IT4CANNABIS INSIGHTS

IT4cannabis

IT4CANNABIS.COM VOLUME 1

Understanding Cannabis Cybersecurity

With the recent legalizations of recreational marijuana in New Jersey and New York, the cannabis industry is poised to grow quickly. For the most part, this is excellent news.

However, as the industry grows, so too do opportunities for cyber criminals. Cannabis firms, like many small businesses, are vulnerable to cyber-attack because they lack experience in cyber-defense as well as the resources to mitigate risk.

Cannabis is a unique industry. Though the product itself has been around for 5,000 years, only recently has it started to become legal and regulated. This leaves few in the cannabis space with the experience other firms may have in setting up an IT infrastructure or a cybersecurity plan. As a result, we've already begun to see cannabis-focused attacks in States where it has been legalized.

Cannabis firms, however, do have one major IT advantage more established companies may not have: they are not stuck building their businesses on top of legacy technologies and procedures. This presents both a challenge and an opportunity for cannabusiness owners. If they can prioritize setting up a robust cyber posture, they will find themselves better able to manage the challenges they will encounter as their businesses grow.

Top Cyber Risks for Cannabusinesses

Understanding the risk areas your cannabusiness can face is the first step towards protecting what you are working so hard to build. You need to know hackers typically target three areas within the seed-to-sale lifecycle:

Cultivation. Significant intellectual property (IP) can be found in the cultivation step. Hackers are after intellectual property such as strain data and technology practices. Lose either of these to cyber criminals and it could be the end of your business.

Cannabis payment systems. Cannabusinesses are reliant on third party payment systems since they cannot use the federal banking system. Most of these applications have not been designed with security in mind. As a result, they provide a large attack surface for would-be hackers who can steal funds and then infiltrate the payment system and work their way into compromising the cultivator's IP.

Medical and customer information. Medical information and Protected Health Information (PHI) are tempting targets for attackers and potential clients are going to want to know that you are keeping their data safe.

The Top Threat: Phishing

Like other small and mid-sized businesses (SMBs), cannabusinesses can fall prey to hackers employing phishing campaigns. Phishing is defined as 'the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.'
Annoying on its own, phishing poses a unique threat to businesses of all sizes because it serves as a vehicle of attack for more serious cyber-crime such as ransomware.

According to the 2020 Verizon Data Breach Investigations Report, phishing has led the way as the preferred method of attack since the end of 2018. This is not surprising. Phishing is low cost to execute and possibly high reward, depending on who the phish might be able to fool.

It makes sense that as logical controls such as firewalls, VPNs, and other IT defenses become more sophisticated, attackers seek to exploit the infrastructure's most vulnerable point of entry: the users themselves

Take Prudent Steps to Protect Your Business

There is one simple fact of life when it comes to cybersecurity: prevention is always more cost-effective than recovery. There are several steps you can take to prevent or mitigate cyber-attacks on your cannabusiness:

Start from the ground up
As mentioned previously, your cannabis company is likely not encumbered by legacy software and processes. As a result, cybersecurity software and processes do not need to be stacked on or integrated into an existing set of operations. Rather, they can be 'baked into' your company at an early stage. This will make the inevitable need to scale up cybersecurity operations within your company much easier.

Therefore, now is a good time to consider how you want your company's back-end IT infrastructure to look, rather than just letting it develop on an "as needed" basis. Based on your business model you may want to consider Implementing a cloud or Software as a Service (SaaS) in the early stages of growth. This can provide more flexibility as your company grows. The key here is having a good roadmap of where you want your company to go and then figuring out how various technology investments such as Point of Sales (PoS) or Enterprise Resources Planning (ERP) systems can get you there.

Inventory your technology assets
This is also a good time to inventory your IT assets to allow for a more robust IT security posture down the road. There are companies that have been around for decades that still do not have a handle on what equipment they actually have on hand. In this regard, the cannabis industry has an advantage.

Educate your employees
Instituting a phishing awareness campaign for your employees so they can build their awareness about potential threat vectors and thereby reduce your company's vulnerability to data breaches.

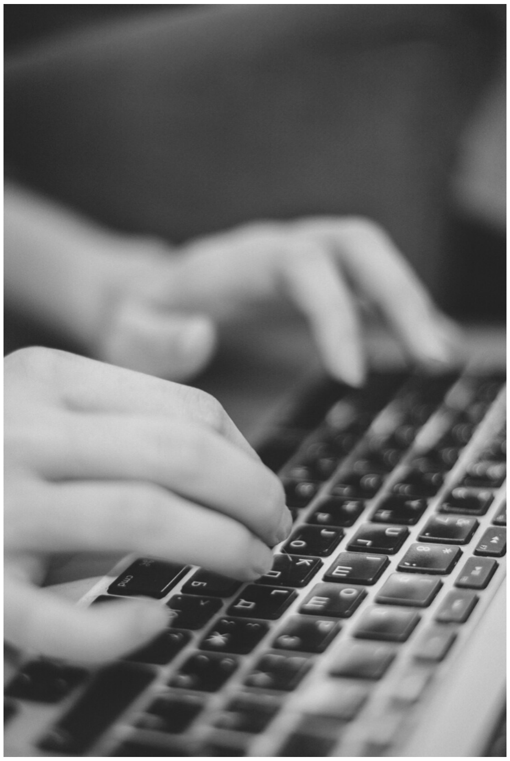
Back up your data
As a small firm, you need not pay for expensive, real-time data replication. A simple and cost-effective offsite backup can go a long way towards mitigating the effects of a ransomware attack. Sure, it might take longer to restore your data in the event of an emergency, but a slow restoration is better than none at all.

Establish your formal IT policies now
As your firm grows, you may be asked to provide proof of your company's dedication to IT Security. A way to establish this early is to formalize your written procedures for handling, storing, and backing up your data.
It is also prudent to establish a formal policy outlining which devices can use your company data. As a small firm, you may not yet have 'company owned' devices, but establishing an early policy for which devices can manage your data will go a long way toward showing your clients your firm is aware of and properly managing its IT security.

Connect with a trusted IT advisor
No doubt you and your employees are wearing many hats – development, sales, customer service, finance, etc., etc. – and cybersecurity and IT infrastructure can end up at the bottom of your To-Do list. By establishing a relationship with an experienced and trustworthy Managed Services Provider (MSP), you can focus on your business and let them monitor your environment for threats.

Discover your IT system vulnerabilities before cyber criminals do

At IT4cannabis, we know that technology is in every stage of your cannabis company's growth – and it needs to be managed and secured effectively. Take our no-cost Discovery assessment and get a comprehensive view of your current vulnerabilities – not just in your organization's IT network but across your entire business. It's time to understand cannabis cybersecurity before your business goes up in smoke.



"Understanding the cyber risks your cannabusiness can face is the first step towards protecting what you are working so hard to build."

MEET THE AUTHORS

Karl Kispert, President & CEO IT4cannabis and Infoaxis, Inc., focuses on cybersecurity, managed services, and cloud transformation for clients in the cannabis, manufacturing, retail, law, medical, and financial service industries.
Reach Karl at:
201.316.1566 or
kkispert@it4cannabis.com

Joshua Silberman, CISSP, CCSP, CISA, is a cybersecurity leader responsible for the direction, design, and development of cloud transformation and cybersecurity at IT4cannabis.
Reach Joshua at
201.316.1523 or
jsilberman@infoaxis.com

Get started on the path to better security with a no-cost Discovery Assessment.

www.it4cannabis.com/cybersecurity-assessment