try to break into your computer. They call, claiming to be computer techs associated with well-known companies like Microsoft. They say they have detected a virus or malware on your computer to trick you into giving them remote access or paying for software you don't need. The catch: these scammers take advantage of your reasonable concerns about viruses and other threats. They know that computer users have heard time and again that it's important to install security software. But the purpose behind their elaborate scheme isn't to protect your computer – it's to take money. They also may install remote tools on your devices to capture your data, copy your keystrokes and ultimately steal credit cards or login information.

3. **E-mail Scams –** Offers, detailed sales pitches, links to informational websites. These seemingly harmless e-mails are actually the makings of an Internet crime. They'll ask for your credit card information to buy a fake product or to pay for shipping on a "free product."

   The most common e-mail scams used to steal your identity are (as found on www.onguardonline.gov):

The "Nigerian" E-mail Scam. Con artists claim to be officials, businesspeople or the surviving spouses or former government honchos in Nigeria or another country whose money is somehow tied up for a limited time. They offer to transfer lots of money into your bank account if you will pay a fee or "taxes" to help them access their money. If you respond to the initial offer, you may receive documents that look "official." Then they ask you to send money to cover transaction and transfer costs and attorneys' fees, as well as blank letterhead, your bank account numbers or other information. They may even encourage you to travel to the country in question, or a neighboring country, to complete the transaction. Some fraudsters have even produced trucks of dyed or stamped money to try to verify their claims.

The Catch: The e-mails are from crooks trying to steal your money or your identity. Inevitably in this scenario, emergencies come up requiring more of your money and delaying the "transfer" of funds to your account. In the end, there aren't any profits for you, and the scam artist vanishes with your money. The harm sometimes can be felt even beyond your pocketbook: according to State Department reports, people who have responded to "pay in advance" solicitations have been beaten, subjected to threats and extortion and, in some cases, murdered.

Phishing E-mail Scam. E-mail or pop-up messages that claim to be from a business or organization you may deal with – say, an internet service provider (ISP), bank, online payment service or even a government agency. The message may ask you to "update," "validate" or "confirm" your account information or face dire consequences. One very popular scam occurs when the boss asks an employee to go buy Apple iTunes cards as client gifts and inadvertently sends the credit card details to the scammer. You could lose hundreds or even thousands of dollars!

The Catch: Phishing is a scam where Internet fraudsters send spam or pop-up messages to reel in personal and financial information from unsuspecting victims. The messages direct you to a website that looks just like a legitimate organization's site, or to a phone number purporting to be real. But these are bogus and exist simply to trick you into divulging your

personal information so the operators can steal it, fake your identity and run up bills or commit crimes in your name.

4. **Spyware –** Spyware is software installed on your computer without your consent to monitor or control your computer use. Clues that spyware is on a computer may include a barrage of pop-ups, a browser that takes you to sketchy sites, unexpected toolbars or icons on your computer screen, keys that don't work, random error messages and sluggish performance when opening programs or saving files. In some cases, there may be no symptoms at all.

Four Ways To Protect Your Company From Identity Theft

While it's impossible to plan for every potential scenario, a little proactive planning and proper network precautions will help you avoid or greatly reduce the impact of the vast majority of cyber identity theft you could experience.

Step #1: Make Sure Your Backups Are Encrypted

It just amazes me how many businesses don't have the security of encrypted backups. Encryption takes every little keystroke that you type and every little piece of data in your computer and turns it into dozens – or hundreds – of other characters. For example, just one letter "A" could turn into 256 different letters, numbers and symbols when it is encrypted. It basically makes it a whole lot more difficult for a hacker to figure out what the data is. On the other hand, if you don't have encryption, you are opening yourself up to a big risk of your identity and other important data being swiped. That is why it is important to make sure your backup is properly secured.

Step #2: Make Sure Your Virus Protection Is Always On and Current

You would have to be living under a rock to not know how devastating a virus can be to your network. With virus attacks coming from spam, downloading data and music files, instant messages, websites and e-mails from friends and clients, you cannot afford to be without up-to-date virus protection.

Not only can a virus corrupt your files and bring down your network, it can also hurt your reputation. If you or one of your employees unknowingly spreads a virus to a customer, or if the virus hijacks your e-mail address book, you're going to make a lot of people very angry.

Step #3: Set Up a Firewall and Update It Regularly

Small-business owners often assume, *"Why would anyone target my company? I'm just a small business."* But in today's threat landscape, that thinking can be devastating.

Cybercriminals don't discriminate by size — they target opportunity.

I learned this early in my cybersecurity journey. During a test environment setup, we connected an unprotected device — no firewall, no endpoint security — to the Internet for monitoring. **Within 15 minutes**, the machine was bombarded by unauthorized attempts to access open ports, install malware, and inject code. By the end of the first hour, we recorded over **13 GB of malicious files**, including ransomware droppers, crypto miners, and remote-access trojans — none of which could be removed without a full system wipe.

This was not a high-value server or a high-profile business. It was just **a lonely device on the Internet — and that was enough**.

Most small businesses don't realize that attackers often use **automated bots** to scan the Internet 24/7, searching for open, unprotected ports. The moment they find one — even if it's on your receptionist's PC or a forgotten printer — they can:

- **Delete your files**
- **Install unremovable data bombs**
- **Turn your device into a "zombie" to send spam or launch attacks on others**
- **Trigger your ISP to block your Internet access due to outbound abuse**

And if those malicious files can't be deleted — which is common — your only option may be to **reformat your drive and start from scratch**. That means losing everything unless you were backing up — and most SMBs aren't doing that correctly either.

That's why setting up a firewall isn't optional — it's your digital front door. And just like the lock on your home, it needs to be **updated, managed, and monitored** regularly to be effective. That's where a Managed Firewall comes in — not just to block threats, but to adapt to them in real time.

Your data, reputation, and operations are worth protecting — and a firewall is your first line of defense.

Step #4: Update Your System with Critical Security Patches as They Become Available

If you do not have the most up-to-date security patches and virus definitions installed on your network, hackers can access your computer through a simple banner ad or through an e-mail attachment.

Not too long ago, Microsoft released a security bulletin about three newly discovered vulnerabilities that could allow an attacker to gain control of your computer by tricking users into downloading and opening a maliciously crafted picture. At the same time, Microsoft released a Windows update to correct the vulnerabilities; but if you didn't have a process to ensure you were applying critical updates as soon as they become available, you were completely vulnerable to this attack. It is an easy way for someone to gain access to your information and steal your identity.

Here's another compelling reason to ensure your network stays up-to-date with the latest security patches. Most hackers do not discover these security loopholes on their own. Instead, they learn about them when Microsoft (or another software vendor) announces the vulnerability and issues an update. That is their cue to spring into action and they immediately go to work to analyze the

update and craft an exploit (like a virus) that allows them access to any computer or network that has not yet installed the security patch.

In essence, the time between the release of the update and the release of the exploit that targets the underlying vulnerability is getting shorter every day.

By taking these proactive actions in your business, you are building a formidable defense against identity theft, one of today's most dangerous cyberattacks. Of course, if any of your employees work from home or on the road, there's a whole new world of potential security threats you may be up against. The next chapter will shine a light on the risks your business faces if employees are working from home, as well as what you can do now to mitigate those risks.

Chapter 9:
Staying Secure While Working From Home

Today more than ever before, business owners are taking advantage of this fast-growing trend among small and medium businesses that is drastically increasing productivity, cutting costs and driving more profit to the bottom line. Is it a new management style or marketing trend?

No – it's telecommuting, which is simply allowing your staff to work from home. When you see the bottom-line impact it has on profits and productivity and talk to business owners who rave about how much money it's saving them, you'll start to see how working from home is more than a necessity today – it's an opportunity.

Common Myths, Mistakes And Misconceptions About Allowing Your Employees To Work From Home

One of the most common fears many business owners have about allowing their team to work from home is the loss of control they have over their employees. Most think that unless someone is standing over them, employees will be unproductive and work far fewer hours.

But the proof says something entirely different. Upwork, an online freelancing platform, estimates 22% of the American workforce — more than 36 million people — will work remotely by 2025. Not only does it save business owners in overhead, studies show that employees get MORE done when working outside of an office environment.

An HR and workplace benefits consulting firm known as Mercer surveyed 800 employers. Ninety-four percent of those employers stated that work productivity was the same or even higher among their employees who work from home.

A survey conducted by Owl Labs suggests that employees are not only more productive, but actually are happier and work more hours when working from home. They reported that these remote workers had less stress, more focus and a better work-life balance. These remote workers also worked longer than 40 hours a week 43% more compared to employees who worked in the office.

Even small businesses report savings of $85,000 to $93,000 per year by lowering their turnover rates, reducing their operating costs (gas, utilities, office space and furniture) and increased productivity after implementing work-from-home programs. (Source: International Teleworking Advocacy Group)

Cyber Security Risks For Telecommuters

While there's clear evidence today of the many benefits of allowing your team to work from home, those benefits come at a heightened risk to your network and data. Remote work can present a unique challenge because work-from-home environments usually don't have the same level of cyber security found within your office.

Here are six of the top cyber security risks you should be cautious of when implementing a work-from-home team.

1. **Public WiFi –** From Starbucks to libraries to doctors' waiting rooms, public WiFi seems to be just about everywhere nowadays. While it's convenient to just hop on a public WiFi, it poses significant security risks to your network. First, other people have access to that same network, and without a firewall between you and them, there's potential for someone nearby accessing the same data that you can. Second, any interested observers on your current network or the public networks can monitor your traffic since it's not encrypted.

2. **Personal Computers and Devices –** When your staff is working from home, it may be more convenient for them to use their home PC or devices to run reports, send e-mails or even access your network.

   You and your IT team have probably gone to great lengths to ensure your work computers have the latest updates installed, run antivirus scans and block malicious sites. However, most business owners and IT staff rarely follow the same security procedures for personal computers and devices, such as ensuring the work device has the Windows firewall enabled to protect it from other home computers and Internet of Things (IoT) devices. Essentially, by introducing a personal computer to a work network, even remotely, you're putting the company network and your business at unnecessary risk. Even beyond the risk to your data is the potential liability and financial risk through violations of policy, practices or both.

3. **Risk of Theft –** While you know there's a threat of cybercriminals hacking your network and stealing your data, you probably rarely think about someone stealing the computers in your office. However, because laptops and tablets are portable and much easier to steal, there is a greater chance of theft.

   Advise your employees to never leave their work computers or devices in a vehicle or unattended in a restaurant. It only takes a few seconds for someone to break into your car or even the trunk and take a laptop. While on the road, it's smarter to always keep your laptop on your person. Because a stolen laptop means a lot worse than simply replacing a computer, it can also be a productivity and records nightmare. The worst-case scenario? The theft is actually a hacker who is after the personal data and passwords left on the laptop!

4. **Flash Drives –** Your IT team goes to such great lengths to keep your network safe. And it can all be brought down by a cheap little thumb drive or flash drive. Most families have several of these portable drives in random desk drawers and kids' rooms. If an employee picks up a random thumb drive, it's like playing Russian roulette – will it contain malware or not?

A classic hacking technique is to drop off several thumb drives at an office or public location. Most people will appreciate the free drive and take it home for future use. By doing so, they could possibly unleash a virus or malware onto the computer and possibly even your network! In a study presented at a hacker conference, a Google researcher dropped off 297 USB drives in hallways, parking lots and outdoor areas on the University of Illinois's Urbana-Champaign campus. Inside the drives was special software that would allow them to immediately "call home" when plugged in. Of the 297 USB drives, 98% were picked up and 45% were plugged in and called home!

Bottom line: never use a flash drive if you don't know what's on it and who gave it to you.

5. **Sending Sensitive Information Via E-mail –** Your remote employees won't think twice about sending e-mails either from their work computer or their personal laptop. However, when you're sending sensitive data, such as financial information, passwords or proprietary product information, there's always a chance it could be intercepted by a third party.

   Encrypting the data attached to an e-mail prevents an unintended recipient from intercepting and viewing the data. Also, be sure your device is set to have all stored data encrypted in case of theft.

6. **People Are Watching –** You've already been warned about using public WiFi. There's another risk if you're in a public place doing work. It's other people. If you're in a coffee shop, you should always be aware of your sight lines. Anyone behind you can see everything you're typing. Cybercriminals have strong observational skills to easily watch what you are doing and steal confidential information.

Four Steps To Take To Ensure Secure Work-From-Home Environments

Now that you better understand the cyber security risks of allowing your team to work from home, we want to give you the tools, technologies and insights into creating a more productive remote business environment. Here are four

considerations to getting you set up and running a productive and protected work-from-home business.

Use Two-Factor Authentication VPN

VPN stands for virtual private network. It's essentially a private, encrypted tunnel that goes direct to your IT network in your office. Ideally, you'll want your VPN to support two-factor authentication. This means that it's doubly secure because your employees will need to call in to access the network.

Ideally, your employees would be accessing corporate resources through a VPN remote access rather than a cloud-based "virtual desktop" solution, such as GoToMyPC or Zoho. These products are not as secure, but they are still better than not using anything and exposing your network to risk.

Use A Secure WiFi Access Point

Without a secure WiFi access point, you're essentially leaving a back door open to hackers. That's because WiFi signals are often broadcast far beyond your employees' homes and out into the streets. Yes, drive-by hacking is popular among cybercriminals today.

A few tips for using a secure WiFi access point: First, use a stronger encryption and a more complex password. Second, hide your network name so your neighbors or people in your proximity cannot see your network. Third, use a firewall.

Improve Your Password Strategy

The strength of your passwords may be the first line of defense that shields against would-be hackers. Make a point to reevaluate your passwords and inform your team to create stronger passwords. While it's convenient to save your passwords in a web browser, it also lessens your security. Because web browsers simply require their own password or PIN to access saved passwords, a skilled

hacker can bypass this hurdle. Once they access your saved passwords, they can steal as much as they want – credit card information, customers' private data and more.

Another tip is to never use the same password for more than one account or website. Too many people utilize one password for all of their accounts. If that single password ever gets leaked, ALL of their accounts are compromised. Instead, by using different passwords, you only have to change the one password on the compromised website or software.

To make it far easier to deal with multiple passwords, you should consider a password manager to keep all of your passwords in one place. These password managers feature robust security.

Provide Company-Approved Computers

You have practically zero control regarding what's on your employees' home computers and who is using them. That same computer they access your network with could be used to download music and apps, play video games, surf controversial sites and receive potentially dangerous e-mails.

While it may seem like an added expense to issue company-approved computers or laptops to all of your work-from-home employees, the investment could prevent a much more serious cyberattack that could cost your business far more. Many business owners today are providing their employees laptops rather than PCs and monitors so they can easily take them home. Just make sure they protect their company laptop and never leave it in their car or unattended in a public place.

Whether your employees are currently working from home or you're considering the benefits of letting them work remotely, apply these tips to help protect your team, their computers and your network and data.

Chapter 10:
Technical Terms In Plain English

Too often, IT services providers "hide" behind acronyms and technical terms. By making technology harder to understand, they keep themselves in a position of being valuable and necessary. After all, the less you understand, the more you depend on them.

Everyone on our team has the heart of a teacher. We believe you should understand your computers and network because they contain your important data. Therefore, we always strive to educate and inform whenever possible. If you're ever confused or questioning why your IT consultant is recommending a product, service or strategy, please ask them. If they dismiss your questions, they are salespeople – not teachers – at heart.

In an effort to be as transparent as possible, we've included plain English definitions for some of today's more common technology terms.

Access Point – A device that allows wireless-equipped computers and other devices to communicate with a wired network.

ASP: Application Service Provider – A third-party company that manages and distributes software-based services and solutions to their customers over a wide-area network, usually the Internet.

Authentication – The process of identifying yourself and the verification that you're who you say you are. Computers where restricted information is stored may require you to enter your username and password to gain access.

BYOD: Bring Your Own Device – A business and technology policy that allows employees to bring in personal mobile devices and use these devices to access company data, e-mail, etc.

Cloud Computing – Internet-based computing, whereby shared resources, software and information are provided to computers and other devices on demand, as with the electricity grid.

Content Filtering – Software that prevents users from accessing or sending questionable content via your Internet. Content filtering is used to block job application sites, dating sites, gambling sites, shopping sites, as well as pornography, explicit language and images. Many programs also screen inbound and outbound e-mails for offensive and confidential information. This software is not designed for virus, worm or hacker prevention.

CPU: Central Processing Unit – The brains of a computer.

CSP: Cloud Service Provider – A business model for providing cloud services.

Dark Web – The unknown, hidden part of the web that consists of websites that use the public Internet, but requires specific software for access and is not indexed by search engines. Stolen data on the dark web is traded, sold and used for financial or political gain.

Deep Web – Ninety percent of the web is actually the deep web, just below the surface of the World Wide Web. Web developers and companies tell Google not to index the information so it's not searchable.

Default Gateway – In a TCP/IP network, this is the gateway that computers on that network use to send data to, and receive it from, computers and networks outside of the local network. Typically, this is the router or firewall that connects the local network to the public Internet, although it might also be a router that connects to another remote server or computer within the same company.

DHCP: Dynamic Host Configuration Protocol – A method for dynamically assigning IP addresses to devices on request, rather than explicitly programming an IP address into each device. If you have a server on your network, configuring that server as a DHCP server will make it much easier to add or reconfigure individual workstations on the network.

DMZ: Demilitarized Zone – A separate area of your network that is isolated from both the Internet and your protected internal network. A DMZ is usually created by your firewall to provide a location for devices such as web servers that you want to be accessible from the public Internet.

DNS: Domain Name Server (or Server) – An Internet service that translates domain names into IP addresses. Even though most domain names are alphabetic, hardware devices (like your PC) can only send data to a specific IP address. When you type www.microsoft.com into your web browser, or send an e-mail message to someone@business.com, your web browser and e-mail server have to be able to look up the IP address that corresponds to the microsoft.com web server, or to the mail server that receives e-mail for business.com. DNS is the mechanism for doing this lookup.

EHR/EMR/PHR: Electronic Health Record/Electronic Health Record/ Personal Health Record – These terms are used interchangeably to refer to patient-centered health records.

Encryption – The manipulation of data to prevent accurate interpretation by all but those for whom the data is intended.

Endpoint Protection – Also referred to as endpoint security, it's an approach to detecting malicious activity while protecting secure networks, including servers, computers and devices from an attack.

Ethernet – Ethernet is the standard wired network technology in use almost everywhere today. If your computer is connected to a network via a cable, it's likely using an Ethernet cable. That cable plugs into an Ethernet port on your computer.

Firewall – A device or software program designed to protect your network from unauthorized access over the Internet. It may also provide network address translation (NAT) and virtual private network (VPN) functionally.

Hosted Applications (e.g., Hosted Sharepoint or Hosted Exchange) – A service whereby a provider makes a software (e.g., e-mail) and space available on a server so its clients can host their data on that server.

IaaS: Infrastructure as a Service – In the most basic cloud-service model, providers of IaaS offer computers – physical or (more often) virtual machines – and other resources.

ISP: Internet Service Provider – Your Internet service provider is the company that provides you with your Internet connection. For example, your ISP may be Comcast, Time Warner or whatever other company you're paying each month.

LAN: Local Area Network – A small network that's confined to a local area. For example, your home network or an office network is a LAN. A LAN connects a group of computers for the purpose of sharing resources such as programs, documents or printers. Shared files often are stored on a central file server.

Mail Server – A networked computer dedicated to supporting electronic mail. You use a client program like Microsoft Outlook for retrieving new mail from the server and for composing and sending messages.

Microsoft Exchange Server – The server side of a client server, collaborative application product developed by Microsoft. It is part of the Microsoft Servers line of server products and is used by enterprises using Microsoft infrastructure products. Exchange's major features consist of e-mail, calendaring, contacts and tasks; support for mobile and web-based access to information; and support for data storage.

MSP: Managed Services Provider – A proactive and responsive business model for providing information-technology services. A managed services provider can save you considerable money by minimizing costly network disasters while decreasing downtime by providing proactive solutions. By ensuring your network and data are secure, reliable and running just as it should, MSPs provide peace of mind.

Multi-Factor Authentication – An authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession and inherence. Two-factor authentication is a type, or subset, or multi-factor authentication.

Nameserver – A computer that runs a program for converting Internet domain names into the corresponding IP addresses and vice versa.

Network Interface/Network Adapter – Your computer's wired Ethernet connection and WiFi connection are basically both network interfaces. If your laptop was connected to both a wired connection and a WiFi network, each network interface would have its own IP address. Each is a different connection.

Next-Generation Endpoint Security – Beyond traditional endpoint security solutions, next-generation endpoint security utilizes modern artificial intelligence and machine learning to provide real-time analysis of user and system behavior. These advanced tools address threats and also learn from threats and continuously adapt methods and combat them with greater speed and efficiency.

Patch – Piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance.

Port – When an application wants to send or receive traffic, it has to use a numbered port between 1 to 65535. This is how you can have multiple applications on a computer using the network and each application knows which traffic is for it.

Protocol – An agreed format for transmitting data between two devices. TCP and UDP are the most common protocols. The ICMP protocol is also used, but primarily so network devices can check each other's status. Different protocols are ideal for different types of communication.

Remote Desktop – A Windows feature that allows you to have access to a Windows session from another computer in a different location.

Remote Login – An interactive connection from your desktop computer over an Internet connection to a computer at a remote site.

RMM: Remote Monitoring and Management – A piece of software managed services providers use to monitor the performance of endpoints and other IT assets remotely. From a single device, you can monitor systems, remotely access devices, review data, deploy patches and more.

Router – A device used for connecting two local area networks (LANs); a device that passes traffic back and forth. You likely have a home router. The router's job is to pass outgoing traffic from your local devices to the Internet and to pass incoming traffic from the Internet to your devices. A router is also used if you have multiple office locations and you need all devices to communicate to the home office servers.

SaaS: Software as a Service – A software distribution model in which a third-party provider hosts applications and makes them available to customers over

the Internet. SaaS is one of three main categories of cloud computing, alongside infrastructure as a service (IaaS) and platform as a service (PaaS).

SAN: Storage Area Network – A dedicated storage network that provides access to consolidated, block level storage. SANs are primarily used to make storage devices accessible to servers so the devices appear as locally attached to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the regular network by regular devices.

SIEM: Security Information and Event Management – A software solution that aggregates and analyzes activity from many different resources across your IT network. SIEM collects security from network devices, servers and more.

SMTP: Simple Mail Transfer Protocol – An Internet standard for e-mail transmission.

SOC: Security Operations Center – A centralized unit that deals with security issues on an organizational and technical level. A SOC within a building or facility is a central location from which staff supervises the site, using data processing technology. Typically, a SOC is equipped for device monitoring such as hacker threats.

Spam – E-mail spam, also known as junk e-mail or unsolicited bulk e-mail, is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail. By definition, spam is unsolicited and sent in bulk. Spammers collect e-mail addresses from chatrooms, websites, newsgroups and viruses that harvest users' address books and are sold to other spammers.

Spear Phishing – Phishing attempt directed at specific individuals or companies. In contrast to bulk phishing, spear phishing attackers often gather and use personal information about their target to increase the probability of successfully getting their victim take action.

SSL: Secure Socket Layer – Small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the HTTPS protocol and allows secure connections from a web server to a browser. Typically, SSL is used to secure credit card transactions, data transfer and logins, and more recently is becoming the norm when securing browsing of social media sites.

Switch – Serves as a controller, enabling networked devices to talk to each other efficiently. Through information-sharing and resource allocation, switches save businesses money and increase employee productivity.

TCP/IP: Transmission Control Protocol/Internet Protocol – An agreed-upon set of rules that tells computers how to exchange information over the Internet. Other Internet protocols, like FTP, Gopher and HTTP, sit on top of TCP/IP.

Threat Actor – Any individual or group of individuals who attempt to conduct malicious activities against enterprises. Threat actors can be internal or external.

Two-Factor Authentication – An extra level of security achieved using a security token device; users have a personal identification number (PIN) that identifies them as the owner of a particular token. The token displays a number that is entered following the PIN number to uniquely identify the owner of a particular network service. The identification number for each user is changed frequently, usually every few minutes.

URL: Uniform Resource Locator – The global address of documents, websites and other resources on the web.

Virus – A program intended to alter data on a computer in an invisible fashion, usually for mischievous or destructive purposes. Viruses are often transferred across the Internet, as well as by infected diskettes, and can affect almost every type of computer. Special antivirus programs are used to detect and eliminate them.

VoIP: Voice over Internet Protocol – A means of using the Internet as the transmission medium for phone calls. An advantage is you do not incur any additional surcharges beyond the cost of Internet access.

VPN: Virtual Private Network – A network constructed by using public wires (the Internet) to connect nodes (usually computers and servers). A VPN uses encryption and other security mechanisms to ensure that only authorized users can access the network and the data it holds. This allows businesses to connect to other servers and computers located in remote offices, from home or while traveling.

WAN: Wide Area Network – A larger network used to connect two or more locations. If you have two or more offices and want to send and receive data securely between them, a WAN is ideal.

WAP: Wireless Application Protocol – A set of communication protocols for enabling wireless access to the Internet.

WEP: Wired Equivalent Privacy – A security protocol for wireless local area networks defined in the 802.11b used in a wireless network. WEP provides the same level of security as that of a wired LAN.

WiFi: Wireless Fidelity – A generic term from the WiFi Alliance that refers to any type of 802.11 network. Products approved as "WiFi Certified" are certified as interoperable with each other for wireless communications.

WLAN: Wireless Local Area Network – The computers and devices that make up a wireless network.

WPA: WiFi Protected Access – A standard designed to improve on the security features of WEP.

Chapter 11:
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 with you recently – in the last three months – to specifically review and discuss what they are doing NOW to protect you?** Have they told you about new and inexpensive tools such as dark web monitoring for your company's credentials or advanced endpoint security to protect you from attacks that antivirus is unable to detect and prevent?

  If you are outsourcing your IT support, they should, at a MINIMUM, provide you with a quarterly review and report of what they've done – and are doing – to protect you AND to discuss new threats and areas you will need to address.

- **Do they proactively monitor, patch and update your computer network's critical security settings daily? Weekly? Or 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 or cyber liability?**

  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? You should ask if they have an Errors-and-Omissions (E&O) insurance policy, as well as a cyber liability policy.

- **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 NOT?

- **Have they told you if they are outsourcing your support to a third party? 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 cyber security threats and technologies, rather than just winging it?** Do they have anyone on staff experienced in conducting security risk assessments? Does their business have key partnerships with today's most prominent IT vendors?

- **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 90-day password update for all employees that falls within the National Institute of Standards and Technology? 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 "multi-factor 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 and financial information, social security numbers, etc., you may be required by law 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 searched thing online. This can expose you to sexual harassment and child pornography lawsuits, not to mention the distraction and time wasted on your dime, with your company-owned equipment.
- **Have they given you and your employees any kind of cyber security awareness training?** Have they offered to help you create an AUP (acceptable use policy)? 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 into place.
- **Have they implemented random phishing e-mails to test your employees?** There's no better education than real-life scenarios. Of course, if they fail the phishing tests, those employees should attend additional training.

- **Have they properly configured 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, like social security numbers, from being sent or received.
- **Do they allow your employees to connect remotely using GoToMyPC, LogMeIn or TeamViewer?** 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 new tools available that monitor cybercrime websites and data for your specific credentials being sold or traded. Once these are detected, it notifies you immediately so you can change your password and be on high alert.
- **Do they offer a Security Information and Event Management (SIEM) solution to ensure unwanted traffic isn't coming from within your own network?** SIEM software is critical in today's security world because it can detect and log as many as 25,000 events per second.

A Free Cyber Security Risk Assessment Is The ONLY Way You Can Really Be Sure

A security assessment is exactly what it sounds like – 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 cancer 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 organization AND give you a better chance of surviving a cyberattack.

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

You want a qualified "Sherlock Holmes" investing on YOUR behalf who is not trying to cover up inadequacies or make excuses; bringing to you a confidential report you can see and understand.

Our Free Cyber Security 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 Cyber Security Risk Assessment to a select group of businesses. This is entirely free and without obligation. EVERYTHING WE FIND AND EVERYTHING DISCUSSED WILL BE STRICTLY CONFIDENTIAL.

This assessment will provide verification from a qualified third 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: At no cost or obligation, one of my lead consultants and I will come to 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. Your time investment is minimal: one hour for the initial meeting and one hour in the second meeting to discuss our Report of Findings.

When this Risk Assessment is complete, you will know:

- **If your login credentials and your employees' are being sold on the dark web.** We will run a scan on your company, right in front of you, in the privacy of your office if you prefer (results will NOT be e-mailed or otherwise shared with anyone but you). 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 fast** if ransomware locked all your files. *In far too many of the computer*

networks we've reviewed over the years, the owners were shocked to learn the backup they had would NOT 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 your IT systems, backups, and security controls are in sync with compliance requirements for HIPAA, GLBA, and SOX**, and if you are using best practices to ensure **data integrity, access control, encryption, audit readiness, and business continuity**.

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 STRICTLY CONFIDENTIAL.

Why FREE?

Frankly, we want the opportunity to be your IT company. We know we are the most competent, responsive and trusted IT services provider to small businesses in The United States and Mexico.

However, I also realize **there's a good chance you've been burned, disappointed and frustrated by the complete lack of service and the questionable advice** you've gotten from other IT companies in the past. In fact, you might be so fed up and disgusted with 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. 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 Free Cyber Security Risk Assessment, shrug it off, worry about it "later" or dismiss it altogether. This 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.

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 that the attack on your business will be far more costly, disruptive and devastating.

You've spent a lifetime working hard to get where you are today. Don't let some lowlife thief operating outside the law in another country get away with taking that from you. And certainly don't "hope" your IT guy has you covered.

Get the facts and be certain you are protected.

Contact us and schedule your free, CONFIDENTIAL Cyber Security Risk Assessment today: www.cmitcybersolutionsla.com. Feel free to also reach out to me directly at 213-870-8888 or e-mail: bsolano@cmitsolutions.com

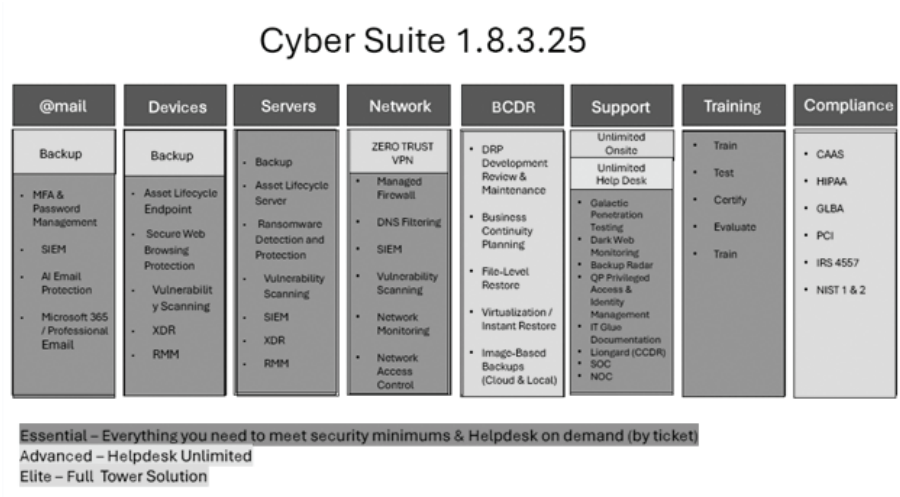
Chapter 12:
The Top 8 Reasons You'll Want To Outsource Your IT Support To Us

Choosing the right IT partner is a critical decision for any business. At CMIT Solutions of LA, Irvine, Mexico, and South Africa, we combine global capabilities with local care to deliver world-class technology support tailored to your needs. Here are the top 8 reasons businesses like yours choose to outsource their IT support to us:

1. **Mitigation of Risk:** We provide proactive, multi-layered protection against the most perilous cyber threats of the present day, such as AI-driven attacks, ransomware, phishing, and insider risks. This approach minimizes your vulnerability to regulatory penalties, data loss, and downtime. Typically, we minimize the risk to 99%.
2. **Operational Efficiency:** Our team use established, enterprise-level methodologies to enhance and refine your IT operations. From remote monitoring to automated patching and documentation, all systems are designed to operate more efficiently, rapidly, and with minimal disruptions. Our clients have experienced reductions in their IT costs ranging from 8% to 20%.
3. **Personalized World Class Service:** We guarantee that you will receive personalized, world-class service in less than 15 minutes after submitting a ticket during business hours. Our clients benefit from the best of both worlds: the responsiveness and relationship of a local partner, combined with

the strength and resources of a nationwide network. We know your name, business, industry, and objectives, and we have 300 offices throughout the United States. Our areas of expertise include Finance, CPAs, Legal, Health, Construction, Manufacturing, Distribution, and Professional Services.

4. **Experience, Knowledge, and Capabilities:** With 28 years of experience in the IT industry, we have developed a robust Cyber Suite (1.8.3.25) that is designed to provide the most secure, efficient, reliable, and sustainable services ever created in the marketplace for the SMB. This solution is designed to eliminate the need to deal with 25 vendors, as there is only one representative, CMIT Solutions of LA, Irvine, Mexico, and South Africa. The suite is supported by 8 towers. We collaborate with a number of industry-leading vendors, such as Microsoft, Datto, Kaseya, Barracuda, ConnectWise, and Galactic Advisors. Please refer to the following:



5. **Predictable Costs:** No more surprise invoices or unpredictable IT bills. Our flexible, flat-rate service plans give you consistent monthly costs, while adapting to your growth and budget over time.
6. **Business Continuity & Disaster Recovery:** We don't just back up your data — we design end-to-end continuity plans to ensure that your business keeps running, no matter what. Whether it's a cyberattack, power outage, or natural disaster, we'll have you back online quickly and confidently.
7. **Compliance & Risk Management Expertise:** We support businesses operating under regulatory frameworks like HIPAA, GLBA, SOX, NIST and IRS 4557. We ensure your systems are aligned with required controls, from data encryption to access management and audit readiness.
8. **Strategic IT Partnership**: We're not just IT support — we're your technology ally. Through ongoing Technology Business Reviews (TBRs), we align IT investments with your business goals, helping you plan ahead, avoid costly mistakes, and stay competitive.

CONCLUSION.-CMIT Solutions of LA, Irvine, Mexico, and South Africa Cyber Suite 1.8.3.25 claims their value as:

1 Solution, 8 Towers that powers 3 reasons to outsource or CO-Source your IT area in 2025 to CMIT Solutions of LA, Irvine, Mexico and South Africa.

Book Order Form

If you enjoyed this book, share it with others! Use this form to order extra copies for friends, colleagues, clients or members of your association. Please allow 2-4 weeks for delivery.

Quantity Discounts:

1-9 copies = $19.95 each, 10-49 copies = $16.95 each

50-99 copies = $13.95 each

100 or more copies = Call for discounts and wholesale prices

Information:

Name: _____

Company: _____

Phone: _____

Address: _____

City: _____

State/Province: _____

Zip/Postal Code: _____

# of Copies _____ @ $_____ Total: $ _____

Add shipping and handling @ $3 per book $ _____

Please make check of money order payable to:

CMIT Solutions of LA, Irvine, Mexico, and South Africa

Credit Card: ❑ Visa ❑ MC ❑ Amex ❑ Discover
Card Number:
Expiration Date:
Signature:

Thank You for Your Order!

ABOUT
BILLY SOLANO

Billy Solano is an accomplished technology executive and entrepreneur with over 28 years of experience transforming businesses through innovative IT and cybersecurity solutions. As CEO of CMIT Solutions of Los Angeles and Irvine, Billy leads a dynamic team dedicated to delivering comprehensive technology services to small and medium-sized businesses across the United States and beyond. His leadership has propelled CMIT Solutions to new heights, earning accolades such as recognition from the Calabasas City Council as a Certified Cybersecurity provider, the Managed Services Excellence Award from Barracuda Inc., and Cybersecurity certification from ConnectWise.

Billy's professional journey began in 1997 at JD Edwards, where his exceptional sales talent and strategic relationship-building quickly elevated him from a newcomer to Vice President and General Manager within just four years. He played a pivotal role in securing major clients like Grupo Modelo, Coca-Cola, and Telcel—achievements that caught the attention of Accenture. As a partner at Accenture for a decade, Billy specialized in outsourcing and business development, driving major transformation projects for industry leaders and spearheading the creation of new business lines in Latin America.

In 2013, Billy founded Opera Consulting, establishing it as a global SAP business partner and further cementing his reputation for delivering enterprise technology solutions. His entrepreneurial spirit led him to the United States, where he acquired CMIT Solutions of LA in 2018 and expanded its offerings to include advanced cybersecurity services. Billy is also the creator of the "Highly Effective Executive" program, a methodology for executive performance that has been taught in Mexico, Brazil, and the U.S., reflecting his passion for mentoring and leadership development.

Billy holds a Bachelor of Business Administration from Universidad Anáhuac México and a Master of Science from National University in La Jolla, California, along with advanced studies in business performance management and strategic planning.

Beyond his professional accomplishments, Billy is known for his vibrant personal life and diverse interests. He enjoys golfing, running, biking, yoga, and is an avid Ferrari enthusiast, having founded and served as president of the Ferrari Owners Club in Mexico. He also has a deep appreciation for wine and loves exploring vineyards around the world. Billy resides in Calabasas, California, with his wife Laura and their two children, Dali and Billy Jr., sharing a passion for sports, outdoor activities, and family barbecues.

From his meteoric rise in the Latin American tech industry to his successful ventures in the United States, Billy Solano exemplifies adaptability, strategic vision, and a relentless commitment to leveraging technology for business growth and positive impact.

For more information, contact Billy Solano at CMIT Solutions:
Phone: 818-877-8738
LinkedIn: linkedin.com/in/billy-solano
Email: bsolano@cmitsolutions.com
Website: www.cmitcybersolutionsla.com