New Jersey Law Journal
STATEWIDE LEGAL AUTHORITY SINCE 1878
An ALM Publication
VOL. 227 NO. 32 MONDAY, AUGUST 9, 2021 NJLJ.COM

CYBERSECURITY

Law Firm Cybersecurity in a COVID-19 World

By Karen Hornbeck

It is no surprise that law firms continue to be an attractive target for cyberthieves. Law firm data systems hold various types of confidential information about corporate clients, and include nonpublic information about corporate development, business strategy and planned transactions that hackers could use for a variety of malevolent uses. In addition, firms generally also store a wealth of personally identifiable information, including protected health information and payment information, for clients, parties, witnesses, and employees. The dramatic shift to remote working due to COVID-19 has increased the complexity of the cybersecurity challenges firms face.

Rawpixel.com / Shutterstock

The Effect of COVID-19

The advent of COVID-19 saw the nearly overnight change from office-based work to remote work. The speed with which employees moved to working from home brought about an additional layer of risk, and forced firms to quickly attempt to secure the remote work environment. This section is meant to highlight controls that remote working has brought to light, and to drive internal expectations as well as conversations with your firms.

First, ensure your firms have an *information security policy*. The policy should clearly state and outline key elements of their information security program, including who the policy applies to, details outlining all the various security protocols employees are expected to comply with, and how the firm will support them in complying (i.e., which tools and resources they will provide) with the policy. This policy should be incorporated (at minimum) into the firms' annual training, and employees and contractors need to confirm that they have received the training.

Additionally, ensure your firms have a thorough, tested *incident response plan*. A solid Incident Response Plan will include protocols for containment, notification, remediation, monitoring and related issues. It will also assign specific responsibilities to designated personnel and have third-party vendors on standby to ensure that important tasks do not fall through the cracks. With an Incident Response Plan in place, law firms can respond rapidly to a breach, limiting its scope and reducing damages. That said, simply having a plan is not enough—it is just as important that the firm actually tests the plan with the identified roles/employees. The worst time to find out that the plan has the wrong person assigned to a critical task is during an actual incident or breach—by conducting a full walk-through during normal business, the plan can be modified to address any needed areas.

***Karen Hornbeck** is a senior manager with Consilio, a global leader in e-discovery, document review, risk management, and legal consulting services.*

At home, ensure that employees and contractors have changed their router passwords, which are often left as the default when purchased. For a great exercise highlighting the lack of general password security, look up Troy Hunt's "Have I Been Pwned," which is a site dedicated to showing email addresses, passwords, and other personally identifiable information that has been compromised in a data breach.

Firms should also deploy m*ulti-factor authentication* (MFA) technology. MFA adds additional levels of authentication to an account login as opposed to a single-factor authentication, where users only need to enter a static username and password combination. Two-factor authentication (2FA) is the most common form of MFA, and adds an additional layer of security by requiring an additional layer or form of verification (often a temporary PIN or code).

Full disk encryption (FDE) of firm laptops is an additional requirement that all firms should explore and consider making mandatory. FDE uses an algorithm, or cipher, to convert a physical disk or logical volume into an unreadable format that cannot be unlocked by anyone without the key or password that was used to initially encrypt the drive. Therefore, even if a laptop is stolen and the hard drive is removed, the contents are still encrypted. The price point for encryption software has come down to the point that it is no longer cost-prohibitive when compared to both the benefits it provides and the risk of a stolen, unencrypted laptop.

As COVID restrictions ease and people move back to their local coffee shop to work for a few hours, the risk of utilizing an open (or barely secure) WiFi connection arises. Firms should require that employees and contractors log into a VPN whenever connecting to a public WiFi. A *VPN,* or *virtual private network*, sends the computer's traffic through an encrypted "tunnel," making it extremely difficult to decipher or intercept. Having a VPN application on firm laptops provides users with this encryption on-the-go.

Firms also need to establish rules and implement technology for cell phones and mobile devices. *Mobile device management* (MDM) software stores all company-related information in one area that is password-protected and secure. MDM software also remotely establishes required security settings (including minimum password strength), forced encryption, and the ability to perform a remote device wipe to remove all data if the device is lost or stolen.

Just as important as the technical controls above is effective and frequent information security training. The increase in the remote workforce actually makes this more important than ever before. All firm employees and contractors should be trained on the following:

- The firm's information security policy,
- How to identify and report a phishing attempt / recognizing suspicious emails,
- Malware identification,
- Password security and MFA / 2FA,
- Use of encryption and use of portable storage devices (USBs, etc.),
- Avoiding / securing public WiFi,
- Social media,
- Escalation processes and where to ask questions.

In addition to the above technical, administrative, and organizational recommendations, there have been multiple articles written over the past several years that offer additional, more specific, technical advice on what and how to secure data and information at law firms. Building upon these, the next sections propose additional ideas on how to secure the information shared with your outside counsel, from an organizational and process perspective.

Preferred Provider Network

The first is to establish a *preferred provider network* (PPN). Also referred to as a preferred legal network, these networks are a strategically chosen, consolidated group of law firms, which legal departments utilize for the vast majority of their work. The main benefit of utilizing a PPN in the frame of law firm cybersecurity is that your critical information and data is going to a smaller number of firms, thereby reducing overall risk. There are additional benefits to utilizing a PPN, including cost reduction, deepened relationships, and compliance with diversity and inclusion goals, but for our purposes, the fewer firms that have your sensitive and confidential information and data, the fewer firms that will require audit and enforcement of outside counsel guidelines, as we'll discuss next.

Outside Counsel Guidelines

Strong, clear *outside counsel guidelines* (OCGs) provide the basis for the cybersecurity discussions that need to take place between all corporate legal departments and their law firms. Corporate clients should use their OCGs as the basis for an honest discussion around both goals and, ultimately, expectations. For purposes of this article, we will focus on the cybersecurity aspects of OCGs, and how to align your law firm's goal of client satisfaction with your goal of secure information.

In our work with corporate clients, we have found more and more are laying out specific requirements in their OCGs, with the following items becoming commonplace:

- Firm has information security, data privacy, and incident response policies and larger programs (staff, training, roadmap, etc.).
- Client will be notified of data center moves.
- Client will be notified within 72 hours of incident (note that we also see many clients ask that their case manager or managing attorney be notified immediately of any suspected incident).
- Client information is disposed of within a certain number of years after close of matter.
- Client information is encrypted (both at rest and in transit).
- Incident response policy is fully established and tested.
- Firm employees do not have access to the information and data of all clients (firms should institute a need-to-know policy and employ corresponding technology).

Conducting Assessments

And finally, it is critical to assess the security and privacy controls in place whenever information is sent to any third-party vendor, law firms included. Outside counsel firms should not be immune from these assessments, given the breadth of sensitive and confidential information they receive from clients. Assessments provide an objective measurement of a firm's administrative, technical and physical controls, and provide a launching point for the discussion around expectations.

Any assessment should cover, at a minimum, the following areas:

- *About the Organization.* Information regarding contact person and organization.
- *Geography.* Locations in which the organization's information may be stored or from which it may be accessed: this is critical for the organization to understand what regulations they may be required to comply with.
- *Standards and Certifications.* Recognized industry standards to which the organization adheres.
- *Information Security.* Programs and professionals in place to protect client information, including executive and support roles and responsibilities, policies, training, etc.
- *Privacy.* Risks and capabilities related to the protection of personal information, including executive and support roles and responsibilities, policies, training, related to CCPA, GDPR, HIPAA, and other key privacy regulations.
- *Storage, Recovery, and Retention.* Practices relating to the storage of both paper and electronic information, disaster recovery, and data disposition (how long is information retained, are retention practices consistent across the organization, disaster recovery and business continuity).
- *Workforce.* Safeguards relating to employees, contractors and subcontractor personnel, partners, affiliates, and any other third parties who may have access to the organization's information. This includes the identification of high-risk / high-value information and related workforce access controls, information handling controls, etc.
- *Security Controls.* Security aspects of the data storage environment, including networking, data center, wireless security controls, information access controls, physical security controls, etc.
- *Monitoring & Incident Response.* Tools and procedures relating to security monitoring, auditing, and incident response.
- *Third Parties.* Organizations or individuals who are not client employees or contingent workers, such as technical or support services, as well as external entities who may have access to client matter information.
- *Mobile & Remote Access.* Practices relating to the access and control of portable computing devices such as smartphones, tablets and laptops.
- *Application Security.* Practices related to hosted software applications within the organization, encryption of high-risk / high-value information, etc.
- *Cloud Services.* Controls around cloud-based storage, and understanding of risks associated with cloud-based services.

Law firms have not only an ethical, but a professional obligation to secure their clients' information and data. With the right combination of strategy and technology, law firms can truly be trusted stewards of their clients' information. However, it is critical that corporate legal departments ignite conversations around how their firms plan for and implement cybersecurity as proactive, routine business, not just in times of a breach or incident. ■