WARD AND SMITH, P.A.
ATTORNEYS AT LAW

Media Mention: Angela Doughty on Privacy and Data Security for Attorneys

July 16, 2018

Given the nature of law firms and the amount of sensitive information they collect and maintain about their clients, it is imperative that they store and handle it in the most secure way possible.

In a recent *North Carolina Lawyers Weekly's* virtual roundtable, privacy and intellectual property attorney Angela Doughty discussed the differences between privacy and data security, as well as the ways law practices could assess and handle the protection of clients' sensitive information.

Here's a recap of the article:

> There is a distinction between privacy and data security, but the two are interrelated in how law firms collect, handle and store sensitive client information. Doughty explained how they differ and how they are related.
>
> Doughty said, "Privacy laws govern the collection, use and handling of data. Data security involves the implementation of security measures adequate to protect the authenticity, confidentiality and integrity of the data. The applicability and requirements of these privacy laws directly impact the data security mechanisms required. Frustratingly, these privacy laws and data security requirements vary significantly from law to law and country to country and the penalties for noncompliance are often substantial."
>
> She continued, "To understand the level of data security required, the firm must first understand the privacy laws that apply to the data it collects and stores. A firm can have data security mechanisms implemented and still not be compliant with applicable privacy laws. A firm's failure to comply with the applicable privacy law and corresponding data security requirements can result in legal and regulatory liability for both the firm and, in certain industries, its client."
>
> Doughty concluded, "The unfortunate reality is that no security mechanism is flawless, and many believe that security incidents are a matter of when, not if. The consequence of this is that firms must (i) protect against security incidents by employing the requisite security mechanisms (technical safeguards) and (ii) position itself to best minimize its risk and liability under applicable privacy laws (administrative and procedural safeguards). To do so, the firm must understand what privacy laws apply to the data collected, the data security requirements under each applicable privacy law, and the proactive (policies and procedures) and reactive (notifications, containment, remediation) requirements when there is a security

incident."

What are some common mistakes that law firms make when it comes to data security, and what are the biggest risks?

DOUGHTY: Law firm employees are often the biggest data security vulnerability. It is important to provide employee education, on an ongoing basis, about the firm's privacy and data security policies, confidentiality expectations, and ways to reduce the risk of a security incident (phishing scams, HIPAA training, encryption standards). It is also a good idea to put technology in place to prevent employees from inadvertently or maliciously, violating the firm's policies – e.g., removing ability to download or upload, limiting access to certain websites, and restricting access to sensitive data.

A majority of law firms have Bring Your Own Device (BYOD) policies that allow attorneys to access the firm's network and then download client data to the device while out of the office. While this type of remote access is now a necessity for most lawyers, firms must understand and manage the risks related to this type of external access to its systems from personally owned devices. It is important to ensure the same levels of security are required for these devices as are required for internal devices – e.g., current antivirus and malware protection, mandatory complex passwords, encryption and remote wiping capability should the device be lost or stolen.

Cloud vendors and other outsourced resources that will store, transport or have access to client or employee information also present risks. All vendors (cleaning companies, shredding companies, SaaS providers) should be thoroughly vetted based on the scope of access, type of access and the type of information that will be accessible to such vendors. All vendors with data access should, at minimum, execute a confidentiality agreement. For vendors that obtain access electronically, law firms should confirm that vendor requires passwords, encryption and maintains current antivirus and malware software. All vendor contracts should be reviewed for indemnification clauses, liability limitations and the allocation of responsibility for a security incident or breach. Additionally, if a law firm stores certain categories of information such as protected health information, financial institution customer information or European data subject information, the firm must ensure that the additional restrictions on that information are also required of the vendor.

What data assets should a law firm be trying to protect?

DOUGHTY: All client information must be protected. Additionally, the personal information of the law firm's employees must be protected. However, the level of protection required for the client data and the employee data collected and stored by a law firm varies depending on a variety of factors, such as the circumstances under which the data was collected, the source of the data and the terms of any contract or consent provided when the data was collected. For this reason, it is important the firm understands all of its data assets – including the source of the data – and not just the existence of the data to ensure proper protection.

For example, if a law firm obtains a medical record from a doctor, then the protection required must comply with the privacy and security obligations of HIPAA. If, on the other hand, the same medical record is obtained directly from the client, then the record must still be protected as a confidential client record but not to the level of HIPAA's requirements, Likewise, the notifications required in the case of an unauthorized disclosure of this same medical record would vary depending on these same factors.

What technologies and/or processes should a firm have in place to protect clients' sensitive information?

DOUGHTY: Encryption represents one of the simpler security measures available for managing security risk. However, encryption is not a one-size-fits-all solution, nor does it ensure the complete avoidance of a security incident. There are different forms (e.g., email, full-disk, file, etc.) and levels (128-bit, 192-bit, 256-bit) of encryption that can be implemented in different ways (data in transit, data at rest and data backups.

Breach prevention technology includes encryption but also includes firewalls, antivirus and malware software, and other technologies aimed at preventing a breach.

Active breach detection technology aims to actively identify, track and stop any hacker that breaks through the breach prevention technology.

All law firms need a security incident response plan. The purpose of the plan is to allow the firm to recover as quickly as possible from an incident by planning for business continuity and minimizing of mitigating the effects of the incident, as well as the protection of the firm's clients. Security incidents involve internal and external resources and result in multiple moving parts, which makes having a structured and systematic process for how to handle the incident very valuable.

How does a law firm assess its vulnerability?

DOUGHTY: Law firms should assess and test their IT structure through periodic self-audits by firm management and external information technology consultants to determine where system vulnerabilities exist. These processes include technological components like scanning a system, engaging a vendor to attempt to hack the firm's system, and testing backups, as well as practical components like sending engineered phishing emails to employees to determine whether further training for employees is necessary.

Law firms should also asses the types of data it stores to ensure it has all legally required policies and security measures (administrative, procedural and technical safeguards) in place. Different types of data require different types of safeguards and failure to comply with these requirements has the potential of making both the firm and the client vulnerable to legal and regulatory action. For example, if the law firm servers as a business associate for a covered entity or has access to a financial institution's customer data, it must comply with the legal requirements of HIPAA and GBLA, which are more stringent than the standard ethical confidentiality obligations

Why are law firms and lawyers a significant target for hackers?

DOUGHTY: Law firms hold vast amounts of valuable information, such as financial records, health records, confidential trade secrets and other intellectual property. This type of personally identifiable, sensitive and financially valuable information all in one place makes law firms desirable targets because it allows hackers to access a large amount of that sensitive data in one place.

What laws and ethics rule apply to law firm data security and privacy?

DOUGHTY: There are various state, federal and international privacy and data security laws that impose legal obligations on law firms. Examples of federal and international laws include the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Fair and Accurate Credit transactions Act (FACTA), and the General Data Protection Regulation (DPR). Howver, the applicability of these and the other federal and international laws is dependent upon the data collected and stored by the law firm. The specifics of the privacy and data security laws of each state vary, but all impose requirements to protect the personally identifying information (PII) entrusted to any business

(which includes law firms) from unauthorized access or disclosure. Failure to comply with state, federal and international regulations can result in civil suits, regulatory investigations and/or monetary penalties.

As lawyers, outside of these legal obligations, we have a professional ethical obligation to maintain the confidentiality of the information entrusted to us by our clients. Our ethics rules prohibit us from revealing information related to our representation of a client unless the client provides informed consent the disclosure is implied based on necessity to carry out representation, or it falls within an explicit.

We also have an ethical confidentiality obligation to make "reasonable efforts" (take affirmative measures) to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. The reasonableness standard requires consideration of various factors, including the sensitivity of the information, the likelihood of disclosure, the availability and cost of safeguards, and the adverse effect the safeguards will have on an attorney's ability to represent the client.

Our ethical competence obligation to remain informed about changes in the law, including the benefits and risks associated with the technology required to provide competent representation, intertwines with our confidentiality obligation to analyze and determine reasonable efforts for preventing the unauthorized and inadvertent disclosure of client information. The result is that attorneys must remain knowledgeable about relevant technology in order to comply with their ethical duties of competence and confidentiality. Failure to comply with their ethical duties of competence and confidentiality. Failure to comply with ethical obligations can result in disciplinary action and malpractice claims.

Once a law firm realizes its data has been breached, what are the steps it should take?

DOUGHTY: If the firm has a security incident response plan, it should follow that plan. These plans contain the specific steps, the individual roles and responsibilities of both individuals within the firm and external third parties, and resources available for the response. It is important to always keep in mind, and another reason incident response plans are so valuable, that security breaches can result in legal action, which means evidence preservation and external counsel for attorney-client privilege is important.

If there is no plan, the first step is to engage an IT professional to identify and contain the source of the security incident (quarantine file, wipe lost device, etc.). Efforts to restore and recover the information should follow, as understanding what information was potentially accessed or disclosed is vital for determining applicable laws and notification requirements.

The firm should also simultaneously engage legal counsel. It is important to make a legal determination as to whether there has been an actual breach. The term "breach" has significant legal meaning when determining the potential legal obligations and liability of the law firm that has experienced a security incident.

Should a law firm carry cyber insurance, and if so, what features should the firm want in its policy?

DOUGHTY: Cyber insurance is highly recommended due to the financial impact of data breaches. Cyber insurance coverage can mean the difference between surviving the security incident and going out of business. The best cyber insurance coverage includes coverage for costs such as the IT professionals required to contain, remediate and restore the firm's data and systems, the legal representation

responsible for making the breach determination and handling any applicable notice requirements, and other business disruptions associated with a security incident. However, not all cyber insurance policies are created equal, and many have exceptions in coverage that can render them ineffective for the purpose in which the firm intends. It is important to review any cyber insurance policy with counsel and the insurance provider to ensure that coverage is appropriate, comprehensive and does not contain excessive exclusions.

If a law firm has a limited budget for security, what should its priorities be?

DOUGHTY: Encryption. The form, level, and implementation of the encryption protection will vary depending on the type of data collected and stored and the firm's data retention and destruction policies, but all firms should be utilizing some type of encryption.

Intrusion Protection. Maintaining up-to-date firewalls, antivirus and malware software on all devices (PCs, laptops, tablets and phones) that are used to access client information. This includes daily updates to ensure all patches are implemented and scanning personal laptops used to access the network to ensure they have the requisite level of protection. This also includes regular scans of the system and network vulnerabilities.

Passwords. Require complex passwords and, if possible, dual authentication for accessing firm networks and data remotely. Enforcing certain password requirements (specific number of characters, mandatory password changes every 90 days, etc.) is an inexpensive and effective way to protect firm data.

Education. The firm and its employees should understand the type of data the firm collects, the firm's legal obligations for that data, and the policies and procedures that describe the firm's expectations about how that data is kept confidential and secure. These policies include security policies for email, voice-mail, mobile devices, etc., social media policies and data policies for data collection, storage, transmission, retention and destruction.

Vendor Contracts. All vendors that will have access to the firm's data should be required to execute an agreement that imposes confidentiality obligations and addresses the restriction on access, disclosure and retention/destruction of data. Many times, it is important that these agreements also include indemnification clauses, liability limitations and proper allocation of responsibility for a security incident or breach.

Can data stored in the cloud be considered safe, and what should lawyers tell clients about their use of the cloud?

DOUGHTY: Cloud-based mechanisms and service providers can be an efficient and effective way to store data, and many come with advanced security measures already in place. However, law firms should do their due diligence in selecting cloud provider's security mechanisms to ensure that data is protected both at rest and in transit. Additionally, even top-notch security measures are not the silver bullet for malicious infiltration or simple human error. It is still important to ensure that employees are trained and that proper processes are in place to deal with worst-case scenarios.

The virtual roundtable discussion was sponsored in part by Ward and Smith. To read the entire article, click here.