Let's Get Technical

Data Security for Law Firms

By Veritext
Introduction

We have received a lot of questions about security and the ethical implications around using modern technology in law, so we're going to look at a lot of these technologies and hopefully demystify them and install some best practices.

- The risk of cybersecurity is the 4th concern of a law firm, behind profits, new clients and increased revenue
- Law firms are the 7th highest target for cyber criminals
- 1 out of 4 firms have had a data breach
- Each breach costs $4M on average


Law Firm Cyberattacks

The attacks on law firms show thieves scouring the digital landscape for sophisticated types of information. Law firms are attractive targets because they hold trade secrets and other sensitive information about corporate clients, including details about undisclosed mergers and acquisitions that could be stolen for insider trading.


What Hackers Steal

Hackers often steal large amounts of information indiscriminately and then analyze it later to see how it could be useful, making it difficult to determine early on in these types of investigations whether any information was actually used for insider trading, observers said.


The potential vulnerability of law firms is raising concerns amongst clients, who are conducting their own assessments of the law firms they hire, according to senior lawyers at a number of firms.

Information Sharing

Law firms last year formed an information-sharing group to disseminate information about cyberthreats and other vulnerabilities. It is modeled after a similar organization for financial institutions. 75 law firms have joined the group.


Ethical Concerns

ABA Rule 1.1

“To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated to relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.”

The ABA Commission explained . . . “These tasks now require lawyers to have a firm grasp on how electronic information is created, stored, and retrieved . . . notable developments' in technology that have impacted the practice of law to include electronic communication; mobile electronic storage; third-party servers; how clients find lawyers; virtual offices; and online practice management."
Sending Sensitive or Confidential Information Via Email

As you deal with sensitive information, you need to be aware that email is not a secure method of communication. If the documents are from Veritext, you can use our built-in email function that sends a secure link to download the files. If they are not from Veritext, we recommend services like ShareFile from Citrix.
**Definition:** Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. (Source: [https://en.wikipedia.org/wiki/Phishing](https://en.wikipedia.org/wiki/Phishing))

**Spear Phishing:** Phishing attempts directed at specific individuals or companies have been termed “spear phishing.” Attackers may gather personal information about their target to increase their probability of success. This technique is, by far, the most successful on the internet today, accounting for 91% of attacks. (Source: [https://en.wikipedia.org/wiki/Phishing](https://en.wikipedia.org/wiki/Phishing))

**Clone Phishing:** Clone phishing is a type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a resend of the original or an updated version to the original. This technique could be used to pivot (indirectly) from a previously infected machine, and gain a foothold on another machine, by exploiting the social trust associated with the inferred connection due to both parties receiving the original email. (Source: [https://en.wikipedia.org/wiki/Phishing](https://en.wikipedia.org/wiki/Phishing))


**Whaling:** Several phishing attacks have been directed specifically at senior executives and other high-profile targets within businesses, and the term “whaling” has been coined for these kinds of attacks. (Source: [https://en.wikipedia.org/wiki/Phishing](https://en.wikipedia.org/wiki/Phishing))

China hacked into major partners’ emails, Then used that to forward information to their servers. In the case of one firm, the attacks took place over a 94-day period, starting in March of 2015, and resulted in the hackers stealing around 7 gigabytes of data. The information was used for insider trading and intellectual property. (Source: [http://fortune.com/2016/12/07/china-law-firms/](http://fortune.com/2016/12/07/china-law-firms/))
Fighting Phishing

To fight phishing in your firm, we recommend training services like KnowBe4. https://www.knowbe4.com

These services include video training for employees, quizzes, even real world tests. These tests send fake phishing emails to see if employees leak private or confidential information.
When employees click incorrect links or divulge sensitive information, they are presented with a warning Web page. This instructs them it was a test, and what they need to do in the future.
Ransomware

Ransomware is computer malware that installs covertly on a victim's device (e.g., computer, smartphone, wearable device), and that either mounts the cryptoviral extortion attack from cryptovirology that holds the victim's data hostage, or mounts a cryptovirology leakware attack that threatens to publish the victim's data, until a ransom is paid. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, and display a message requesting payment to unlock it. Source: https://en.wikipedia.org/wiki/Ransomware

For more information on Ransomware, go to http://resources.infosecinstitute.com/ransomware-attacks-on-law-firms/#gref
To Protect Against Ransomware:

1. Install and use an up-to-date antivirus solution.
2. Make sure your software is up-to-date.
3. Avoid clicking on links or opening attachments or emails from people you don't know or companies you don't do business with.
4. Have a pop-up blocker running in your web browser.
5. Regularly backup your important files!

10 Ways Law Firms Can Make Life Difficult For Hackers

By Taylor Armerding

1. More/better employee training
2. Keep backups disconnected from the network and the Internet
3. Install all patches and updates
4. Update software – especially when it is no longer supported
5. Block executable files, compressed archives and unidentified users
6. If you use Cloud storage, make sure your firm controls the encryption key
7. Make your cybersecurity program meet the needs of potential clients
8. Have clear, effective restrictions on remote access and mobile devices
9. Set systems to capture log data for forensic purposes if a breach occur
10. Share threat information