White Paper

FOR HACKERS, CONFIDENTIAL ATTORNEY COMMUNICATIONS ARE EASY PREY

INTRODUCTION

"Ask hackers why they attack law firms, and their reply — to riff on bank robber Willie Sutton's famous quip — would no doubt be: 'Because that's where the secrets are.'"

"FBI Warnings: Criminal seeks hacker — to break into international law firms…"

"A Russian cybercriminal has targeted nearly 50 elite law firms, including four in Chicago, to collect confidential client information for financial gain."

"Hackers broke into the computer networks at some of the country's most prestigious law firms, and federal investigators are exploring whether they stole confidential information for the purpose of insider trading..."

"THERE ARE ONLY TWO TYPES OF COMPANIES: THOSE THAT HAVE BEEN HACKED, AND THOSE THAT WILL BE. EVEN THAT IS MERGING INTO ONE CATEGORY: THOSE THAT HAVE BEEN HACKED AND WILL BE AGAIN."

- ROBERT MUELLER, FBI DIRECTOR, MARCH 2, 2012

It reads like a monologue for Jimmy Fallon's late night show, except these quotes are dire warnings from the American Bar Association's official website, posted almost a year ago under the worrisome title, "CYBERSECURITY: ETHICALLY PROTECTING YOUR CONFIDENTIAL DATA IN A BREACH-A-DAY WORLD."

Have you read the post?[1]

WHAT SECRETS DOES THE LAWYER KEEP?

From the moment you start work, whether at home, in the car, or at your office, your very existence is shrouded in secrecy and privilege. If you talk to your client, your communications are covered by the attorney-client privilege. The draft pleadings on your computer screen, as well as your browser history for doing the legal research, fall within the attorney work-product doctrine. Should your client be a business, it is likely it will share proprietary information with you that could include anything from the secret to Nestle's chocolate to a company's confidential expansion or bankruptcy plans. In the corporate world, you are often privy to insider information and material facts that would make a trader drool, or you may be interacting with the CPA who has just audited a client's confidential books.

Pass from the world of business to the intimacy of personal relations, and your client may entrust you with his personal tax returns, secrets about his or her marriage and private affairs, or reveal confidential medical records showing the existence of heart problems that may impact life insurance applications. Routine personal injury cases involve layers of the above, from medical records to private financial or wage information to personal habits, and defending anyone in a criminal case adds to all the foregoing the privilege against self-incrimination.

Indeed, even when you take a diversion from the client side of things you may face internal administrative issues invoking the privacy of your employees and/or their spouses and families, from wage garnishments to disability claims. So let's face it: until you lay your head on the pillow at the end of the day, where for a brief time your thoughts are your own, everything you hear, say, read, send or store may be implicated in one way, shape or form to the privileges, confidences and secrets that rule your life as a lawyer functioning in the American legal system. Which means, from the time you awake until the time you go to bed, you are at risk.

[1] americanbar.org/content/dam/aba/multimedia/cle/materials/2016/04/ce1604lpi.authcheckdam.pdf

According to Law360.com[2], there are **383 law firms in North America with 100** attorneys or more as of the end of 2016. Law firms' make-up approximately 21% of the professional services market in the U.S.[3] — meaning that it is possible that twice as many incidents were reported by large law firms than there are large law firms in existence! This does not account for incidents that went unreported. A question to ask yourself — "Does your firm report cybersecurity incidents publicly?"

INCIDENTS AND BREACHES REPORTED BY PROFESSIONAL SERVICES ORGS WITH 100+ EMPLOYEES 2016:

Incidents Reported (Formal Incident Report Filed Publicly): 3,016

- Low Impact: 51
- Large Impact: 21
- Unknown Impact: 2,944

Breaches Reported (Confirmed Sensitive Data Lost and Reported Publicly): 109

- Low Impact: 37
- Large Impact: 8
- Unknown Impact: 64

WHERE ARE THE SECRETS KEPT?

A law firm's information management world used to be much simpler — one made-up of pleadings, letters, faxes, file folders, calendars, charts, photographs, X-ray films, even microfiche. In the modern world, those times are now referred to as "the good old days". Back then, security was enabled by locks on office doors and the really sensitive stuff was kept in locked fireproof file cabinets. Standalone offices had burglar alarms and law firms occupying commercial buildings had 24-7 roving security in the building and the parking lot, as well as the watchful eye of the receptionist in the lobby. Documents, memos, and evidentiary items rode in a legal briefcase that was often locked and was either kept on the attorney's person or in close proximity thereto or in the locked trunk of the car. You didn't leave your open files on the table at the local coffee shop and didn't expose them willy-nilly to anyone or anything. Anyone posing a threat to the security of your files could be seen — they had to physically be present to obtain access to anything sensitive.

Oh, how things have changed. Today *everything* is digital. Hackers can remotely access and/or download your entire database of information, every single file and folder and entry page. While pleadings, testimony, depositions and letters still get printed, they are written, reviewed, edited, shared, saved, housed, stored and filed online. The desktop computers, laptops, tablets, mobile phones, thumb drives, flash drives, and SD cards are used to hold anything and everything, from sensitive corporate secrets for your business clients to the personal details underlying a custody dispute or medical claim for an individual client. Indeed, all the confidential stuff of yore now transforms into Word documents, PDFs, spreadsheets, and images.

HOW ARE THE SECRETS COMMUNICATED?

In today's connected world, the private, confidential, proprietary, and secret information entrusted to, generated by, or stored within the digital systems of the attorney are all communicated in some way. They can be static, meaning they are accessed by individuals, and they are put in motion, meaning they are transmitted from the sender to someone else. Think of all the Word, Adobe PDFs, and Word Press documents you have in your office today that contain secret information. Think of all the emails,

[2] https://www.law360.com/articles/772291/law360-reveals-400-largest-us-firms
[3] https://www.selectusa.gov/professional-services-industry-united-states

texts, messages, and wall posts that you and all the members, attorneys, clients, law clerks, paralegals, legal assistants, secretaries, admin, investigators, analysts, vendors, outside experts and consultants in whom your firm reposes these secrets, and consider that all of these people may communicate some or all of the secret information in all, any or some combination of each communication method listed. It is literally mindboggling the opportunity that the hacker has to access your secrets and those of your clients — past, present and future.

WITH ALL THOSE SECRETS, YOU ARE EASY PREY…

As a group, lawyers lag far behind many other industries in terms of cybersecurity and protection of confidential data and information. Here are some very recent alarm bells:

On February 17, 2017, in an article entitled *Law firm websites hacked due to WordPress exploit; expert warns of reputational risk of cyber security incidents*, wrote: "Over 100,000 websites were hacked into and defaced in the past fortnight following the discovery of an undisclosed critical vulnerability in the WordPress content management system (CMS). ***Research suggests that recently hacked parties included dozens of law firms, including those specialising in IP law.*** A security expert tells *World Trademark Review* that this type of incident can cause significant reputational damage for firms — even ***potentially leading to the loss of clients***… Of those hacked, many law firms were targeted. ***For the most part, the exploit affected smaller, boutique law firms as major law firms will rarely run with a WordPress back-end.*** Research by *World Trademark Review* discovered affected firms include Brent Rathgeber Law & Advocacy, PalettaLaw, BSA Ahmad Bin Hezeem & Associates LLP and Barre M. Sakol. Furthermore, International Investigators Incorporated, a US-based private investigation firm which offers services including IP due diligence checks, was also defaced — with the hacker even advising the website's administrator to 'please update your wordpress…'."

On March 28, 2017, under the title *Cyber security: Lawyers are the weakest link*, by Jonathan Ames, TheLawyer.com wrote:

"With threats ranging from hacktivists to Chinese spies, ***it's time for law firms to get their data security act together***… In space, no one can hear you scream, but cyberspace will soon be alive with the shrieks of lawyer pain as client confidentiality disappears out a gapingly wide-open digital window… Law firms are in the front line of cyber security threats, with hackers increasingly targeting the legal profession for the goldmine of sensitive and confidential client data firms hold. And that threat is becoming so prevalent that cyber specialist practitioners envisage a time soon when bank and corporate general counsel — as well as those in charge of family offices — will insist on law firm security audits as part of routine panel reviews… This is not the stuff of science fiction or scaremongering, according to the experts. One cyber security specialist relates that a top 10 City firm chief information officer is convinced of the inevitability of a ***prominent legal practice going down in flames as a result of a cyber attack*** breaching client confidentiality and rendering the practice's wider reputation and market position untenable… ***Some suggest the financial services sector is starting to see law firms as the 'soft underbelly' in the cyber security battle.*** While they themselves have recognised the threat, upgraded systems and implemented state-of-the-art layers of defence, ***their lawyers, argue some senior bankers, are a weak link. Firms holding vast quantities of confidential information regarding financial services sector clients are a target for hackers because they are behind the cyber security curve.***[4]

The alarm bells are ringing all across the land, and as with all such bells, the authorities are responding.

[4] https://www.thelawyer.com/issues/28-october-2013/cyber-security-lawyers-are-the-weakest-link/

THE ATTORNEY'S DUTY TO SAFEGUARD SECRETS

"Never write if you can speak, never speak if you can nod, never nod if you can wink." — Attributed to the 19th century Boston political boss Martin Lomasney.

To think that the words of a gangster would be wise counsel to a 21st Century attorney.

With all those Secrets, you are easy prey… and risk substantial legal, reputational and ethical repercussions, UNLESS…

The Top Four Steps You Can Take Now to Mitigate Risk:

1. **Encrypt sensitive documents** — this is the number one suggestion made by security professionals the world over. While there is much debate in current politics about the legality of nation states to access encrypted information, it is imperative that you, as a practicing attorney, take every measure possible to protect the privileged information shared with you by your clients. Encryption technology has advanced immensely in recent years, including methods for protecting the sensitive information within documents much like a digitized redaction process would work.

2. **Understand, review and adopt the FTC guidelines for businesses and their responsibilities to protect client and third-party information.**

    a. The Guidelines can be found here: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

    b. The FTC has successfully won legally binding consent decrees against firms that did not do enough to protect sensitive information. Know how this can impact your firm. (See White paper **"The Five Most Dangerous Words in Business Cyber Security: 'It Wont Happen to — Case-in-Point: Lessons Learned from FTC v. Wyndham")**

3. **Limit the use of personal end point devices for transport and communication of sensitive information.** The age of the internet has resulted in ubiquitous use of smart phones, tablets, thumb drives and other means of conveniently accessing, sharing and storing information. While this convenience is a powerful force in business, it also reduces the control your organization has over how sensitive information is handled. Barring access of these devices to your corporate networks may be too draconian, but certainly the access to and transport of sensitive information should be limited to devices under which your organization has control, and on which security applications are managed and operating per company specifications.

4. **Educate Your team.** The potential for debilitating damage is great. Not only does a breach expose the firm to reputational and client loss, it also opens up the possibility of FTC regulatory response, client lawsuits, class-action law suits and, if the hackers are successful, ransomware and other extortion ploys. All of the security technology and measures available today can be undone in an instant by an unwitting employee who clicks on a phishing link, and enters their username and password into a bogus sign-in screen, thus giving away their network access credentials to the attackers. This happens every day. Educating your team, ALL of them, to these risks is an important step toward meeting the requirements to satisfy your obligations to provide affirmative cybersecurity protection to your clients.

WHAT DOES THIS MEAN TO YOU:

No matter what kind of sensitive information is involved, lawyers and law firms have an ongoing affirmative legal, fiduciary and ethical obligation to develop and implement for themselves and their companies the latest cybersecurity technologies; the latest methods and protocols for protection, education and training; and the most effective means for responding to, correcting, and remedying any prior security breaches. Put another way, it is time for every attorney and law firm to review and consider cybersecurity reform, making cybersecurity a way of life to ensure reasonable data and information security. Anything less makes confidential attorney communications easy prey for today's virulent hackers.

ABOUT WINDTALKER:

As cyber-attacks are increasingly sophisticated and a persistent threat to every individual, business, and organization, the typical industry response is to lock information assets down with more restrictive governance policies and security controls. However, when information assets are restricted, the effectiveness and efficiency of a business is significantly impacted. With information being the life blood of an organization, it needs to flow to customers, employees, and business partners. This challenging misalignment of security controls to business process leaves us with either too much or too little security, or the classic business vs. risk decision. The industry lacks a solution that addresses the real problem: protection of the content, "the data" no matter where it travels… Until Now!

WindTalker is a content security platform that allows for the protected movement and sharing of information which integrates with existing popular software. We simply apply encryption to specific portions of sensitive content within unstructured data formats such as documents, emails, text, and images. WindTalker protects these elements of sensitive data, such as personally identifiable information, company secrets, or client-attorney privileged information, while still allowing the movement and sharing of information without major interruption to the way you do business. Using a simple "Click — Protect — Share" philosophy, WindTalker leverages the user's knowledge and skills to enhance the security of the organization. WindTalker provides true control over "Need to Know".