MELAND | BUDWICK

Burner Phones, Sexy Strangers: How IP Thieves Are Targeting Lawyers

https://melandbudwick.com/2020/04/02/burner-phones-sexy-strangers-how-ip-thieves-are-targeting-lawyers/

Raychel Lean

When West Palm Beach intellectual property lawyer Steven Greenberg of Shutts & Bowen has an important call with a client, he doesn't use his phone. He uses the phone on his phone, otherwise known as a softphone, where everything is encrypted and no one can listen in.

"Why is that important? Because even the U.S. government is listening," Greenberg said.

Greenberg runs off his own computer network, uses a secure text messaging service and doesn't buy phones from third-party vendors like Verizon and T-Mobile. Because buying directly from the manufacturer ensures he'll get regular security updates and have no additional junk applications.

He also disables the camera and audio features on devices, avoids hackable wireless earphones like AirPods and, when abroad, carries a burner phone with nothing personally identifiable on it.

"It sounds like I want to wear tin foil round my head, right?" Greenberg said. "Here's the thing: I have all these databases, like all people like me have, that have all this critical information about our clients."

It's not easy keeping trade secrets. Here's what the attorneys taking the most precautions say all lawyers should be doing to protect client information.

State-sponsored theft

Every day, it seems someone tries to get into Greenberg's computer network.

“One day it’s the Ministry of Agriculture in the People’s Republic of China, and the next day it’s somebody from the University of Florida,” Greenberg said.

For that reason, it’s important to remain a moving target by changing passwords constantly and using two-factor authentication. That way, when Greenberg’s information gets onto the Dark Web, it’s useless.

“If somebody breaks into a bank, you know what the damage was, you can see it. The money’s gone, the door’s broken,” he said. “But if somebody’s steals your data, you don’t even know it was stolen.”

Billions stolen

While most trade secrets litigation Eric Ostroff handles at Meland Budwick, P.A. in Miami stems from business partner disputes, some derive from a less common but “devastating” kind of theft, by hackers looking for any information they can use.

> “There’s been literally billions and billions of dollars of value to American companies that have been stolen by foreign governments through foreign actors,” Ostroff said.

Though it sounds far-fetched to say state governments have offered money to American executives or broken into hotel rooms to put malicious software on laptops, it does happen, according to the FBI.

For that reason, Ostroff says attorneys and clients should be careful when traveling abroad.

“If, in the middle of the night, an attractive member of the opposite sex knocks on your door, you should be wary of that circumstance, because governments do use that technique, according to the FBI,” Ostroff said.

Law firms are a popular target for hackers, according to Ostroff, particularly if they’re handling high-profile cases, company mergers and acquisitions.

“If that information got out that a certain company is going to get purchased by

another company at a 50% premium, there's a huge amount of money to be made," Ostroff said. "One of the things that hackers have determined is that, oftentimes, the law firms haven't had the same level of protection as the clients, so it could be easier to hack the law firms."

The American Bar Association in a 2018 formal opinion said that lawyers have an ethical duty to take reasonable measures to protect confidential client information.

That means solo practitioners, small and midsize law firms should pay careful attention, according to Ostroff.

"You can't say, 'I'm just a lawyer, I don't understand,' " he said. "Lawyers have an obligation to understand the issues, and bring in either higher or outside consultants to come in and assist with these issues whenever necessary."

Public Wi-Fi is a no-no

Greenberg Traurig shareholder Kate Black helps technology and health care companies with data privacy and information protection issues at the firm's Miami and San Fransisco offices, Before that, she was global privacy officer for genetic testing company 23andMe and handled privacy and security for electronic health records at the U.S. Department of Health.

Black's best advice: Split up sensitive information when possible.

"If you're storing client files in one data center, you should make sure to store emails and other sorts of correspondence separately," Black said. "That way, if a hacker or an attacker were ever to get access to one database, they wouldn't have the full record."

There's no archetype hacker to look out for, according to Black.

"The idea that there's some man in a dark hoodie on a computer somewhere is, unfortunately, not the reality," Black said. "There are very sophisticated hacker networks that have been established that are very well-funded and operate in just as sophisticated a way as an organization or a company would."

Black advises clients not to use free Wi-Fi as several companies have had information about a case or important matter mysteriously end up in the news or

the public domain after doing so.

“Oftentimes, if you’re in a public space and you get access to public Wi-Fi, it is operated by a nefarious actor and operated only so that they can then access and steal information about individuals who have access to their WiFi network,” Black said.

Traveling abroad for work can also be risky, according to Black, who suggests checking with IT staff that devices are encrypted and carry as little sensitive data as possible.

“I’ve had many clients who have had computers either fully taken from them at the crossing of a national border or had to log in and provide the government with the ability to search through their files,” Black said.

However, it can be just as dangerous if employees leave their laptop unattended or lose their phone, Black said, so having the ability to remotely wipe a device is crucial.

‘Systematic’ attacks

For Samuel Lewis of Cozen O’Connor in Miami, who grew up “as something of a hacker at a time when that didn’t necessarily have the negative connotations that the terms has today,” his computer programming background proves useful for clients with intellectual property concerns.

“Information has become big business,” according to Lewis, who said lawyers need to understand that cyber attacks are now not only regular occurrences, but they’re “systematic” and sometimes led by foreign governments.

When Lewis last deployed a new server at his home in 2016, the attacks were almost immediate. Using a security log that recorded IP addresses trying to infiltrate, he discovered that two of the repeated attempts came from networks he could trace to adjoining office blocks in Beijing, China.

“When you see something like that, the reality is very much of an eye opener,” Lewis said. “It is now organized to the point where people aren’t even really trying to hide.”

Now that attorneys are switching to remote litigation because of court closures

over COVID-19, the challenge, in Lewis's view, will be ensuring client data security from home.

"There are a lot of people who are running the systems or the networks the way that the cable providers or the phone providers had installed, and that may or may not be truly secure," Lewis said. "It will be interesting to see how many people do run securely now that we really have no choice but to figure out how to work effectively while we are working remotely."

The FBI is open to working with companies to prevent trade secrets theft, notes Ostroff, who suggests calling the local branch office with any concerns.