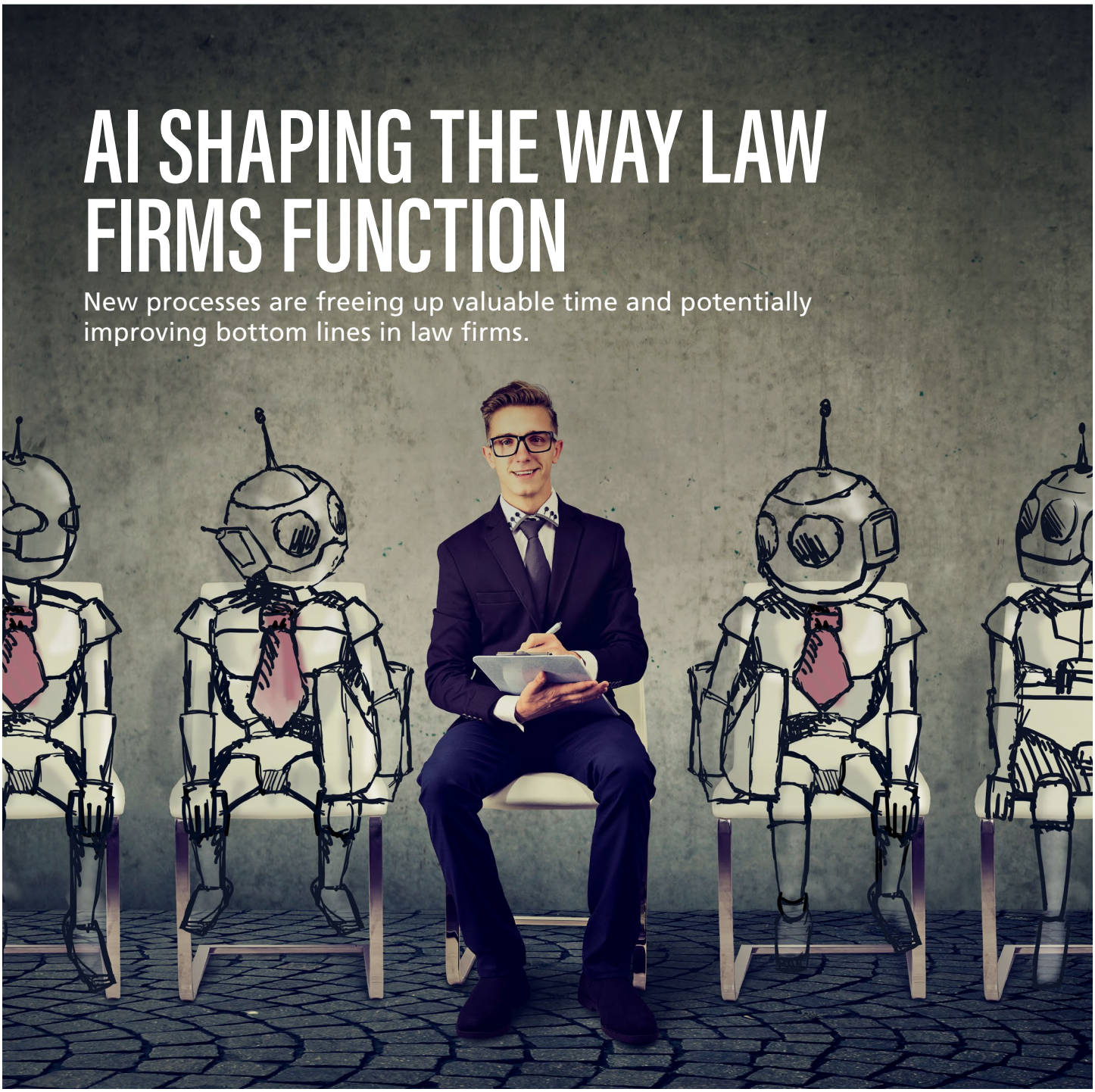
OCTOBER 2018
VOLUME 37 • ISSUE 9

LEGAL MANAGEMENT

THE MAGAZINE OF THE ASSOCIATION OF LEGAL ADMINISTRATORS



AI SHAPING THE WAY LAW FIRMS FUNCTION

New processes are freeing up valuable time and potentially improving bottom lines in law firms.

PROLAW.

BECAUSE THE NEED FOR CRITICAL DATA DOESN'T STAY IN THE OFFICE.

RUN YOUR BUSINESS FROM WHEREVER YOU ARE. ProLaw® Mobile from Thomson Reuters Elite™ moves at the speed of business to help you make the most of every minute. You can view current matter information and documents, schedule and save appointments, and save emails and attachments. Enter your time when you're in transit or between appointments. And know your entire team is current because the unified ProLaw database is always up to date. It's software on the move for lawyers on the go.

THE ONE OFFICE SOLUTION. PROLAW.COM

©2014 Thomson Reuters L-390527/4-14
Thomson Reuters and the Kinesis logo are trademarks of Thomson Reuters.

THOMSON REUTERS™

LEGAL
MANAGEMENT

OCTOBER 2018
VOLUME 37 • ISSUE 9

FEATURES

LEGAL INDUSTRY/BUSINESS MANAGEMENT BY KYLIE ORA LOBELL
AI IS SHAPING THE WAY LAW FIRMS FUNCTION 19
New processes are freeing up valuable time and potentially improving bottom lines in law firms.

OM COURSE BY MARK BREWER
CLIENTS TURN UP THE HEAT ON CYBERSECURITY 24
Expectations and regulations aren't getting any easier to deal with. Here's how your firm can learn to stand the heat and stay in the kitchen.

OM COURSE BY ERIN BRERETON
COULD DATA ENCRYPTION BE YOUR LAST LINE OF DEFENSE AGAINST HACKERS? 28
Some firms are using the technology to protect electronic communications and other files. Find out what it entails.

COLUMNS

BIG IDEAS: A MESSAGE FROM ALA'S PRESIDENT 4
Fore!

BP PERSPECTIVE 7
Decrypting Encryption in the Legal Environment

INNOVATIONS 11
Information Rights Management: The Next Step in Information Governance and Security?

THINKING OUT CLOUD 14
Getting Down to Cloud Basics

TEST DRIVE 16
Technology to Go

DEPARTMENTS

INDUSTRY NEWS 32
Information Security in the Digital Age

TIPS AND TRENDS 35
7 Strategies and Tools to Help Boost Your Law Firm's Social Media Performance
Why Should Law Firms Have Two Brokers When It Comes to LTCI?

ALA NOW

ALA FACES 40
Anniversaries, Awards and Appointments

LEGAL MANAGEMENT STAFF

PUBLISHER
Oliver Yandle, JD, CAE
oyandle@alanet.org

EDITOR-IN-CHIEF
Theresa Wojtalewicz
twojtalewicz@alanet.org

ASSOCIATE EDITOR
Kate Raftery
kraftery@alanet.org

ADVERTISING OPPORTUNITIES
Robert Leighton
advertising@alanet.org

ART DIRECTOR
Jeff Wojciechowski
Straight North, LLC

GRAPHIC DESIGNERS
Abby Burkle
Straight North, LLC

Cristina Muzzio
Straight North, LLC

WEB TEAM
Eric Michalsen
Straight North, LLC

Greg Wixted
Straight North, LLC

Copyright © 2018 Association of Legal Administrators. All Rights Reserved.

APRIL CAMPBELL, JD
2018–2019 ALA President
Director of Administration
McCullough Hill Leary, PS

Fore!

Look into my crystal ball. No, really, look in to it. What do you see? We talk about hindsight all the time, but how often do you discuss foresight? Maybe you are talking about it and don't even know it.

What will the future look like? This is a question we find ourselves asking more and more in the legal industry … and it is one that the ALA Board of Directors asks ourselves every time we meet. We have an obligation to you, our members, to keep ALA relevant to you as you navigate the profession.

> "We have an obligation to you, our members, to keep ALA relevant to you as you navigate the profession."

The word "foresight" has popped up quite a bit in association and industry publications, as we try to figure out what the future holds. Foresight is the ability to predict what will happen and what the needs will be in the future. It is more than just a guess. It requires some research, observation and luck.

So what do we know? Or what can we guess? We know that 10 years from now only about 5 to 10 percent of the workforce will be Baby Boomers and that Generations Y and Z will make up about 70 percent of the workforce. With that information alone, we should be able to come up with some predictions regarding the leadership styles and work habits and requirements that will be the norm in our workplaces.

TECHNOLOGY AND AI PAVE THE WAY

I had the pleasure of attending the ALPMA (Australasian Legal Practice Management Association) conference last month, and it was eye-opening to see how law firms and attorneys are developing technology so they can get into and stay in the game. They have developed technology to assist with a faster, more efficient divorce process, methods to buy and sell real estate without the need for attorneys, and a modernized client intake process where a bot gathers client information before the attorney and client meet for the first time. These great examples highlight how firms and businesses are really trying to change the way users experience their services.

In shaping my thoughts about developing foresight, I try to picture everything around me in my office to figure out what can be done (better) through technology. At the ALPMA conference, one of the speakers mentioned that the careers of radiology, ophthalmology and long-haul trucking could soon be taken over by technology and artificial intelligence (AI) and no longer exist for humans. In what areas of law is that most likely to happen? His suggestion was to look for the areas that have large amounts of money on the table and large data sets available. My mind has been racing ever since I sat in that session.

KEEPING UP WITH CHANGE

If you are like me, thinking about all of this makes your head spin. I love the idea of it, but then I stress out thinking about how I am going to keep up with — and on top of — all this change. That is when my Board member hat goes on and I start thinking about all the resources we need as members, how ALA can provide them, and what changes we need to make as an Association to ensure we can deliver. I know the old adage is "If it ain't broke, don't fix it," but things are moving too quickly to risk letting something break down until it is no longer of use. That is what the Board is working on this year: not waiting, deploying some foresight and trying to stay ahead of the game. I promise there is more information to come soon.

I will leave you with the description of a slide that was shown during a presentation at the ALPMA conference. It included a drawing of an operating room from the 1800s, a photo of a present-day operating room, a drawing of a courtroom from the 1800s and a photo of a present-day courtroom. The operating rooms could not have been more different from each other, highlighting the technological and medical innovations that have occurred over the centuries. The courtrooms were almost identical except for the clothing and the powdered wigs. It was a great reminder that change in this industry is definitely due and will continue at a quicker pace in the future. ■

acampbell@mhseattle.com
www.linkedin.com/in/april-campbell-ba0954a

The **Job Description Toolkit**

Use this free-to-members resource to improve your hiring process and better manage your employees' performance. It includes:

- Resources and tools for writing job descriptions — including an easy-to-use, editable template
- Guide to creating job descriptions that apply ALA's Uniform Process Based Management System (UPBMS) taxonomy
- 40+ sample job descriptions — using the UPBMS — in the areas of legal support services, finance, HR, marketing, technology and IP

Improve your hiring process!

ALA Association of Legal Administrators

alanet.org/job-toolkit

LEGALMIND®

SERVING UP A TASTY APPROACH TO TALENT DEVELOPMENT

Select from an extensive menu of topics that you can access anytime, anywhere, from any device.

CLIENT SERVICE DELIVERY

PROBLEM SOLVING

BUSINESS DEVELOPMENT

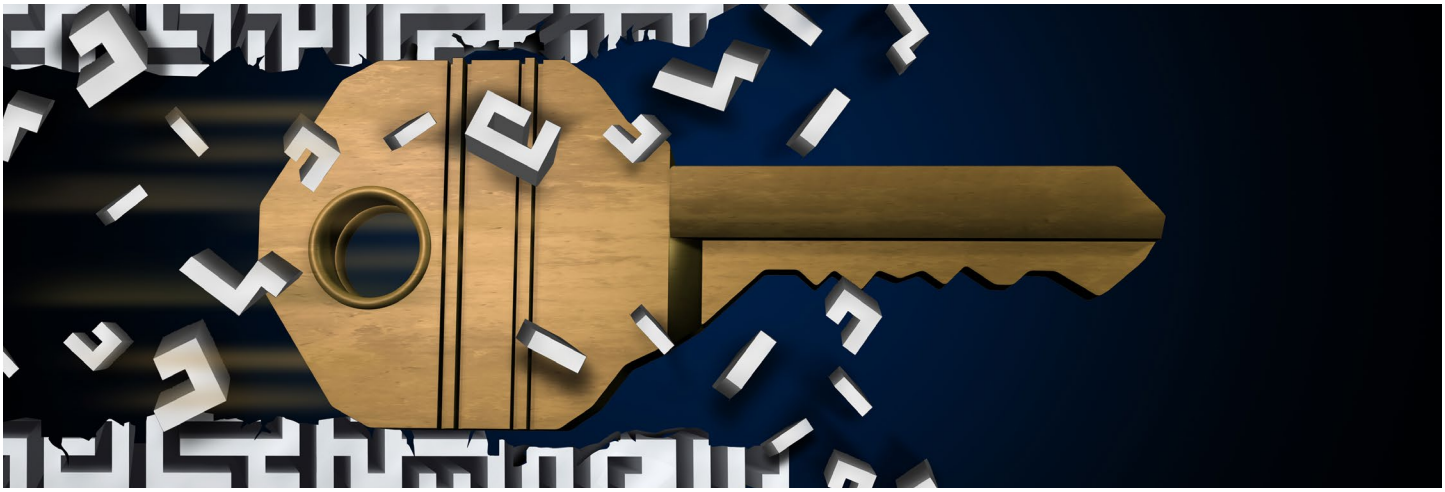
PROFESSIONAL DEVELOPMENT

COMMUNICATION

TECHNOLOGY

Let's Talk! 214.742.6224 | www.travelingcoaches.com/legalmind

traveling coaches



Decrypting Encryption in the Legal Environment

MICHAEL KEMPS & DAVID LAM, CISSP
Kemps (left), Chief Executive Officer, Innovative Computing Systems
Lam (right), CISSP, Vice President, Citadel Information Group

When discussing encryption, three questions typically come up: Why do we need encryption within our system? Are other law firms using it? How do we enable it seamlessly without frustrating our people?

Encryption is one important part of a law firm's overall data security process. As with many things information-security-related, encryption is a word that's thrown about as a significant requirement but without a lot of clarity. This article discusses the reasons for encrypting your data, considers the system requirements for having encryption in place and addresses modern solutions for this practice.

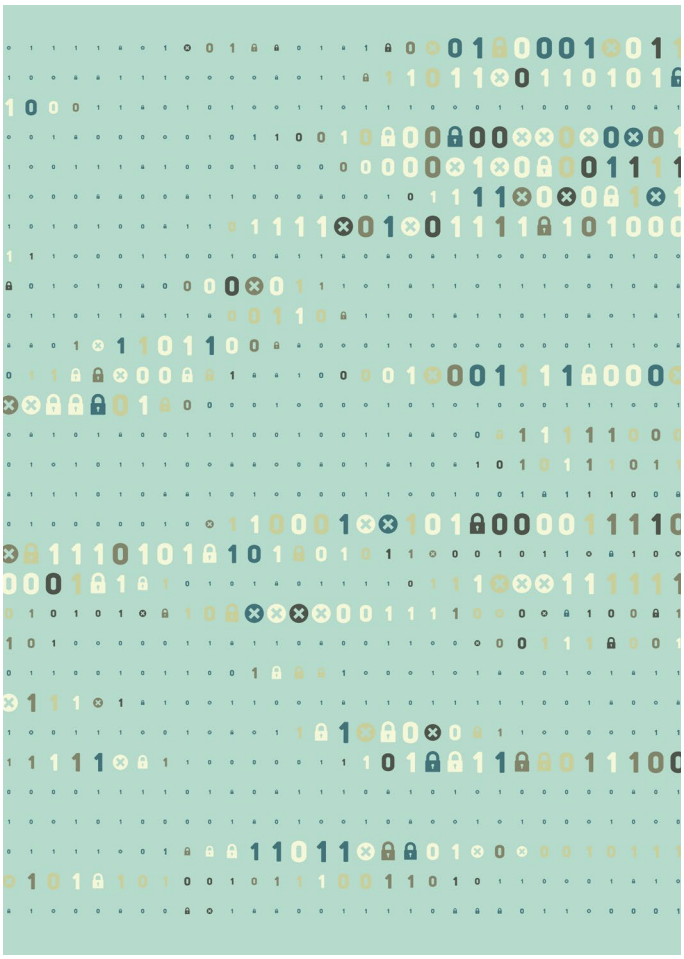
> "Law firms must take numerous steps to ensure that client information is kept confidential, its integrity is maintained and it's available when needed."

In its 2017 Purchasing Survey, the International Legal Technology Association (ILTA) found increasing use of encryption across law firms of all sizes. Encyrption was used for hard drives, email, removable media, smartphone devices, file server volumes and document management systems. This trend demonstrates increasing commitment to the protection of client data from law firm management.

Attorneys have a duty of confidentiality that is broader than the attorney-client privilege. They have both legal and moral obligations to keep confidential information private. Law firms must take numerous steps to ensure that client information is kept confidential, its integrity is maintained and it's available when needed.

ENCRYPTING DATA IN TRANSIT AND AT REST

There are two primary modes for encryption. In the first, data being transferred between two systems, such as your web browser and a website, can be sent encrypted so that someone who is not on either your computer or the web server cannot see it. Thus, your password, account balance and other personal information are not readily readable as they



leave your laptop, go through a public internet connection, pass through multiple stops along the internet and eventually arrive at a server.

The second methodology for encryption involves encrypting the data when it is resting on a system without being used by a program or user. Let's say your laptop is stolen. If your laptop is appropriately encrypted, data written to a disk is not accessible without your password. If someone steals your laptop, they cannot remove the disk and read it with another system. Similarly (though less likely), if someone was to steal one of your servers, they couldn't just pull out your hard drive(s) and access the data on another server.

ENCRYPTION IMPLEMENTATION

Successfully employed, encryption may be implemented while remaining invisible to the end user. Using encryption technologies can also improve security in other areas — such as requiring the use of a virtual private network (VPN) to access your network remotely or requiring a secure website in order to gain access to encrypted data in the cloud.

Implementing encryption does increase processor and memory overhead on your systems. On modern environments, this should not be a problem. However, utilizing encryption with aging systems will likely result in lower performance. In some cases, we have even seen data loss because the system cannot keep up the processing requirements. Faced with significant capital expenditures associated with these upgrades, many law firms are transitioning to cloud technologies as an alternative.

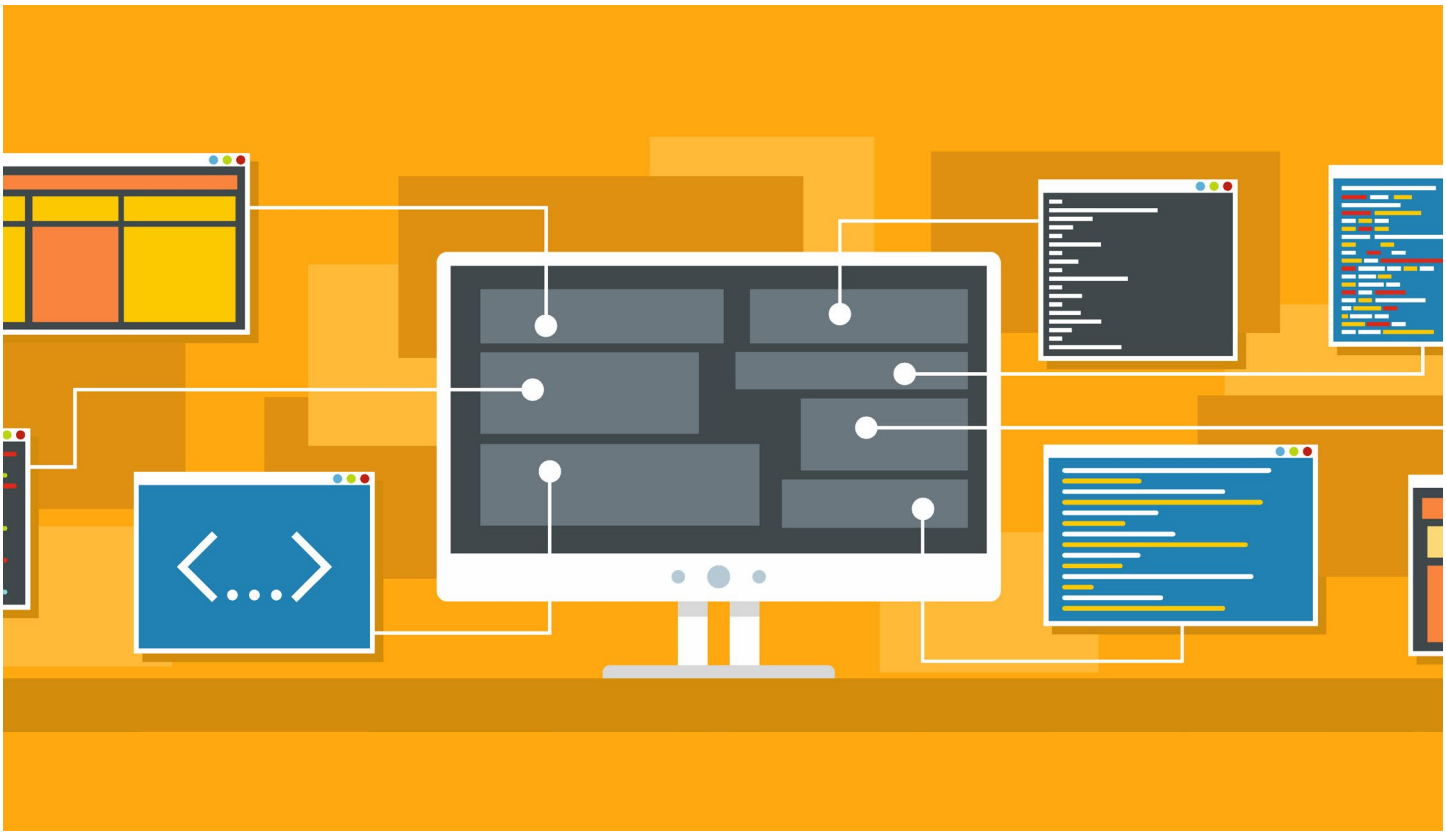
ENCRYPTION AND TECHNOLOGY AUDITS

Encryption requirements around client collaboration are being recognized through more frequent client-initiated technology audits. Clients are increasingly concerned about the secure transmission of emails and matter-related data files. Numerous vendors provide solutions to secure email and documents, although all encryption solutions are not created equal. Encryption can be accomplished within email platforms (e.g. Office 365, Mimecast, Proofpoint, etc.), file-sharing solutions (e.g. Citrix ShareFile) and document management systems (e.g. iManage Share and NetDocuments ShareSpace). These and similar cloud-based platforms ensure that data is encrypted and secured with user-specific access credentials and controls. Many even integrate with on-premises directories and multifactor authentication options.

Integrating third-party encryption solutions into the end-user experience can be a challenge. Vendors typically provide software plug-ins that attempt to seamlessly integrate with the Microsoft operating system and Office suite. Some excel at this better than others, so they need to be evaluated and piloted prior to adoption. The additional demand on processor and memory caused by Outlook and Word add-ins can cause performance and stability problems, so proceed with caution.

CLOUD ENCRYPTION

As mentioned before, cloud offerings can meet rigorous compliance and security requirements at a more reasonable cost than previously available. Today, more and more law firms are taking advantage of cloud computing resources. Top-tier cloud providers (e.g. Amazon Web Services, Microsoft Azure, etc.) provide fully integrated encryption technologies by default and without the same hardware requirements that may be needed locally. When properly deployed, these technologies can be more secure than traditional on-premise installations.



ENCRYPTION'S PLACE IN INFORMATION SECURITY STRATEGY

It is important that encryption be considered as part of a law firm's overall information security strategy.

A fully protected legal technology environment, whether on-premises or cloud-based, must include more than just encryption and file-sharing policies. First, the law firm must have a method for managing information security, known as an Information Security Management System (ISMS). Without policies and standards to know what to do, law firms are often left with major gaps in their information security posture. Internal information technology teams and third-party technology vendors often lack sufficient information security expertise or bandwidth. Developing an internal committee, supported by appropriate information technology and information security expertise, is becoming more commonplace and is considered a minimum starting point for managing information security.

When properly integrated into your information security strategy, encryption will ensure that your law firm's duty of confidentiality is met while protecting both the firm's data and its reputation. ■

ABOUT THE AUTHORS

Michael Kemps is the Founder and Chief Executive Officer of Innovative Computing Systems. He founded the company in 1989 after developing relationships with several law firms that eventually became early clients.

mkemps@innovativecomp.com
www.innovativecomp.com
twitter.com/ICSGetsIT
www.linkedin.com/company/innovative-computing-systems-inc/

David Lam, CISSP, is a Vice President at Citadel Information Group. Lam has 31 years of IT experience focusing on securely managing information for small and medium businesses. He is a Certified Information Systems Security Professional (CISSP), Certified Protection Professional (CPP) and Certified Six Sigma Black Belt.

dlam@citadel-information.com

KONICA MINOLTA

All Covered

IT SERVICES FROM KONICA MINOLTA / **LEGAL**

THE LAW FIRM OF THE FUTURE. HERE. NOW.

kmbs.konicaminolta.us/legal

PRODUCTS, SOLUTIONS AND SERVICES
THAT WILL USHER YOU INTO THE FUTURE:

- **MANAGED VoIP SERVICES**
- **INTEGRATION OF LEGAL TECHNOLOGIES**
- **PRINT MANAGEMENT/ COST RECOVERY**
- **MANAGED IT AND CLOUD SERVICES**
- **WORKFLOW ANALYSIS AND DOCUMENT MANAGEMENT**
- **LAWYER'S HELP DESK**

Providing innovative technology for the legal community for decades through relationships built on trust and delivery of world-class service.

KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC. 100 Williams Drive, Ramsey, New Jersey 07446
© 2018 KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC. All rights reserved. KONICA MINOLTA and the KONICA MINOLTA logo are registered trademarks or trademarks of KONICA MINOLTA, INC.

IAN RAINE
VP of Product Development, iManage

Information Rights Management: The Next Step in Information Governance and Security?

As the guardians of privileged and sensitive data, law firms have their work cut out for them on the security front. External bad actors are constantly trying to get their hands on firms' confidential information through cyberattacks, while insiders pose a threat of their own if they use their internal access rights to view content they shouldn't.

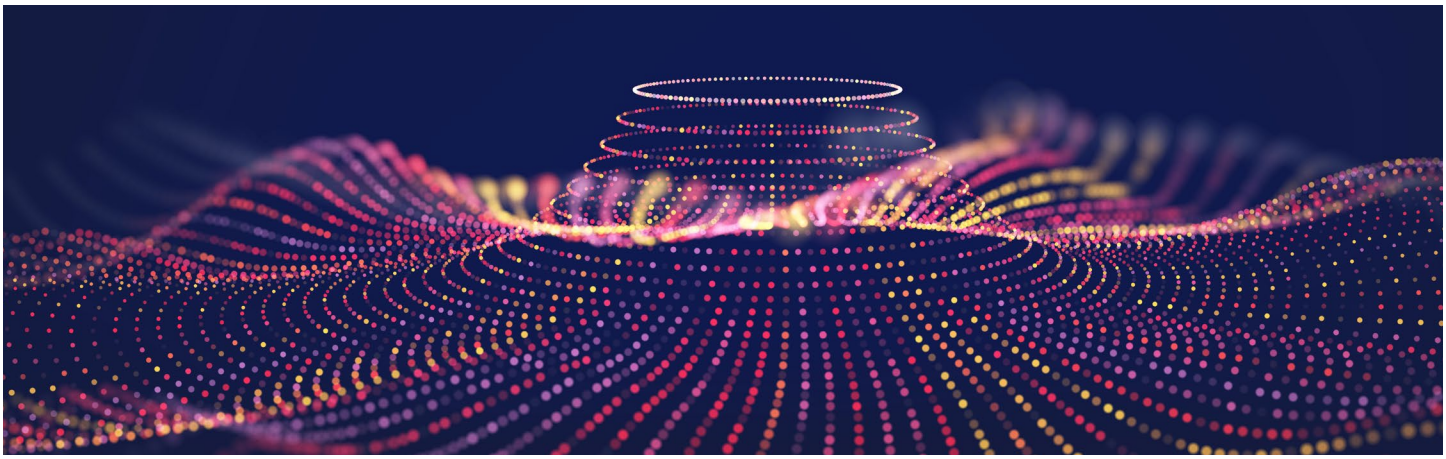
> "Information rights management ensures that protection travels with the document always, even beyond the perimeter of the DMS or even outside the firm."

As if that wasn't enough to keep law firms up at night, data leakage can occur through far less nefarious and much more mundane events than cyberattacks or internal sabotage. For example, a lawyer could accidentally email a confidential document to the wrong recipient. That's right: a simple user error — like sending a finalized contract to your old colleague Jane Smith instead of your client Jan Smith — can wreak just as much havoc on your firm's reputation as an external or internal breach.

For these reasons and more, law firms and legal departments should be implementing comprehensive security and information governance strategies. And increasingly, organizations are recognizing that information rights management (a type of digital rights management) could play an important role in these strategies.

PROTECTION THAT TRAVELS WITH THE DOCUMENT

So what exactly is information rights management, and what does it do? In summary, it encrypts a document and then restricts who can access it and what they can do with it. Information rights management is flexible in that the restricted operations for a document can vary — for example, preventing printing or re-saving to a different location, disabling the ability to copy or restricting viewing and editing of the data.



At this point, you might be saying to yourself: "I have a very good document management system (DMS) and a need-to-know security solution that segregates content and controls which files someone can access. Why do I need information rights management?"

A DMS and a need-to-know security solution can certainly provide a very effective layer of protection for sensitive documents — as long as the documents stay within the "perimeter" of those products. However, if somebody within a law firm were to export a document from the protected workspace of their DMS and drop it into an unprotected Windows file share or email it to someone, then the access control and protection provided by the DMS and security solution are lost.

That's why information rights management is so important: It ensures that protection travels with the document always, even beyond the perimeter of the DMS or even outside the firm. It doesn't matter if a document is exported to a file share, checked out to a local C drive or attached to an email — whenever a document from a sensitive matter or restricted workspace leaves the DMS perimeter, information rights management ensures that it continues to be protected while it's "out in the wild."

Information rights management is only useful, of course, if it has been applied to documents. And people will only implement information rights management if it's an easy, frictionless process.

An ideal information rights management solution will automatically stamp a document with policy that reflects the DMS's security settings as soon as it leaves the perimeter. All the various permissions — the users who are allowed access, the types of operations that are allowed with the document — will follow the document as it circulates outside the DMS perimeter, automatically protecting against the possibility of that content getting into the wrong hands.

DATA LOSS PREVENTION MADE EASY

Think of the uncontrolled copies of sensitive documents that are sitting around a firm as locally stored items on users' laptops. Consider the number of documents that are accidentally emailed to the wrong person or emailed to someone who then, without the original sender's knowledge, forwards it on to somebody else.

Information rights management aims to address these problematic scenarios, helping to cut down the potential for data leakage. With information rights management, there is a greatly reduced chance for somebody who wasn't supposed to receive a document to access and view its contents, regardless of whether they obtained the file through malicious activity or through user error.

Consider information rights management as one more piece of the security puzzle that is coming down the road for law firms or legal departments. Security is an ongoing journey, and information rights management could very well be the next step in information governance for organizations that want to ensure greater levels of protection for their critical files and sensitive information. ■

ABOUT THE AUTHOR

Ian Raine is the VP of Product Development with iManage. He has more than 25 years of experience in the IT industry, building information governance and records management software products for the enterprise.

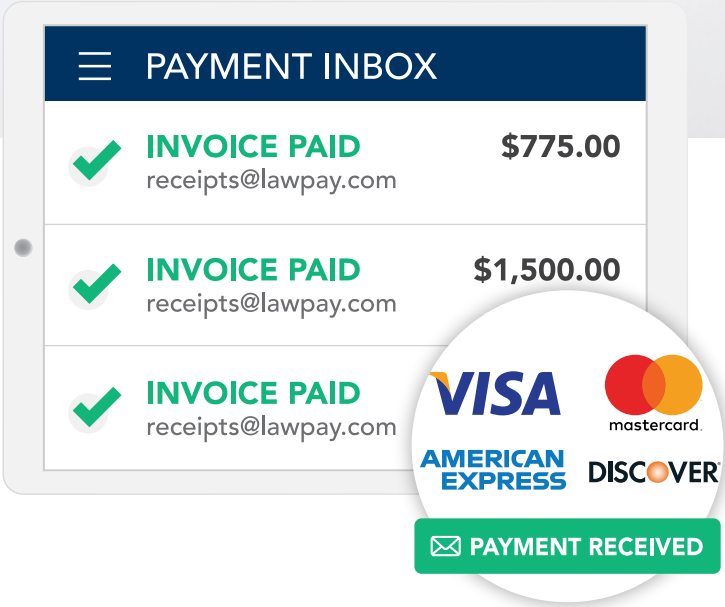
LAWPAY IS FIVE STAR!

★★★★★

In our firm, it's actually fun to do our billings and get paid. I send our bills out first thing in the morning and more than half are paid by lunchtime. **LawPay makes my day!**

– Cheryl Ischy, Legal Administrator
Austin, Texas

Trusted by more than 35,000 firms and
verified **'5-Star'** rating on ★ Trustpilot



LawPay®
AN AFFINIPAY SOLUTION

THE #1 PAYMENT SOLUTION FOR LAW FIRMS

Getting paid should be the easiest part of your job, and with LawPay, it is! However you run your firm, LawPay's flexible, easy-to-use system can work for you. Designed specifically for the legal industry, your earned/unearned fees are properly separated and your IOLTA is always protected against third-party debiting. Give your firm, and your clients, the benefit of easy online payments with LawPay.

866-921-0115 or visit **lawpay.com/ala**

LawPay is proud to be a VIP Business Partner of the Association of Legal Administrators.

ALA VIP℠ Value in Partnership

Special offer for ALA members.
Call for details

LawPay is a registered ISO of Citizens Bank, N.A.

KENNY LECKIE
Senior Technology and Change Management Consultant, Traveling Coaches

Getting Down to Cloud Basics

Cloud, cloud, cloud — it's hard to go a day without hearing about it. Let's think this "cloud thing" all the way through by taking a high-level look at the following questions: What is it? Is it safe? What are the benefits? What are the risks? Why should I care?

> "Keeping data safe is paramount for an organization and its individuals, so cybersecurity must be addressed."

WHAT IS IT?

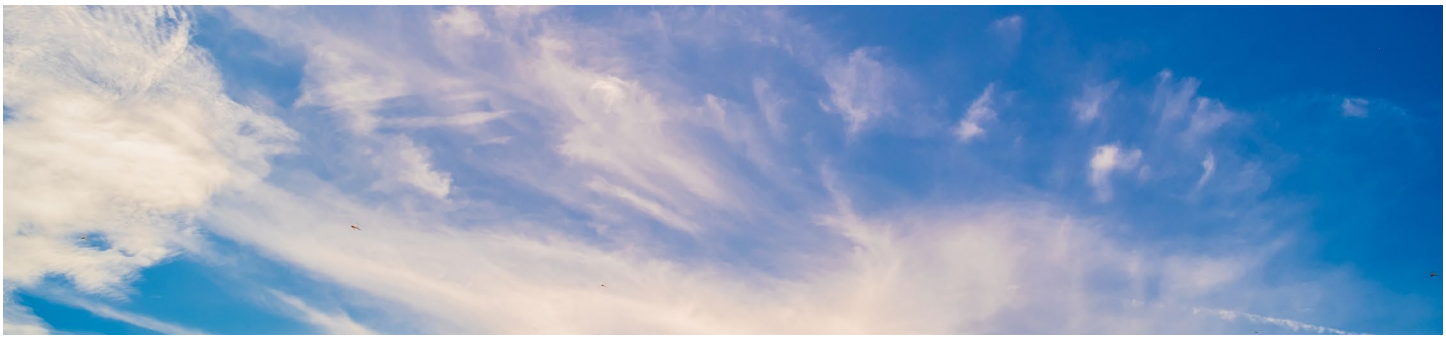
Cloud computing refers to "the practice of using a network of remote servers hosted on the internet to store, manage and process data, rather than a local server or a personal computer" (thank you, Google). In our firms and in our lives, we access data all the time. So where is it? A cloud service hosts your data and information on servers that are located somewhere other than your server room or personal computer. You may hear people discuss "on premises" (or "onprem") versus "hosted" (aka "in the cloud"). The difference is where the data is located and how you access it.

Here are some examples of cloud computing services: Microsoft Office 365, Google Cloud, Apple iCloud, Amazon Web Services, and HR and payroll systems like ADP. Most people use cloud computing services every day whether they realize it or not.

IS IT SAFE?

Keeping data safe is paramount for an organization and its individuals, so cybersecurity must be addressed whether the information is housed onprem or hosted. Ask yourself: Where is the data that matters to you? How do you access it? Is it protected? Is it backed up and recoverable?

As Adam Levin, Chairman of identity protection service CyberScout, told *NBC News*, "It is no longer realistic to believe that we can prevent these attacks from happening, but we can be prepared to minimize the damage and recover quickly." Cloud-based tools that focus on protecting data are in a better position to provide the types of safeguards that might otherwise be cost prohibitive to the average company or individual.



WHAT ARE THE BENEFITS?

With cloud services housing your data, you no longer have the responsibility of maintaining, securing and protecting the hardware required to keep that data onprem. The onus of responsibility is shifted to the service provider. This frees you up to manage your technology resources rather than maintain them. Also, the subscription model of most cloud computing services allows you to adjust for needs quickly. You can scale your costs immediately to adapt to your current business needs. Budgeting becomes more scalable and predictable.

Other benefits of cloud computing include:

- Instant disaster recovery built into the service
- Built-in business continuity plans
- Accessibility options that would require extra effort to provide with onprem solutions
- Increased mobility options for a highly mobile workforce
- With many of the services, instant collaboration and coauthoring options internally and with clients

Cloud computing allows a business to be nimble and creates the type of connectivity that meets the demands of today's workforce.

WHAT ARE THE RISKS?

Whether your data is onprem or in the cloud, there are constant risks surrounding its protection. You are responsible for conducting due diligence and making sure the proper safeguards are in place to protect your information. With cloud computing, it is important to read the terms of service. Know the difference between a "consumer-grade" system and an "enterprise" solution. Consumer-grade products and services offered by cloud providers like Dropbox and Google have very different conditions around their rights to the data versus yours. For work-related information, you should never use a consumer-grade service. Cloud providers offer professional enterprise services that you should use instead.

Another risk has to do with the way you access the data. The new "perimeter defense" is no longer your network — it's your identity. The way you verify that users are who they say they are when accessing data is vital. Authentication methods have broadened beyond simple usernames and passwords. Whether you are using cloud services or onprem services, you should implement multifactor authentication. The risks outweigh the inconvenience by far.

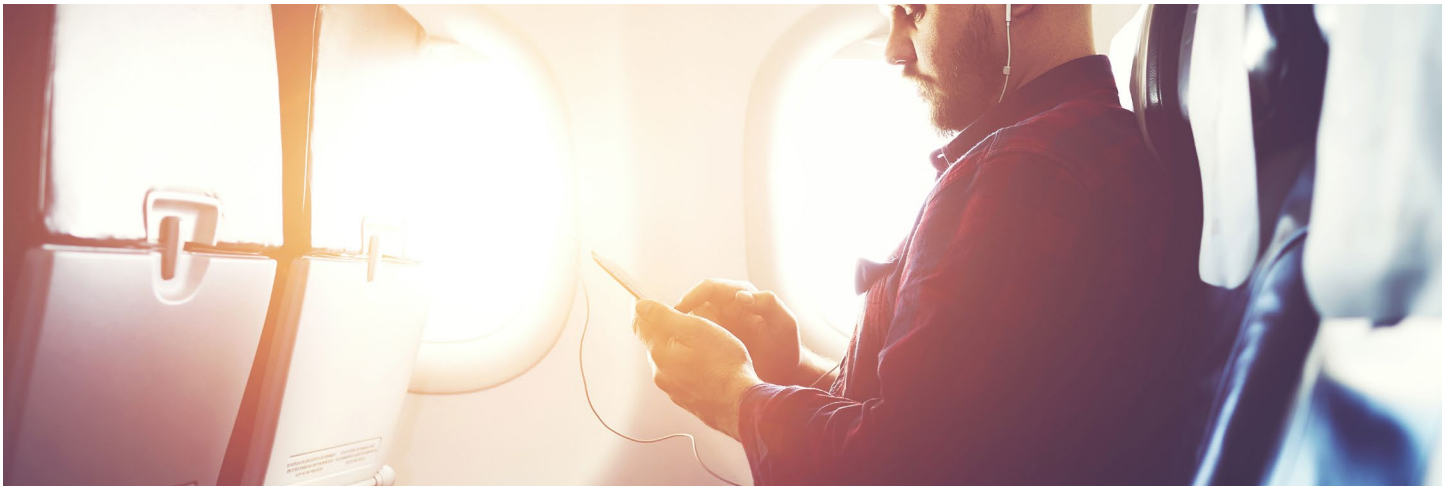
WHY SHOULD I CARE?

The cloud is the great equalizer for businesses. It levels the playing field for companies of all sizes. The agility the cloud provides allows you to adjust to constantly changing business and client demands, making this a compelling way to approach technology in your organization. Clients who once resisted cloud services are now using them and expecting that you do the same. If you are not in the cloud now, you will be soon. If you haven't started planning out your cloud strategy, you should. The times are changing, and we must change with them. ■

ABOUT THE AUTHOR

Kenny Leckie is a Senior Technology and Change Management Consultant with Traveling Coaches. He helps clients develop and deploy custom programs with an emphasis on user adoption and increased return on investment. Leckie is a Prosci Certified Change Practitioner and a Certified Technical Trainer, and he was named 2018 Innovative Consultant of the Year by the International Legal Technology Association.

kleckie@travelingcoaches.com



BILL & PHIL
William Ramsey, Partner, Neal & Harwell
Phil Hampton, Consulting President, LogicForce

Technology to Go

Our motto has always been "Have tech. Will travel." If you have ever been behind us at airport security, you probably switched to another line. We tend to slow the process down a bit with all our tech gadgets. But we love our gadgets because — minus the security screening — they make our travel so much easier. Here are just some of our favorite travel tech gadgets and apps.

> "Sometimes the best tech is really just low tech."

BOSE QUIETCOMFORT 35

A pair of **Bose QuietComfort 35** wireless headphones is an essential travel accessory for us, especially on particularly long trips. These bad boys are not cheap, but we think that Bose sets the standard for noise-canceling technology. It is so nice to slip these headphones on and simply shut off the noise in the plane, train or automobile while streaming music or movie audio from our phone or tablet. The over-the-ear fit is very comfortable, and the battery life is well over 15 hours. These headphones now even have Amazon Alexa and Google Assistant voice control built in.

EMEET M1 AND BOSE SOUNDLINK MICRO

While not all our travel is business-related, a good bit of it is; consequently, we sometimes find ourselves participating in online meetings and conference calls in the back of an Uber, in a hotel room or in an airport lounge. We always pack an ultra-portable smart speaker that we can use to stream audio from our phone while on the go. Two of our favorites are the **eMeet M1** Bluetooth speaker and the **Bose SoundLink Micro** Bluetooth speaker. The eMeet M1 is really good as a speakerphone on the road when you have multiple people on the call at your location. The Bose SoundLink Micro has that really rich Bose sound and also happens to be waterproof.

HIPMUNK

There seems to be an endless parade of travel aggregator sites that all promise to find the best flight, hotel and rental car deals. The one app we find incredibly easy to use and very helpful is **Hipmunk**. Hipmunk is especially informative in selecting flight reservations. We love

the way Hipmunk displays the available flights based on a scale ranking the flights from least painful to most painful, taking into account the price, any layovers, and departure and arrival times. We started using Hipmunk several years ago just for airline reservations, but you can now use it to book your entire trip with just a click of a button. Hipmunk really has become a digital travel assistant.

AIRHOOK

Sometimes the best tech is really just low tech. We hate using the foldable tray tables on airplanes because they're germ magnets. So we love that there are creative, smart people who think like we do because some of these people came up with a wonderful invention, the **Airhook**. The Airhook is just a smartphone/tablet holder combined with a cup holder that attaches to the tray table in its upright position. Three problems solved at once. This is about the smartest tech we can think of that doesn't require electricity.

SKYROAM SOLIS

We all know that so-called "free Wi-Fi" is a big security risk when traveling, so we always bring along our own personal Wi-Fi device. Generally the Wi-Fi device from our mobile phone carrier, for which we pay a monthly fee, is just fine for domestic travel. Accessing secure mobile Wi-Fi can be trickier when traveling internationally, however. The **Skyroam Solis** 4G LTE global Wi-Fi hotspot is a great travel accessory for the international traveler. This device works in more than 130 countries, and you can access fast internet speeds at the click of a button with no need for foreign SIM cards. You pay just for what you use, and there are no limits or contracts.

COWAROBOT AND MODOBAG

Finally, the ultimate in travel tech can be seen in a new genre of suitcase called "smart luggage." We have tried many types of smart luggage at various points along the "smartness" continuum. At the far end are two budget-busting smart suitcases that really take this tech to a new level. The **Cowarobot** is a $1,500 smart suitcase that is really a luggage robot. This self-moving suitcase will actually follow you as you wind your way through a busy airport. And, if that isn't crazy enough for you, check out the Modobag, a $1,500 smart suitcase that you can actually ride to your airline gate. When you see Bill riding his **Modobag** and Phil leading his Cowarobot like a pet dog, you will have witnessed the apex of smart travel tech — or perhaps the ultimate in frivolous tech spending. You decide.

See you on the road. ■

ABOUT THE AUTHOR

William Ramsey, Partner at Neal & Harwell, and **Phil Hampton**, Consulting President of LogicForce, are best known for *The Bill and Phil Show.*

www.twitter.com/BillandPhil

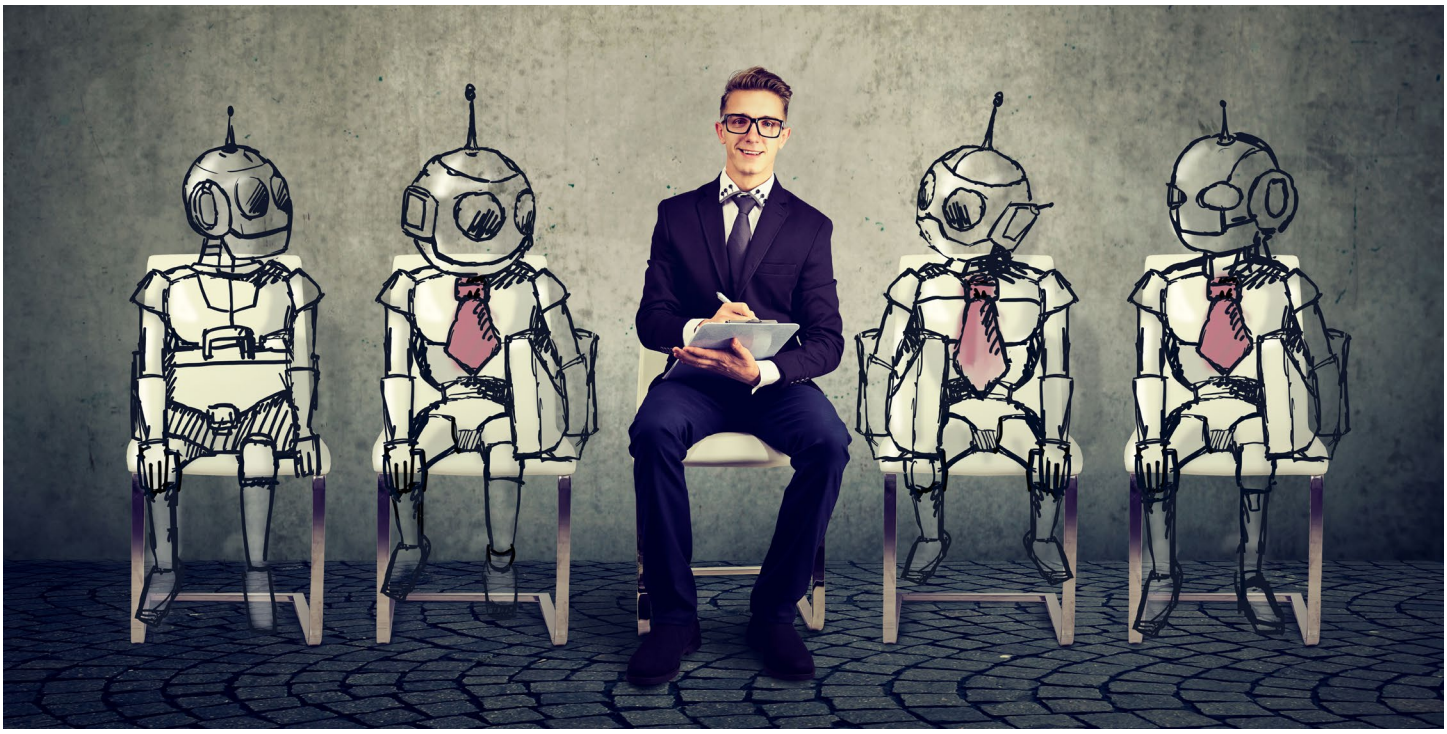
FEES. BILL. PAID.

The only four-letter words
you'll be using
when you use Tabs3.

Tabs3
Reliable Software. Trusted Service.

Billing PracticeMaster® Financial

FREE TRIAL at Tabs3.com



AI Shaping the Way Law Firms Function

New processes are freeing up valuable time and potentially improving bottom lines.

KYLIE ORA LOBELL
Freelance Writer

Artificial intelligence, or AI, has definitely become a media buzzword. But businesses truly are utilizing AI to perform tasks more quickly and gain deeper insight into their customers and clients. It is cheaper and smarter than manual human input for some tasks and can result in better bottom lines for organizations.

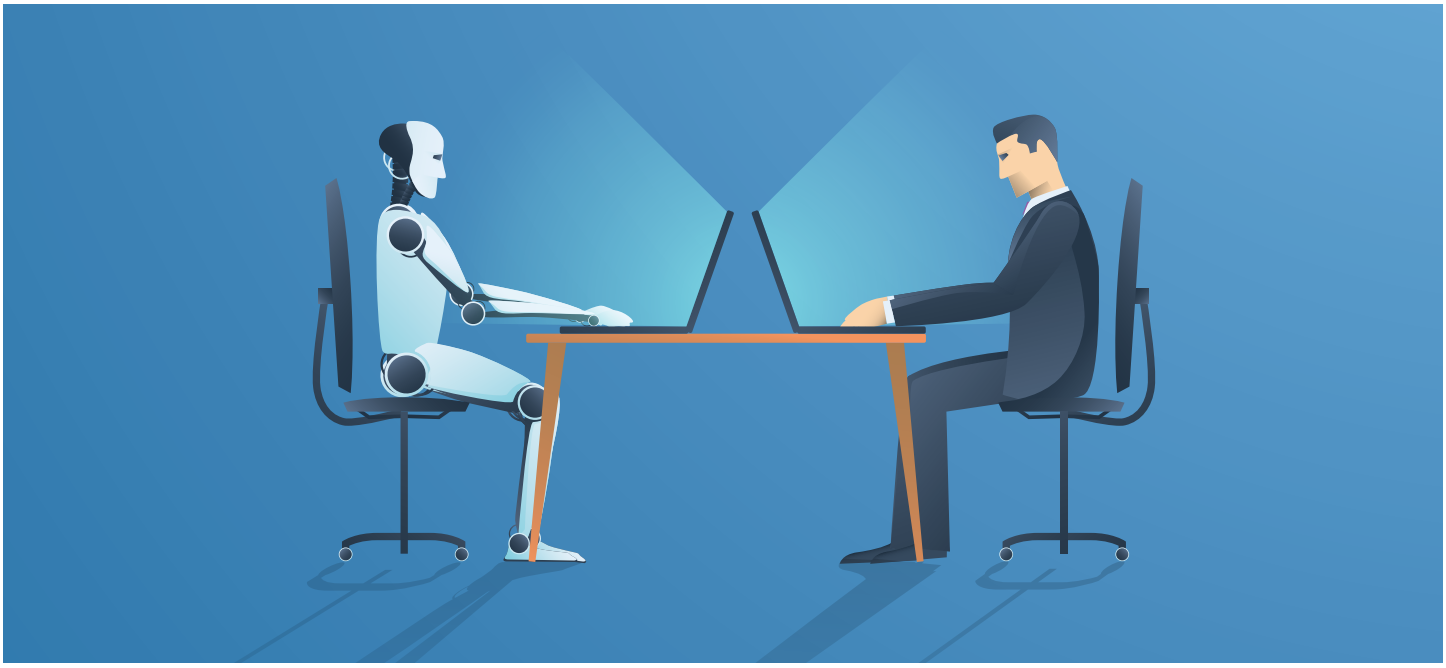
Law firms are catching on to the AI trend and will continue to use it at an even higher frequency in the future. "AI is making a huge impact in the legal industry," says Alistair Wye, Lead Product Strategist for iManage RAVN. "AI technology enables lawyers to work more efficiently, deliver more valuable insights to their clients and create entirely new services that might previously have been cost prohibitive."

If you want to use AI within your own law firm, you first have to start at the basics. You need to learn about AI and how it can help you improve your firm's own performance.

WHAT IS ARTIFICIAL INTELLIGENCE?

While animals and humans are born with natural intelligence, computers and other machines have artificial intelligence. AI gives machines the ability to learn from experience and make decisions based on past processes. Powered by natural language processing and deep learning, they can look at huge data sets and recognize patterns to determine their path of action. The more AI does, the smarter it becomes.

Powered by natural language processing and deep learning, they can look at huge data sets and recognize patterns to determine their path of action. The more AI does, the smarter it becomes.



Some examples of AI are self-driving cars and chatbots. Self-driving cars determine when to hit the brakes and when to speed up; chatbots learn how to speak to humans based on certain keywords and phrases they may be using. Other examples of AI include Siri, Alexa, Amazon's product recommendation feature and Netflix's entertainment recommendation engine.

Relatively speaking, AI is in its infancy. In the future, corporations are going to invest heavily in it, and it's going to become much more sophisticated. In 2016, AI spending was at $7.8 billion worldwide. By 2020, it's expected to reach $46 billion — a 768 percent increase. Law firms will have to continue using this exciting technology to drive their organizations forward.

HOW AI IS BEING USED IN THE LAW FIRM

One area in which law firms are benefiting from AI is document review. When humans do it, it can be extremely costly and inefficient.

"Law firms have been under pressure from clients to manage document review more efficiently and cost-effectively," says JR Jenkins, Marketing Director at e-discovery software company Ringtail. "AI — mainly predictive analytics — are making a significant impact on this front, allowing attorneys to decrease the sheer number of documents they must manually review and thus increasing the amount of time they have to spend reviewing a matter's most important documents."

Law firms are also using analytics at each stage of e-discovery, not just when they are reviewing a massive and complex case, according to Jenkins. "An example of this is the emerging use of social network analytics, which help identify unusual patterns of activity — activity that may indicate wrongdoing and offer important insight for investigations."

When law firms are doing e-discovery with AI, they can easily "see facts, connections, relationships, unknowns, etc. across the data sets and build strategies based on facts versus supposition," says Billy Hyatt, Chief Executive Officer of Cicayda, a cloud-based software provider.

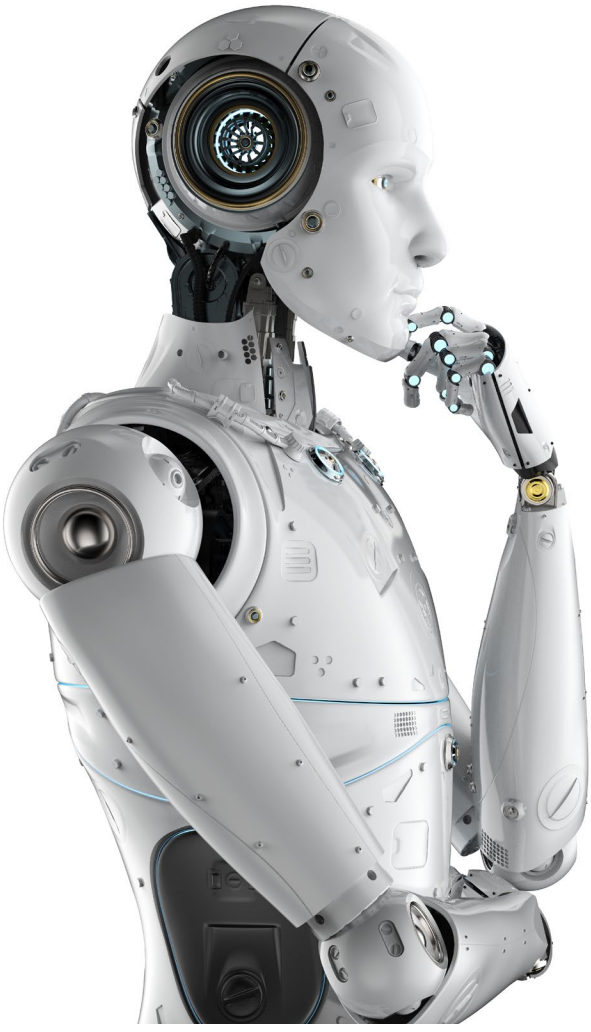
As the world becomes increasingly connected online, more data is going to become available to attorneys. But they can't sort through it all with their legacy workflows like linear

"With AI, document review, classification and extraction rules can be applied to improve accuracy and consistency of review."

review, Technology Assisted Review (TAR) and predictive coding, Hyatt says. These workflows are not cost-effective or accurate enough to perform thorough discovery. "AI, particularly in discovery, will be highly advantageous to the law firms or corporation legal departments that embrace it."

Discovery is going to happen faster, and it will also be more accurate than humans. When dealing with large sets of data, there is bound to be some human error.

"Given the amount of data attorneys deal with and the inconsistencies in decisions from different personnel when reviewing documents — especially when acting across jurisdictions (e.g. dates, currencies, etc.) — there is bound to be some risk of human error," says Wye. "With AI, document review, classification and extraction rules can be applied to improve accuracy and consistency of review."



With AI insights in their back pockets, attorneys can make well-informed decisions and have smarter case strategies, Jenkins says. "[This] can lead to better case outcomes and earlier recognition of exposure or risk in any investigation or matter, to inform decision-making about whether to settle, proceed, etc."

AI is also helping on the business side of running a law firm. A firm that uses AI has a competitive advantage over one that doesn't, because it can deliver speedier and more accurate results.

"[AI] creates new business opportunities, enabling law firms to deliver new services to clients that may have been too time-consuming or expensive in the past," says Wye. "Likewise, automating review processes with AI frees up attorney time, increasing opportunity for firms to tackle higher-value work in greater volumes."

If AI is doing the hard, repetitive labor instead of humans, it is going to save law firms money. They will be more attractive to clients because they can pass on that savings when doing their billing. "The costliest tasks at law firms are usually large-scale repetitive review processes," Wye says. "These can be automated or augmented, reducing the amount of lawyer time billed to these tasks, thereby saving client money."

Karl Dorwart, Senior Director of FTI Technology's Contract Intelligence Group, says that AI is also transforming contract management. "AI is bringing more efficiency to contract-related tasks and helping law firms provide contract management services to their clients."

According to Pratik Patel, Vice President of Innovation and Products at Elevate, AI is giving law firms the ability to review, tag, cleanse and position "unstructured time entry data to gain better clarity into things like pricing or billing compliance.

"While humans are slower and prone to error when processing and reviewing patterns in big data, there are certain skills that AI can never replace."

… This application of AI is meant to save time and effort rather than it being used to 'replace' lawyers."

WILL AI REPLACE ATTORNEYS AND OTHER LAW FIRM EMPLOYEES?

AI is faster, more accurate and smarter than humans in many ways.

According to one study by McKinsey, 22 percent of a lawyer's job and 35 percent of a law clerk's job could be automated. And Deloitte Insight found that more than 100,000 legal roles could be automated by 2026. Lower-skilled jobs, like legal secretarial positions, are going to be especially affected.

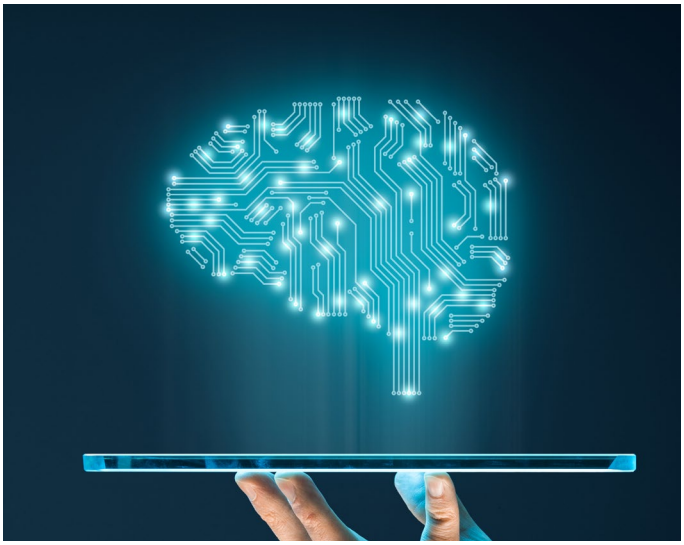
Does this mean that AI is going to completely take over the law firm? In the future, will there even be a need for attorneys and law firm support staff? Indeed, there will be.

The Deloitte Insight study also showed another side of the legal job market. Despite cutbacks of lower-skilled workers, as of 2016, there was already an increase of 80,000 jobs, which were higher-skilled and offered better pay. Many of these new jobs are focused on developing and creating the technology being used now and in the future.

"While humans are slower and prone to error when processing and reviewing patterns in big data, there are certain skills that AI can never replace," says Wye. "Critical thinking, including context and nuance, is something AI looks unlikely to solve in any measure that generalizes to every type of task or transaction at a law firm or in general."

Wye adds that humans are much quicker and more accurate when it comes to navigating ambiguity that AI cannot understand, as well as making judgment calls. After all, the law is rarely black and white.

"Legal is both a science and an art, in some cases where the art can yield better results than the science," Patel says. "Strategy sessions, status updates and basic personal interaction — the lawyer equivalent to bedside manner — can never be replaced by machines. They can be augmented, but never replaced."



GETTING STARTED WITH AI AT YOUR LAW FIRM

AI software providers can help law firms take advantage of new and efficient technology. When combined with stellar attorneys and support teams, AI can give a firm a competitive advantage, make it better at what it does and improve its bottom line.

After all, Jenkins says, "The more law firms can harvest AI's capabilities to provide newer, faster, better services, the more benefits they will reap and pass on to their clients." ■

ABOUT THE AUTHOR

Kylie Ora Lobell is a freelance writer living in Los Angeles. She covers legal issues, blogs about content marketing, and reports on Jewish topics. She's been published in *Tablet Magazine, NewsCred, The Jewish Journal of Los Angeles* and *CMO.com*.

kylieoralobell@gmail.com
twitter.com/kylieoralobell
www.linkedin.com/in/kylieoralobell

inavero®

What can Net Promoter® Score do for your law firm?

Leading firms use NPS® to maximize service quality, differentiate from the competition, and win new clients.

© 2018 Inavero, Inc. All Rights Reserved. Net Promoter, NPS, and Net Promoter Score are trademarks of Satmetrix Systems, Inc., Bain & Company, and Fred Reichheld.

Learn more at inavero.com →

Clients Turn Up the Heat on Cybersecurity

Expectations and regulations aren't getting any easier to deal with. Here's how your firm can learn to stand the heat and stay in the kitchen.

MARK BREWER
Freelance Writer

Cybersecurity has been a hot topic for law firms for some time. But as regulations and other requirements grow, clients are ratcheting up their expectations for law firms to keep their data secure.

According to James Harrison, Chief Executive Officer of INVISUS, a cybersecurity company with law firm experience, law firms that do business with regulated companies are considered business associates, and business associates that hold client data are, under law, subject to the same data security requirements as the businesses they represent. If a law firm is compromised, the client must answer to regulators.

"So there's downward pressure on law firms from the marketplace to evaluate their compliance with best practices in data security and privacy," he says.

THE INFORMATION SUPPLY CHAIN

Law firms are expected to follow best practices that stem largely from state, federal and international laws. Law firms holding data from health care organizations must follow HIPAA

"There's downward pressure on law firms from the marketplace to evaluate their compliance with best practices in data security and privacy."

regulations. If they host data on European Union citizens, it must be handled in accordance with the General Data Protection Regulation (GDPR). There are also requirements under the Gramm-Leach-Bliley Act and new regulations for financial services companies from New York's Department of Financial Services.

Some clients may have additional requirements under their general liability or cybersecurity insurance policies. And all 50 states have legal requirements on how companies must respond to data breaches.

And if you use a third-party company for IT operations or store client information in the cloud, these vendors are also considered business associates and must comply with your clients' requirements. So it's up to law firms to vet their vendors.

"We call it the information supply chain," says Harrison. "If you look at the flow of data — who touches it and has access to it — you need to follow that trail and verify that everyone is following the same best practices."

MORE QUESTIONS THAN ANSWERS

Proof of compliance is one expectation that's breathing down the necks of law firm leaders. Law firms are required to complete long, detailed technical questionnaires to do business with many companies. Some require on-site audits, forcing law firms to show higher levels of compliance and proof. "It's sweeping the legal industry," Harrison says. "If a law firm hasn't seen a questionnaire or audit, it's just a matter of time before they start seeing them on a regular basis."

Many law firm management professionals are simmering with frustration over these requests and are at a loss to answer many of the questions. Others have had time to adapt.

"I spend hours and hours on it every week," says Lori Hughes, ALA's Region 5 Director and the Lead Operations and Information Security Officer at Miller Nash Graham & Dunn LLP, a law firm with 160 attorneys in three states. She has been answering questionnaires since 2015 — on HIPAA compliance, insurance requirements and, more recently, cybersecurity.

One questionnaire included more than 300 questions in just one section. And the questionnaires and audits have been snowballing — Hughes says Miller Nash started with about a dozen in 2015; they now see more than 50 per year.

While you may be tempted to pass audits and questionnaires off to your IT department or vendor, less than 50 percent of these evaluations are IT-related, according to Harrison. Cybersecurity requirements now touch human resources, facilities and firm management. The days of cybersecurity simply being a matter of IT applying security patches are long gone.

Hughes says that requirements may include physical security, such as having paper documents in locked rooms, clean-desk policies and guest badges that time out. Many want copies of firm policies, incident response plans and disaster response plans. On the technical side, companies expect features like encryption of laptops and drives, intrusion detection and response, anti-malware capabilities and penetration testing. Many companies require security awareness training for all firm employees.

BEAT THE HEAT WITH A PROCESS AND PLAN

"Cybersecurity a moving target. It's not something you can set and forget," Harrison says. "What happens the next time you land a key client and they have a new type of data they intend to share with you?"

Unfortunately, as client expectations increase and regulations evolve, law firms are often left in the dark about how to navigate this dynamic landscape. But specialized expertise can help them avoid turning cybersecurity into a daunting and costly task.

Harrison counsels clients not to overkill compliance. "Develop a formal plan that is simplified to the needs, size and scope of the firm and that meets the core of the cybersecurity standards," he says. "That way you can afford it, manage it well and be defensible." Being defensible against a client audit

Cybersecurity requirements now touch human resources, facilities and firm management. The days of cybersecurity simply being a matter of IT applying security patches are long gone.

or a data breach boils down to your preparation and plan, he adds.

"Cybersecurity is a process and should be part of the firm's other ongoing processes for conducting business," says Joseph Burton, Of Counsel at Duane Morris LLP in San Francisco, California, and Principal Consultant at Wescott Cyber Consulting. "It's really a risk management problem requiring input and oversight from management, and having a cybersecurity program that considers technology solutions, process solutions and administrative solutions."

The process-oriented approach contrasts what many firms have done in the past (or what some may be doing today).

"We call it the information supply chain. If you look at the flow of data — who touches it and has access to it — you need to follow that trail and verify that everyone is following the same best practices."

"Technical solutions are usually applied in an ad hoc, one-off manner without any thought as to how that fits into your overall security needs," Burton says.

While larger firms have the capacity to hire a full-time chief security officer or chief compliance officer, this may be too much for small and midsize firms. Burton suggests getting outside advice from a cybersecurity consultant or vendor who can assist your firm in meeting client requirements, answering questionnaires and completing on-site audits.

They can also help firms follow the information supply chain. INVISUS walks law firm clients through a risk management process that includes sending questionnaires to vendors. "Reputable cloud companies and document management software companies have been dealing with this for the last year or two," Harrison says. "They should be able to instantly reply with proof of compliance."

STEP BACK BEFORE STEPPING AHEAD

Over time, the requirements will only get more involved and complicated. Now is a good time for firms to take a step back and analyze cybersecurity from a management perspective. The trick is to know which standards to adhere to and to develop a process and a plan to ensure that your security measures are working.

With specialized expertise, legal management professionals can get ahead of the rising heat. Experts agree that it's important to find a vendor with law firm experience. They know your business, can drill down to requirements specific to your practice, and guide your firm into being an attractive partner for clients with regulatory and other cybersecurity needs. ■

ABOUT THE AUTHOR

Mark Brewer is a freelance writer who helps decision makers understand technology, trends and ideas to make them more effective in their work.

815-565-7272
mark@markbrewerwriter.com
markbrewerwriter.com

Succession & Contingency Planning Solutions

Exclusively for ALA Member Firms and Attorneys

NextPath Legal provides a proven 360-degree, all-inclusive, written Succession & Contingency Plan. Through hands-on collaboration with each firm, we tailor a Succession Plan to meet the needs of the four most important constituents of a solid firm plan:

1. **Plan for the Partners**
2. **Plan for the Clients**
3. **Plan for the Successors**
4. **Plan for the Firm**

The focus of our work is centered on the **Protection and Preservation of Firm Assets and Clients.**

All plans include a full review of essential risk management elements to manage the planned, the unplanned, and the "what ifs". From this review we develop a customized Contingency Plan, which includes:

- **Personalized individual attorney plans for short, medium, and long-term contingencies**
- **Full current "in place" insurance review**
- **Full recommendations for asset protection and insurance needs that match the customized Succession Plan**

NEXTPATH LEGAL
Succession Solutions

Exclusive to Association of Legal Administrator Member Firms of 5+ Attorneys with an additional 5% discount for CLM.

NextPath Legal was formed by Affinity Consulting Group and GLJ Benefit Consultants in order to meet the Succession and Contingency Planning needs of Law Firms and Attorneys. Initial plan consultations provided by an Affinity consultant. Insurance consultations offered by a licensed GLJ Benefit Consultants agent.

© Copyright NEXTPATH LEGAL 2018

Contact us at **614.385.2198**

Could Data Encryption Be Your Last Line of Defense Against Hackers?

Some firms are using the technology to protect electronic communications and other files. Find out what it entails.

ERIN BRERETON
Owner, Chicago Journalist Media

With pending financial transactions, Social Security numbers and other potentially lucrative pieces of information whirring back and forth in attorney and client emails and residing in documents on servers, law firms can be particularly tempting targets for cybercriminals.

Recent research indicates they're pursuing law firms' data more aggressively. The amount of firms that have experienced a data breach rose from 14 to 22 percent between 2016 and 2017, according to the most recent American Bar Association Legal Technology survey.

Firms with 10-99 attorneys were particularly plagued with breach issues; firms with 10-49 attorneys reported the most incidents, followed by firms that employ 50-99 lawyers.

Still, acceptance of encryption has grown at a slow pace in the industry. From 2011 to 2017, email encryption use grew just 13 percent — and in 2016, it actually declined.

WHAT ENCRYPTION INVOLVES

Concerns about keeping Klein Law Group's financial and other information secure prompted

"It's not very difficult for somebody to grab an email off the internet, change an account number and send that email back on its way. The next thing you know, we're wiring money to Nigeria."

the Founder of the 10-employee Boca Raton, Florida, firm, Eric Klein, to start using encryption software several years ago.

"We do real estate closings and also have a title agency as part of our practice; hackers know lot of money is involved with real estate transactions," Klein says. "It's not very difficult for somebody to grab an email off the internet, change an account number and send that email back on its way. The next thing you know, we're wiring money to Nigeria."

When used in tandem with firewalls and other protective measures, encryption can offer firms an additional layer of protection. Essentially, the technology scrambles the content of an email or document before it's sent or stored so the text is unreadable if intercepted.

Items can later be unencrypted using two numeric keys — series of numbers that verify someone is authorized to send, save or access an item.

An attorney, for example, could send a message with software that encrypts it using a key that's linked to the attorney's identity, identifying she's the one who sent the message. When the attorney's client receives the email, he'd need to provide a separate key that the attorney had previously given him to be able to access the text.

If a hacker were to intercept that encrypted email in transit, without knowing what key to enter, its content would look nonsensical — preventing the hacker from obtaining any sensitive information it contained.

WHY SOME FIRMS CHOOSE ENCRYPTION

The American Bar Association issued new guidance last year addressing the role encryption can play in firms' ethical obligation to protect electronically stored information.

The association noted that while email messages provide a reasonable expectation of privacy in routine communication with clients, newer communication methods, such as texting, may not — making it "not always reasonable to rely on the use of unencrypted email."

Some state bars have also introduced breach-related direction. For example, Klein says that if he were hacked, he'd have to explain to the Florida Bar what his firm did to try to prevent it.

Even if attorneys don't lose their license over breach issues, the bar can, he says, potentially still reprimand them, making encryption and other security measures a worthwhile investment.

"Anyone who researches you could see it and say, 'Oh, he's been reprimanded because he didn't protect clients' information; that's not the guy I want to use,'" Klein says. "It affects your reputation — and that's what lawyers trade on."

Clients may also be a motivating factor for using encryption. Because they can face financial and other risks if information relating to their business is stolen, some are urging firms to use the technology.

Even if attorneys don't lose their license over breach issues, the bar can potentially still reprimand them, making encryption and other security measures a worthwhile investment.

When insurance, investment and talent management services firm Marsh & McLennan decided to reach out to law firms it worked with in 2012 and ask them to start encrypting email communication, a few already had encryption systems in place, according to Senior Assistant General Counsel Ronnie Brandes.

Others, she says, were happy to add the functionality.

"We work with personally identifiable and health information protected under HIPAA, so encryption and making sure data is transmitted securely is always at the forefront of the company's mind," Brandes says. "We started having these conversations with the firms we have the longest relationship with, and none of them really put up a fuss. They also saw it as a way to practice good cyber hygiene."

Heather Clauson Haughian … says she's seen more clients request clarification about the firm's encryption and other security practices — in some instances as early as when the engagement letter is presented.

Heather Clauson Haughian, Cofounder and Chief Technology Officer of business law firm Culhane Meadows, which has offices in seven U.S. cities, says she's seen more clients request clarification about the firm's encryption and other security practices — in some instances as early as when the engagement letter is presented.

"As the legal industry is getting more educated [about encryption], so are our clients," Haughian says. "We've got [clients in] highly regulated industries that actually provide us with audit questionnaires that say: Are you doing these things? What protections do you have in place?"

WHAT TO ENCRYPT

Firms may opt to encrypt some items they feel contain particularly sensitive information and not others — all email exchanges, for instance, or possibly individual files in various locations, documents stored on servers or entire laptop operating systems.

Randolph Kahn, Founder of information consultancy Kahn Consulting, teaches a course on electronic information law and policy at the Washington University School of Law in St. Louis, Missouri. He suggests discussing what information should be encrypted as early in the relationship as possible to gauge clients' feelings.

"Have those conversations upfront so the ground rules are properly established — there's an understanding that we're going to encrypt certain kinds of conversations going forward," Kahn says.

Once the firm decides which items will be encrypted, he suggests creating a formal policy that indicates the specific ways and instances when data should be encrypted.

"Law firms shouldn't leave to chance how their lawyers evaluate and conclude when to use or not use encryption technology," says Kahn. "Mistakes happen. A policy increases the likelihood employees will get it right."

WAYS FIRMS CAN ENCRYPT FILES

Although some encryption options may require clients to log into the encryption system before they can view an email or document, some will automate the verification process if both parties have previously authenticated each other's identity.

Klein Law Group's software will send an email containing the firm's name and logo with a link leading to an online portal where a recipient can securely access a message, or it can deliver encrypted messages to known recipients with the key information to confirm Klein sent it and decrypt the message.

When the message arrives in the recipient's inbox, it looks like any other email except for a footer that lets the recipient know it's been encrypted. While that type of system may require some setup, it can be beneficial for clients who feel repeatedly keying in a password will be a hassle.

"One of the realities of encryption is it usually adds steps to the process, which for some clients is not preferred," Kahn says. "[However], encryption tools come in all varieties, colors, flavors and sizes, some of which are really intuitive and simple, and others that are not so simple."

Firms can also choose solutions that scan and encrypt content they perceive is a risk, according to Kahn, such as a birthdate. Other systems will automatically encrypt all documents and outgoing messages, lessening user responsibility to identify sensitive information.

The software Culhane Meadows chose, for instance, doesn't require firm members to indicate which individual items should be encrypted.

The fact that the encryption software would be running in the background, providing constant security support, was a major selling point for the firm, according to Haughian.

"The platform takes it off our plate so it's something we don't have to worry about," she says. "If I know I'm going to upload a document to the system in the cloud, during the transmission process, it will be encrypted in transit. I know when it's sitting in a data center, it's encrypted — there's nothing I have to do to activate that." ■

ABOUT THE AUTHOR

Erin Brereton is a freelance writer, editor and content strategist who has written about the legal industry, business, technology and other topics for 20 years.

breretonerin@gmail.com
twitter.com/erbrer09
www.chicagojournalist.com

Information Security in the Digital Age

By Ann Nickolas

With numerous high-profile breaches and rapidly evolving global business environments, the way that law firms collect, store and destroy information is coming under increased scrutiny (much like a cross-examination). As a result, many firms have taken action to refine their security protocols and create digital safeguards to assess the practices of their staff. However, as the legal industry continues to digitize, physical data security is increasingly becoming an afterthought when establishing an information security strategy.

Most law firms do not have a physical security plan in place to prevent and protect against the threat of negligent employee behavior — which happens to be one of the main causes of data breaches.

With 25 percent of information breaches caused by employee error, law firms need employee training around the treatment of physical data. Yet one in four law firms admits they have never trained their staff on information security policies, nor do they have these policies in place.

To ensure that critical client and business information in all formats remains confidential and protected, law firms must establish an all-encompassing information security strategy that includes policies on physical data protection.

YOUR OWN EMPLOYEES COULD BE YOUR BIGGEST THREAT

Data security is important to American consumers looking to work with a law firm — 83 percent of them feel that data protection is important when deciding which firm to hire. Furthermore, 40 percent are concerned that the security of their confidential information could be at risk when providing information to a lawyer. To maintain relationships with potential and existing clients, it's critical that law firms are aware of consumers' concerns and examine the factors that could pose a threat to their business. While outsider threats should certainly be considered when establishing a security strategy, law firms must also assess internal staff to mitigate the risk of a breach or theft.

Two in five law firms admit that their employees have lost items containing sensitive customer data, including company mobile phones and laptops, paper documents, and USB drives. As a result, 18 percent say that sensitive company data had been put at risk and a data breach occurred. Of course, mistakes are sometimes unavoidable, but law firms need to be proactive in establishing a culture that is committed to data security at all levels of the business. It's helpful to continually remind employees about how to handle confidential information both inside and outside the office — whether that means simply encouraging employees to double-check that they have all notes and paperwork in their possession when traveling or advising that all confidential documents be securely locked away or shredded within the office.

ARE MESSY DESKS AND OUTDATED EQUIPMENT PLAGUING YOUR FIRM?

While many functions within the legal industry have been digitized, law firms continue to produce and store confidential physical assets from client depositions, discovery documents, plaintiff statements and corporate information — which tend to pile up in the office. A cluttered workplace not only signals disorganization and sloppy business practices to potential clients, but also poses a threat to your businesses' security and ability to comply with industry privacy laws and legislation. For example, the General Data Protection Regulation (GDPR) came

With 25 percent of information breaches caused by employee error, law firms need employee training around the treatment of physical data.

into full effect for organizations with business dealings in the European Union on May 25, 2018; the regulation determines how long documents should be kept, making the retention and pileup of data even more risky.

One way to prevent breaches or theft within the office is to implement a Clean Desk Policy that specifies how employees should manage their workspace. The policy specifically instructs employees to clear their desks and offices of any visible information whenever they're not physically there to protect it — computer monitors, paper documents, and even Post-it Notes must be securely cleared or locked away. Further, unused or dated documents must be securely shredded before being discarded.

Digital devices need to be monitored as well — technology gets dated quickly, and legacy equipment can increase a firm's vulnerability to attacks. Keeping all equipment, from computers to mobile phones to hard drives, up to date is critical. It's important to ensure that outdated equipment is securely destroyed before being discarded. Even if your hard drive disposal process includes erasing, reformatting, wiping or degaussing, you are still vulnerable. As long as the drives are physically intact, all private information can be retrieved — proper physical destruction is the only method that is effective.

At the end of the day, reputation is everything, especially in an industry where consumers have many options to choose from. Protecting your reputation means protecting your clients' information, both digital and physical, through an all-encompassing information security strategy. ■

ABOUT THE AUTHOR

Ann Nickolas is Vice President of Shred-it, where she oversees new business development and account management for customers in the commercial, health care and government verticals. Nickolas helps businesses secure their confidential information with products, services, policies and training that help protect them from the risks, fines, penalties and loss of revenue that come with an information breach.

www.shredit.com/en-us/home

Experience Webinars Live and On-Demand

For the best value in online education, look no further than ALA's webinars — dozens of sessions spanning functional specialties and topics for every legal management professional. They're hosted by speakers who come highly recommended, either directly from attendees of ALA conferences or from industry word of mouth.

You can view webinars live, allowing you to participate and ask questions in real time, or at your leisure. Dozens of webinars are scheduled throughout each year, and the on-demand catalog — which goes back to 2013 — is continually updating.

Log on for continuing education!

Learn more at ***alanet.org/webinars***

7 Strategies and Tools to Help Boost Your Law Firm's Social Media Performance

By Dorothy Rausa

Let's face it: social media is here to stay, and it's how people consume news and information. To remain competitive in today's constantly evolving digital world, law firms need to continually adapt their social media strategies to ensure optimal performance of their posts. Moreover, prospective clients are increasingly using social media for research, networking and vetting law firms. Effective social media posts can build brand recognition, credibility and trust. Firms can provide added value and stay top of mind by posting engaging, relevant and timely content that targets their current and potential clients.

Want to take your law firm's social media performance to the next level? Start by using any of the following seven strategies and corresponding tools:

1. **Target Marketing:** Identify your law firm's target audience and how they are using social media. The better you understand how your target audience is engaging on social media, the better you can adapt your strategy to improve your content's relevance and drive higher-performing posts. A law firm's target audience consists of clients, prospects, alumni, recruits, referral sources and media.

   Tools: Sprout Social and Audiense

2. **Social Media Management:** Social media management platforms allow users to streamline their campaigns. They allow users to manage their law firm's multiple social media profiles in one place, schedule posts in advance and post to multiple platforms at once. In addition to saving time, they also provide useful analytic reports you can use to measure the impact of your social media campaigns.

   Tools: Hootsuite, Sprout Social, Buffer and CoSchedule

3. **Influencer Marketing:** This is a big trend in marketing, and law firms are no exception. Influencer marketing is a way to connect with and leverage the solid reputations of industry leaders, bloggers and experts by having them share your content so you can gain exposure to a new audience — their followers. Think of it as an electronic referral to your firm's services. Today's consumers are looking for "reviews," and there is no better way to position your law firm's posts than to have a top influencer share your content.

   Tools: BuzzStream Discovery, BuzzSumo and Pitchbox

4. **Images:** Visual images bring your content to life and increase engagement. Statistics show that posts with an image are shared more than those without one. The tools available to create custom images can also correctly size your images to meet the dimensions required for each social media platform.

   Tools: Canva and Crello

5. **Hashtags:** Hashtags (#) are used to aggregate posts that relate to the same subject. Typically, you should only use hashtags for one word, without spaces or punctuation, and be certain to include them within your message. It's best to post any links directly following the text of your post and

To remain competitive in today's constantly evolving digital world, law firms need to continually adapt their social media strategies to ensure optimal performance of their posts.

insert any hashtags after the link. Users find it easier to access the link after they read a post rather than having to scroll through a list of hashtags. To optimize your hashtags, use any of the following tools to determine the top trending and most relevant hashtags associated with a particular topic.

Tools: Hashtagify, Tagboard and HashAtIt

6. **Videos and Podcasts:** Video content marketing is a powerful tool in today's social media landscape. Video usage in a law firm's marketing content strategy is increasing and will continue to reach new heights over the next year. Many consumers would much rather watch a short video clip than read text, especially while browsing on social media. Videos also personalize a user's experience and help you connect with current and potential clients on a more personal and relevant level.

Tools: Blurbiz, Rocketium, Wavve and Spark Video

7. **Google Alerts:** Create a Google Alert for your law firm's current clients, prospects and attorneys. Google will scour the internet daily on each alert you set up, and you can receive any resulting information via email "as it happens" or "once a day."

Tool: Google Alerts

Creating consistent, engaging thought leadership posts provides value to your target audience. It positions your law firm so that your message hits the key marketing goal of ensuring your content is delivering the right information to the right people at the right time. But just having a presence on social media is not enough; networking online is just as important as making in-person connections. Remember, it is called social media for a reason — because it's social engagement! Interacting on social media includes liking, commenting and sharing others' posts.

By employing some of these strategies and tools, law firms can uncover a deeper understanding of their social media footprint and develop smarter content strategies. ■

ABOUT THE AUTHOR

Dorothy A. Rausa is the Director of Business Development and Marketing at the California-based labor and employment law defense firm of Carothers DiSante & Freudenberger LLP. She has been an ALA member since 2001 and is a Past President of the Orange County Chapter of ALA.

drausa@cdflaborlaw.com
www.shredit.com/en-us/home
twitter.com/rausadotcom
www.linkedin.com/in/dorothyrausa

Why Should Law Firms Have Two Brokers When It Comes to LTCi?

By Megan Ellis

Understanding various types of insurance takes a lot of time and training. Long-term care (LTC) or long-term care insurance (LTCi) is no exception. The average person does not know about or understand it due to its complex nature. Anyone looking at LTCi could benefit from some form of guidance when it comes to making an educated decision about what might be the best plan for them.

Just like that average person, the average insurance broker may have a vast knowledge of health insurance, vision insurance, dental insurance and life and disability — but when it comes to the complexities of LTCi, they also need education.

Brokers seek out experts to help understand and explain the technicalities of long-term care insurance.

THE VALUE OF THE SPECIALTY

Long-term care insurance incorporates different components than other types of insurance. These plans include many nuances and they work differently than other types of benefits that are offered in an employees' benefit package. For example, LTCi rates are based on the age at which you apply for coverage and are designed to be stable. In contrast, health insurance rates are based on usage and will likely change each plan year.

Studies demonstrate that 99 percent of people who purchase an LTCi policy hold onto it for life. This shows us that this type of benefit is something that people take time to decide on, really dive deep into the details of, and genuinely want to make the best determination for themselves now and for their future. Therefore, it is essential that people have the tools and the trained professionals to clarify the facts for them.

So why would a law firm want to bring in a LTCi specialist to interpret the details? Most lawyers are fact finders and would want to be equipped with all the data necessary to make an informed decision. An expert in the field of LTCi is a broker who only sells LTCi and who knows the available LTCi plans inside and out.

If a lawyer or legal management professional specializes in a certain field, they tend to become skilled in that field. They have an adept knowledge of the technicalities of that discipline. The same is true with LTCi in the insurance industry. A brokerage firm that focuses solely on long-term care insurance would be considered an expert in that area.

If you are part of a law firm that only has one insurance broker to educate your employees on all your benefits, you may be missing out on some much-needed expertise. Many brokers would be the first to admit they have a lack of knowledge when it comes to LTCi. They would also be the first to agree to bringing on an authority on the subject.

An LTCi-specialized broker can help you avoid potential liability — something that law firms are likely more hypersensitive to

Brokers seek out experts to help understand and explain the technicalities of long-term care insurance.

than most businesses. Bill reconciliations can catch numerous billing mistakes through audits when a new client has an existing LTCi plan. An example of this was a client who had 3,400 participants and had to make 540 corrections. They had 98 unreported terminations, 150 eligible employees who should have been added to the plan, 29 date-of-birth corrections, 163 division corrections and 39 name corrections. These mistakes can, and will, open your firm up to unrealized liability.

There really is no better value to adding an expert, but many are concerned about what bringing on an LTCi authority might cost you monetarily. The majority of insurance products generate a commission that pays for the servicing of that plan. LTCi is no different, so bringing in a specialist to assist your LTCi plan doesn't cost your firm anything.

If you are a law firm that would like to have an LTCi specialist talking to your employees about their options, you need to have your current insurance broker partner with an expert in the LTCi field. This partnership will relieve that broker of having to play the part of the all-knowing. The task of implementing, servicing and auditing your LTCi plan will move to the LTCi broker.

Do you have questions about LTCi? You can be sure that others do, too. Let me know what your questions are, and we will try to address them in a future column. ■

ABOUT THE AUTHOR

Megan Ellis is the Vice President at LTC Solutions. She has more than eight years of industry experience and more than 11 years of sales experience. Ellis manages LTC Solutions' sales team and forges relationships between carriers, brokers and employer groups. She is an expert on the current state of the LTC marketplace and educates insurance agents across the country via state-filed continuing education courses.

mellis@ltc-solutions.com
425-658-7517

LAW FIRM RECRUITERS: Post open staff positions to attract qualified candidates with the experience and knowledge you're looking for.

Post Your Résumé to ALA's Job Bank

ALA Association of Legal Administrators

With more than 600 open positions in legal management posted each year, ALA's Job Bank can help you find that "next step" in your career.

- Post your résumé for free
- Search for open positions in legal management
- Share open positions with your network
- Subscribe to our weekly Career Connection Newsletter

Learn more at alanet.org/careers.

ALA
Association of Legal Administrators

The **All-New** Job Description Toolkit

Debuting this month, this new benefit for ALA members helps legal managers accurately describe duties for ever-evolving positions — increasing the chances they'll hire the right person for the job!

- Resources and tools for writing job descriptions — including an easy-to-use, editable template
- Guide to creating job descriptions that apply ALA's Uniform Process Based Management System (UPBMS) taxonomy
- Sample job descriptions — using the UPBMS — in the areas of legal support services, finance, HR, marketing, technology and IP

Improve your hiring process!
Better manage your employees' performance!

alanet.org/jobs

Anniversaries, Awards and Appointments

MEMBERS ON THE MOVE >> >> >>

Barbara Bumblis

Lisa W. Jacobs

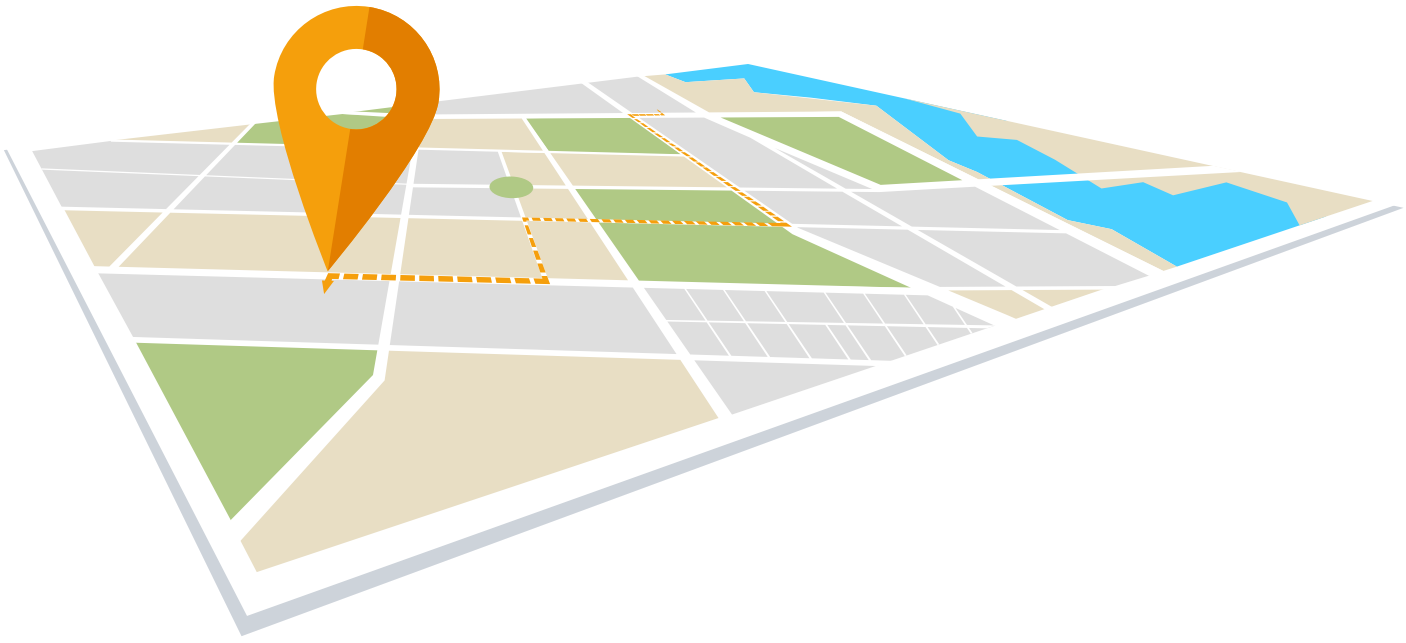
Michael Orce

Diane Scheffler

Barbara Bumblis, a member of the Middle Tennessee Chapter, is now Office Administrator at Baker Donelson Bearman Caldwell & Berkowitz, PC, in Nashville, Tennessee.

Lisa W. Jacobs, a member of the Capital Chapter, is now Office Administrator at Cooley LLP in Reston, Virginia.

Cindy Muniz, CLM (not pictured), a member of the Mile High Chapter, is now Firm Administrator at Coombe Curry Rich & Jarvis in Denver, Colorado.

Michael Orce, an independent member from Region 1, is now Chief Operating Officer at Robinson & Cole, LLP, in Hartford, Connecticut.

Diane Scheffler, an independent member from Region 2, is now Chief Operating Officer at Troutman Sanders LLP in Atlanta, Georgia.