CYBER RISK MANAGEMENT: THE VITAL ROLE OF LEGAL MANAGEMENT PROFESSIONALS

This CE course will help legal managers understand their key role in helping manage the firm’s data breach risks and meeting compliance requirements.
FEATURES
OPERATIONS MANAGEMENT BY MARK BREWER
DON'T TAKE THE BAIT .............................................................................................................. 11
It’s critical for firms to take steps to reduce phishing attacks.

CONTINUING EDUCATION COURSE BY JAMES HARRISON
CYBER RISK MANAGEMENT: THE VITAL ROLE OF LEGAL MANAGEMENT PROFESSIONALS … 15
This CE course will help legal managers understand their key role in helping manage the firm’s data breach risks and meeting compliance requirements.

OPERATIONS MANAGEMENT BY ERIN BRERETON
TECH TRENDS THAT COULD CHANGE HOW FIRMS OPERATE ............................................ 21
From document review to providing visual evidence, new tools are emerging to help firms work faster and more effectively.

COLUMNS
BIG IDEAS .................................................................................................................................... 3
Gettin’ Techy with It

BP PERSPECTIVE .......................................................................................................................... 6
A Primer on Using Attorney Trust Accounts

THINKING OUT CLOUD ................................................................................................................. 9
It’s Time to Embrace Cloud Computing

TEST DRIVE ................................................................................................................................ 26
Teaming Up with Microsoft Teams

DEPARTMENTS
TIPS AND TRENDS ...................................................................................................................... 29
Cybersecurity Compliance: 4 Questions You Need to Ask

ALA NOW
ALA FACES .................................................................................................................................... 31
Member and Chapter News

AT ALA ........................................................................................................................................ 32
What’s Happening at Headquarters?
Gettin’ Techy with It

“We are trying to solve 21st century problems with 22nd century technology using 19th century business structures,” said Yves Bergquist, Director of the Artificial Intelligence and Neuroscience in Media project at the University of Southern California.

There’s a lot to unpack in that fairly short sentence. I’ve been pondering it since I read it in a summary of a panel session that Bergquist participated in during the South by Southwest Conference in Austin, Texas, this past March. My takeaway is that technology, including artificial intelligence (AI), enhances the way we work, including our ability to solve problems and improve society overall.

It’s pretty ambitious stuff. However, if you think about it, we hold a reminder in our hands daily of how far we’ve come — our smartphones are more powerful than the computers used by NASA during the Apollo missions. The way we work in the legal industry has changed dramatically in just the last 25 years, and we’ve had a front row seat watching technology shape the practice and business of law.

This edition of Legal Management is about technology trends shaping the industry right now, so read on. Perhaps take the continuing education course on cybersecurity for credit and consider how you as a leader in the business of law are using technology to improve your organization.

ALA’s vision is to empower our members to be leaders and managers in the business of law, and technology is a large component of that. With that in mind, ALA is involved in several initiatives that place us right in the middle of what’s evolving and shaping our future.

One is our membership in the Global Legal Blockchain Consortium (GLBC, legalconsortium.org), which is comprised of more than 250 large companies, law firms, software companies and universities that have joined together to develop standards to govern the use of blockchain.
technology in the business of law. Specifically, the GLBC focuses on the following:

- The interoperability between large corporate legal departments and law firms
- Productivity improvements and cost savings in the operation of legal departments and law firms
- The use of blockchain to fortify and augment existing legal technology investments, adding important functionality to legacy systems to extend their useful life

ALA is also a founding member of the SALI Alliance (that’s Standards Advancement for the Legal Industry, sali.org), which is a nonprofit organization comprised of legal industry professionals from legal operations, law firms and solution providers with the goal of developing open, practical industry standards for efficient and innovative legal services.

Additionally, ALA has established itself as a contributor and host to the annual Global Legal Hackathon (globallegalhackathon.com), the world’s largest legal technology hackathon. This event brings the legal industry together with technology and innovation with one purpose — rapid development of solutions for improving the legal industry worldwide. I’ve been fortunate to have participated in the Global Legal Hackathon twice; both times were amazing and insightful experiences.

The business of law is not a single component, nor is developing leaders in that space. That’s why ALA is involved in a number of emerging areas so we can stay abreast of trends in our industry while also being a part of shaping our industry for the future.

I hope that you enjoy this tech-focused edition of Legal Management and that you are reminded that ALA is your source for networking, knowledge and resources, which means you can boldly go into the future prepared to succeed and thrive as our industry continues its evolution.

Want to know more about the Global Legal Blockchain Consortium or the Global Legal Hackathon? Drop me a note and we can continue the conversation.

---

jcornell@shb.com
linkedin.com/in/jameslcornell
twitter.com/jamescornell3

---

2020 ALA Annual Conference & Expo

MAY 3-6
SALT PALACE CONVENTION CENTER
SALT LAKE CITY, UTAH

#ALAConf20 Keynote Speaker:

Dr. Catherine Sanderson
Manwell Family Professor of Life Sciences (Psychology)
Amherst College

The Science of Happiness

Learn practical (and relatively easy!) ways to increase your own psychological well-being with cutting-edge research from the field of positive psychology.

Learn More
You’ve dreamt of the perfect practice management platform.

We’ve built it.

Cloud-based practice management software for the modern firm

- Robust time, billing & complete accounting
- Advanced reporting
- Smart email management
- Cutting edge iOS & Android apps

We are a mid-sized firm and Zola definitely helped us grow. It’s a fantastic cloud-based solution for a firm with multiple locations and attorneys that need to collaborate on a single platform.

~ Dunlap, Bennett & Ludwig PLLC 100+ Users

Zola has a dedicated team that ensures a streamlined and highly accurate migration process for a hassle-free transition from a wide range of cloud and legacy applications, including:

zolasuite.com/ala  855-997-1574
A Primer on Using Attorney Trust Accounts

Almost all lawyers in private practice are required to maintain a firm trust account under their state’s attorney trust account rules. The rules in various states might be written differently, but the concepts are the same. So let’s get into it.

What goes into an attorney trust account (or IOLTA/IOTA account)?
- Client funds that have not been earned by you.
- Funds deposited and held in escrow for an event, contract or costs.

What doesn’t go into an attorney trust account?
- Your money — when you earn it, take it out and transfer it to your operating account.
- Nonrefundable retainers (absent an agreement to the contrary). Also, be aware that in many states a retainer is not the same as a prepayment of fees. It’s simply a fee to ensure your firm will be ready and willing to help a client as needs arise. Therefore, nonrefundable retainers are similar to a flat fee and are generally earned when they are paid. An exception is that many states still require that flat fees for which work has not been performed should still remain (for safekeeping) in the attorney’s trust account. You can dole them out to yourself as work is completed and billed. That requirement is not the same in all states, so check your own rules.

What comes out of a trust account?
- Payment for attorney work that has been completed. If it is paid to you, make sure you always have a billing to back up the payment or transfer of funds from your trust account. Don’t pay your bills, overhead, payroll, etc. directly from the trust account. That’s a big mistake — always transfer the funds to your operating account first.
- Payment of costs, transactions, closings or settlements that the attorney is making on behalf of a client from funds in the trust account deposited there for that purpose.
• Refunds to a client in appropriate circumstances (i.e., the fees and costs for the matter completed is less than the amount prepaid into the trust account).

**What is the correct procedure for taking money out?**

Every penny removed from a trust account should have some sort of invoice or written recordation of the movement of that money and its purpose. In my office, I only remove attorney’s fees from my trust account once per month based upon the previous month’s billings. Payment for costs may come out, but in each instance I have an invoice that is either placed or digitally scanned into the client’s file for reference purposes. Remember: in many states, like California and New Jersey, your trust account may be subject to random audit — and it better balance.

The best way to do this is to make sure you balance it like any other normal account at least monthly and always have a backup document or digital record for every penny that has come in and come out. Many billing programs record and keep track of money in your trust account. So when you take it out, the billing invoice will recap what was in there at the start of the month, the deduction being made with this invoice, and the resulting balance left in trust after the invoice.

**RISK ASSOCIATED WITH SLOPPY RECORDKEEPING**

All attorneys holding clients’ funds in an attorney trust account have a duty of recordkeeping. We are fiduciaries and the fiduciary legal standard puts the burden on the lawyer to prove that it was done right, not on the client to prove it was done wrong. Typically, trust funds are used for short-term deposits — things like money to be expended on attorney’s fees or costs in a relatively short period of time, such as under six months.

If, however, a client is required to deposit funds for a longer period of time or larger purpose like a cash bond or a real estate closing, the lawyer should give the client the opportunity to have those segregated into a separate fund where it might earn interest for the client. Under normal IOLTA programs, no trust account will earn interest that can be divided and paid to the individual clients.

And remember, if you choose to have a third-party bookkeeper maintain your trust account, you are still responsible for the conduct of those people.

**HANDLING DISPUTES AND REFUNDS**

If your client disputes the fee you desire to draw from the funds deposited in trust, only the disputed portion need remain in the trust account until the matter is resolved. When a client demands a return of unearned money still held in an attorney trust account, the refund should be given right away. Failure to refund money to a client entitled to it can subject the lawyer to a civil suit for conversion, breach of fiduciary duty and claims of theft.

**BEST PRACTICES**

There are several rules to keep in mind when creating or managing a trust account:

1. Make sure that you are starting your trust account pursuant to your state’s rules and in an eligible institution when the state requires such eligibility.
2. Know what you put in there.
3. Know what comes out of there.
4. Keep accurate records of all money and property entrusted to you.
5. Have the right attorney-client agreement provisions to use the trust funds.
6. Keep the client informed of the balances as necessary.
7. Know how to resolve disputes over money held in trust.

The ability to use money in a trust is a great tool for the smooth operation of your law office. Always respect your fiduciary duty and keep an eye on those funds.

**ABOUT THE AUTHOR**

Claude E. Ducloux is an attorney licensed in Texas, Colorado and California and is the Director of Education, Ethics and State Compliance at LawPay. He speaks regularly on legal ethics, law office management and trial-related topics. In 2011, he won the highest statewide award from the State Bar of Texas for lifetime contribution to continuing legal education, and he has been invited to speak in more than 250 programs since 2009. He’s served as course director of numerous institutes and advanced courses.

**WE’VE GOT LOTS MORE ON TRUST ACCOUNTS**

For more information on trust accounts, check out our CE course, “How to Ethically Oversee Trust Accounts” at legalmanagement.org/features/how-ethically-oversee-trust-accounts. Bonus: You can earn CE credit.
HERE’S TO THE LAW FIRM OF THE FUTURE

The Law Firm of the Future is Here. Now. Konica Minolta and All Covered have the products, solutions, and services that will redefine the future of your organization.

MANAGED VoIP SERVICES
SECURITY AND COMPLIANCE
INTEGRATION OF LEGAL TECHNOLOGIES
PRINT MANAGEMENT & COST RECOVERY
MANAGED IT & CLOUD SERVICES
WORKFLOW AUTOMATION & DOCUMENT MANAGEMENT
LAWYER’S HELP DESK
MOBILE MANAGEMENT SOLUTIONS

For more information visit kmbs.konicaminolta.us/legal
It’s Time to Embrace Cloud Computing

In every endeavor, there will always be some level of resistance. Some will point to possible risk factors, others will disagree with the promises of greater efficiency and heightened productivity, and some might even argue that the new “solution” simply isn’t all that new or all that necessary. It seems that for every cheerleader, there’s a naysayer.

And when it comes to deploying cloud solutions in legal firms, the naysayers are slowing down the industry’s entry into a new world of managing information, collaborating with stakeholders and streamlining processes. With all the potential benefits at stake, the cheerleaders need to cheer louder.

The migration to cloud computing is in full swing. Gartner predicts the fastest-growing market segment this year will be cloud system infrastructure services. Second will be cloud application infrastructure services. In fact, Gartner claims that the increasing adoption of cloud-first strategies will have an effect on nearly every vendor and service provider in business today. The legal profession, though it may have lagged in adopting the latest automation tools, will not prove the exception. This is especially true as law offices continue to undergo a transformation toward a more client-based business model.

In fact, automation has provided countless advantages in the law office. It can help lawyers be more effective at their job by taking over many of the rote tasks that they used to perform. Take document review, for example. What is usually an expensive, time-consuming process can now be handled almost entirely by automation. But what argument can lawyers make for moving to a cloud-based system? Isn’t automation with on-premises technology completely adequate?

“Information is the lifeblood of a firm, and how that information is handled makes all the difference. Cloud computing is easier, safer, faster and more efficient.”

RYAN ANDERSON
Founder and Chief Executive Officer, Filevine
CLOUD-BASED TECHNOLOGY: TAKING AUTOMATION TO THE NEXT LEVEL
In recent surveys, more than 30% of organizations polled said that cloud investments were among their top three priorities. The reasons vary, but the top-ranking benefits of cloud computing are as follows:

- **Security:** Storing data off-site strikes fear into some, but the fact is that data is safer in the cloud. Cloud providers make it their business to monitor and maintain data security and integrity. It would be hard to imagine that a law office could, even if they wanted to, maintain a security staff dedicated to keeping their in-house data safe and do a better job than today’s cloud providers.

- **Flexibility:** Cloud technology is not an all-or-nothing proposition. Instead of making investments in new tools and associated hardware, lawyers can take advantage of Software as a Service (SaaS) offerings, select platform and infrastructure options, and create a customized system that fits their firm’s needs — and that will scale easily.

- **Accessibility:** Instead of filing cabinets full of documents, data stored in the cloud is immediately accessible. Data can be searched, filtered, printed — but never lost or misplaced.

- **Connectivity:** With cloud connectivity, data can be made available anywhere in the world and on any connected device: smartphone, tablet, laptop and so on. In addition, employees can become much more mobile, which often translates into greater efficiency and overall convenience.

- **Collaboration:** Boardrooms and offices can be replaced with virtual meeting rooms. Documents can be shared, information exchanged and conferences held regardless of location.

- **Data storage:** The sheer amount of data that a firm collects needs to be stored somewhere, and there’s no size limit in the cloud. All the firm’s data can be securely stored in a central location.

MAKING THE MOVE TO CLOUD COMPUTING
Cloud computing isn’t the wave of the future; it’s here today. The world is plugging into the cloud, and law offices that remain tied to their on-premises technology might find themselves left behind or out of business. Like all companies, law firms work with information — gathering it, processing it, accessing it and distributing it.

Information is the lifeblood of a firm, and how that information is handled makes all the difference. Cloud computing is easier, safer, faster and more efficient. And maybe best of all, it lets lawyers focus on the reason they became lawyers to begin with: the people, not the paperwork. Firms that don’t ride today’s wave of cloud technology will be left in the dust.

ABOUT THE AUTHOR
Ryan M. Anderson is the Founder and Chief Executive Officer of Filevine, a case management system for attorneys. From its launch in 2015, Filevine has focused on first-to-market innovation and award-winning design. Before starting Filevine, Anderson was a founding partner at a law firm focusing on personal injury, mass torts and employment class action.

filevine.com
Don’t Take the Bait
It’s critical for firms to take steps to reduce phishing attacks.

A large global law firm with offices in more than 40 countries experienced a debilitating cyber attack in late June 2017. According to reports, the attack originated in the firm's Ukraine office, where an administrator clicked on a malicious link that brought the firm to its knees for at least three days.

While public evidence suggests that the attack did not result in the exposure of sensitive information, the firm sustained a significant business disruption and may have suffered reputational damage.

But how many law firms can withstand three days of technical chaos in a deadline-driven environment? An attack like this can deal a death blow unless the firm has considerable resources to remediate quickly and minimize disruption to operations.

THE RISKS ARE ENORMOUS
Malicious links are often packaged in phishing emails, which trick the reader into revealing login credentials or other confidential information, generally with the intent to create a misfortune the sender can profit from.

The risks are enormous. A successful phishing attack can cost firms precious cash in remediation or ransoms. Computer systems can be paralyzed for days or weeks. Secret,
sensitive and personally identifiable information can be exposed — and the reputational risk can be severe.

Phishing attacks are soaring. According to the U.S. Office of the Director of National Intelligence, more than 100 million phishing emails are sent every day. About a third make it past default cybersecurity.

But clever criminals are staying a step ahead of prevention efforts. And law firms are juicy targets, housing a treasure trove of sensitive information while being perceived as lagging in security. Why target a major corporation when their law firm is easier to breach?

“Phishing has been going on a long time, but firms haven’t prepared for it as much as they need to,” says Eli Nussbaum, Managing Director at Keno Kozie Associates, a Chicago-based law firm technology consultancy. “Every day, a firm gets hit and they’re learning the lesson. Eventually all firms will learn, but today, we’re in a learning curve. The more I learn about security, it becomes a function of when, not if, it will happen. You need to be prepared for it.”

**LAW FIRMS ARE AT A DISADVANTAGE**

Phishing scams continue for one good reason: They’re successful enough for criminals to make huge profits. As protection evolves, so does the threat. “The bad guys are constantly evolving their attacks and are moving more quickly. They are even automating the process of stealing login credentials to start the process of getting into your email system in real time,” says Nussbaum.

Phishing works by sidestepping protection technologies. With 100 million attacks daily, firms are statistically at a disadvantage. And it only takes one successful breach to open a big can of worms.

**TAKING THE BAIT: WHAT MODERN PHISHING LOOKS LIKE**

Phishing is not new, and many firm employees may think they understand it well enough to not take the bait. The reality is that nearly anyone, under the right circumstances, can be tricked. According to Verizon’s 2017 data breach report, about one-third of phishing emails are opened.

All phishing runs on one simple idea — to trick the user into a response. Phishing is now more likely to be shaped by “social engineering,” which is an approach that plays on people’s good nature and business need to be helpful and responsive in order to trick them into bypassing normal security procedures. It’s a practice designed to deceive the most vigilant users with emails that are generally urgent in nature, requesting immediate information or action. The idea is to get the user to act now and think later.

The most successful attacks look like emails the recipient is expecting. This type of attack, known as spear phishing, blends in with email traffic. They tend to send legitimate-looking emails that appear to come from partners or clients, often with detailed instructions to wire a large sum of money.

Cybercriminals can pull this off because they’re already in the target firm’s email system reviewing privileged conversations and looking for a ripe opportunity to make a play.

"With the right technology in place, firms can further advance their cause by having and enforcing data retention and destruction policies to prevent the stockpiling of sensitive information that is not being used."

**KEEP YOUR PROTECTION SOFTWARE UPDATED**

Cyberattacks are perceived as requiring a cyber solution. Certainly, technology plays a necessary role in protection. “You need to have a solid perimeter and solid mitigation solutions and keep your systems up to date. The system you installed last year — unless it’s a managed solution — is going to be out of date,” Nussbaum says.

Antivirus and antimalware tools are a must. Advanced malware protection that uses artificial intelligence to keep up with threats can help narrow the gap between known and
emerging threats. But these tools are only as good as the last update or, for advanced tools, the latest attack.

With the right technology in place, firms can further advance their cause by having and enforcing data retention and destruction policies to prevent the stockpiling of sensitive information that is not being used. Also important are clear procedures for handling requests for sensitive information or large financial transactions.

BUILDING AWARENESS IS KEY
But experts say that user education is the most important part of reducing phishing attacks in law firms. Nussbaum suggests starting with annual training for user awareness. If firm employees and partners know what a risky email looks like, they will be less likely to take the bait and suffer the embarrassment of being the gateway to a breach. Many companies offer online training programs.

Secondly, Nussbaum says, “Phishing should be discussed frequently. People don’t learn unless they’re reminded. Rinse and repeat. Don’t let them get too far away from it before you remind them again because they will forget. You constantly need to keep it top of mind.”

One technique for staying top of mind is simulated phishing campaigns. Sometimes called ethical phishing, these campaigns send random test emails to users to see who clicks through. Small campaigns can be run throughout the year, with the simulated emails becoming progressively advanced. You can also run a phishing campaign before an educational effort to get a baseline on how susceptible your firm is to an attack.

Several companies offer simulated phishing campaigns, including KnowBe4 and Trend Micro. Simulated phishing campaigns are relatively inexpensive, costing tens of dollars per user per year.

A more involved technique is tabletop exercises where key firm security stakeholders run a simulated attack to go through the response process. This helps prevent attacks because the simulation can reveal obvious gaps in technology and processes, as well as aiding in preparing a successful response to an attack.

Firms can’t avoid phishing attacks. But given the risks, they can take concrete steps with technology, processes and user awareness to mitigate that risk. Even with the best protection, a firm can still fall victim. Being prepared with a sound response to an attack will ease the impact on the firm’s ability to continue doing business — and help preserve the firm’s reputation.

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.

mark@markbrewerwriter.com
markbrewerwriter.com
Kiss paper checks goodbye

You deserve a payment solution that doesn’t leave you waiting and wondering.

xoxo LawPay

Paper checks are notoriously unreliable. They get lost in the mail, they get tossed in the laundry, and they carry a lot of sensitive information around with them wherever they go.

LawPay changes all of that. Give your firm’s clients the flexibility to pay from anywhere, anytime. Most importantly, we ensure your firm stays in compliance with ABA and IOLTA guidelines.

It’s easy to get started

866-921-0115 or visit lawpay.com/ala
Cyber Risk Management: The Vital Role of Legal Management Professionals

This CE course will help legal managers understand their key role in helping manage the firm’s data breach risks and meeting compliance requirements.

**COURSE DESCRIPTION**

Law firms have become a major target of cybercriminals, making the protection of confidential information a major responsibility in the business of law. Firms now face increasing pressure from both clients and regulators to demonstrate they have implemented a current information security plan and are compliant with specific best practices for protecting against and responding to data breach incidents. This course will help legal management professionals better understand the risks, regulations and the important leadership role they have in cyber risk management within the firm.

**COURSE OBJECTIVES**

1. Identify the cyber risks associated with law firms.
2. Recognize the basics of good cyber risk management for your firm.
3. Outline what should be included in an information security plan.
4. Develop a clear understanding of cybersecurity compliance law and privacy standards.
5. Describe what should be included in a breach response plan.
LAW FIRMS TARGETED

Law firms are an attractive target for cybercrime because they handle sensitive information that is worth a lot of money on the underground black market. A recent American Bar Association survey revealed that one in four law firms with over 100 attorneys have suffered from data breaches. Moreover, 52% of firms with 10 to 50 attorneys reported having had one or more cyberattacks or breach incidents — more than twice the rate of larger firms.

Making these statistics worse, the cost of recovering from even a small data breach incident continues to rise to potentially catastrophic levels. The 2019 Ponemon Institute Cost of a Data Breach Report shows the average cost for a small business to recover from a data breach incident is now $2.74 million. Loss of clients was one of the single biggest cost factors in the report. The bottom line is that a single data breach incident brings enough damage and losses to tip the scales in favor of spending more time and money on cyber risk management efforts.

The Ponemon report also revealed that 54% of breaches are due to malicious or criminal attack. Meanwhile, 25% are due to system glitches and IT problems, and 24% are due to employee error or negligence.

Firm administrators and executive management should be aware of these evolving threats and must be proactive in managing this unavoidable risk. In today’s digital age, preventing data breaches and maintaining a formalized information security plan has become an essential business management practice for law firms.

MANAGEMENT OVERSIGHT

Cyber risk management is an ongoing process and requires input and oversight from firm management. Information technology (IT) managers certainly have a vitally important role to play in safeguarding electronic data and preventing cyberattacks. But executive involvement and oversight is now a must. Under federal and state laws, executive management is responsible for data security and privacy efforts, including proper response to security breach incidents.

It is highly recommended that firms create a cyber risk management committee, including the firm administrator, chief operating officer (COO) or executive director, the IT and HR managers, and at least one managing partner. Contrary to what most think, this committee and management responsibility typically is not led by an IT manager but by a legal management professional or administrator who has high-level visibility and reach into all operational areas of the firm. For most legal managers, this new area of responsibility is an opportunity to grow and expand, becoming more valuable to the firm.

For legal management professionals, the basics of good cyber risk management include:

- A basic understanding of cybersecurity compliance requirements.
- The development and implementation of an organization-wide information security plan.
- An ongoing commitment to keep the firm current and compliant with evolving data security and privacy standards.

CYBERSECURITY COMPLIANCE

Start with the baseline understanding that every law firm must comply with one or more specific data cybersecurity laws or standards. This depends on the type of client data collected or handled by the firm as well as the location of the persons or entities whose information is handled. Ignorance of these regulations and standards is not defensible.

Federal Laws

There are multiple federal data security and privacy regulations that could apply to a law firm. Most commonly, medical- or health care-related information can require compliance with HIPAA-HITECH. Financial data can require compliance with the Gramm-Leach-Bliley Act (GLBA) and other federal banking or securities cybersecurity regulations. While firms are not considered “covered entities” under these laws, they are required to adhere to these standards as a “business associate” or service provider to client organizations in the health care or financial services industries. Failure to comply can result in significant fines and penalties in the wake of a data breach incident.
**State Laws**
All 50 states have cybersecurity or data breach response laws that apply to any business collecting information on residents of their state. While a firm may only have office locations in one state, they must comply with the state laws in every state in which they collect data on persons or entities. The most notable of these more recent laws include the New York Department of Financial Services Cybersecurity Regulation and the California Consumer Privacy Act (CCPA).

**International Laws**
Virtually all major international markets and countries now have cybersecurity and data privacy laws. Most notable among them is the General Data Protection Regulation (GDPR) from the European Union. Firms that collect or process data on citizens in any of the E.U. nations must comply with this law that mandates consumer privacy protections. Penalties for noncompliance are stiff and enforcement bodies within the E.U. have investigated and fined thousands of organizations around the globe.

**Client Requirements**
Law firms face increasing pressure from clients to demonstrate compliance with cybersecurity laws and specific industry standards such as NIST, ISO 27001, SOC 2, FFIEC or others. Compliance with data security and privacy language in client contracts and successfully responding to cybersecurity questionnaires has become an important part of the business of law today.

Indeed, more firms are receiving information security audit requests or security assessments from key clients. Depending on the type of information the firm handles, these security assessment requests can follow one or more regulatory or industry security standards including HIPAA, GLBA, SOC 2, ISO 27001 or others. Some clients are also requiring on-site audits, forcing firms to show higher levels of compliance and documentation. While it may be tempting to hand off these assessment questionnaires to an IT manager, most of the assessment questions are not IT related and involve HR, facilities and other areas of firm management. Gone are the days of cybersecurity simply being an IT issue.

Legal managers should ensure that the firm is ready to respond to these types of security assessments and effectively demonstrate that they have implemented and maintained a formalized information security plan that meets minimum standards.

**INFORMATION SECURITY PLAN BASICS**
Firms should establish and uphold a comprehensive information security plan, which provides a framework of data security policies and procedures. The plan should meet minimum government and business standards for safeguarding protected client and employee data against exposure, loss or theft. It should meet the needs and objectives of the firm and be manageable by the firm’s cyber risk management team. The plan should include at least these main components:

1. **Management Responsibilities**
   While information security and privacy are the responsibility of all personnel within a firm, a successful information security program requires a commitment from top management to proactively build a culture of security and enforce the firm’s information security plan. The plan should outline management responsibilities for implementing and maintaining data security and privacy objectives. The primary duties of top management include:
   - Defining the firm’s security strategy and objectives.
   - Assigning relevant roles and responsibilities.
   - Allocating sufficient financial and human resources.
   - Responding to breach incidents.
   - Promoting a culture of security within the firm.

2. **Risk and Compliance Assessments**
   Conducting a comprehensive cybersecurity risk and compliance assessment is not only a best practice, it’s a common requirement in all government and industry cybersecurity standards. Assessments should identify potential threats and vulnerabilities while evaluating the current level of compliance with regulatory requirements, client expectations and industry best practices. Firms should complete an assessment at least annually. It should also be done in response to security incidents or upon changes in geographic market, regulatory environment or firm operations.

3. **Technical Safeguards**
   Reasonable and appropriate cybersecurity protections and vulnerability management systems should be in place to protect against growing internal and external threats to confidential information. Firms should determine what technical safeguards are reasonable and appropriate to their size and scope of business and ensure they meet minimum industry and regulatory cybersecurity standards. Examples of technical safeguards include vulnerability testing, computer and network security, intrusion detection systems, IT asset inventory controls, access rights management, encryption, data backup, and employee computer and mobile device security policies.
4. Physical Safeguards
The firms’ security plan should include measures to prevent unauthorized physical access to buildings, offices, computer equipment and confidential paper documents. At a minimum, firms should consider including policies and procedures for office/building security, document storage, and secure document and equipment disposal.

5. Security Awareness Training
Employee error and negligence is one of the leading causes of data breach incidents. Firms should have a formalized cybersecurity awareness training program in place to ensure all personnel, including management, receives ongoing training on the latest information security best practices.

6. Third-Party Risk Management
Third-party service providers, vendors and business associates who have any access to protected client and employee information can be a serious security risk to the firm. Third-party risk management is also often referred to as “vendor risk management.” To mitigate information security risks from third parties, the firm’s strategy should include measures to assess the cybersecurity readiness of vendors and service providers. Firms should also establish an information security agreement with these third parties that outlines minimum acceptable data security standards and incident response steps.

7. Privacy Rights Management
Newer laws such as the GDPR and CCPA require firms to be prepared to make additional disclosures to clients about the firm’s personal data collection practices, the use of the information and to whom the information is disclosed. To be compliant, firms must be able to:
- Locate and deliver specific information in a timely manner.
- Identify contracts that may constitute a sale of data under new broad definitions.
- Have established specific policies and procedures, including but not limited to protection against discrimination of individuals who exercise their privacy rights and opt out of the use of their personal information.

8. Business Continuity
Adverse or disruptive events such as natural disasters, power failure, ransomware and other denial of service attacks, or even widespread hardware failure can create a variety of information security risks and can render client information inaccessible. To follow industry best practices and meet regulatory requirements, the firm should have a business continuity plan (BCP) in place. At a minimum, this includes policies and procedures for data backup, system and data recovery, and the security and availability of client information during adverse or disruptive events.

9. Breach Response Plan
With law firms being targeted by cybercriminals, it is almost certain that every firm — no matter its size and sophistication — will experience information security problems or data breach incidents that put clients and the firm at risk. Timely and appropriate response to even a small data breach incident is critical in order to meet U.S. and international regulatory mandates.

To minimize reputational, legal and financial risks, firms should have a formalized breach response plan, including at least:
- Incident response team duties
- Breach discovery and containment procedures
- Reporting to authorities
- Communications and PR strategy
- Victim notification and remediation
- Post-incident review, correction and training

REVIEWS, UPDATES AND REPORTING
Cybersecurity risks are evolving and growing at unprecedented rates. To keep current and stay compliant, it’s necessary to conduct regular reviews and updates of the firm’s data security and privacy practices. Among other things, this includes regular vulnerability testing, updates to the employee training program and information security plan.

Firms should assess, review and update their overall information security plan at least once a year, after a data breach incident, or when significant changes to business operations or regulations occur. Examples of changes to business operations could include firm merger or acquisition, the opening of new office locations or geographic markets, or special cybersecurity requirements from a key client. New or updated U.S. federal and state laws or international data security regulations may also necessitate a review of the firm’s security plan.

The information security plan review and update process should include:
• Conducting a full risk and compliance assessment based on current regulatory requirements and industry best practices.

• Identifying and addressing newly discovered security risks or gaps in compliance.

• Updating the information security plan to document and incorporate necessary changes to policies and procedures.

• Training on new policies and procedures for executive management and employees.

**Management Reports**

In order to help firm executives and partners meet their obligation to effectively manage cyber risks, legal management professionals should be prepared to provide the executive team with regular reports that summarize the firm’s current efforts to follow its information security plan and meet minimum regulatory and business standards. These types of risk and compliance reports are typically preceded by a scheduled review and assessment process. There are helpful programs and tools available that help simplify and automate these regular reviews and management reporting.

**AN ONGOING COMMITMENT**

With the escalating data security threats against law firms, cyber risk management has become an essential function in successfully managing law firms large and small. To be sure, businesses, government agencies and other organizations are demanding their legal counsel stay current with the latest data security and privacy best practices. Government cybersecurity regulations will continue to evolve, and the pressure to be compliant will continue to mount.

Cybersecurity and compliance shouldn’t be looked at as a necessary evil. Rather, it’s an opportunity to become more forward-thinking, increase client trust, and help mitigate financial and reputational damages that inevitably come with even small data breach incidents. The cost of implementing an information security plan can be substantial and should be managed just like any other significant budget item.

It’s important to remember that cyber risk management is an ongoing process and commitment. Information security is more than security software, and compliance is not a onetime event. Managing cyber risks and staying compliant is an ongoing process of assessment and implementation of proper safeguards, followed by consistent training and improvement. It’s vital that the firm stays current with the latest protections and best practices to protect their clients and meet the changing threat landscape.

With their consistent involvement and reach into most or all operations of the firm, legal management professionals are best suited to lead the firm’s cyber risk management effort. This is an incredible opportunity to expand skills and become more valuable to the firm. With the help of outside experts, and by embracing the training, tools and resources available today, legal managers can quickly become prepared to lead and manage the firm’s information security plan and cybersecurity compliance tasks.

**ABOUT THE AUTHOR**

James Harrison is the Founder and Chief Executive Officer of INVISUS. With 20 years of cybersecurity experience, he’s considered one of the industry’s foremost experts on cyber risk management. He is responsible for the development of the company’s cybersecurity, identity theft and data breach prevention and compliance product lineup. He is the creator of the InfoSafe® cybersecurity compliance and certification program that is used by businesses and law firms throughout the U.S. and internationally. Harrison regularly speaks and trains at various industry and trade conferences including most recently at the 2018 ALA Annual Conference & Expo.

james@invisus.com

linkedin.com/in/james-harrison-b703b71/

---

**EARN YOUR CE CREDIT**

Now that you’ve read the course, take the exam to earn your CE credit. Please use the information below to register for the exam. A confirmation email will be sent to you with additional details. Please check your junk/spam folder, as it may be filtered there. To register, please visit bit.ly/30OLw9C. Members pay $49; nonmembers pay $69. Once you have registered, please visit alanet.org/elearning to access the exam. If you have any questions, please email us at elearning@alanet.org.
#ALACconf20 Keynote Speaker:

Dr. Catherine Sanderson  
*Manwell Family Professor of Life Sciences (Psychology)*  
*Amherst College*

**The Science of Happiness**

Learn practical (and relatively easy!) ways to increase your own psychological well-being with cutting-edge research from the field of positive psychology.

"This was one of the **best keynotes** I've heard!"

"Amazing! Great info and well presented. **Entertaining** and **energetic**."

"Very engaging, **inspiring** and **thought provoking**. Loved the speaker. Great tips I can start implementing to change behavior."

"Catherine was engaging and on point. I thoroughly enjoyed her anecdotes and **real life applications** for finding and maintaining happiness."

Join 1,500 of your peers for knowledge, networking and innovation on May 3-6, 2020, at the Salt Palace Convention Center in Salt Lake City, Utah.

**REGISTER TODAY**

📞 1-888-593-7243  
✉️ info@alaannualconf.org  
🌐 ALAannualconf.org
Tech Trends That Could Change How Firms Operate

From document review to providing visual evidence, new tools are emerging to help firms work faster and more effectively.

The legal industry doesn’t seem to be shying away from adding new technology — tech investments reached a record amount, $1 billion, in 2018, according to a Wolters Kluwer survey.

More than half (53%) of U.S. and European attorneys say their organization’s technology investment will increase within the next three years.

When it comes to transformational newer tools — virtual reality or artificial intelligence (AI), for example — lawyers generally acknowledge they can be beneficial, but a number report resistance to adopting them. Lack of knowledge is a major factor. Less than a quarter of attorneys say they understand machine learning, AI or blockchain technologies very well.

EMERGING TECH
Although some firms and legal departments may be hesitant to implement them, other industry members foresee a brighter future for emerging technologies, including the following:
1. **Artificial intelligence:** AI — essentially, machines’ ability to replicate human behavior by performing tasks and executing complex thought and decision-making processes — isn’t a completely new concept in the legal realm.

Firms have used tools that employ AI for years in e-discovery document review, and now some are using the technology to analyze contracts and identify areas for attorneys to review, according to Bobbi Basile, Managing Director in the Legal Transformation and Innovation practice at HBR Consulting.

“The first iteration of innovation has been on efficiency — the management and running of the firm and insight into financial performance and other areas,” Basile says. “The next iteration is now focusing on client experience and providing value.”

Since adding an AI-based analytics platform late last year, Pillsbury Winthrop Shaw Pittman LLP has been examining how it can use its AI capabilities to understand large data sets from clients. They might also use AI to encode and create classification models that can be used on multiple cases, according to David Stanton, a Litigation Partner who also heads up the firm’s information law and electronic discovery practice and oversees the litigation support department.

The international law firm may also try to use the tool to deconstruct long email chains and other communications to be able to search messages and, for example, identify unique content chronologically.

“Historically, a lot of money has been spent looking at big sets of documents where 80% were nonresponsive, just to confirm they are,” Stanton says. “Machines have gotten good at helping us put our attention [toward] documents that actually matter.”

2. **Blockchain technology:** Often associated with Bitcoin, blockchain systems bundle each new action with previous actions, essentially verifying each new item because it’s part of a longer chain of events — such as financial transactions — that are already considered to be accurate. Each transaction is recorded automatically, and the involved identities can be encrypted.

While legal didn’t even make the list in a PwC tally of industries considered to be leaders in blockchain development, Wolters Kluwer found that 48% of firms and legal departments are still in the planning phase of leveraging this new technology. Meanwhile, 70% of firms and departments that are tech-advanced plan to be using blockchain by 2022.

Attorneys’ expected applications include using blockchain in compliance tasks (55%) and contract management (54%).

“There’s interest in blockchain, and even firms that are developing specialty [items] around it,” Basile says. “Because clients are starting to embrace it, [legal counsel is required] to have participated in and be prepared to deliver services in that environment.”

3. **Wearables:** Fennemore Craig attorneys have been adding clients to their Apple Watch VIP list so their emails and texts are seen right away. Additionally, the firm was an early Google Glass adopter, according to Marc Lamber, the Chair of its personal injury practice.

The firm, which has locations in Nevada, Colorado and Arizona, has used the technology to illustrate the daily hardships encountered by a client who was a double amputee from a first-person perspective.

“When Google Glass was first introduced, we thought it may prove to be an excellent opportunity to tell our clients’ stories in a very powerful way,” Lamber says. “It also opened the line of communication with this client because he could communicate with us remotely using voice activation.”
Russell D. Knight, Founder of the Florida- and Illinois-based Law Offices of Russell D. Knight, wonders if clients one day could expect attorneys to utilize a device like the one he’s seen judges increasingly assign in divorce cases, which remotely conducts breath-based blood alcohol tests while simultaneously photographing the individual.

“Sooner or later, some client is going to want permission for a computer to snap a photo of the attorney working on their case to verify billing. Why wouldn’t computers take screenshots of what they’re working on every six minutes and of them at the same time?”

While clients might be able to eventually request that of a service provider, employers trying to track productivity or other operational aspects that involve employees may seem like more of an invasion of privacy, according to Knight.

“When you wear something like a bracelet that says you took 2,000 steps, [employers might say] ‘What are you doing? You were supposed to be at a desk,’” he says. “People are open to it until they start having to do it, and then realize the implications.”

4. Virtual reality: Using a headset, the technology can provide immersive 3D experiences — such as transporting a jury directly into an accident scene an attorney is trying to describe, according to Lamber.

“As lawyers, one of the biggest challenges in a case is showing the decision-makers what actually happened,” he says. “In the old days, we’d use demonstrative exhibits, visual aids and witness statements. With virtual reality, we can put them in the car at impact. That’s powerful — [and] has the potential to be a game changer in the practice of law.”

Two years ago, when Matthew Stubenberg was IT Director at the Maryland Volunteer Lawyers Service and Co-Chair of the Maryland State Bar Association’s Young Lawyers Section Technology Committee, he spearheaded an effort to create virtual reality videos designed to help attorneys learn how to handle pro bono work and to help new lawyers get comfortable appearing in court.

The Young Lawyers Section used discretionary funds to buy a 360-degree camera and filmed the footage in a law
school courtroom. The VR experience was then shared on YouTube, where it could be viewed using a device such as Google Cardboard, according to Stubenberg — who is now helping to conduct three studies involving virtual reality’s impact on legal work as Associate Director of Legal Technology at Harvard Law School’s Access to Justice Lab.

“For a lot of new attorneys, it’s these unwritten procedural steps that you’re worried about making a mistake on,” he says. “The goal was to take away some of that mystery. Virtual reality tricks your brain into believing you were there, so it’s no longer your first time in court. You have to decide what to look at; [in] a regular video, the director makes the decision for you [and] cuts to whatever is important. You retain less information that way.”

NEXT-GEN TECH TOOLS
While VR’s applications may seem vast, Lamber notes the technology’s adoption can face some challenges. A judge would need to authorize the technology’s use in the courtroom; opposing counsel would also be able to access it.

“The other challenge is cost,” he says. “Hiring expert reconstructionists and scanning a scene to create a meticulously accurate model can easily run into the six figures — perhaps taking litigation expenses beyond what a case might be worth.”

VR isn’t the only type of emerging tech that may run into implementation roadblocks. Regulatory uncertainty is the biggest barrier to blockchain acceptance, according to PwC’s findings. Plus, the expense of incorporating AI functionality can be a deterrent for firms — particularly if they’re smaller.

However, legal departments and firms that do decide to invest in innovative technology may find it provides numerous benefits.

“Law firms are seeking more ways to differentiate themselves with clients and to attract talent by modernizing the practice of law. Because attorneys entering the profession have grown up with technology their entire lives, they are taking that information into consideration [in regard to] where they want to spend or begin their career.”

The capital for new tech tools often comes out of the partners’ pockets; thus, adding these tools can understandably be a significant decision. With mounting demand for increased efficiency, though, it’s one that could potentially pay off.

“Law firms are resistant to change, [but] technology has a way of seeping in,” Stanton says. “It will take clients not only demanding these changes but investing in them. The most effective use will be with clients who are committed to collaborating to put these kinds of things together.”

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
chicagojournalist.com
This member benefit keeps getting better ...

Allow ALA’s Event Planning Plus program to take care of some or all of your meeting planning needs, from selecting agendas and hiring speakers to selecting venues and budgeting.

**ALA Speaker Services**
Browse agendas to find a presentation that meets your specific needs. All sessions are delivered by ALA-vetted speakers. New speakers and topics are added throughout the year!

**Retreat Locations**
Whether the goal is to bond and have fun or to advance important initiatives and develop strategies, we have a location in mind for your event. We’ll help you choose experiences and venues aligned with your desired outcome.

**Meeting Planning Request**
ALA’s meeting planning team can take the reins for your next chapter or firm event. You’ll take advantage of ALA’s buying power while continuing to meet your daily job requirements and impressing your team with an inspiring outcome.

**Planning Outlines**
Get links to templates including event budgets and outlines.

Get started today!
[alanet.org/epp](https://alanet.org/epp)
Teaming Up with Microsoft Teams

We live in a world of apps — lots of apps. As the popular saying goes, if there is some activity in the office or home that you want to pursue, the usual response is, “Is there an app for that?”

We have our collection of favorite apps that we use for personal productivity and to communicate with family and friends. But sometimes the sheer volume of available apps makes it increasingly difficult to keep our business-oriented projects organized and easily accessible. We use one app for email, another for instant messaging or chatting, another for calendaring, yet another for file sharing, online meetings, project management, white boarding … and the list goes on and on. Pretty soon we spend more time searching for content across multiple apps than we do working on the projects that the apps are supposed to be supporting.

STOP, COLLABORATE AND LISTEN

If you’re like us and are beginning to feel the onslaught of app overload, take heart — there’s an app for that, too. Collaboration or chat apps are platforms that allow users on a team or business group to work together using myriad apps. Yet chat apps keep all the team activity neatly organized and easily accessible under the roof of the collaboration framework.

Team collaboration apps are not new, but their widespread acceptance and use in professional workplaces is a new phenomenon experiencing tremendous growth. Slack was really the first modern collaboration app we ever used seriously. It launched in 2013 and quickly rose to become the dominant application for collaboration and chat just as these types of tools were gaining widespread acceptance in the marketplace.

We were initially skeptical when seemingly always-late-to-the-party Microsoft launched a Slack competitor, Microsoft Teams, in 2017. But, to our surprise, Microsoft Teams — owing much to the huge popularity of Office 365 — has seen explosive growth over the last two years and now eclipses Slack in popularity in recent user surveys.
In short, Microsoft Teams allows you to seamlessly communicate and collaborate with members of multiple teams using various software tools within the application. If you are a Microsoft Office 365 subscriber (which we highly recommend), then you already have Teams and can begin using it without any additional cost. If you don’t use Office 365, you can still download and use a free version of Microsoft Teams.

We both already have Office 365, so we decided to start using the Teams app for new projects rather than setting them up in Slack. Just like Slack, Teams can be used on any platform. For our Apple team members who think Microsoft is just for geeks, we tricked them into using Teams because the iOS version of the app is slick and fully functional. There is both a stand-alone app as well as an online web version.

We were already familiar with the Channels organization within Slack, so we very quickly acclimated to the similar organizational layout in Teams. Unlike Slack, however, Teams is obviously deeply integrated with the rest of the Office 365 ecosystem, which makes it a natural tool to extend the usability of the products that we have been using in our office for years. Most of us work regularly in Word, PowerPoint and Excel. For the most part, the extent of our collaboration with colleagues involves emailing a document as an attachment. (As Bill is fond of saying, that type of collaboration is so “2000-late.”)

Now think forward to the 21st century. You’re working on a contract, brief or presentation, and you need to get feedback from one or more team members. You simply click on the collaboration channel that has been set up in your Teams app and share the document with your colleagues who are authorized on that channel. You can then chat online, initiate a video call and even edit the document in real time with everyone that you invited participating. You do this without leaving your office, home or even the beach. (Phil added this last edit while on vacation.)

Even more valuable is the ability to quickly access any and all activity that has transpired on a particular project, subject or channel right within the Teams app. Whether the activity is a series of email threads, meeting notes, call recordings or online chat sessions, we no longer have to search through hundreds of apps to see how the activity was created — we have everything right there win the Teams app.

While Teams is tightly integrated with Office 365, you are not restricted to using only Microsoft products within the app. There is a huge array of apps that you or your team can use right within the Teams interface. For example, if there is a particular YouTube video that we wish to share with our team members, we can simply link that video within Teams, and everyone can view the video without leaving the Teams app.

At last, we think we have found the solution to “death by a thousand apps.” We just didn’t realize it was going to be another app. But Microsoft Teams has become our favorite method for aggregating a host of useful tools all within a single interface that all our team members can use, regardless of their computing platform.

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.

twitter.com/BillandPhil

No-Cost WEBCASTS from the Solutions Series

ALA relies on its business partners to share solutions for pressing issues and hot topics in the legal industry as they work closely with legal management professionals. In these free webcasts — available live and on-demand — they pass along an abundance of knowledge.

Watch now! legalmarketplace.alanet.org/events
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. You can view them live or at your leisure; the continually updating on-demand catalog goes back to 2013.

Check out these upcoming webinars:

**OCT. 16**
Blockchain: An Evolution or Just the Next Passing Thing?  
*Teresa J. Walker, Waller Lansden Dortch & Davis, LLP*

**OCT. 17**
Law Firm Profitability: More About Navigating the New Normal  
*Frederick J. Esposito Jr., MBA, CLM, Rivkin Radler LLP and the Legal Lean Sigma Institute*

**OCT. 23**
Creating a Culture of Accountability  
*David O’Brien, WorkChoice Solutions*

**NOV. 5**
Redirecting Negative Behavior  
*Judy Ryan, LifeWork Systems*

**NOV. 7**
Building Accountability into Your Culture  
*Debbie Foster, Affinity Consulting Group*

**NOV. 12**
The Ethical Considerations of Law Firm Leadership: 13 Things You Might Not Be Thinking About But Should Be!  
*John Remsen Jr., TheRemsenGroup and the Managing Partner Forum*

**NOV. 19**
Driving Data-Driven Change: Strategy, Planning and Leadership  
*Marcie Borgal Shunk, The Tilt Institute*

Learn more at [alanet.org/webinars](http://alanet.org/webinars)
Cybersecurity Compliance: 4 Questions You Need to Ask

By James Harrison

Cybersecurity is about risk management. Firms and legal departments feel pressure not only to protect confidential data for their clients but also to comply with information security and privacy laws such as Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR) and the forthcoming California Consumer Privacy Act (CCPA). These types of regulations have raised the stakes for firms in protecting confidential data.

Here are four questions legal management professionals should ask to better promote cybersecurity compliance within their firm.

WHAT CYBERSECURITY REGULATIONS APPLY TO OUR FIRM?
Start with the baseline understanding that every law firm, including yours, has specific data protection laws and industry standards they must follow. Keep in mind that cybersecurity regulations and requirements evolve and change constantly, so it’s important to ask this question and evaluate on a regular basis.

To determine which laws and standards you should be compliant with, evaluate the type of data your firm handles on a day-to-day basis. For example, medical- or health care-related information can require compliance with HIPAA. Financial information can require compliance with the Gramm-Leach-Bliley Act (GLBA) and other banking or securities cybersecurity regulations.

Another consideration is the location of the person or entity whose data you hold. All 50 states have data breach response or cybersecurity laws, and they are updated frequently. Your firm should be compliant with the regulations in each state and country where individuals or entities whose personal data you have collected reside. If you have data on persons in California, New York or anywhere in Europe, pay close attention — their new data security and privacy laws come with significant penalties for noncompliance.

Finally, look at your client contracts for data security and privacy requirements. More companies are requiring their law firms to comply with specific industry cybersecurity standards ascribed by the National Institute of Standards and Technology (NIST), ISO 27001 and others.

To fully evaluate which federal, state and industry regulations apply to your firm, you may consider getting outside help from a cybersecurity compliance service provider. To keep things simple, it’s recommended that you establish a single information security plan with best practices that are common across these major regulations and industry standards.

HOW DO WE IDENTIFY OUR COMPLIANCE GAPS?
A good risk and compliance assessment will help you match up your firm’s current security and privacy practices with regulatory and industry standards. Some firms bring in outside consultants and spend days on in-depth administrative and
With the escalating data security threats against law firms, cyber risk management has become an essential function in successfully managing law firms, large and small.

technical analysis. But for most, using a third-party compliance self-assessment program with review and consultation by outside experts is a simpler, quicker and more affordable way to score your compliance and assess your firm’s risk level.

Your completed risk and compliance assessment should result in an executive summary detailing the things the firm is doing well and the specific areas that need attention. This report should also help you determine the potential financial risk to the firm should a breach incident ever occur.

While compliance assessments deal mostly with policies and procedures, you may also consider doing cybersecurity vulnerability testing at the same time to look for security problems and measure compliance against the technical requirements for your firewalls, websites and computers.

WHAT’S OUR PLAN TO GET AND STAY COMPLIANT?
If you can’t immediately answer this question, it’s time to focus your firm’s attention on creating a formalized, documented information security plan that ensures your firm stays on track. If you already have a plan, perhaps it’s time to reevaluate and update it.

Your plan should establish a clear directive that outlines your firm’s data security and privacy practices, including which members of the management team have oversight and enforcement responsibilities. Your plan should include not just what you will do to protect client data, but how. This should be a living plan with at least annual reviews and updates.

HOW DO I EXPLAIN THIS TO FIRM MANAGEMENT?
Knowledge is power. You may have to help create a narrative that frames cybersecurity compliance as a business issue — not just an IT issue — and a critical part of the firm’s reputation and success. Even a small data breach incident can result in significant reputational damage, financial losses and regulatory fines.

Notably, IBM Security’s 2019 Cost of Data Breach Report found that data breaches now cost companies an average of $3.92 million. The bottom line is that a single data breach incident brings enough damage and losses to tip the scales in favor of spending more time and money on cybersecurity compliance.

There are two things you can do to help make this a priority for the firm:

1. Ask to form a cyber risk management committee, which should include the firm administrator, IT and HR managers and at least one managing partner.

2. Spend a little bit of money to conduct a risk and compliance assessment and share the results with the executive team.

Tackling these four questions isn’t always easy, but it can cement firm administrators and managers as essential business enablers. Cybersecurity compliance can be complex and costly in today’s business climate without expertise and proper tools. But the right solutions make it simpler and more affordable to help you reduce risk and stay ahead of changing compliance requirements.

ABOUT THE AUTHOR
James Harrison is the Founder and Chief Executive Officer of INVISUS. He is the market strategist and product visionary for the company, responsible for the development of its identity theft, cybercrime, and InfoSafe® cybersecurity compliance product lineup. As an industry expert, Harrison regularly speaks and trains at various industry and trade conferences including recent national conferences for ALA. INVISUS has partnered with ALA VIP business partner BreachPro to provide the InfoSafe and iDefend Business program to ALA member firms.

james@invisus.com
linkedin.com/in/james-harrison-b703b71/
Heather A. Duncan, a member of the Mile High Chapter, is now Chief Operating Officer for Vogel Law Firm in Fargo, North Dakota.

Jessica A. Gerhardson, a member of the Minnesota Chapter, is now Business Director at Greenberg Traurig, LLP, in Minneapolis, Minnesota.

Richard C. Gibson, a member of the Capital Chapter, is now Director of Office Administration for Ropes & Gray LLP in Washington, D.C.

Brenda C. Homan, a member of the Dallas Chapter, is now Office Manager at Dorsey & Whitney, LLP, in Dallas, Texas.

Jason D. Horvath, a member of the Mile High Chapter, is now Director of U.S. Pricing and Profitability for Dentons US LLP in Denver, Colorado.

Amanda C. Moellendick, a member of the Northern Virginia Chapter, is now Firm Administrator at BrigliaHundley, PC, in Tysons Corner, Virginia.

Deirdre Ann Petersen, CLM, an independent member, is now Firm Administrator at Barnwell Whaley Patterson & Helms, LLC, in Charleston, South Carolina.

Becca Stutsman, a member of the Dallas Chapter, is now Office Administrator of the Dallas and Plano, Texas, offices of Spencer Fane LLP.

Jennifer Vuong, a member of the Calgary Chapter, is now Talent Coordinator at Dentons Canada LLP in Calgary, Alberta, Canada.

Jane Michelle West, SHRM-SCP, SPHR, a member of the Dallas Chapter, is now Director of Operations for The Bassett Firm in Dallas, Texas.

ALA is sad to report that Ettastine H. Williams, who was a member for 17 years, passed away recently at the age of 64. She had been the Human Resources Manager at BakerHostetler in Washington, D.C. Our thoughts are with her family, friends and colleagues.

We must also pass along news of the death of member Nicole Nemeth, who was 43. She was a member of the Dallas Chapter and worked as the Accounting Manager for Neal Ashmore Family Law Group in Lewisville, Texas. Contributions in her memory can be made to the In-Sync Exotic Wildlife Rescue and Educational Center.
What’s Happening at Headquarters?

REGISTER NOW FOR THE 2020 ANNUAL CONFERENCE & EXPO

Make plans to attend the industry’s most significant annual event for legal management professionals, ALA’s Annual Conference & Expo, taking place May 3–6, 2020, in Salt Lake City, Utah. Do this for you, your career and your firm. We can promise you will have difficult learning choices to make — more than 70 educational sessions will be offered as part of our elevated program. Our business partners will be there in full force in a redesigned Exhibit Hall, and there will be ample opportunities to connect with colleagues. Learn more and register here: alanet.org/conf20.

NEWLY RELEASED: 2019 COMPENSATION AND BENEFITS SURVEY

The 2019 Compensation and Benefits Survey Report and the 2019 Large Firm Key Staff Compensation Survey Report have been officially released. Purchase your copy now so that you have full access to data that can help you develop new positions and evaluate the competitiveness of your compensation packages.

This year, ALA added data for more than 25 additional positions — mainly in the growing and often well-paid areas of marketing and technology. Overall, the report contains numbers for more than 90 roles, derived from the surveyed compensation of more than 10,000 legal industry professionals all over the United States. Download — for free — the accompanying Executive Summary, which pinpoints nationwide and regional trends and year-over-year changes. Order your copy today: alanet.org/compsurvey.

ALA’s 2019 Compensation and Benefits Survey

Every year, new job titles and levels of responsibility crop up as the industry evolves, and ALA’s Compensation and Benefits Survey helps define these new positions and their value to firms.

- Over 40 metro areas with dedicated sections
- More than 90 positions
- Enhanced marketing and technology sections

PURCHASE THE FINAL REPORT! alanet.org/compsurvey
DON’T MISS THE NOVEMBER SUMMIT SERIES

A new round of Summit Series webcasts is coming in November! This time around, legal industry expert Ari Kaplan will interview academics, consultants and authors.

- **November 1**: David H. Freeman, JD, the Founder of Law Firm CultureShift®, is a highly rated business development consultant and coach. That’s exactly what he’ll be discussing in Creating a Culture of Business Development.

- **November 8**: Dr. Mark Goulston’s diverse résumé includes work as an FBI hostage negotiation trainer, a psychiatrist, a suicide prevention expert, an executive coach, and an international consultant. His program, *Talking to Crazy: How to Deal with the Irrational and Impossible People in Your Life*, is based on his best-selling book of the same name.

- **November 15**: Anthropologist Philip Folsom translates his firsthand study of human and animal behavior to the worlds of executive coaching and culture development. In *Using Lessons from Tribes to Create Highly Functional Teams*, he will describe what ideas can have a transformational impact on the health and performance of your organization.

You can view all the previous webcasts — nine in total — whenever and wherever you want for on-demand legal industry knowledge. Remember: members can watch them all for free at alanet.org/summit.

---

REVIEWED YOUR MEMBER PROFILE LATELY?

We want to draw your attention to the My Media tab. Log in to my.alanet.org to find this convenient library of much of the content you’ve been granted access to through purchases or as part of your participation in ALA — think surveys, e-learning courses and conference recordings.

If you attended the 2019 and 2018 Annual Conferences, you can now view all the recorded education sessions we currently have available. This is part of the Legal Management Resource Hub initiative. Make sure to check My Media again when we add the hubs for C-suite, finance and law firm management essentials. (If you didn’t attend in either of those conference, you can get access by purchasing the suite of recordings.)