Growing Cyber Threats Against Cannabis Retailers

FOREWORD

It may seem ironic that a retired FBI special agent who led numerous drug trafficking investigations is now helping legitimate businesses in the cannabis industry defend themselves against cybercriminals. However, continuing the mission to protect and serve is never more natural – or needed – than in today's world where cybercrime can harm so many people in so many ways.

In the midst of ongoing debate around the legalization of marijuana, a clear trend toward regulated acceptance has emerged in the United States and Canada. As of July 2019, the sale of marijuana for medicinal purposes is legal in 34 U.S. states, 10 of which also allow sales for recreational use through state-licensed dispensaries. In January, 2020, Illinois will become the 11th U.S. state to legalize the sale of marijuana for recreational purposes. Operating in an unusual federal legislative environment where the cannabis industry is still entirely illegal, legitimate cannabis enterprises have all the responsibilities of a traditional business. In Canada, recreational cannabis is legal federally. Each province and territory governs how cannabis can be sold, where stores may be located and how stores must be operated. Provinces and territories are also given the freedom to lower the federal possession limit, increase the minimum federal age, restrict where cannabis may be used in public and add requirements surrounding personal cultivation.

While they share with all retailers the duty to protect customer data and financial records, cannabis businesses must acknowledge a heightened state of sensitivity around privacy issues. For example, one of the topics covered in this report is how cybercriminals in possession of cannabis customer names may threaten to extort these customers by publicizing their purchases.

I invite you to read about the current state of cyber threats and how legitimate cannabis retailers can bolster their cyber security maturity. In particular, the section outlining the "Three Pillars of Cyber Security" offers pragmatic guidance validated by Kroll practitioners with frontline cyber investigations insight.

Given the evolving and still contentious nature of marijuana sales in certain areas – and the fact that new cyber exploits and threats arise every day – we hope cannabis retailers recognize that fighting their industry-specific cyber threats is not a "one and done" exercise. This white paper offers a starting point. Vigilance and resiliency will be key for protecting your business and your customers from cyber threats today and into the future. You can count on Kroll to help with the most preeminent experts in the field, global resources and practical solutions to your cyber risk challenges.

Matthew Dunn
Associate Managing Director, Cyber Risk
Kroll, a division of Duff & Phelps

INTRODUCTION

Retailers have long been favorite targets of cybercriminals, and today's burgeoning cannabis retail industry is not immune. In fact, for several reasons, cannabis dispensaries are ripe for crippling cyberattacks.

Across the retail landscape, cybercriminals are looking for the same payday in their assaults: sensitive and valuable data such as credit card information, personally identifiable information (PII) and even trade secrets and/or intellectual property. Cannabis retailers are particularly attractive targets not only for the coveted customer data they hold; cybercriminals are always on the lookout for businesses operating in a young and rapidly growing industry, like the cannabis sector, where many retailers have not incorporated mature cyber security practices into their business processes.

> A study conducted by IBM and the Ponemon Institute in July 2018 determined the global average cost of a data breach to exceed $3 million.

For a cannabis retailer, the financial losses associated with a data breach, especially for a smaller operation, can be devastating. A study conducted by IBM and the Ponemon Institute in July 2018 determined the global average cost of a data breach to exceed $3 million. This figure factored in costs for remediation, notification and credit monitoring, which are mandatory components of data breach response in most states. According to the U.S. National Cyber Security Alliance, 60% of small businesses that have suffered a data breach have gone out of business within six months.

A public perception of weak cyber security can also severely shake consumer confidence and negatively affect a company's future sales and growth. A February 2019 survey of Americans found that after a retailer's data breach, a significant number of people across all age ranges are not likely to shop again at that store: 40% of Gen X (ages 40-54) are least likely, followed by 26% of millennials (ages 23-38) and 34% of baby boomers. Customers may understandably be extremely reluctant to provide their personal information when purchasing marijuana from a retail dispensary whose network was previously compromised due to an immature cyber security strategy

CURRENT CYBERCRIMES TARGETING THE CANNABIS INDUSTRY

The vast majority of cyber compromises today result from attacks targeting "the people at the keyboards," i.e., employees, contractors and third parties with access to a company's network. Employees of cannabis retailers are prime targets for cyberattacks aimed at stealing or compromising their credentials. Once criminals are in, they conduct reconnaissance and identify databases which contain sensitive information that can be monetized through a variety of fraudulent activities or simply sold to other criminals operating on dark web forums.

While the theft of sensitive data is a security concern for any retailer, cannabis businesses face a compounded threat due to the commodity they sell. This threat increases for medicinal marijuana dispensaries, which maintain protected health information (PHI), as those types of records are much more valuable on dark web forums than common PII due to the additional information they contain. Although medicinal marijuana dispensaries are not covered entities under the Health Insurance Portability and Accountability Act (HIPAA), which would restrict how they are able to utilize patient data, they must still comply with strict state privacy laws. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) applies to all personal data, health or otherwise. Provinces and territories have the right to create their own rules and regulations as long as they are "substantially similar" to PIPEDA.

Email-Based Attacks

Cannabis industry employees need to be cognizant and on alert for attacks being deployed every day through emails with malicious software embedded in hyperlinks or attachments. Today's phishing emails are very convincing and often the product of a previous compromise of a co-worker, customer, vendor, business partner or just someone the recipient trusts. These emails no longer notify recipients that they've inherited millions of dollars from a Nigerian prince. Instead, modern hackers leverage publicly available information to conduct research on businesses and their employees, then send extremely credible emails to employees. Believing the emails were sent from a trusted source, unsuspecting victims end up clicking on links or opening attachments that download malware such as ransomware, banking trojans, keystroke loggers, point of sale (POS) malware, etc.

In recent months, numerous retailers have had their networks compromised after receiving an email purchase request contained in a Word document. Unsuspecting employees who try to access the information in the Word document are immediately advised to upload the latest version of the software and download macros to view the document. Once downloaded, the purported macros execute embedded malware that enables hackers to move laterally throughout the victim network, searching for sensitive data.

All businesses are susceptible to this kind of cyberattack, but companies just starting out with a relatively new workforce, which characterizes many marijuana retailers today, face a higher risk.

> Cannabis dispensaries are especially vulnerable because they deal in a commodity whose use remains contentious despite marijuana's legalization in the states where it is sold.

Ransomware Attacks

Ransomware continues to be a favorite of cyberattackers. Ransomware attacks are more sophisticated than the cyber "smash and grabs" that I witnessed during my days as a Special Agent with the FBI. Those attacks targeted small companies and individuals and sought to encrypt data (files and photos) on personal devices. Victims were forced to pay $300-$500 in Bitcoin or other cryptocurrency to obtain a decryption key and regain access to their files.

Ransomware has evolved to the point where it is usually delivered after cybercriminals have already infected corporate networks with a trojan such as Emotet, Trickbot, Bokbot, Dridex, Qakbot, etc. After these trojans are embedded in a corporate network and cybercriminals learn how the network is configured, they then deploy a variant of ransomware simultaneously across the network, effectively shutting down the business. These trojans are usually delivered by an end-user clicking on a link or opening a malicious attachment in an email. I cannot overemphasize how education and vigilance regarding email practices is crucial for preventing ransomware attacks.

Video Surveillance and the Internet of Things

All states that have legalized marijuana sales require retailers to incorporate video surveillance in their facilities as a mandatory security feature. The retention period to maintain this video data ranges from 90 days to one year, depending upon the state. Having your image recorded and stored while you shop for marijuana raises major privacy issues, but the cyber security risks for potential extortion raises the stakes for cannabis retailers.

CYBER EXTORTION

While the above-referenced cybercrimes are commonly used to target retailers, cannabis dispensaries are especially vulnerable because they deal in a commodity whose use remains contentious despite marijuana's legalization in the states where it is sold. Cyber extortionists are constantly trying to get access to sensitive data that they can use to threaten victims with exposure if a demand (usually paid in cryptocurrency) is not met.

Cybercriminals that gain access to a marijuana dispensary's client database could attempt to extort high-profile customers, like politicians, business executives, professional athletes, entertainers, clergy, etc., who may not want the public to know that they are using marijuana, even if it is legal. This unexpected negative exposure could potentially threaten clients' livelihoods. Cannabis retailers must consider the additional privacy customers expect when they provide their personal data to a dispensary to conduct a transaction.

Another concern for marijuana retailers is their higher-than-average potential to become targeted by nation-state actors. Over the years, nation-state actors have aimed at everything from government databases and cleared defense contractors to insurance and healthcare companies. Nation-state actors conduct their attacks for intelligence-gathering purposes. Whether the goal is to steal intellectual property from a cleared defense contractor or to gather information on government employees for potential recruitment activities, these large data breaches result in a treasure trove of information for the intelligence services of U.S. adversaries. The marijuana industry's controversial commodity places it at higher risk for intelligence-gathering and potential co-opting/recruitment activities.

Many retailers now use video surveillance equipment that is accessible through the internet. While these Internet of Things (IoT) devices offer the convenience and flexibility of remote access and monitoring, the security risks associated with these devices are often overlooked. For example, many of these devices are accessed using default passwords, i.e., the password provided by the manufacturer. These passwords are often universal, easy to guess or even posted on the manufacturer's website to help users set up a device. Other risks arise from the habit of people using the same password to access multiple databases/platforms or from accessing the device from an unsecure or compromised network.

Cannabis retailers should consider these vulnerabilities when connecting devices to their network. If security measures such as VPN, multi-factor authentication, segmentation and the policy of least privilege are not implemented to limit access to the video (including storage and transfers to backups), then cannabis retailers should understand they are at greater risk for this data to be compromised and monetized by cybercriminals.

There are additional IoT risks for cannabis retailers that grow and cultivate plants. Many grow operations utilize automated, internet-accessible watering, temperature and humidity control systems and lighting programs. The same IoT vulnerabilities that accompany video surveillance exist with these systems. For example, if a competitor were able to access these environmental systems through weak cyber security measures, they could overwater, create cold temperatures or turn off lights that could effectively cause a crop failure.

Cash-Based and Nontraditional Financial Transactions

As most U.S. banks are federally regulated institutions, the Federal Deposit Insurance Act prohibits them from conducting transactions related to federally prohibited activities. While marijuana has been legalized in Canada and in most U.S. states, it is still classified as an illegal Schedule I

drug under the U.S. federal Controlled Substances Act. Until it is recognized as a legal commodity under federal law, credit cards or debit cards linked to a credit account cannot be used as acceptable forms of payment at marijuana dispensaries. Banks are unwilling to risk violating federal anti-money laundering laws by financing cannabis businesses or supporting these financial transactions for their customers. This presents obvious physical threats to cannabis businesses that are consequently predominantly cash-only transaction facilities.

To mitigate the risk of harm to employees and customers from potential thieves, cannabis retailers are exploring alternatives to pure cash transactions. Several purchasing options have become available through online payment systems such as payment cards connected to specific cannabis mobile apps, private banks (not federally regulated), marijuana-specific POS systems and cryptocurrencies. While these options may reduce the physical threats created by having exorbitant amounts of cash at retail premises, the risk of theft by cyber tactics must be considered. The storage of customers' sensitive data through online transactions or in-store electronic transactions puts additional responsibilities on retailers to protect that data and process it safely.

This is especially true for businesses that grant access to their network to third-party vendors when processing transactions. Cannabis dispensaries should implement measures to encrypt their customers' data and segment their processing systems from their network wherever possible. If a cannabis dispensary is going to accept cryptocurrency payments, it should secure its cryptocurrency wallet against cyber theft through basic security strategies such as encrypting private keys and utilizing an external (hard token) cryptocurrency wallet.

Digital Marketing Vulnerabilities

While the cannabis industry has its own unique regulations, dispensaries are similar to other retailers in that they need to provide good customer service while continuing to generate future revenue. Like many retailers, dispensaries rely on marketing techniques to develop and grow their customer base. Knowing a client's preferences and anticipating their shopping and spending habits can significantly factor into good marketing strategies. Many cannabis dispensaries aim to anticipate how much and how often a customer will purchase their product and also how to provide current and future clients with information regarding new products or special offerings. To successfully employ these types of marketing techniques, cannabis dispensaries need to acquire and maintain personal information that includes names, addresses, telephone numbers and email addresses.

Legislation in all "cannabis legal" states requires customers to provide a government-issued identification to prove they are of the legal minimum age to purchase marijuana. To facilitate this process for returning customers, many dispensaries maintain customers' proof of age in their databases. Although various U.S. laws restrict how long dispensaries can maintain and utilize this type of sensitive data and PIPEDA strongly suggests appropriate retention periods, the mere fact that it does exist on a database for any given time presents a risk of exposure to attack by cybercriminals.

CREATING A STRONG CYBER SECURITY STRATEGY

A strong cyber security strategy is built on a foundation of knowing the specific threats your industry faces and what critical business data is being maintained on your network. A risk assessment conducted by independent cyber security experts can identify (1) the various measures that need to be in place to satisfy the three pillars of cyber security discussed below and (2) the pragmatic steps that can mitigate any identified vulnerabilities. Penetration tests and vulnerability scans can also provide valuable insight into network weaknesses just waiting to be exploited by cybercriminals.

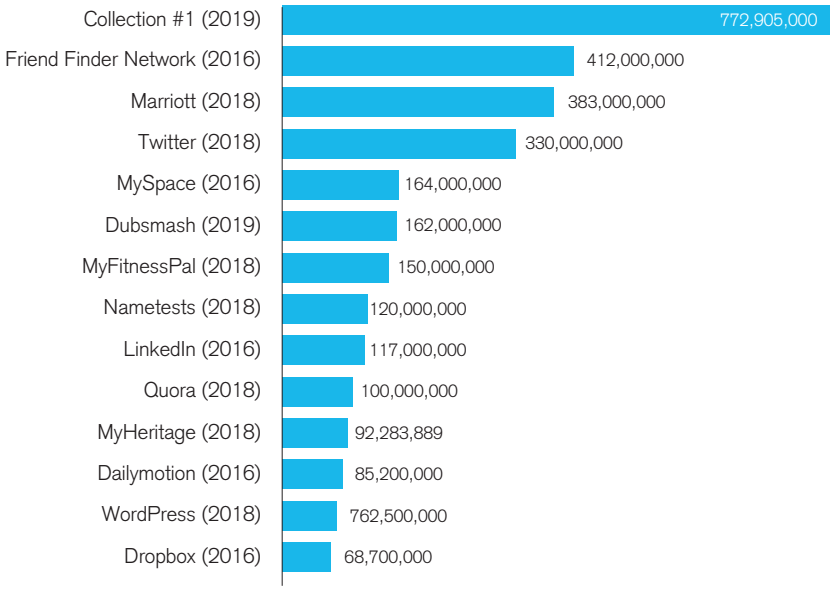
THE THREE PILLARS OF CYBER SECURITY

What steps should a retailer in the cannabis industry take to build a strong cyber security strategy that gives customers peace of mind that their sensitive and personal data is being protected? By developing a strategy based on the three pillars of cyber security — **People, Policies and Technology** — cannabis businesses will be in a much better position to reduce their vulnerabilities and mitigate the various threats targeting their networks.

As previously stated, end-users are the primary vector for cyberattacks. However, employees can also be your first line of defense if properly trained. Marijuana retailers must educate their employees on current trends of attacks that cybercriminals use to compromise accounts, leading to exposure of sensitive data. Some best practices include the following:

- Implement a security awareness training program and deliver training to all employees, especially senior management, as many of today's cyber scams target executive-level employees.
- Build training programs that include phishing and social engineering tests that expose employees to the types of scams favored by cybercriminals; highlight the damage that could result to a business if these types of attacks go unrecognized as attempts to compromise the network.

EMAIL & PASSWORD BREACHES



Number of Compromised Accounts (millions)

Many of today's cybercrimes are successful not because malware or code injection attacks are so sophisticated, but rather because mature cyber security policies are absent or security processes are not being followed. Cybercriminals target companies every day, and marijuana retailers possess valuable information that criminals would love to access. To build a mature cyber security strategy, one needs to develop or revise security policies to mitigate prevailing cyber threats. Here are some policy/process suggestions:

- **Password Policy:** Credential theft and password reuse are some of the most common avenues that cybercriminals leverage to get access to a victim's network. Due to the sheer volume of data breaches over the years, there are now literally billions of stolen emails and passwords being traded on dark web forums.
- **Multi-Factor Authentication (MFA):** Access requests should be authenticated through methods such as SMS, push-notification or hard token. MFA is especially critical when accessing VPN, email and any database containing sensitive data.
- **Acceptable Use Policy:** Restrict employees' access to freely surf the internet and visit suspicious websites, which can pose a risk for infecting your network from a "drive-by" malware attack (i.e., downloading a website that has been compromised with embedded malware).
- **Least Privilege Policy:** Only provide your employees with access to the platforms and databases on your network that they need to perform their responsibilities. Restrict administrative rights to only those who absolutely need it and require privileged users to utilize a separate 'admin' account when they need to perform administrative functions. This type of role-based authorization may reduce the level of exposure to sensitive data if an account with limited access is compromised.
- **Encryption Policy:** Encryption is a great means to protect confidential or sensitive information from being accessed by cybercriminals. States that have legalized cannabis for medicinal

purposes require the use of encryption when dispensaries report transactions from patients to appropriate state health or cannabis commissions ((similar to HIPAA and PIPEDA requirements). Individuals who are authorized to receive medicinal marijuana are issued state medical cards that are entered into a database shared by dispensaries. The database provides the authorized quantity of medicinal marijuana that can be sold to a patient, similar to other prescription medications.

Although there is no regulation regarding the tracking of individuals purchasing marijuana for recreational purposes, dispensaries are required to send electronic notification of the RFID codes of the marijuana product sold to comply with "Seed to Sale" regulations. Most states limit the quantity of recreational marijuana that can be purchased/possessed by an individual at one time. However, there are no central databases to document this information that would alert a dispensary that a customer had already exceeded his/her daily purchase limit. This type of tracking/enforcement concept is being discussed in various state legislatures where cannabis has been legalized.

PASSWORD MUSTS

Minimum 15-character password or passphrase

Mandatory upper- and lower-case letters, numbers and special symbols

No dictionary words

Change passwords every 90 days

Different passwords for critical accounts

Use multi-factor authentication in conjunction with strong passwords

Marijuana retailers should establish a policy that requires the encryption of any sensitive data maintained on their network or data stored in temporary memory files (susceptible to memory scraper malware). An encryption policy would facilitate future compliance with any tracking/enforcement legislation, as well as provide a layer of security to protect sensitive customer data from cybercriminals.

- **Bring Your Own Device (BYOD) Policy:** With so many employees now working remotely, whether on a full- or part-time basis, employees often use their own devices to log into the corporate network to conduct their work. A lack of a restricted BYOD policy can result in employees infecting the corporate network with malware contained on their personal devices. A solution to this added risk would be to enforce the use of a VPN when connecting to a corporate network.
- **Incident Response Plan (IRP):** Because we exist in a world of "assumed breach", it is important that every cannabis dispensary have an Incident Response Plan (IRP). At a minimum, the IRP should define what constitutes a cyber "incident" and identifies the members of the Incident Response Team as well as their assigned roles and responsibilities when dealing with an incident. Once a comprehensive IRP is established, an annual table-top exercise, facilitated by independent cyber experts, should be conducted to enable the Incident Response Team to practice how they would respond to a cyber incident in accordance with the plan.

Many effective technical solutions exist that can help organizations, including cannabis retailers, protect their networks and alert responders to suspicious activity that is either attempting to take hold or already executing on their network. Some of these essential tools and best practices include, but are not limited to, the following:

- **System Hardening** – Implementation of configuration changes to enhance security by eliminating potential attack vectors.
- **Patch Management** – Ongoing installation of security updates for hardware and software assets.
- **Firewall** – Device to manage access to an organization's network.
- **Intrusion Detection System (IDS)** – Device to monitor a network for malicious activity or policy violations.
- **Endpoint Detection and Response (EDR)** – Solution to monitor processes on network computer endpoints for suspicious or malicious activity.
- **Data Loss Prevention (DLP)** – Solution to monitor, detect and block sensitive data in use, in transit or at rest in order to prevent data leakage.
- **Mobile Device Management (MDM)** – Solution to monitor, manage and secure employee mobile devices.
- **Dark Web Monitoring** – Solution to search the dark web for personal information, stolen credentials, intellectual property, etc.
- **Third Party Risk Assessment** – Solution to assess the security program maturity for third party organizations that access or store data on an organization's behalf.

CONCLUSION

Regardless of the commodity, retailers are trusted to handle and store their customers' sensitive data in a manner that will protect it from being compromised by cybercriminals. Cannabis dispensaries must recognize that they are not immune from being targeted by cybercriminals; in fact, they are at greater risk than most because of the controversial commodity they deal in. For cannabis dispensaries, developing a mature cyber security strategy is imperative in order to combat daily cyberattacks.

As of July 2019, recreational cannabis in Canada is legal federally. Across the border, 34 U.S. states authorize the sale of marijuana for medicinal purposes, 10 of which also allow its sale for recreational use, all through state-licensed dispensaries. Meanwhile, legalization proposals continue to be debated or advanced in many of the remaining states.

The best practices described in this report can help existing and prospective marijuana retailers become better equipped to identify vulnerabilities and implement the necessary measures to mitigate cyber threats. They also provide cannabis businesses the framework to develop a mature cyber security strategy that protects the data in their network and enables a business to thrive while providing customers a sense of security when they share their sensitive, personal information.

EMPOWERING CANNABIS INVESTORS AND ENTREPRENEURS TO MAKE CONFIDENT DECISIONS

- Cyber Risk Management
- Security Risk Management
- Due Diligence
- Valuations
- Corporate Finance and M&A
- Fraud and Corruption Investigations

Kroll | A Division of DUFF & PHELPS

CONTACTS

Matthew Dunn is an associate managing director in Kroll's Cyber Risk practice, based in Nashville. Matt serves Kroll's clients with an exceptional combination of professional experiences garnered in his decades of service with the Federal Bureau of Investigation as well as in the practice of law handling litigation matters in both federal agency and private practice contexts. While with the FBI, many of Matt's assignments involved global investigations, which informs his perspective on cyber and other threats. **matthew.dunn@kroll.com | +1 615.483.6593**

About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security and data and information management services. For more information, visit www.kroll.com.

About Duff & Phelps

Kroll is a division of Duff & Phelps, a global advisor with nearly 3,500 professionals in 28 countries around the world. Our clients include publicly traded and privately held companies, law firms, government entities and investment organizations such as private equity firms and hedge funds. We also advise the world's leading standard-setting bodies on valuation and governance best practices. For more information, visit www.duffandphelps.com.