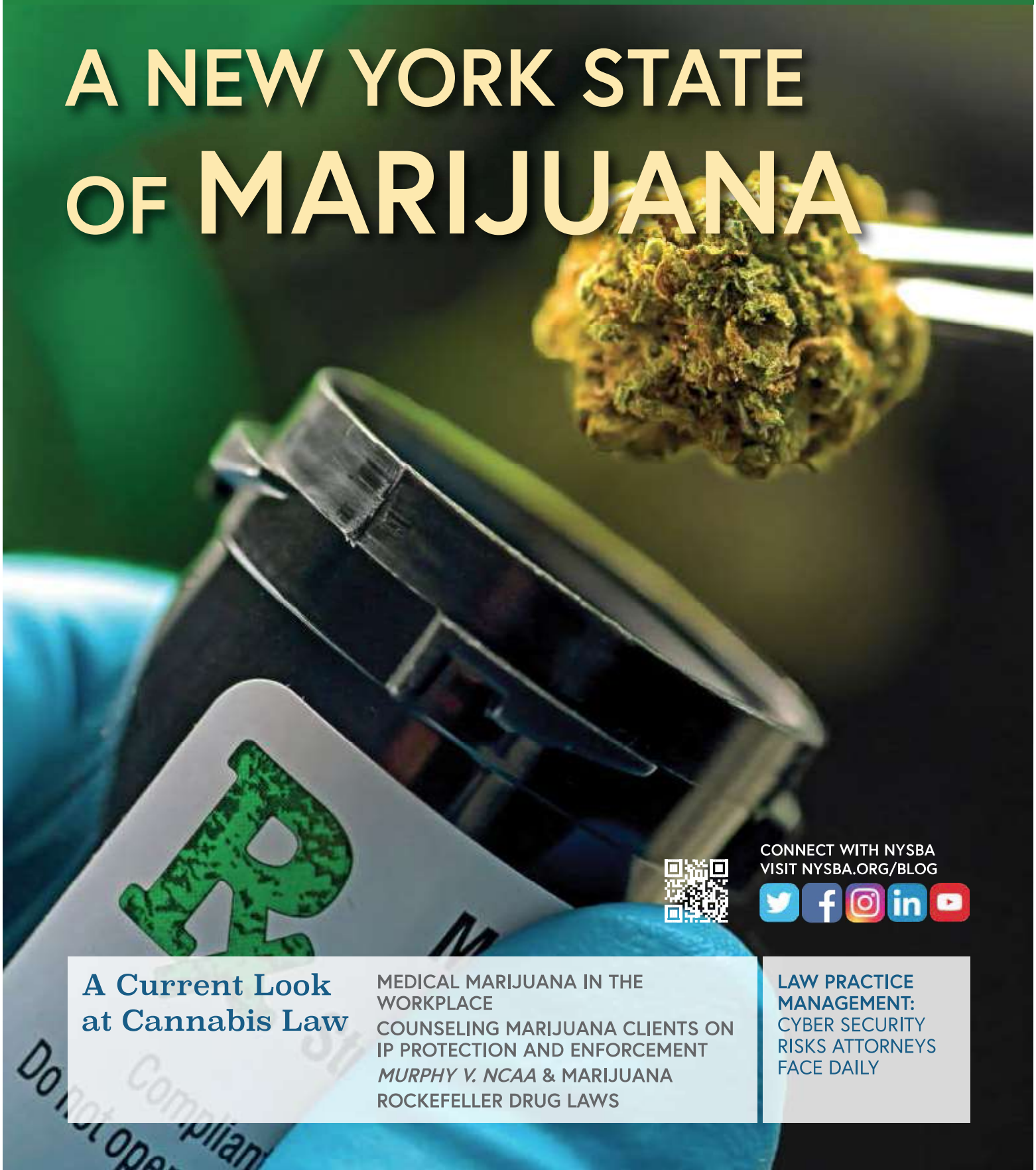
NEW YORK STATE BAR ASSOCIATION
Journal
NYSBA
JULY/AUGUST 2018
VOL. 90 | NO. 6

A NEW YORK STATE OF MARIJUANA



CONNECT WITH NYSBA
VISIT NYSBA.ORG/BLOG

A Current Look at Cannabis Law

MEDICAL MARIJUANA IN THE WORKPLACE
COUNSELING MARIJUANA CLIENTS ON IP PROTECTION AND ENFORCEMENT
MURPHY V. NCAA & MARIJUANA
ROCKEFELLER DRUG LAWS

LAW PRACTICE MANAGEMENT:
CYBER SECURITY RISKS ATTORNEYS FACE DAILY

A Day in the Life of an Attorney: The Cybersecurity, Technology, and Crime Risks We Face

By John Bandler

Attorneys face cybercrime threats every day that jeopardize our practice, clients, and family. This is true for solo practitioners and members of large firms, representing individuals or multi-national conglomerates, and in all practice areas. Knowledge, awareness, and effort are required to protect from cybercrime and fraud threats.

Let's review a day in the life of Lex, our fictional lawyer, to illustrate the threats to our professional and personal lives, and see how crime, cybersecurity, information security, technology, and safety are related and enmeshed in our lives.

THE DAY BEGINS

It is midnight so the calendar day has officially begun, but Lex and his family are asleep. His home is quiet, as is the neighborhood. Lex is an attorney in a small firm, handling many legal issues for his clients.

Elsewhere, the worldwide cybercrime economy is hard at work across every time zone. Some cybercriminals are awake and at work on their schemes. Others have set in motion computer programs to perform malicious work without ever needing rest – so called "bots." These cybercriminals collectively control an army of computers throughout the world, many of them infected with malware and transformed into malicious tools without their owners' knowledge.

One program is trying to gain access and compromise the administrator portals of millions of websites, one of which is LexLaw.com. First it tries to log in as user "admin," with a password of "admin," but access is denied because this is not the website's username and password. It tries a different guess, is denied, and the process continues.

A different program attempts to log into email accounts, including Lex's work and personal email accounts. Lex's passwords are long and complex, and are unlikely to be guessed by this program. He also uses two-factor authentication, which means that guessing the password is not enough – the hacker would need possession of Lex's smartphone to get the one-time code from his email provider.

A third bot has been scanning the internet looking for connected devices. It finds Lex's home internet connection, starts to communicate with his router, and tries to gain access. It goes through a list of default usernames and passwords (including username "admin" and password "admin") but is unsuccessful and keeps trying. It runs through a sequence of hacking attacks but that doesn't work either. Recently, Lex updated his router's firmware to patch it against these vulnerabilities, and he also rebooted it according to the FBI's May 2018 advisory, a step which could help ensure it is not infected by malware.

Lex's children are sleeping, their smartphones and laptops are off and charging in the living room. The children are frequently tempted to check their devices, but know this is not allowed at night. However, some of their classmates are still awake and communicating with each other by social media, text, and email. Some messages are funny and harmless, but some are cruel or inappropriate, and all of them are sacrificing rest and relaxation.

Nearby, someone is trying to gain access to Lex's Wi-Fi network through password guessing, and is also attempting to access the network administrator portal. Whether this person merely wants to borrow Lex's internet connection or do something nefarious is unknown, but fortunately the Wi-Fi password is long and complex, and the router is patched.

LEX WAKES UP

At 6 a.m. Lex's alarm rings and he is up before the family. He logs into his computer and then checks LinkedIn, which prompts him to boost his contacts. That sounds like a great idea, so he clicks the button to accept the suggestion, is prompted for a password so he enters his LinkedIn password, but gets an error message. By now he realizes that LinkedIn wants the password to his email account, which fortunately is different from his LinkedIn password. It would have been unfortunate to give LinkedIn access to his email account and its contents, and for automatic invitations to have been sent all over.

Lex reviews an email he drafted last night, summarizing legal options for a client. After some final touches it is ready to send so he types the first few letters of the client's name into the "To" field, then hits enter for the autocomplete function to fill in the address. He is about to hit "Send" when he takes a last look and realizes he is about to send it to the wrong person! That would have been disastrous, so he corrects the email address, takes another look to confirm, and then sends it on its way. He wonders if this day will be a continual test of his information security knowledge and awareness.

Lex gets ready, says goodbye to his spouse and children, starts the drive to the office and then receives a call from Janet, his client in a pending real estate transaction. She is buying a home and wants to know if there are any updates on the closing. Lex tells her the recently scheduled date, and they discuss the details.

> **Lex**: Janet, remember what I told you when you first retained me. Any payment instructions will be confirmed with a phone conversation between us. Any changes to those payment instructions will also be confirmed by phone.

Janet laughs and says she remembers his earlier warning about this fraud risk, sometimes known as "business email compromise" or "CEO fraud." She promises not to rely on an email, since emails can be hacked or spoofed.

Lex had conducted this call while keeping his hands free and ensuring sufficient attention is devoted to the dangerous task of driving the car. After they hang up, Lex feels his smartphone vibrating and is tempted to check it, but resists. The constant demands of technology upon our attention and concentration are a challenge, but he soon reaches his destination and checks his text and email messages.

He is representing a client in a contract dispute where the settlement offer was accepted and the attorney for the opposing party has now emailed payment instructions. He asks that Lex's client wire the funds as soon as possible to the account provided, and indicates he is unavailable to talk by phone. Lex is about to forward the instructions to his client, but decides to wait and verify the instructions. Soon, he is in his office and calls opposing counsel.

> **Lex**: Hi Michael, Lex here. I got your email, I just wanted to confirm a few things.
>
> **Michael**: Hi Lex, what email?
>
> **Lex**: The email you sent me with the bank wiring instructions.
>
> **Michael**: Impossible, I didn't send that. I am still waiting to hear back from my client.
>
> **Lex**: You didn't send me an email 15 minutes ago?
>
> **Michael**: No, I didn't send anything.

Clearly, something is not right. Someone has impersonated Michael and knew a lot about this pending transaction. Fortunately, Lex knows what to do, and the two discuss their next steps. (You can learn this too, in an upcoming NYSBA *Journal* article.)

Lex is meeting a colleague at a local coffee shop, gets there first, grabs a table by the window and checks his phone. He

John Bandler helps firms, businesses, and individuals with cybersecurity, crime prevention, and investigations. He is former prosecutor and police officer, and the author of the comprehensive book, "Cybersecurity for the Home and Office." You can find him online at: https://cybersecurityhomeandoffice.com or https://bandlerlaw.com. LinkedIn: www.linkedin.com/in/johnbandler.

is frustrated by the slowness of his cellular service and the shop offers free Wi-Fi, which Lex considers using. But then his imagination starts working; he wonders if another customer in the coffee shop might be a malicious hacker, and whether the coffee shop maintains their Wi-Fi network securely. Have they heeded the FBI advisory or patched their router? Lex knows that connecting to public Wi-Fi networks has risks, and decides that today it is not worth it.

Just then, he receives a text from Bill, who is on the way and asks that Lex get his coffee. Lex gets up, makes the purchase, and as he is returning to the table he panics. He realizes that he had left his cell phone on the table and his laptop in his bag under the table. As he walks back quickly he sees that his phone is no longer on the table, and his bag with the laptop is missing. His mind is racing because he is not sure if he locked the phone before he got up – maybe right now the thief is sifting through all of his emails and contacts? Then he looks to the side and sees Bill, staring at him with a mischievous smile while holding Lex's phone in one hand, and briefcase in the other.

> **Bill**: Hi there Lex, you look nervous! Don't you remember learning that the first principle of information security is maintaining physical security of your computers?

Bill is right; that was one of the many gems of knowledge contained in the book they both read, *Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security*." Bill absorbed all of the practical information in the book, and now re-reads it periodically to savor the mellifluous prose. (Remember, this article is a work of fiction, with occasional attempts at humor and shameless puffery.)

> **Lex**: Bill, you are right, but this has been a tough day for me. An hour ago, a fraudster tried to redirect a bank wire, and I almost forwarded those instructions to my client. Last night I had a dream about botnets and automated password attacks, and now you give me heart palpitations with this prank, after I bought your coffee.

Bill apologizes but Lex concedes it was a good lesson, and they both discuss the potential implications if Lex's smartphone or laptop were stolen. It affects all three of the main information security principles– confidentiality, integrity, and availability. What data could the thief have accessed? What if the thief could send emails from Lex's system, and alter data? How would Lex's access to his data be affected? They agree on the importance of keeping possession of one's devices, and locking them after use.

After they say goodbye, Lex gets a call from Sandra, who is in charge of training at his firm.

> **Sandra**: Hi Lex, how is your day going so far? Quick question. Is there a connection between attorney professional responsibility, cybersecurity, and technology?
>
> **Lex**: There certainly is! Think about the attorney duties of competence and confidentiality. See the NYS Rules of Professional Conduct and the ABA Model Rules, especially...
>
> **Sandra**: Do you know of any training that covers those?
>
> **Lex**: Yes, I saw a CLE on cybersecurity for lawyers. Protecting yourself, your clients, and your family from cybercrime, privacy, and fraud threats. It was fantastic. I got two ethics credits and knowledge which I am putting to use today.
>
> **Sandra**: Thanks. Send me the information and I'll check it out. Maybe we can do something for the firm. See you later.

Lex returns to the office until noon, then goes to his parents' house for their weekly lunch. As soon as he gets in the door he receives a text from a colleague about to send a letter but requesting a final review. Lex considers his options: His smartphone screen is tiny but his parents have a computer which is well maintained – thanks in part to Lex – so he decides it is safe enough to use for this purpose (unlike a computer in a library or hotel).

Lex launches the web browser in a "private" or "incognito" window so that the computer will not store too much information about his activity. He navigates to his law firm's web portal and enters his username and password, which is not enough to gain access because his firm has implemented multi-factor authentication. Lex is prompted for his one-time code, which he retrieves from his smartphone and types in. He has now proven to the system that he both *knows* his password and *possesses* his smartphone, providing two types of authentication, and the system grants him access. This greatly increases security over passwords alone, which can be guessed or stolen.

Lex accesses the document and reads it, then lets his colleague know that it is good. He "logs out" of his cloud account, then takes a quick look at his parents' computer to make sure it is running properly and safely. He runs a malware scan using reputable free software, and checks that the web browser is updated and not running any unnecessary plug-ins or extensions.

Lex's parents are not getting younger, and they face different cybersecurity and technology challenges compared to his children. It takes effort to ensure that his parents are able to use technology easily, safely, and while staying connected to friends, family, and the world. Pop-up messages, phishing emails, malware, scareware, and technical support scams make computing difficult for everyone, but are especially challenging for seniors. After lunch Lex returns to his office and starts going through his messages.

James, a potential client, has left a message to continue their discussion about his financial institution and the New York State Department of Financial Services regula-

tion called "Cybersecurity Requirements for Financial Services Companies." Lex calls him back and they talk.

> **James**: Lex, thanks for calling, I've got you on speakerphone and with me is Anthony, my general counsel. What do I need to do to comply with this regulation?
>
> **Lex**: We can help with that, but first we should evaluate your current information security program.
>
> **James**: I'd rather not get sidetracked with that, because I need to comply with this cybersecurity regulation, and yesterday. I say yesterday in a literal sense, because I must sign a document saying that I complied with the regulation for the past year.
>
> **Lex**: We should talk about that attestation later. But first we should see how your information security program aligns with what the regulation requires. The regulation is really about information security, not just cybersecurity.
>
> **Anthony**: Lex, let me interject because I don't agree. The regulation title says cybersecurity, and the text mentions cybersecurity throughout! Let me count it, 1, 2, 3 . . . [counting continues] . . . 73, 74, 75! Seventy-five mentions of "cybersecurity" and hardly a mention of "information security," except once in passing, and when spelling out "CISO." If New York State wanted to issue an information security regulation, that's what they would have called it, so we have to go by their original intent.
>
> **James**: Exactly. Besides, is "information security" really important? All I hear about in the news is "cybersecurity" and "cyber," so I think we should focus on that.

Lex explains that the rule addresses all aspects of information security, which encompasses cybersecurity, making the case that it is an information security regulation. Lex speculates why the term "cybersecurity" was used so much in the title and text of the regulation, and suggests that they think holistically under the ambit of "Cybersecurity and Information Security."

> **James**: That's very persuasive. Can you give us a quick and free information security lesson?
>
> **Lex**: Of course. For starters, think "CIA": confidentiality, integrity, and availability. Keep your data and systems *confidential* and from being hacked or stolen. Ensure they maintain *integrity*, that no one can alter or change information without authorization. And keep them *available*, so that operations can continue and are not subject to outages or disruption. That includes backing up your data.
>
> **James**: Wow, how did you learn all of that?
>
> **Lex**: I read a marvelous book about cybersecurity, and it helped me take charge of my information security and help my clients. I can come by, give you a copy, and we can get started on your issues. Are you free at nine tomorrow morning?
>
> **James**: Sounds good, see you then.

Lex reviews a number of email messages from strangers who are requesting legal representation, each willing to pay lucrative legal fees in exchange for what seems to be some very simple legal work, including:

- Finalizing the settlement documents of a nearly completed deal, receiving the settlement funds and then forwarding them – after keeping a hefty fee – to the client.
- Finalize contract documents for the purchase of equipment, receive the payment, keep a large fee, then forward the remainder to the seller.
- Help several different foreign residents (one of whom is a Nigerian prince) secretly transfer funds out of their respective countries.

Lex spots the indicators of fraudulent schemes – criminals trying to recruit him to receive stolen funds, to act as an unwitting money launderer or "money mule." He marks these as spam and deletes them. Then Sandra arrives at his office door.

Pop-up messages, phishing emails, malware, scareware, and technical support scams make computing difficult for everyone, but are especially challenging for seniors.

> **Sandra**: Hi Lex, how has your day been? Can you tell me what you think about this cybersecurity training outline for the firm?
>
> • User knowledge and awareness.
>
> • Information security basics: CIA.
>
> • Device security: Don't lose them, use passwords, and check settings.
>
> • Cloud data security: Use strong passwords and two-factor authentication.
>
> • Back up data and test the backups.
>
> • Business Email Compromise prevention through verbal confirmation of any funds transfer instruction.
>
> **Lex**: I think you nailed it, perhaps add a section on network security and I will think some more on it. We should buy a dozen copies of this book to give out [*gesturing*], and we should set a date and start fleshing it out.

By now it is time to leave. Lex shuts down his desktop computer, scans his desk and office for any sensitive documents that need to be put away, then makes his way out of the office, saying his goodbyes. The receptionist has left for the day, so the front door has been locked, and Lex makes sure it locks behind him. Information security – and the safety of the firm's employees – requires good physical security.

It has been a busy day, but Lex feels glad that he has protected himself, his firm, clients, and family from many threats, and looks forward to a relaxing evening at home.