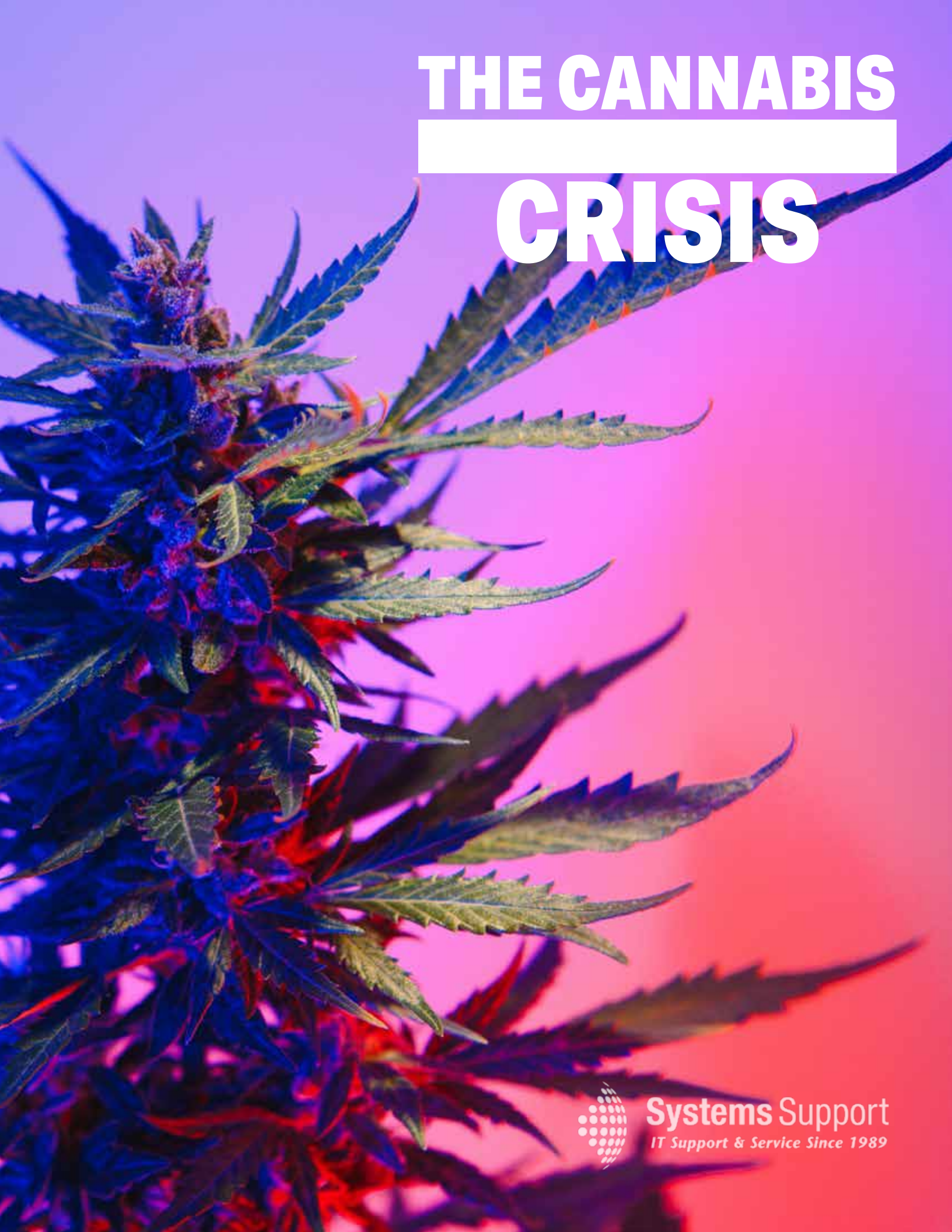
THE CANNABIS CRISIS



Systems Support
IT Support & Service Since 1989

Table of Contents

From The Desk Of: William MacFee
President, Systems Support Corporation

Dear Colleague,

My name is Will MacFee of Systems Support Corp. We specialize in being the outsourced I.T. department for cannabis businesses from the Cape to Boston. I started in the Nuclear Industry working on safety systems and brought the same defense-in-depth approach to cybersecurity for businesses like yours, which face unique challenges. We deliver a balance of risk-informed defense measures with a common-sense approach so companies don't lose the efficiency they need to grow.

Over the last couple of years, my team and I have seen a significant increase in calls from business owners desperate for help after a ransomware attack, data breach, or other cybercrime incident. When they call, they're scrambling to salvage their operations. Often, their entire business is completely on lockdown. ALL their data—customer information, inventory tracking, banking information—is either corrupted or held for ransom, preventing them from fulfilling obligations to their customers. The cannabis industry is just as vulnerable, if not more so because of stricter scrutiny and tighter data requirements.

They're scared and intensely angry. They feel violated and helpless. Embarrassed. How can money be taken from their bank account WITHOUT their permission or knowledge? Why didn't their I.T. company prevent this from happening? How are they going to tell their customers that their data is now in the hands of criminals? They're in disbelief, saying, "We didn't think we had anything a cybercriminal would want!"

What makes this even more unforgivable is that ALL of the business owners coming to us for help after a serious attack had an I.T. company they trusted to protect them but realized all too late that the company wasn't doing the job it was PAID to do.

As a business owner I know how hard you work to succeed. I understand the risks you've taken, the personal sacrifices you've made. To me, it's a gross insult to have it all taken away by some cyber-scumbag hidden behind a keyboard, who will NOT be held accountable for their actions.

To make matters worse, many so-called "I.T. experts" aren't doing the job they were hired to do – and that truly angers me. As the CEO of a cannabis business, you're FORCED to trust that your I.T. company or team is doing the right things to protect your organization. When they fail, this expensive, devastating, business-interrupting disaster lands squarely on YOUR desk to deal with.

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

Dedicated to serving you,

William MacFee,
President

ABOUT SYSTEMS SUPPORT:

Since 1989, Systems Support has worked with Boston and South Shore small businesses to help them use the best of enterprise technology. The company was started by brothers Brian and Willie MacFee.

Brian MacFee grew up in Weymouth and went to Wentworth and Northeastern University after high school. Brian's job as a Test Engineering Manager at LTX where he first encountered the IBM PC. In the late 80's, Brian noticed these personal computers showing up on people's desks, and became involved in networking them together, and productivity skyrocketed. After some conversations with his brother Willie, Systems Support was started on the front deck of Brian's home.

Fast forward to 2008, after installing over 7000 computers in over 50 schools in Boston and Providence, Brian assumed full ownership of the company in 2008 as Willie retired. Fast forward again to 2016 and Brian's son Will joins the company.

Will MacFee grew up in Marshfield and after school went to North Carolina State University for Nuclear Engineering. At school he worked on various simulation projects and passed the exam to operate the school's nuclear reactor. After school, he worked for two years at the Nuclear Regulatory Commission in the Office of Nuclear Reactors. With the nuclear industry slowing down, Will joined Systems Support bringing the safety mindset from the reactor world. Coupled with the technical skills from networking computers during simulation research, Will learned quickly.

Fast forward a few more years to 2023, and Brian retires on his 64th birthday. Will MacFee, his son, takes over as President of the company. Brian trained him well, and Will has helped the company meet the new challenges of running an IT business.

Over the past few years, IT has rapidly changed from "digital plumbing" to security compliance. As cybercrime made headlines and hit businesses of all sizes, the needs of companies changed. Today, IT companies not only have to make sure everything works as expected but also must defend against cyberattacks like email compromise and ransomware. Every day the threat actors get better, and we need to as well.

Rather than take an approach of sealing every door and battening down the hatches, Will used another mantra from the NRC: "reasonable assurance of adequate protection". There are plenty of common-sense steps to take to protect a company's data assets. No solution is perfect, and if one understands the risk the choice is easier for what actions one has to take.

When you work with Systems Support, you have a direct relationship with the people providing the service. We hate bureaucracy (Will saw enough of it at the NRC) so we do everything we can to make it easy to do business with us. You will work with the same name and faces on a consistent basis, people who know your business and your people. When you work with us, you become part of the family.

Systems Support

IT Support & Service Since 1989

Phone: 781-734-7261 | www.systemsupport.com | 462 Plain Street, Suite 206, Marshfield, MA 02050

When You Fall Victim to A Cyber-Attack by No Fault of Your Own, Will They Call You Stupid... Or Just Irresponsible?

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

But if your cannabis business is the victim of a cybercrime where client data is compromised, you will NOT get such sympathy. You will be instantly labeled as "irresponsible." Regulators will investigate you, and your customers will question what you did to prevent this from happening. If the answer isn't adequate, you can face serious fines and lawsuits—even if you trusted an outsourced I.T. support company to protect you. Claiming ignorance is not an acceptable defense. This giant, expensive, and reputation-destroying nightmare will land squarely on YOUR shoulders.

But it doesn't end there…

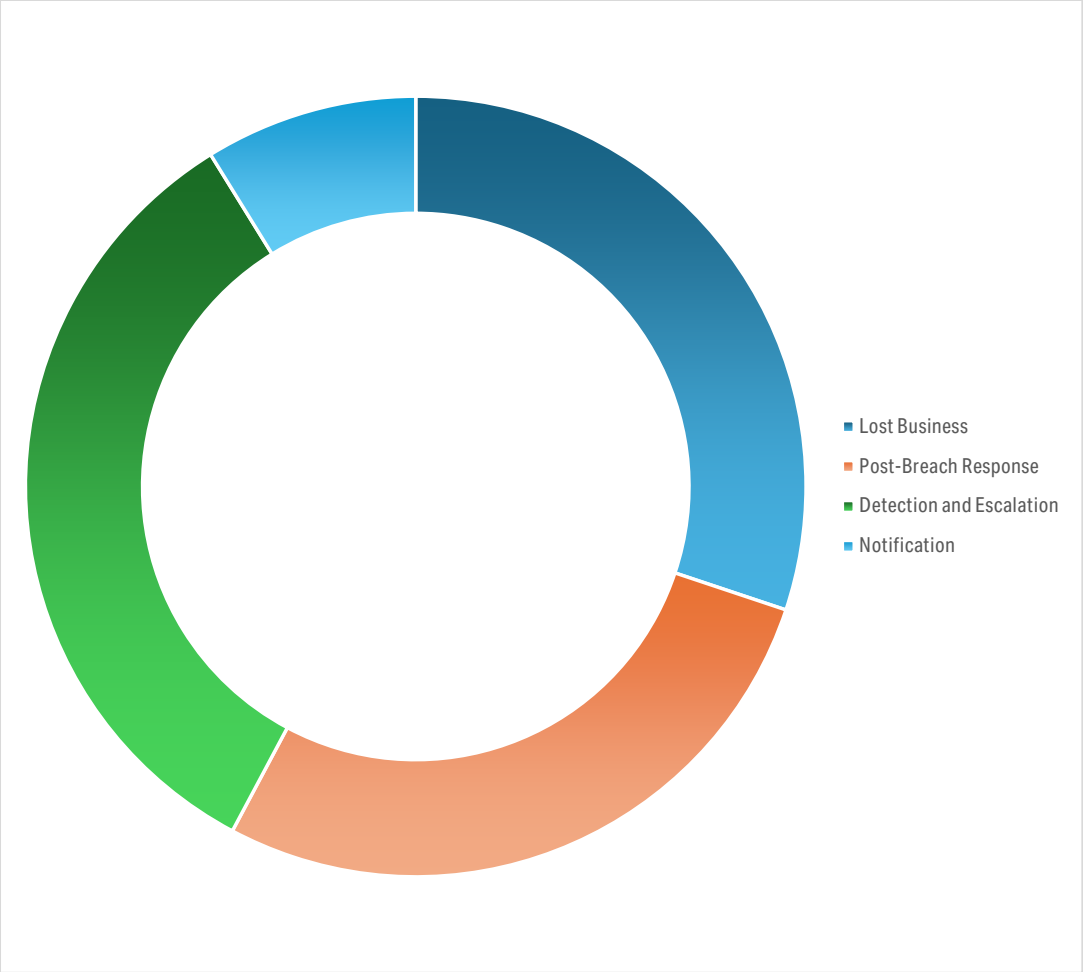
According to state and federal laws, you will be required to inform your customers that YOU exposed them to cybercriminals. Your competitors will have a field day. Customers will leave in droves. Morale among employees will tank, and they will BLAME YOU. Your bank is NOT required to replace funds stolen due to cybercrime (check your policy), and unless you have a very specific type of insurance policy, any financial losses will be denied coverage.

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

Schedule Your Free Cyber Security Risk Assessment Today!

Visit www.systemsupport.com or call our office at 781-837-0069.

Cost of a Data Breach



The average cost of a data-breach worldwide reached $4.88 million in 2024 (closer to $10 million in the United States) from $4.4 million in 2023. Lost business accounted for $1.47 million; detection and remediation cost $1.63 million; follow up, including regulatory fines, accounted for $1.35 million; and notifications cost approximately $430,000 on average. IBM Cost of Data Breach Report 2024

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

In the cannabis industry, you already know about the escalating threats—from ransomware to hackers—but it's very possible you are underestimating the risks specific to your business. It's also likely you're NOT fully protected and are operating under a false sense of security, underserved and ill-advised by your outsourced I.T. company.

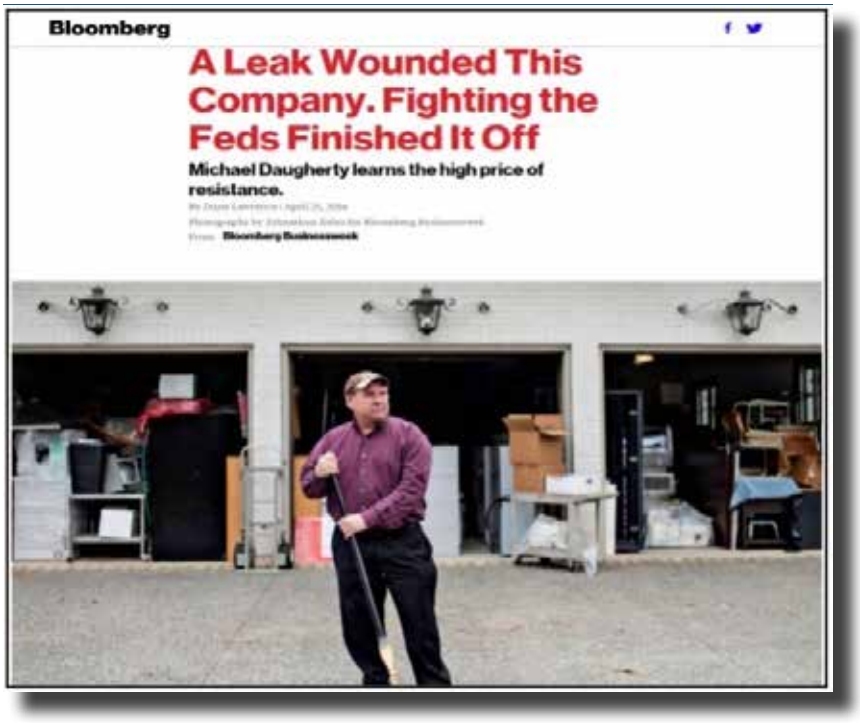
If your I.T. provider has not discussed protections tailored for the cannabis industry, such as secure seed-to-sale systems, or helped you develop a comprehensive cyber "disaster recovery" plan, your business is at risk. This is not an issue to take lightly. Should a breach occur, your reputation, your finances, your compliance with cannabis regulations, and even the viability of your business could be on the line.

This Is Too Serious a Matter to Delegate Without Your Oversight

Cybersecurity in the cannabis industry is not something you can completely delegate to your I.T. team or software providers. ONE misstep—a single employee clicking a malicious email, using a weak password, or unknowingly downloading compromised software—can result in devastating consequences.

Take the case of Michael Daugherty, former CEO of LabMD, as a cautionary tale. His company, which tested blood and tissue samples, was required to comply with strict data privacy laws. He thought his I.T. team had his business protected, but a single employee downloading a file-sharing program led to over 9,000 patient files being exposed. Hackers exploited this vulnerability for extortion. When Daugherty refused to pay, the fallout was catastrophic: regulatory investigations, employee attrition, financial losses, and eventually, the closure of his business.

Now imagine this scenario in the cannabis industry, where compliance requirements and reputational risks are even more intense. The loss of customer data or breach of regulatory compliance can lead to lawsuits, loss of licenses, and clients fleeing to competitors who seem more secure.



Schedule Your Free Cyber Security Risk Assessment Today!

Visit www.systemsupport.com or call our office at 781-837-0069.

Don't Believe "Not My Company, Not My People"

Because That's Exactly What Cybercriminals Count On

If you think your cannabis business is "too small" to be targeted, think again. Cybercriminals count on small businesses to let their guard down. Right now, there are over 980 million malware programs in existence (source: AV-Test Institute), and 70% of cyber-attacks target small businesses (source: National Cyber Security Alliance). You don't hear about these breaches because many small businesses fear the bad PR, lawsuits, and regulatory repercussions of going public.

Companies with fewer than 100 employees receive 350% more social engineering attacks than larger enterprises.

The average ransomware demand is now $84,000 (source: MSP Alert), and the average downtime from a ransomware attack exceeds 25 hours. Even a single incident can lead to over $100,000 in financial losses—not to mention the reputational damage, regulatory fines, and legal liabilities.

This is not just about money. This is about safeguarding the business you've worked tirelessly to build, ensuring compliance with cannabis regulations, and maintaining the trust of your clients and partners. Don't wait until it's too late. Take proactive steps to protect your cannabis business today.

70% of cyberattacks are aimed at small and medium -sized businesses.

"Not My Dispensary...Not My Grow Operation...We're Too Small," You Say?

Don't think your cannabis business is in danger because you're "small" and not a big corporation like Amazon, Experian, or Target? That you have "good" people and adequate protections in place? That it won't happen to you?

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

The cannabis industry's reliance on technology for compliance—seed-to-sale tracking, point-of-sale systems, and payroll—makes you an even more attractive target to attackers.

Half of small businesses don't have a cybersecurity plan and 33% rely on free tools rather than professional solutions.

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

What would happen if ransomware locked all of your seed-to-sale tracking data for days or weeks?

Are you "too small" to deal with a hacker using your company's server as ground zero to infect all of your clients, vendors, employees, and contacts with malware?

Are you "too small" to worry about someone draining your payroll account or inventory records?

Schedule Your Free Cyber Security Risk Assessment Today!

Visit www.systemsupport.com or call our office at 781-837-0069.

It's NOT Just Cybercriminals Who Are The Problem

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

They DELETE everything. A common scenario: An employee is fired or quits due to dissatisfaction but not before permanently deleting crucial files and emails. Without proper backup systems, this data loss can be catastrophic. Even if you pursue legal action, the costs in time, legal fees, and business disruption often outweigh any compensation you might recover.

They leave with YOUR co data, and confidential in personal devices, as well a cloud applications, such a file-sharing platforms (Dro example), that your I.T. dep about or forgets to change fact, according to Osterma businesses experience dat turnover, and 87% of empl data with them. They may s become competitors, or us

ompany's files, client formation stored on s retaining access to s social media sites and pbox or OneDrive, for artment doesn't know the passwords for. In n Research, 69% of a loss due to employee loyees who leave take sell it to competitors, se it at their next job.

Funds, inventory, trade secrets, client lists, and HOURS stolen. Employees can exploit vulnerabilities in inventory management systems to skim products or funds over time. StatisticBrain reports that 75% of employees have stolen from their employers at some point. Theft can range from taking inventory to manipulating financial records. Then there's the massive productivity drain: employees wasting time on personal errands, social media, or gambling on your dime. These distractions not only cost money but could expose your business to legal jeopardy, especially if employees access high-risk sites prone to viruses and phishing scams.

The cannabis industry is already under intense scrutiny and faces unique regulatory requirements. A cyberattack or data breach could not only cripple your operations but also put your licenses and reputation at risk. Is it worth taking the chance?

What does the industry say about Systems Support?

Brian Cusick
Founder
T. Bear, Inc.

"Confidence in knowing your assets are digitally secure"

The biggest benefit we've experienced since utilizing the services of Systems Support has been the confidence in knowing our data and equipment are secure. We know that if an issue should arise, there is a sound, responsive team in place to immediately tackle any issue. The staff have always been timely, supportive, and willing to break things down into layman's terms so we know what is occurring and why.

If you are on the fence looking for managed IT services for your business, look no further. The confidence instilled in knowing your assets are digitally secure is worth it alone, but the personal care and relationship System Support works to create is what will keep you working with them.

Charles Yon
Chief of Staff
Native Sun Cannabis

Peace of Mind

I can't express enough how grateful I am to have System Support as our IT partner. Since they took over our IT operations, the single biggest benefit to both me and my company has undoubtedly been the peace of mind it has brought us. Knowing that System Support is diligently monitoring our IT environment allows me to focus on the initiatives that will drive my business forward. This peace of mind is truly invaluable, and I can't thank them enough for it.

What sets System Support apart from other IT firms we've worked with in the past is their exceptional attention to detail and their outstanding communication. Unlike other IT Managed Service Providers, System Support not only delivers top-notch technical solutions but also ensures that every aspect of our IT infrastructure is meticulously handled. Their team's communication is second to none – they keep us informed every step of the way, ensuring we always have a clear understanding of what's happening with our IT systems.

To anyone on the fence about choosing System Support as their IT firm, I would say this: Work with System Support, and you won't be disappointed.

The *Real* Damage Cybercrime Can Inflict On Your Cannabis Business

Reputational Damage:

A data breach in the cannabis industry can be particularly devastating due to the high level of trust required between operators and consumers. Customers trust you with personal information, including purchase histories tied to compliance tracking. A breach could expose sensitive customer data and make headlines, permanently damaging your reputation. With the cannabis market being so competitive, losing trust could mean losing your business.

Government Fines, Lawsuits, and Compliance Risks:

The cannabis industry is subject to strict regulations. A data breach could lead to non-compliance with state and federal requirements, including seed-to-sale tracking laws. Failure to notify affected customers and regulators could result in severe penalties. Regulatory bodies don't distinguish between big corporations and small operations—if you're careless with data, you're liable. And while the cannabis industry isn't subject to HIPAA, similar obligations may apply depending on how patient data is handled.

The Cost of a Breach:

One ransomware attack could cripple your operations. For cannabis businesses, this could mean the inability to process transactions, track inventory, or comply with mandatory reporting requirements. Downtime alone can lead to revenue loss, and emergency IT restoration costs add another layer of financial strain. Additionally, you may be required to provide credit-monitoring services to customers whose data was compromised. Can you afford to shoulder these costs?

Bank Fraud and Vendor Exploitation:

Cannabis businesses often face challenges in accessing traditional banking services, leading to a reliance on alternative financial solutions. This makes you an attractive target for fraud. Hackers could intercept emails or manipulate transactions, draining accounts before anyone notices. Vendors handling payroll and accounting can also pose risks if they don't have robust cybersecurity protocols.

Internal Threats:

Disgruntled or careless employees are a significant threat. A departing employee with access to cloud platforms, inventory systems, or financial records could steal trade secrets, delete critical files, or even compromise your seed-to-sale tracking system. Without proper controls, even routine employee errors could lead to breaches.

WHAT CYBER CRIMINALS WANT:

In the information age, data is a valuable currency and businesses often hold vast hoards. If you know what kinds of data criminals are looking for, you can better work to protect it inside of your system and mitigate risks.

Personally-Identifiable Information (PII) is the most common type of data stolen or compromised in cyberattacks. While the contents of PII will vary between industries even a home address and email can be valuable to bad actors who will in turn target victims for identity theft and other forms of fraud.

Even companies that don't collect a lot of consumer or customer data will still have **Employee PII**. Poorly secured HR systems could include demographic data, social security numbers, bank information, medical information, and even the results of background checks.

Intellectual Property (IP) is a prime target for attackers. It can be leveraged for all kinds of malicious purposes from selling it to competitors to extortion.

Enterprising criminals can also find opportunities with other corporate information like financial records and non-PII customer data. Don't assume that your business won't be a target just because you don't keep a lot of credit card numbers on file. Some criminals might even simply see your network as the weak link in a chain they can use to attack your other vendors and business partners.

Why the Cannabis Industry is a Target?

Your reliance on technology—from point-of-sale systems to compliance software—creates numerous entry points for cybercriminals. Combine that with the high-value nature of your inventory and financial data, and it's clear why the cannabis industry is such a lucrative target. Failing to address these vulnerabilities is an open invitation for disaster.

Are you prepared to explain to regulators, customers, and stakeholders why your cannabis business wasn't adequately protected? Hoping it won't happen to you isn't a strategy—it's a liability.

Think You're Safe?

Think Again.

It's easy to assume your cannabis business is secure. Maybe your IT provider assures you everything is fine, or you believe your current protections are sufficient. But are they?

The cannabis industry faces unique hurdles when it comes to cybersecurity and compliance. Whether it's protecting customer data, securing seed-to-sale tracking, or maintaining point-of-sale (POS) systems, the stakes are high—and growing every day.

Have your IT and cybersecurity partners recently met with you to address new threats? Have they reviewed protocols, protections, and the latest tools to keep you compliant and secure? If not, they may lack the knowledge, resources, or motivation to stay ahead of evolving risks.

Schedule Your Free Cyber Security Risk Assessment Today!

Visit www.systemsupport.com or call our office at 781-837-0069.

Common Challenges IT Providers Face in the Cannabis Industry

1. Lack of Specialized Expertise:

Many IT providers are generalists who don't understand the cannabis industry's complex regulatory environment. From compliance tracking to POS vulnerabilities, they may not know how to safeguard the unique aspects of your business.

2. Outdated Solutions:

The tools and systems that worked last year might be obsolete today. Cybercriminals constantly adapt, and so should your defenses. Yet, many IT providers fail to recommend updated tools like advanced endpoint protection or dark-web monitoring.

3. Resistance to Change:

Upgrading cybersecurity measures often comes with costs, and some IT firms hesitate to recommend new solutions. But their reluctance could leave your cannabis operation exposed to devastating breaches.

4. Lack of Proactivity:

The cannabis industry operates in a fast-moving and highly targeted landscape. If your IT provider isn't monitoring for threats daily, auditing firewalls, or updating security protocols proactively, they're leaving you vulnerable.

The Cannabis Industry's Unique Cybersecurity Risks

1. Compliance Challenges

Cannabis businesses are held to strict compliance standards, especially for seed-to-sale tracking. A data breach could result in regulatory fines, loss of license, and severe reputational damage. Even minor non-compliance can lead to costly penalties.

2. Point-of-Sale Vulnerabilities

Your POS systems are prime targets for cybercriminals. Hackers can exploit these systems to steal customer data or disrupt operations, leaving you unable to process transactions or meet compliance requirements.

3. Insider Threats

Disgruntled employees or careless vendors pose significant risks. Former staff with access to sensitive systems can steal or delete critical data, while vendors without robust cybersecurity protocols could expose your business to fraud.

4. Limited Access to Financial Protections

The cannabis industry's reliance on alternative banking solutions increases exposure to fraud and financial exploitation. Hackers can manipulate transactions, drain accounts, or exploit gaps in vendor security.

5. High-Value Targets

Cannabis businesses are attractive to cybercriminals due to their reliance on technology, high-value inventory, and sensitive customer data. Without proper safeguards, you're an easy target.

Phone: 781-734-7261 *www.systemsupport.com* *462 Plain Street, Suite 206, Marshfield, MA 02050*

Is Your IT Provider Keeping Up?

- Have they conducted a comprehensive risk assessment in the past year?
- Are they proactively monitoring and patching your systems for vulnerabilities?
- Are you getting monthly reports about your network security?
- Have they implemented advanced cybersecurity tools, such as dark-web monitoring or multi-factor authentication?
- Are they training your employees on cybersecurity best practices and phishing prevention?
- Do they have a ransomware-proof backup system in place?

DON'T WAIT UNTIL IT'S TOO LATE

The cost of a breach—financial, reputational, and operational—can be catastrophic for cannabis businesses. From downtime and fines to the loss of customer trust, the risks are too great to ignore.

Take control of your cybersecurity now. Ensure your IT provider understands the unique challenges of the cannabis industry and is equipped to keep you safe and compliant.

Schedule Your Free Cyber Security Risk Assessment Today!
Visit www.systemsupport.com or call our office at 781-837-0069.

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

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

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

You want a qualified "Sherlock Holmes" investigating on YOUR behalf who is not trying to cover up inadequacies or make excuses, bringing to you a confidential report you can use before others find dirty laundry and air it in harmful ways.

Our Free Cybersecurity Risk Assessment Will Give You The Answers You Want, The Certainty You Need
For a limited time, we are offering a Free Cybersecurity Risk Assessment to a select group of cannabis businesses. This is entirely free and without obligation. EVERYTHING WE FIND AND DISCUSS WILL BE STRICTLY CONFIDENTIAL.

This assessment will provide verification from a qualified third party on whether or not your current I.T. company is doing everything they should to keep your 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 conduct a non-invasive, CONFIDENTIAL investigation of your computer network, backups, and security protocols. Your current I.T. company 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 go over our Report of Findings.

When This Risk Assessment Is Complete, You Will Know:

- If you and your employees' login credentials are being sold on the dark web. We will run a scan on your company, 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 I.T. 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 99% of the networks we've reviewed, owners were shocked to learn their backup 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 I.T. systems, backups, and endpoint protections meet compliance requirements and use best practices to ensure documentation is ready for audits.

If we DO find problems—overlooked security loopholes, inadequate backups, compromised credentials, out-of-date firewall and anti-virus software, or (often) active malware—we will propose an Action Plan to remediate the situation that you can have us implement if you choose.

Again, EVERYTHING WE DISCUSS AND DISCOVER WILL BE STRICTLY CONFIDENTIAL.

WHY FREE?

Frankly, we want the opportunity to be your I.T. company. We know we are the most competent, responsive, and trusted I.T. services provider to cannabis businesses in the region.

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 I.T. 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 I.T. 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 I.T. company if the information we share makes sense and you want to move forward. No hard sell. No gimmicks. No tricks.

Don't Leave Your Business to Chance

You've spent countless hours growing your cannabis business, navigating regulations, and building trust with your customers. Don't let cybercriminals or internal threats undo all your hard work. The risks are real, and the costs of inaction are too high to ignore.
Take a hard look at how you're running your cybersecurity. Are you truly protected? Schedule your Free Cybersecurity Risk Assessment today. The future of your business depends on it.

We know your time is valuable, and it might be tempting to set this aside, deal with it "later," or assume it doesn't apply to your business. But remember: the easy path is rarely the safest or the smartest choice.

Here's a hard truth: at some point, your business will face a cybersecurity threat. If you've taken the right steps, the impact could be minimal—just a brief inconvenience. But if you neglect to act now, the fallout could be devastating, costing you time, money, and your reputation.

You've worked tirelessly to build your business into what it is today. Don't let cybercriminals—operating outside the law and beyond your control—undermine everything you've achieved. And don't rely on blind faith that your current IT provider has all the bases covered. Hope is not a strategy.

Arm yourself with the facts and ensure your business is truly protected.

Contact us today to schedule your free, confidential Cybersecurity Risk Assessment.

Don't Ignore This Critical Call to Action

SCHEDULE YOUR FREE CYBER RISK ASSESSMENT TODAY!

Visit www.systemsupport.com or call our office at 781-837-0069.

Systems Support
IT Support & Service Since 1989

Phone: 781-734-7261
www.systemsupport.com
462 Plain Street, Suite 206
Marshfield, MA 02050

THE CANNABIS CRISIS