Best Practices for Counsel Serious About Cybersecurity

From the recent Equifax hack and Yahoo's massive data breach in 2015 to Sony Pictures' data leak in 2014, it may seem like there's no place where data is safe. Law firms and corporate legal departments can be especially at risk because they oversee a concentration of sensitive information, which can be highly valuable to hold hostage or exploit. In the current climate, it's just not an option for attorneys to simply be aware of cybersecurity needs. It's one of the many areas in which modern-day lawyers must be involved outside of practicing law.

Law firms, corporate legal departments and e-discovery data can be of particular interest to hackers due to the complex and confidential nature of the data that's involved. Often times, there are sensitive documents like business data, trade secrets or other intellectual property that's transferred electronically back and forth during lawsuits, which is why it's more important than ever for the legal industry to spend time focused on cybersecurity.

Research firm Gartner recently estimated that in 2018 spend on cybersecurity will be more than $93 billion. What does this tell us? Cybersecurity has become a focus for many companies. It's time for counsel to join their lead.

WHAT FOLLOWS ARE FIVE RECOMMENDATIONS FOR COUNSEL SERIOUS ABOUT CYBERSECURITY.

Think About Data Security During Data Collection and Data Disposal

It's important that data security is considered even before the collections process begins. The first step to keeping data safe is working with a provider before collections to ensure that only the necessary data is collected. Don't over-collect data that isn't necessary. The less quantity of sensitive information that you have, the better. For the actual collection itself, make sure that the equipment used for collection doesn't have any other data on it. Data should also be encrypted as soon as it is collected to ensure that sensitive data is not compromised.

As important as it is to minimize the data collected down to just the necessary documents, it's just as important to properly dispose of the data collected for a case in a timely manner. This doesn't just mean releasing pending holds. When firms receive a client's data, typically the firm will forward this data to an e-discovery service provider for processing and hosting. At this point, the data should be destroyed at the law firm. It's unnecessary to keep the data on a server at the firm when it can be accessed somewhere else — in particular, a location where the third-party provider has high-tech security systems guarding the data. Many times, this does not happen at law firms, leading to attorneys keeping millions or billions of emails or documents on their machines or server long after the case is closed.[1]

It's also important to ask for the same destruction of data from the opposing party. This is critical for corporate counsel too. Kara Ricupero, Director of E-Discovery and Records and Information Management at eBay Inc., states that she regularly asks her company's outside counsel to "reach out to opposing counsel to get them to return information, or destroy it and provide a certificate of destruction." [2]

Data Should Be Encrypted — *Always*

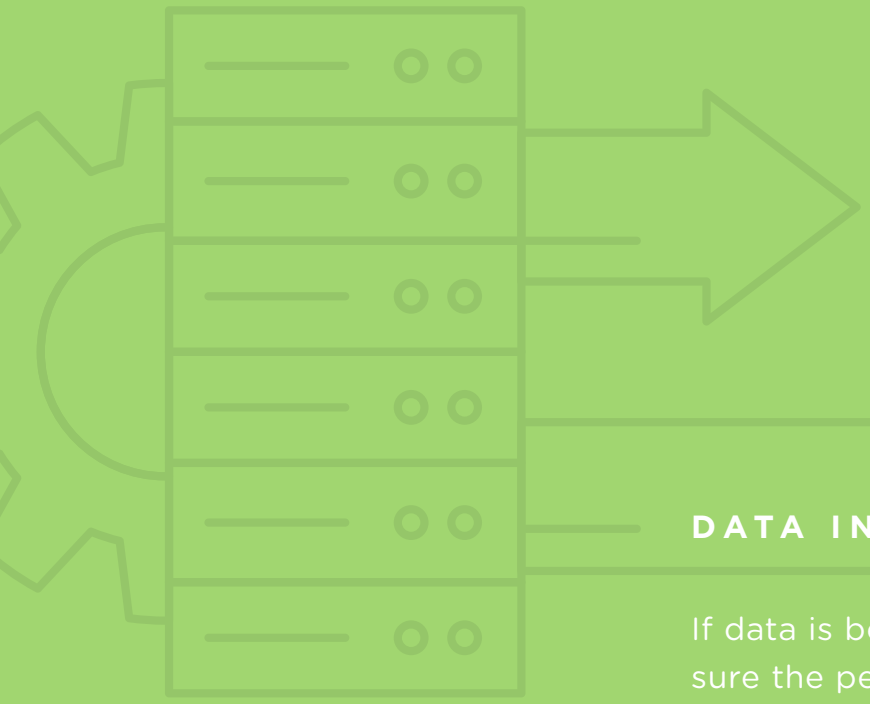
Data encryption means that the data is translated into another form, or code, so that only people with access to a secret key or password can read it.[3] This type of technology is very effective at preventing data theft, even if someone has the physical device.

For portable devices like laptops and other portable media, this is extremely important in the event of physical theft. Many smartphones already come encrypted, as well as with end-to-end encryption for messages and calls so data on these devices is typically already secure. You should already be using either the fingerprint or complex password functionality on your phone, a combination of the two, or require a password if fingerprint or complex password technology is unavailable.

When working with a third-party e-discovery service provider, make sure that they have processes in place to ensure that data is always encrypted — especially in transit. The data should also be encrypted when being viewed in the vendor's software system. There are a few common ways to transport data: via regular mail, through an encrypted FTP site set up on the Internet, or upload it directly through the encrypted e-discovery platform. In most cases, email should not be considered a safe way to send data.

TAKE A DEEPER DIVE

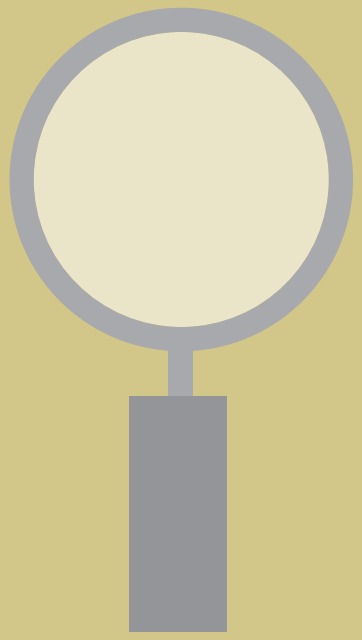
For more about encryption, the American Bar Association provides a deeper look at the types of encryption available and how to ensure data everywhere is safe. [4]



DATA IN TRANSIT

If data is being shipped, it should also be encrypted. In addition, make sure the person receiving the data knows when it was sent, which format and by what method, as well as who should receive the data. Finally, send the encrypted media and the password separately, e.g., hard drive by mail, password by email.

If the data is being sent electronically, it should be done using a secure FTP site. This means that all communications are encrypted, including when the data is being sent over the Internet. If the transfer is sent using a file transfer tool, be sure to confirm with the operator of the FTP site the correct configuration to ensure encrypted transfers. If the transfer is via a web browser, make sure the website domain matches what you would expect and that the URL shows “https” instead of “http.” The transfer should also take place on a secure network — never over a public network.



Thoroughly Vet Third-Party Vendors to Ensure Maximum Safeguarding of Data

When dealing with e-discovery data, partnering with a service provider is an easy way to make sure your data is protected. After all, many vendors specialize in guarding cloud-based data and put multilayered security protocols in place. By contrast, most law firms or corporate law departments may not have the resources or experience to enact this specialized security. Additionally, working with a third-party service provider also automatically anonymizes where the data is present, making it difficult for hackers to know where to go or whom to target. Not all service providers are created equal, however. It's important to understand what security measures a provider takes so you can make the most informed decision about whom to partner with to protect your data.

There are a few things that should be considered when vetting service providers, including where the data is stored (physical and cloud-based) and the protocols and procedures the provider follows for data security.

Working with a third-party service provider automatically anonymizes where the data is present, making it difficult for hackers to know where to go or whom to target.

DATA STORAGE: PHYSICAL AND CLOUD-BASED LOCATIONS

As already emphasized, when data is in transit or being viewed in a platform, it should always be encrypted. It's also important to centralize data access as much as possible and avoid multiple copies of the same data across multiple machines. For instance, having five different hard drives with the same, sensitive data on them increases the chance that one of the hard drives will be compromised. By having the data available in a single location, with access given only to those who need it, you decrease the chance of having your data compromised.

This is not only true for documents collected and reviewed but also attorney work product and privileged communications. With as few data storage locations as possible, it makes it easier to ensure the same effective safeguards are in place in each location.

The same can be applied to cloud e-discovery platforms. For example, if you're working on an e-discovery project, instead of using multiple service providers during different steps in the litigation process, have all the data for legal holds, review, and case management in a single e-discovery vendor and software platform for the case team to log in. If the team can collaborate on the case in a shared software environment, it is more secure than each member

It's also important that the physical location of the servers that the data is housed in is very well protected. Important questions to ask your service provider include:

- Is there a physical security guard at the facility 24/7?
- What kind of access protection do people who enter the facility need? Biometric access like fingerprint technology?
- What additional protocols are in place for safeguarding the physical data? This could include things like intrusion detection, log monitoring and archiving.

> **"We need something that addresses our problem with 'oversharing' our documents. You share a document in a review platform and it's relatively secure, you want to grant licenses to people, that's great. When you start getting requests from lawyers or experts ... things start getting out on thumb-drives, and then you lose control."**
>
> Seth Schreiberg, Counsel, Uber[5]

DATA SECURITY PROTOCOLS AND PROCEDURES

Most reputable service providers you select will have a set of formalized processes and procedures for handling and securing data. This will include a structured response plan or protocol if an issue does arise. Additionally, there are tests the provider can run to ensure security, like penetration testing, which looks for holes in the firewall.

Other security protocols and procedures to look for in an e-discovery vendor include ensuring that the vendor keeps customer data segregated and not mixed together with another customer's data. Make sure the software has user-based access and can limit what data reviewers and members of the case team can view. This limits risk by ensuring the fewest number of people necessary has access to confidential documents.

Additionally, there are independent bodies that create standards for keeping data safe. The industry standard is from an organization called the International Organization for Standardization (ISO).[6] The ISO 27000 series is considered a standard for the e-discovery industry. It's a good idea to make sure the provider you select has a set of industry standard procedures and is regularly certified in those procedures.

Hold Opposing Parties to the Same Strict Security Protocols

The data security measures taken should not stop with just client's counsel. Information security is a core ethical obligation of attorneys, according to the American Bar Association Model Rules of Professional Conduct. For example, Model Rule 1.6(a) requires that attorneys protect their clients' confidences, and Model Rule 1.6(c) requires "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information related to the representation of a client."[7] It does not differentiate between information transmitted orally and data handed over to an attorney, or for that matter, opposing counsel.

This assurance of confidentiality and data security from opposing counsel should start during the pretrial conferences. Currently, pretrial conferences typically focus on scope and how discovery will be performed. Kara Ricupero of eBay Inc. confirms this in her comments on data security in pretrial conferences, "The reality is that it has been an afterthought. As attorneys, it can't be going forward."[8] During these conferences, discussing matters like encrypting confidentially produced documents and keeping them in an encrypted format until they are returned, or destroyed, or outlining what security measures each side will take to protect data, may be necessary. Ricupero acknowledges this could mean information security professionals being more active in these conferences. And, as discussed in the "Data in Transit" section, don't forget to encrypt the data when each side is producing to the other. This is a standard protocol your service provider can implement.

> **"The reality is that it has been an afterthought. As attorneys, it can't be going forward."**
>
> Kara Ricupero, Director of E-Discovery and Records and Information Management, eBay Inc.

Create a Culture of Data Security Within Your Organization

In order for cybersecurity to be a true priority in your firm or company, it should be a cultural norm that employees regularly discuss it and attend related training. Through these trainings, get buy-in from the staff by establishing individual ownership of data security in their day-to-day job. This training and ownership should occur for all staff. In particular, ensure that those who have access to confidential data understand their responsibility to keep it safe and the best practices for avoiding risk.

Since protecting client data throughout the litigation process is an ongoing, ethical obligation for attorneys, counsel should create reliable and defensible processes that are documented, repeatable and can be adapted over time to meet their obligations. While protecting client data is an obligation, in certain states protecting and securely disposing of personal data is also a requirement. The data that generally requires protection includes personally identifiable information (PII) such as Social Security numbers, driver's license numbers, financial account numbers and some health information.[9]

There are some common tactics that can be implemented within an organization to minimize the chance of getting hacked. As part of the staff training, common hacking tactics should be covered. This includes being wary of suspicious emails, tweets and ads by hovering over links to check their validity, which ensures you trust the site and sender, as well as taking additional precautions with executable files (.exe).

Additional best practices relate to the passwords used to protect online accounts and sensitive data. All accounts that have a password should also have a policy that requires, at the very least, a strong password and a frequent password change. If you are using an e-discovery service provider, they should also have a policy for this. Having an online password manager can help employees securely track the strong passwords and eliminate the need to store in unsecure places like in email, written on paper and more.

And while it's important for this culture to be driven from the top of the organization down, individual contributors should not take the readiness of the organization for granted. Ask questions and evaluate your organization's information security robustness on your own, just as you would of a third party.

CONCLUSION

Unfortunately, lawyers and firms can be appealing targets for hackers. Taking proper security measures to keep data as secure as possible helps prevent hacking. Plus, staying up to date on the latest security measures will not only help put your firm ahead of many of your competitors, but also go a long way to keep you and your clients' data safe.

> **"There is a narrow and fleeting window of opportunity before a watershed, 9/11 level cyber attack to organize effectively and take bold action."**
>
> National Infrastructure Advisory Council, August 2017

The time to get serious about cybersecurity has never been more critical. As the National Infrastructure Advisory Council recently wrote in a report: "There is a narrow and fleeting window of opportunity before a watershed, 9/11 level cyber-attack to organize effectively and take bold action."[10]

RESOURCES

[1] https://e-discoveryteam.com/2014/03/16/best-practices-in-e-discovery-for-handling-large-stores-of-unreviewed-client-data/.

[2] http://www.insidecounsel.com/2017/04/27/3-ways cybersecurity-demands-are-changing-e-discov.

[3] https://digitalguardian.com/blog/what-data-encryption.

[4] https://www.americanbar.org/publications/gp_solo/2012/november_december2012privacyandconfidentiality/encryption_made_simple_lawyers.html.

[5] http://blog.allegorylaw.com/panel-next-generation-of-litigation-technology.

[6] https://www.iso.org/isoiec-27001-information-security.html.

[7] https://www.dcbar.org/bar-resources/practice-management-advisory-service/upload/Locked-Down-Information-Security-for-Lawyers.pdf.

[8] https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html.

[9] http://www.insidecounsel.com/2017/04/27/3-ways-cybersecurity-demands-are-changing-e-discov.

[10] https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.

Connecting corporations and law firms

Throughout an entire case, in a single platform

LLM
LIQUID LITIGATION MANAGEMENT, INC.

LLM, Inc. unifies the legal process by combining legal holds, case strategy, matter and budget management, review and analytics in a single, web-based platform. We connect legal strategy to tactics in a way no one else can, so every part of the process is actionable. Our product scales to help corporate and law firm teams gain cost-savings and eliminate inefficiencies.

Connect@llminc.com | LLMinc.com | @LLMInc | 877-820-8308