

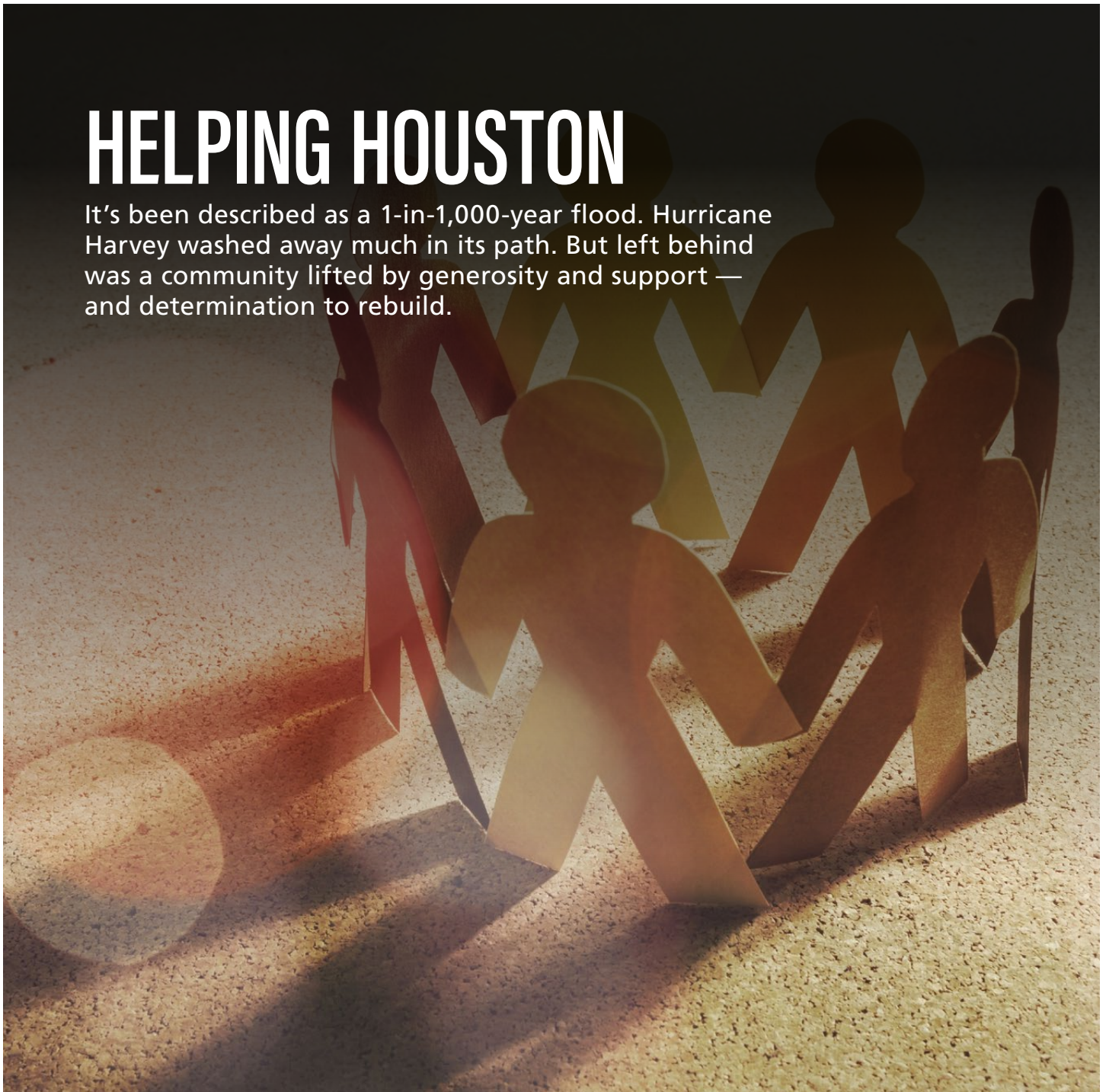
LEGAL MANAGEMENT

OCTOBER 2017
VOLUME 37 • ISSUE 9

THE MAGAZINE OF THE ASSOCIATION OF LEGAL ADMINISTRATORS

HELPING HOUSTON

It's been described as a 1-in-1,000-year flood. Hurricane Harvey washed away much in its path. But left behind was a community lifted by generosity and support — and determination to rebuild.



+60%
1.04.31



Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	1	2	3	4	5
6	7	8	9	10	11	12
		15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2

100%



CLIENT AND MATTER MANAGEMENT

EMILE AND ELECTRONIC FILE MANAGEMENT

CALENDAR MANAGEMENT

Manage Lists

Remote Time Entry

Timer

00:35:15
HR MIN SEC

50%

25%

0%

2004

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





FEATURES

OPERATIONS MANAGEMENT BY CHRIS HOGAN

6 TIPS FOR LAW FIRM CYBERSECURITY 18

The nature of the data law firms collect makes them an ample target for breaches. Here are security steps to take.

SPECIAL FEATURE BY VALERIE A. DANNER

HELPING HOUSTON 22

It's been described as a 1-in-1,000-year flood. Hurricane Harvey washed away much in its path. But left behind was a community lifted by generosity and support — and determination to rebuild.

OPERATIONS MANAGEMENT BY ERIN BRERETON

DON'T ASSUME YOUR DATA ISN'T AT RISK 29

Data and privacy breaches are a growing concern for firms of all sizes. Find out what you need to know to keep information secure.

COLUMNS

BIG IDEAS: A MESSAGE FROM ALA'S EXECUTIVE DIRECTOR 6

Coming Together

BP PERSPECTIVE 8

Telecommuting Does Not Have to Be the Wild Wild West ... Unless You Let It

INSURE YOUR SUCCESS 11

7 Questions to Find the Right Broker

TEST DRIVE 33

Gadget Reviews with Bill and Phil: Amazon Echo Brings a Nice Touch

THINKING OUT CLOUD 13

Data Security and Dictation Efficiency Can Go Hand-in-Hand

DEPARTMENTS

FACTS AND STATS 16

INDUSTRY NEWS 36

Can Your Firm Win the War Against "Wares"?

TIPS AND TRENDS 38

Corporate Clients Are Zeroing in on Outside Counsel Cybersecurity

ALA NOW

ALA FACES 40

Member and Chapter News

JERRY BROWN, ALA VISIONARY, PASSES AWAY 42

LEGAL MANAGEMENT STAFF

PUBLISHER

Oliver Yandle, JD, CAE
oyandle@alanet.org

EDITOR-IN-CHIEF

Theresa Wojtalewicz
twojtalewicz@alanet.org

MANAGING EDITOR

Valerie A. Danner
vdanner@alanet.org

ASSOCIATE EDITOR

Kate Raftery
kraftery@alanet.org

ADVERTISING OPPORTUNITIES

Robert Leighton
advertising@alanet.org

ART DIRECTOR

Jeff Wojciechowski
Straight North, LLC

GRAPHIC DESIGNER

Abby Burkle
Straight North, LLC

Cristina Muzzio
Straight North, LLC

WEB TEAM

Eric Michalsen
Straight North, LLC

Greg Wixted
Straight North, LLC



Who's guarding your firm?

More and more law firms answer **OnGuard™**. Whether you are just starting an information security program or upgrading one, OnGuard™ is the truly proactive defense of your private and confidential data.

EDUCATION - Award-winning *Information Security Awareness Program* to create and sustain a culture of security.

EVALUATION - Annual Risk Assessment, Penetration Test, Vulnerability Assessment and Client Analysis to keep your house in order.

MITIGATION - *Virtual Information Security Officer* for client audit response, policy maintenance, vendor risk management and business continuity programs.

For those who take information security seriously, there is only one answer to the question "Who's guarding your firm?"

OnGuard™





Five minutes
can save your
firm up to 40%.

Discover how to cut costs and gain control.

Yesterday's shipping practices can cost you. Many law firms lose 10-12 percent in revenue due to poor or absent mailroom practices.

Are you processing outgoing mail the old-fashioned way? This can mean lengthy searches for items that were shipped but not received. Spending too much. Or spending hours tracking and charging back shipping costs to clients.

Turn things around and ship smarter with Pitney Bowes. Find out how to cut costs and gain control.

Learn how to ship smarter. Call: 888 540 3777.



OLIVER YANDLE, JD, CAE
*Executive Director, Association
of Legal Administrators*

Coming Together

Hurricanes. Earthquakes. Wildfires. And now, the worst mass shooting in modern U.S. history. Over the last few months, we've seen Mother Nature's wrath and unspeakable evil bring devastation, heartbreak and pain to communities across North America. Watching the news has been anguishing; for those directly affected by these disasters, the process of healing, recovering and rebuilding must seem overwhelming.

But often, these wrenching experiences bring out the very best in us all — acts of bravery, acts of compassion, acts of generosity. One of the greatest strengths of ALA is our network, and that network has come together repeatedly to provide much-needed support and comfort to our colleagues and friends affected by these tragic events. This month's cover story, "Helping Houston," recounts the extraordinary efforts of our members to help their colleagues rebuild after the catastrophic damage wrought by Hurricane Harvey.

Then, right on the heels of Harvey, came Irma to the Caribbean and Florida and Maria to Puerto Rico. We've seen a massive earthquake and aftershocks devastate parts of Mexico, while wildfires have raged (and continue to do so) in the western United States and Canada. And, recently, we are left with heavy hearts after the tragic shooting rampage in Las Vegas.

While our hearts may be heavy, they are also very big. Each time, ALA members have responded in whatever ways they can. Checking in with friends and colleagues in affected areas. Donating money to relief efforts. The ALA community comes together to offer comfort and support.

The needs of these communities will stretch well beyond a few weeks or even a few months. But trying to figure out the best way to help can sometimes be daunting. Our cover story includes information on charitable organizations providing aid to those affected and

“

While our hearts may be heavy, they are also very big. Each time, ALA members have responded in whatever ways they can.”



suggestions on how to ensure your contributions get to those who need your help.

Beyond money, there are other ways to support our friends in need. Although the American Red Cross reports that Las Vegas area hospitals have sufficient blood to supply needs there, the shooting “illustrates that it’s the blood already on the shelves that helps during an emergency,” according to a press release. To donate blood in your area, visit www.redcrossblood.org.

And you can never underestimate the power of a phone call or a note letting friends and colleagues know that you care. The outpouring of support from our members has truly been awe-inspiring to me and a tremendous source of comfort to those in need. Thanks for caring. ■



oyandle@alanet.org





KENNY LECKIE
Senior Technology and Change
Management Consultant
Traveling Coaches

Telecommuting Does Not Mean the Wild Wild West ... Unless You Let It

“

Your ethical obligation to protect firm data extends to any and all ways you connect to that information.”

Telecommuting can be a fantastic benefit provided by your firm. It can also be a dangerous avenue to expose your firm data, client data and personal data to risk and possibly breach. When telecommuting — either full or part time — you must consider things differently than you would when working at the office. Taking some easy steps can make telecommuting the benefit it should be without making it the risk to your firm that it should never be.

THE TELECOMMUTING CONUNDRUM

Telecommuting, or working outside the office, is the new norm for employees who work both in the office and remotely. The ability for an employee to work with ease from wherever he or she is located, is a relatively new phenomenon and has become an expectation of employers and clients.

Our mindset needs to be challenged when working outside the office. A partner in a law firm once told me, “I want to work all the time. My work-life balance is not your issue.” He was right — his work-life balance was not my issue. But being able to bring the mobility and connectivity he needed in line with the information governance and security the firm and its clients required was my responsibility. This new, always-connected-and-able-to-work expectation — coupled with the ease of connectivity — is exciting. However, it also raises concerns.

KEEPING THE WILD WILD WEST AT BAY

There are many great tips for telecommuting effectively and efficiently to stay productive while maintaining proper balance in your life. The steps below, however, will help you do that

work safely, securely and in line with your firm's policies and clients' requirements.

Always follow your firm's sanctioned connectivity processes. There are specific safeguards and steps your firm has provided to connect to firm and client data. Easier does not mean safer. For example, you may feel that sending files to your personal Gmail account so you can pull them up on your iPad is a clever way to get your work done, but it removes the files from the governance rules in place at your firm and makes those files subject to Gmail's terms of service. Have you read those? You may be surprised at what you find.

All devices used for work must be up to date. All laptops, smartphones, tablets, home computers, etc. must be at the proper patch level, have current antivirus and end-point protection, and have the latest security and software updates. New threats constantly attempt to exploit vulnerabilities in the devices and software we use. If you are going to use a device to connect to work, it must meet current standards. The risks go way beyond just your device. Your device could be the inroad to the firm's network.

Only use safe and secure connections. Not all public Wi-Fi connections are safe. Not all home networks are configured safely either:

- **Public Wi-Fi:** If you are sitting at Starbucks, using their public Wi-Fi, make sure you are protecting your information by using virtual private network (VPN) connections on all devices if possible. Even smartphones have VPN options. A VPN creates an encrypted connection for your network traffic and keeps prying eyes from scanning your data. There are even VPN services available for personal use, but for firm or company use, follow your firm's secure connection options. Also, be leery of Wi-Fi options entitled "Free Public Wi-Fi." These are often spurious sites that are attempting to skim your data.
- **Home network:** Add strong protection to your wireless access point and/or gateway given to you by your service provider. Most current home networking gear also allows you to set up a separate "guest" access, which will segregate your guest's network traffic from yours. Set strong passwords on both your network and the guest one. Never leave your home network open (i.e., without security).



Only store data in firm-sanctioned locations. Where you keep your firm and client information matters! Personal- or consumer-grade solutions should not be used for firm data. Personal media (e.g., USB drives), personal online storage accounts (e.g., Dropbox) and personal email accounts (e.g., Gmail) are not acceptable places for firm-related data. If your unencrypted personal USB drive was lost or stolen, could someone get to firm information? With consumer-grade online services like Dropbox and Google, consider whether they meet the information governance and security policies set by your firm. Your ethical obligation to protect firm data extends to any and all ways you connect to that information.

Continually educate yourself on proper procedures and current threats. There are new, clever threats coming out every day. Make it a point to regularly educate yourself on proper procedures and the risks associated with remote connectivity.

I'm a strong believer that mobility and security are not opposing forces. To enjoy the privilege of telecommuting, take simple but important steps to ensure the information you've been entrusted with remains protected and secure. ■

ABOUT THE AUTHOR

Kenny Leckie is a Senior Technology and Change Management Consultant for Traveling Coaches. He works with firms to develop and deploy customized programs with an emphasis on user adoption and increased ROI. He has more than 20 years of combined experience as a Law Firm Trainer, Manager of Support and Training, Chief Information Officer, and now Consultant. He is a Prosci Certified Change Practitioner and a Certified Technical Trainer.



kleckie@travelingcoaches.com



ALA's 2017 Compensation and Benefits Survey

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



Results encompass data for more than 6,000 professionals



Data from more than 1,000 law offices' questionnaires included in the final results



Order your copy of the comprehensive report today!
alanet.org/compsurvey



URI GUTFREUND
National Law Firm Practice Leader
Risk Strategies Company

7 Questions to Find the Right Broker

Having the right insurance brokers can be the most important decision in your firm's insurance programs. The wrong broker can recommend the wrong coverage designs or the wrong companies, as well as cause you to overpay significantly.

“

Peer benchmarking is essential for providing competitive benefits in your marketplace. By understanding where you stand compared to other firms, you can make better coverage decisions.”

Their expertise can assist you with valuable advice so that you have the right coverage and coach you in the process to obtain the lowest premiums and best terms. Just like a real estate lawyer isn't the right lawyer for a private placement offering, your broker must specialize, too.

These are seven questions that you can ask your current broker — or a potential new one — to quickly determine if he or she indeed has the experience and benchmarking knowledge to effectively advise you. We've also given some perspective on the possible answers.

- 1. All Brokers:** *How many law firms like ours (size and specialty) do you represent? Seven to 10 similar firms is a good start. This basic question determines if the brokers “get you.” Will they understand how you work, what you worry about, and internal procedures for getting things done at your firm? This will also be a good indicator of whether they are qualified to opine on the big-picture adequacy of your policies.*
- 2. Professional Liability Broker:** *What are some of your clients' issues on the professional liability application, and what have you done to lower their financial exposure with the structure of their policy? They should have many examples here. The difference between a good professional liability application and a bad one will significantly impact the market results. While any broker can be a conduit to an insurance company, your goal should be to use a professional liability broker who enhances your application so that you obtain the best terms in the market.*

- 3. Professional Liability Broker:** *How many insurance companies do you access for obtaining professional liability insurance?* If your broker uses one or very few companies, you will get skewed market knowledge and are exposed to getting subpar terms. In most states, the markets are very competitive. Using a broker with access to many companies will also save you time later, if you try and compare policies yourself.
- 4. Health Insurance Broker:** *What benefit designs are common for equity partners, contract partners and associates at firms like ours?* Peer benchmarking is essential for providing competitive benefits in your marketplace. By understanding where you stand compared to other firms, you can make better coverage decisions. For example, if your strategy is to provide excellent benefits compared to your competition, what does that mean exactly?
- 5. Benefits Broker:** *How is your understanding of law firm partnership rules impacting your recommendations for the structure of our health insurance, disability insurance and other employee benefits?* These policies must be

customized for law firms for them to be effective in paying a claim down the road. While they don't need be a certified public accountant, you should also ask if they understand the tax rules that apply in the context of these policies.

- 6. Property and Casualty Broker:** *What are the key terms that firm's cyber liability insurance and employment practices liability insurance policy must have?* Your policies must reflect the new structure of law firms (equity, nonequity, of counsels, etc.), have the law firm specific coverages, and have built-in coverages that are unique to law firm exposures in these constantly evolving areas.
- 7. All Brokers:** *What is your claims department like? What is the experience of that group and what is their philosophy on fighting insurance companies?* Your ideal broker will have a dedicated and experienced claims department that is adequately staffed to be responsive to all client needs. They should be involved in all steps of claims processes. Most importantly, they need the skills and unambiguous loyalty to fight insurance companies so that you will get what you deserve in times of a claim. Many brokers say that they will fight insurance companies, but few actually do it. Ask for actual instances and client testimonials where the broker fought for a better result for the insured.

While changing brokers can be a difficult decision due to emotional or business relationships, staying with the wrong broker can be costly and damaging to the financial health of your firm. Using these types of questions can make the broker selection process more efficient and make sure that your firm is with the right insurance broker for your needs. ■

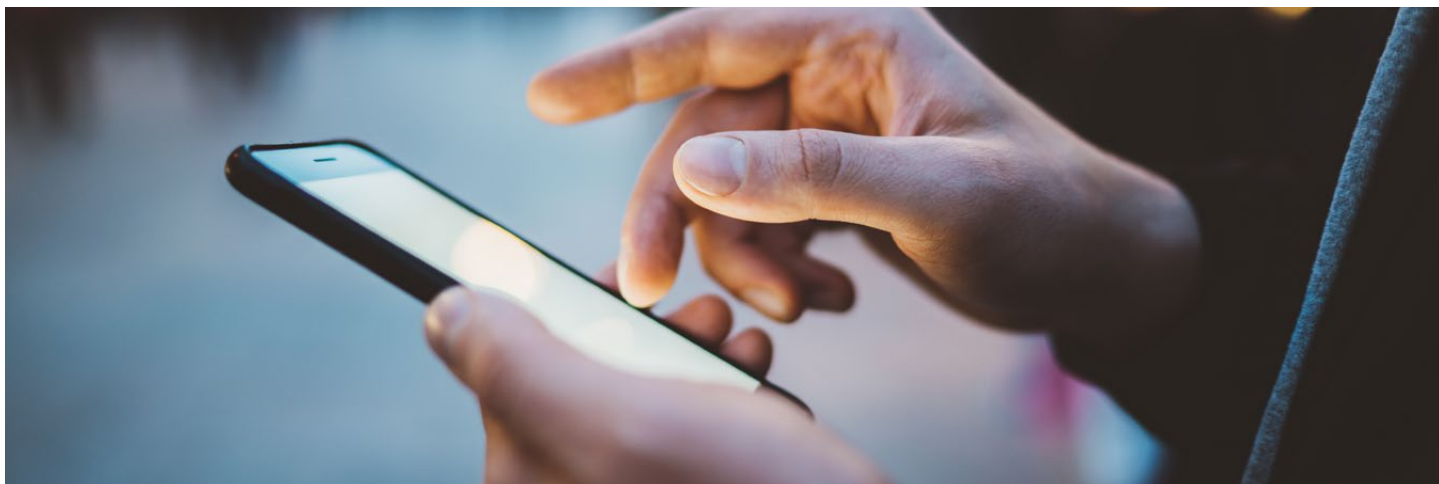


ABOUT THE AUTHOR

Uri Gutfreund is the National Law Firm Practice Leader for Risk Strategies Company, a national top 25 insurance broker. He and his multidisciplinary team advise law firms on all types of insurance and benefits. Gutfreund is a frequent speaker at legal conferences, and a writer and blogger on insurance and risk management.

 ugutfreund@risk-strategies.com

 www.linkedin.com/in/urigutfreund



FLORIAN SCHWIECKER
Leader of Global Sales, Vice
President and Director
Speech Processing Solutions

“

When firms are exploring their mobile and office-based voice technology options, they need to ensure that the functionality is similar to dictation tools attorneys are accustomed to.”

Data Security and Dictation Efficiency Can Go Hand-in-Hand

It is probably no surprise that a 2016 American Bar Association survey found that more than 93 percent of attorneys use smartphones in their practices. What may raise eyebrows is that 73.6 percent of lawyers who participated in the survey report they were using a personally owned smartphone, while only 28.5 percent used a smartphone that the firm owned.

Bring your own device (BYOD) policies raise data security and client confidentiality concerns depending on how attorneys protect their devices. Attorneys use their personal smartphones not only for client-related email and text messages, but also to dictate client letters or confidential memos. A lost or stolen smartphone without the proper security features in the hardware and software means valuable, protected client information could be held hostage by a cybercriminal, damaging the reputation of the client and the firm.

Those types of risks should prompt firms to explore secure mobile dictation technology options and associated BYOD policies. Attorneys and their assistants can then enjoy the productivity of working from any location, as well as the robust security necessary to protect clients' confidential and private information and the firm's reputation.

MOVING TO THE CLOUD

One such security-focused option is migrating more data and systems to the cloud, which is a fast-moving trend for organizations. A survey from the International Legal Technology Association found that 62 percent of law firms were “increasing likelihood of adoption” of cloud-based solutions in 2016, up 11 percentage points from the previous year.

The cloud is proving to be a highly efficient and secure platform for data storage and an important tool for supporting law-firm workflows. Document creation, for example, can be

managed entirely from the cloud. Attorneys can dictate either at the firm, from their smartphone or from a handheld recorder at their home, then transfer the recordings to the cloud. From there, cloud-based dictation workflow management systems offer options for how those documents are created. The most common method is for the attorney's assistant to access and even transcribe the recordings in the cloud. The completed documents are securely stored in cloud for the attorney's review.

Increasingly, attorneys are choosing speech recognition software or using transcription services to create their documents. Some smartphone dictation apps enable users to upload their audio files directly to the cloud to either assign to a transcriptionist or process the completed dictation within the cloud. Using either method, the document is created in a few moments, and the attorney simply needs to review and edit before sending to the client.



SECURITY ON THE GO

Secure cloud options are essential for protecting these recordings and documents. After all, 80 of the 100 largest firms in the United States have been hacked since 2011, and 80 percent of respondents to a legal survey consider cyber/privacy security to be one of their firm's top 10 risks. Careful technology selection and policy concerning permitted software and hardware should be a priority for firms concerned with security.

Here are a few security features to consider when designing the firm's BYOD or mobile device policy:

- **End-to-end encryption:** Dictation recorder apps for smartphones should encrypt dictations in real time using the

advanced encryption standard (AES or Rijndael algorithm) with a key length of 256 bits. Dictation files should be encrypted again when they are sent to the cloud, and again when stored. This end-to-end double encryption is essential for protection from unauthorized access.

- **Server mirroring:** Not only should stored data in the cloud be automatically encrypted, but the cloud platform should also offer server mirroring to keep data reliably secured and accessible to the firm anytime and anywhere.
- **Passcode options:** Fingerprint and numerical passcode options are common on most smartphones to protect your data. Some handheld digital recorders also offer a PIN option to protect against unauthorized use or file playback.

CONVENIENCE TO SUPPORT EFFICIENCY


These mobile devices and apps used for dictation allow attorneys to create documents and save their thoughts from anywhere without taking the time to type them. Although this can increase firm productivity and improve client service, attorneys will not employ these mobile options if the security policies or features make the technology difficult to use.

When firms are exploring their mobile and office-based voice technology options, they need to ensure that the functionality is similar to dictation tools attorneys are accustomed to if they are experienced dictation users. If the attorneys are new to dictation, a simple user interface is important to shorten any learning curve associated with the new technology.

With highly intuitive — but powerful — voice technology and effective security features, law firms can experience the efficiency of mobile-enabled workflows with safeguards to protect client information and the firm's reputation. ■

ABOUT THE AUTHOR

Florian Schwiecker is the Leader of Global Sales, Vice President and Director at Speech Processing Solutions.

 info.na@Speech.com

 www.Speech.com

 twitter.com/fschwiecker



KONICA MINOLTA

All Covered 
IT SERVICES FROM KONICA MINOLTA / LEGAL

THE LAW FIRM OF THE FUTURE. HERE. NOW.

You face pressure to cut costs, increase efficiency and find time-saving solutions. Meanwhile, technology evolves at lightning speed while playing an increasingly significant role in how you must practice law. Konica Minolta's Law Firm of the Future can give you the competitive advantage through:

- Industry-leading advanced technology, solutions & legal applications
- Managed IT tailored for the legal industry
- Information and productivity management tools
- eDiscovery, security and compliance

We understand your challenges and the pace of law firms and are ready to securely lead you into the next era of legal technology.

kmbs.konicaminolta.us/legal



Facts and Stats



THE TOP 10 PASSWORDS

1. 123456
2. password
3. 12345678
4. Qwerty
5. 123456789
6. 12345
7. 123
8. 111111
9. 1234567
10. dragon

Using the top 10 passwords, a hacker could, on average, guess 16 out of 1,000 passwords. Try using (and have your employees use, too) a password manager to set strong passwords. You remember one password — the password manager holds strong, random passwords for all your other accounts.



DID YOU KNOW?

Only **7 percent** of users sign up for two-factor authentication. Without two-factor authentication, if an attacker gets hold of your password, it's game over.



Benefits and Savings – ALA's VIP Program

ALA teamed up with an elite group of trusted partners in business. Through these relationships, ALA members, along with their employers and families, are able to enjoy special benefits and tremendous savings.

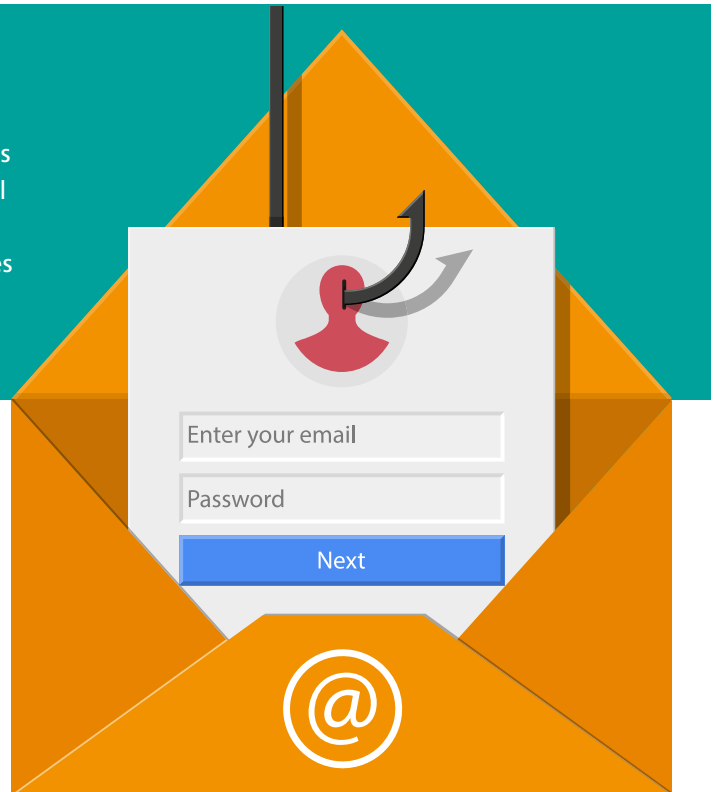
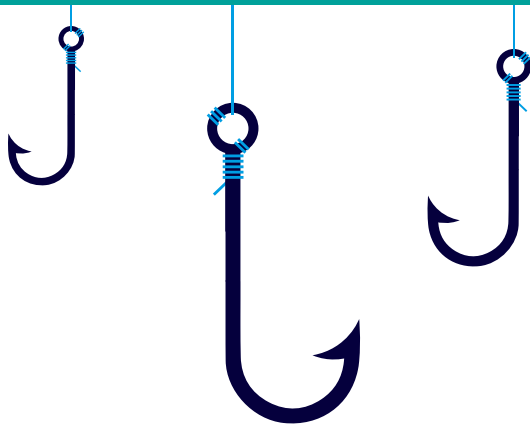
For more information on ALA's VIPSM participating organizations and the services they offer, visit alanet.org/vip or contact ALA's Headquarters at 847-267-1252.

Get the VIP treatment with ALA's
VIP business partners!

▶ alanet.org/vip

EDUCATE ABOUT PHISHING ATTACKS

Avoid phishing by learning to detect signs of suspicious emails — such as incorrect email domains, grammatical errors and requests for sensitive info. A study by JP Morgan found that 20 percent of the bank's employees were duped by a fake phishing email.



PATCH IT UP

Install the latest operating system (OS) patches. Many updates fix bugs in the OS that create security vulnerabilities on both Mac and Windows.

In fact, **80 percent** of all updates to Windows 10 released in 2016 involved security issues.

Source: All data used with permission from Jeff Kerr of CaseFleet. View the complete graphic: www.casefleet.com/blog/law-firm-security-infographic.



6 Tips for Law Firm Cybersecurity

The nature of the data law firms collect makes them an ample target for breaches. Here are security steps to take.



CHRIS HOGAN, CISSP
Certified Forensic Investigator

Cybercrime and data breaches are about as predictable as the winning lottery numbers. And with a shortage of cybersecurity experts to help defend our nation's infrastructure, it basically guarantees there is an unsuspecting law firm that is a target.

Since 2013, more than 9 billion data records have been lost or stolen. While protecting its own systems, national power grids and nuclear plants might be at the forefront of the government's cybersecurity agenda, the cyberthreats are just as real against America's legal system.

Still, it's nearly impossible to be a competitive law firm without the use of technology such as smartphones, cloud-based storage services and video conferencing. What may be great for improving the bottom line can be a nightmare for maintaining an effective level of security for clients. According to cybersecurity firm Mandiant, at least 80 of the largest 100 law firms in the U.S. by revenue have been hacked since 2011.

It's a startling figure and it presents a difficult challenge.

"Cybersecurity is way too much for one person to handle ... sensitive data may reside in many different places; it takes a cybersecurity team to help secure it," says Gina Lopez, a Certified Hacking Forensic Investigator (CHFI) and Senior Cybersecurity Analyst in the health care industry.

"Cybersecurity is way too much for one person to handle ... sensitive data may reside in many different places; it takes a cybersecurity team to help secure it."

TACKLING THE PROBLEM

While security experts may disagree on how to prioritize cybersecurity in a business, there is no wrong answer if your firm has support from leadership to find ways to improve security for the benefit of clients. Here are six tips for firms to consider when looking for ways to improve cybersecurity.

1. Develop a cybersecurity team. Or, at the very least, a cybersecurity mindset. It starts with an overall business security plan that is embedded into the firm's operations. According to research by Jody R. Westby, Chief Executive Officer of Global Cyber Risk LLC, there is a clear need for firms to adopt an enterprise security program. That means bringing in dedicated staff and resources to establish a security framework and take responsibility for protecting the firm's physical and digital assets.

"Skilled personnel are the greatest asset," says Jason Barnes, Senior Consultant at CrowdStrike. "No tool, device or appliance can replicate the effectiveness of a skilled analyst."

For firms with more than 100 attorneys, hiring a team of skilled cybersecurity specialists might be more practical because budgets for security can span multiple departments. In smaller firms, the management staff might be called upon to take a leadership role in helping to secure the business — even if they don't necessarily have a cybersecurity background. This can prove challenging even for firms that consider themselves progressive in their use of technology.

Even if your firm has been successful in implementing a security team, there are only so many issues the team can focus on at one time. Identifying the right security problems to concentrate on is a challenge for any business, but doing something is much better than doing nothing at all.

2. Reduce the complexity of your environment. While nothing can truly be 100 percent secure, an experienced security team will assess an environment and put controls in place to reduce its probability of becoming the next victim of a cybercrime. One of the biggest roadblocks of success is an environment that is overly complex. Over the

years, your law firm may have accumulated technologies that are either obsolete or require a particular level of expertise to maintain. (Such overcomplexity tends to be especially likely in nationwide or global firms.) This puts an unnecessary burden on a security staff that may already be overwhelmed with other responsibilities.

To compensate, firms should be prepared to simplify their environments. "Break it apart logically," suggests Seth Eichenholtz, an e-Discovery Program Manager in the financial services industry. "If it is an overly complex environment but 98 percent of it can be ruled out, then things become more approachable."

There is no set rule that says you cannot start managing the security of your firm in small segments. In fact, a risk-based approach is considered an industry standard best practice. Find out what assets or infrastructure carry the most risk to your business, then begin adopting your cybersecurity strategy around them. For smaller firms, it could be attorney laptops; for larger firms, it may be a web server that hosts a portal for clients.

"Skilled personnel are the greatest asset. No tool, device or appliance can replicate the effectiveness of a skilled analyst."

3. Develop and maintain a dynamic database of technology resources. It is the role of the security team to know about all the technology assets in use at the firm. This isn't an easy task. In fact, as technology changes more quickly and becomes more readily available to attorneys and other firm employees, the task becomes nearly impossible.

"It's very challenging," says Eichenholtz. "It's a constant set of known and unknowns." While the known assets are challenging enough for firms to keep secure, the unknowns can leave a firm without a true understanding of the state of security in their environment.

"There is a wide spectrum of preparedness for cyberattacks in most industries. Most of it consists of the 'it won't happen to us' or 'we've got antivirus, so we're good' attitudes."

Knowing what your assets are is a crucial step in identifying security weaknesses. Whether you track them in a spreadsheet or an asset management application, keeping up with your firm's assets will allow you to prioritize your security efforts.

Third-party service providers or external business partnerships should also be considered when determining which assets may affect your firm's security. While you may not be authorized to make direct changes to the security of those assets, you at least will have the opportunity to document what they are and how they relate to the security of your business.

4. Understand your vendor's cybersecurity posture.

When it comes to the security of a vendor's products, looks can be deceiving — and that's exactly how firms can find themselves at risk. Whether it's a router for your network or a database for your clients, not all vendors create security equally. "It depends on the vendor. One can be more 'on it' than others," says Lopez.

So how do you handle a vendor that doesn't share your security philosophy? Lopez suggests using a new product if a vendor isn't keeping up.

At the end of the day, knowing the security risk a particular product or vendor poses to your firm is an essential part of cybersecurity. "Insist on the best balance of business need and security. Maintain a risk ledger and record every risk acceptance decision," says Barnes. Documenting why a product was chosen and what security risks the product introduces to your environment is a practice that will help your firm become more security conscious when making business decisions that involve technology.

5. **Plan for the worst.** If your firm's cybersecurity is compromised, are you prepared to manage the crisis? "There is a wide spectrum of preparedness for cyberattacks in most industries," says Barnes. "Most of it consists of the 'it won't happen to us' or 'we've got antivirus, so we're good' attitudes."

Firms should take a more aggressive approach when it comes to cyberattack readiness. Eichenholtz suggests internal audits, cyber insurance, multiline business risk assessments, and a thorough understanding of federal and state requirements for breach notifications. Also, simply knowing who you would need to notify in the event of a data breach goes a long way to helping a firm stay ahead of the curve when faced with a cybersecurity crisis.



6. Take control of your data. One of the basic principles of cybersecurity is confidentiality — or protecting data from unauthorized access. But knowing where the data is and how to classify it are some of the biggest problems in business. Law firms collect a lot of information from clients, including financial documents, health data, Social Security numbers and details of specific cases. Knowing that this information hasn't been stolen or viewed by an unauthorized individual can be a daunting task for even the most experienced cybersecurity professional.

And with law firms, data may exist in various places. "Attorneys may walk in and out of a courtroom all day long with both physical and electronic copies of documents containing personally identifiable information for multiple clients. This poses not only a cybersecurity risk, but a physical security risk as well. Firms print a lot more documents than most places — often leaving files laying out. [These files] need to be locked and stored securely when not in use," says Lopez.

While securing hard copies of documents might be straightforward, securing electronic data takes a bit more effort from both the data owner and the data user. Most — if not all — of this information should be classified as highly confidential and have a standard set of security controls in place to protect it.

"Focus on both the very technical issues, but also some simple ones like limiting the ability for users to move data around (USB/external device rights) or ensuring

encryption on all data sent outside the firm's network," says Eichenholtz. While data encryption and restricting user rights are important steps to take in securing confidential data, your firm's security team should continue to evaluate the effectiveness of these controls and adjust as new threats emerge.

Cybersecurity is a shared responsibility for all people who use technology. With the amount of media coverage given to cybercrime, end users can no longer claim ignorance about the risk. Remember, there is no such thing as being 100 percent secure, but a firm can choose to be 100 percent committed to ensuring that cybersecurity is a priority for their business and their clients. ■

ABOUT THE AUTHOR

Chris Hogan, CISSP, is a Certified Forensic Investigator (GCFA and EnCE) and a Director of Security Investigations in the financial services industry. He has more than 20 years of experience in information technology with more than a decade in information security and digital forensics. He is also President of the St. Louis Chapter of the High Technology Crimes and Investigation Association (HTCIA) and serves as Programs Chair for the St. Louis Chapter of CompTIA's Association of Information Technology Professionals (AITP).



chrishogan@unitystl.com





Did You Know?

Fraud and cybersecurity are topics of discussion in ALA's Online Community.

The ALA Secure shared interest group brings members together to alert one another of new schemes, collect resources and recommendations for prevention, and discuss topics such as cybersecurity audits, cyber liability insurance and IT education.

Don't miss your chance to learn methods for combating costly scams and invasions!

Join the conversation! community.alanet.org



Helping Houston

It's been described as a 1-in-1,000-year flood. Hurricane Harvey washed away much in its path. But left behind was a community lifted by generosity and support — and determination to rebuild.



VALERIE A. DANNER
Managing Editor,
Legal Management

ALA member Candace K. Childress, SHRM-CP, has worn many hats over the years as Office Administrator at Blank Rome LLP in Houston. But recently, just like many in the Houston area, she's found herself taking on new roles in the office that she never quite imagined.

The morning of our conversation found her jotting down clothing and shoe sizes for donations. Ten of the 100 employees of Blank Rome's Houston office were directly impacted when Hurricane Harvey wreaked havoc through Southeast Texas — and didn't seem to want to leave. Today, Candace, who also serves as a Region 4 Representative, is heading the effort at the office to round up items for distribution to their affected employees.

As we are talking, she receives an email noting that the Harris County Courthouse can't conduct business until repairs are made: the criminal court's jury assembly room is steeped in 11 feet of water; the elevators aren't fully working in the civil court building. Later that day, the attorneys are holding a meeting, not about the business of law but about the business of rebuilding. They've prepared a PowerPoint presentation that details flood insurance (or lack thereof), how to apply for FEMA assistance, and tips for working with contractors. It also includes information on

“People react to catastrophes in different ways. Be patient with colleagues and continue to support people. When I would get an email or a prayer or a virtual hug, it meant so much — I felt those.”

replacing your driver’s license, birth certificate and other vital documents that may have washed away. Candace notes that some colleagues in Florida have requested the presentation, as they, too, grapple with the cleanup after Hurricane Irma.

It’s both surreal and comforting to Candace. “I’ve watched natural disasters happening, and it’s one thing to look at it on TV and feel so sorry for the people affected — but it’s exponentially worse when you’re living it. You just kick into survival mode,” she says. She didn’t see her husband or one of her sons for two days. Both are with the Houston Police Department and were working 24-hour days to aid in the rescue efforts. She counts herself lucky, though, as her home didn’t sustain flood damage.

All images courtesy of Candace Childress.



Candace Childress of the Houston Chapter snapped this photo of the chip aisle at Walmart. It was a common scene at stores in the area. She said it’s been impossible to find bread, milk, Clorox and plastic gloves.

It’s now been more than a month since Hurricane Harvey devastated Southeast Texas. The amount of water is staggering: *The Washington Post* puts Harvey’s total rainfall at 33 trillion gallons of water after it first made landfall. Jeff Lindner, a Meteorologist with the Harris County Flood Control District, tweeted that 1 trillion gallons of rainfall fell in Harris County

(which includes Houston) over four days. The National Weather Service called the event “unprecedented” and had to add a new color to their maps to represent the rain totals — light purple now reflects areas with 30 inches or more of rainfall. Overhead shots of the region look as if the Mississippi River cut a path through the nation’s fourth largest metropolis.

While the daily coverage has largely disappeared from our newsfeeds, those directly affected still feel the impact. It’s not a process that will be measured in days or even weeks.

But when Mother Nature unleashes her most ferocious efforts, another formidable force is also unleashed — the kindness of human nature.

“That’s been the most fascinating and best thing that’s happened out of this. Everyone is helping everyone,” Candace says. She says everyone at her firm — like so many others in the area — are joining in to assist in the cleanup and recovery. “From top to bottom, everyone is helping. There is no hierarchy.”

EMBRACED BY THE ALA COMMUNITY

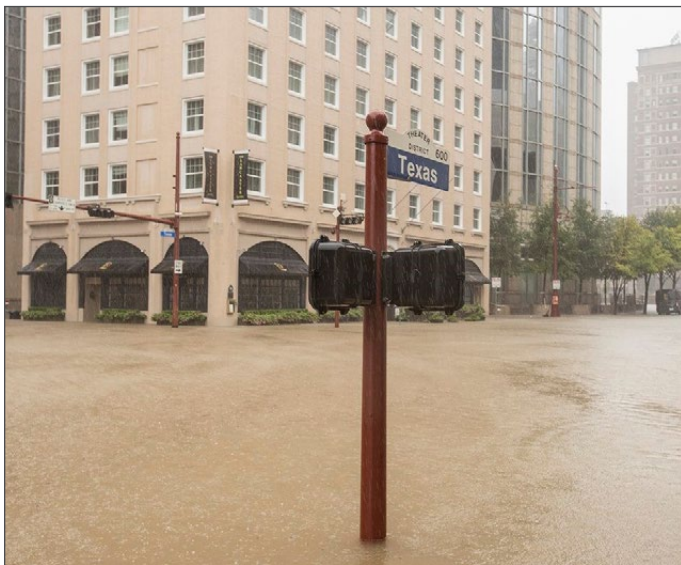
Even before Harvey dissipated and moved out of Texas, ALA members were looking for ways to help.

It happened again with Hurricane Irma. ALA President Gary T. Swisher II, CLM, is Chief Administrative Officer with Clark Partington in Pensacola, Florida. As that hurricane battered his state in September, he received messages from members looking to help. “The efforts our members make to support each other in times like these — it’s one of the things that make me most proud of my ALA membership. We aren’t just there for each other professionally — we want to help when our colleagues face personal challenges, too.”

The support of members looking to help doesn’t surprise Chris J. O’Sullivan, CLM, at all.

“When a big catastrophe happens, people just pull together. The ALA community cares a lot about their members, their law firms and their people; that’s the strength of the ALA,” says Chris, who is the Chief Financial Officer and Firm

“When a big catastrophe happens, people just pull together. The ALA community cares a lot about their members, their law firms and their people; that’s the strength of the ALA.”



An influx of rainwater fills the streets outside the offices of Blank Rome LLP in downtown Houston.

Administrator at Gesmer Updegrave, LLP, and President of the Boston Chapter.

Coincidentally, he was also the Chapter President during Hurricane Katrina and had organized a fundraising challenge in the wake of that storm 12 years ago. Remembering how generous ALA members were then, he knew the same would be true post-Harvey. After discussing it with the Boston Chapter’s Board, they started the same challenge to help Houstonians — each chapter would be encouraged to donate \$5 per member. “For me, what’s been nice about this whole thing is that it’s a good reminder that anyone could have started it. It just has to get going and then people pile on the donations.”

To date, 58 chapters have raised more than \$25,000 to aid the Houston area. (See a complete and regularly updated list of those chapters here: alanet.org/news/2017/09/05/hurricane-relief-brings-together-the-ala-community.) ALA headquarters also donated \$3,500 to the effort.

“It’s been phenomenal,” says Candace. “I can’t tell you how touching it is.”

And it’s not just the donations that have helped. Valerie C. Hayes, PHR, SHRM-CP, the Office and Human Resources Manager with McDermott Will & Emery LLP in Houston and Dallas, says she was touched by the outpouring of messages from ALA members. “I just want to personally thank each and every chapter for keeping Houston in your thoughts and prayers. Many of you also personally checked on me and other Houston Chapter members offering help and support,” says Valerie. “The level of emotional support provided by our ALA friends has been awe-inspiring. We are extremely fortunate to be a part of such an extraordinary group of legal professionals.”

STARTING OVER

If there are any members who have the unfortunate distinction of relating to what Houstonians are going through, it’s those who lived through Hurricane Katrina.

Ray Lightell, CLM, CPA, Chief Operating Officer with Galloway Johnson Tompkins Burr & Smith, APLC, remembers how ALA members from all over were there for them as they began the recovery process.

“You really didn’t know what to do,” he recalls about the early days post-Katrina. He lost his entire house. “To describe it



Boats were the main mode of transportation in rescue efforts. In fact, automotive data firm Black Book estimates it may have ruined up to 1 million vehicles along the Texas Gulf Coast.

"I'm enormously proud of the chapters coming together to do that. The wonderful byproducts of difficult situations are the love, kindness, bravery, courage and gratitude."



Downtown Houston was turned into a river after Harvey.

simply, the life you knew was over — you had to start all over again. You're living in a hotel or motel. The barbershop you went to, the dry cleaners, the grocery store, the Starbucks — all are gone."

Remembering how much ALA members lifted his city up in Katrina's wake, he knew he wanted to get help to Houston members as quickly as possible. When Katrina hit, he recalls how they didn't have immediate access to cash — banks weren't immune to the hurricane's destruction. "People need money in their pockets. They need to know they can go to a store and pay for something and not worry about reaching their credit limit." He knew he wanted to do something a bit different that got money straight into the members' hands as quickly as possible.

So on August 29 — which just so happened to be the 12th anniversary of Katrina — as Ray was driving to work, he decided to start a GoFundMe campaign to help ALA Houston members. He approached the New Orleans Chapter with the idea, and they approved the campaign. As of today, it has amassed \$13,510 in donations. The money was used to purchase gift cards.

Candace says that several ALA Houston members lost everything in the flooding. She says the gift cards from the New Orleans Chapter will be distributed directly to those members.

"What I have been so pleased about is that there's been this enormous pulling together within our Association," says James L. Cornell III, Executive Director at Graves Dougherty Hearon & Moody, PC, in Austin. As Region 4 Director for nearly three years, he knows the Houston members well. "We all talk about one of the things we value most about our ALA membership — the networking and relationships. This is just a wonderful extension into the personal lives of our fellow members. It's other members caring about the impact on people's lives — their ability to earn money and to take care of their families. I'm moved seeing so many people contribute."

FINDING A NEW NORMAL

One thing Ray suggests is to try to establish some semblance of a routine as quickly as possible. That's where work can help. "It's very emotional; people are traumatized, people need a sense of purpose. You don't have a house, but at least you know you can go to the office in the morning. You may not have any clothes, but they'll let you come in with your shorts and flip-flops. One of the better things that happens is going back to work. It's the only normal thing you know. Get back to people you spend time with, some sort of a routine, and continue to help others."

That's where the support from the ALA community is instrumental. After Katrina, Ray's office was able to get up and running within 15 days after the storm, operating in another city using office furniture and equipment donated by ALA members from the Mile High Chapter (Denver).

After her office closed for a week and a half, Candace was relieved when it reopened the Tuesday after Labor Day. A sense of normalcy, however small, was beginning to creep back in.

The first order of business that day was to gather employees and just talk. Some had 9 feet of water in their houses. Some were rescued by boat. And others were feeling a sense of survivor's guilt — grateful that they hadn't suffered much

“You really didn’t know what to do. To describe it simply, the life you knew was over — you had to start all over again.”

damage, but remorseful that their friends were experiencing such anguish when they were largely spared. “Survivor guilt is real and it’s normal,” Candace says.

Right now, Houston is still in the cleanup phase. But each stack of debris being gutted from houses represents pieces of people’s lives. Pieces of the first home they’d saved up to buy. Pictures of their grandparents’ wedding. Priceless keepsakes from the birth of a child. It’s an emotional toll — that place where you take comfort, that nest of security is suddenly gone.

“When you pack up to move, you can go through things, look at them one last time and decide to toss them. In this case, you don’t have that option,” Candace says. She notes one of her friends had to part with a beloved grand piano that the water destroyed. Many are grappling with that now. (Candace says her friend’s husband cut off the pedals from the piano and made it into a shadowbox, so they were able to keep a piece of a cherished possession with them.)

And that seems to sum up the overall outlook there — they are working through this together, determined to rebuild and continue helping — not just each other, but others affected by catastrophes as well. Candace wants to encourage ALA members to remember their fellow members affected by all the recent disasters.

While monetary donations are needed for the foreseeable future to aid in the rebuilding effort, Candace says something just as valuable is needed for the long haul — patience.

“People react to catastrophes in different ways. Be patient with colleagues and continue to support people. When I would get an email or a prayer or a virtual hug, it meant so much — I felt those. It’s not always the tangible things that mean the most; it’s the kindness that comes out from people that mean so much,” Candace says.

James agrees with the sentiment and sees it as another piece that keeps ALA members so closely knit. It’s why he was so pleased to see the organic nature of the Boston Chapter’s challenge. “It was done without prompting or coordination.



Many of Houston’s roads were impassable. It took people who live just 3 miles from Blank Rome LLP 45 to 60 minutes to get to the office.

They just came to help and said here’s what we’re doing and started. I’m blown away by everyone’s generosity and care and enormously proud of the chapters coming together to do that. The wonderful byproducts of difficult situations like this are the love, kindness, bravery, courage and gratitude shown by those involved.”

“It’s what the ALA is all about,” Chris adds. “Sometimes you just need to be reminded of that, that we are one big community. We can not only reach out to a Boston member, but I can reach out to any member. This was just another reminder for me. When one hurts, we all hurt. People were in need, we were able to help in some way and bring light to it.” ■

ABOUT THE AUTHOR

Valerie A. Danner is Managing Editor of *Legal Management*.



vdanner@alanet.org



twitter.com/LegalMgmt

IT'S AN ONGOING EFFORT

Note: This sidebar has information on how you can help those affected by the natural disasters this summer. The web version of this article contains all the links you need to access the lists mentioned below.

The needs in Houston, as well as other areas affected by disaster, will be ongoing for some time.

Due to the high-volume of catastrophic hurricanes this season, the Center for Disaster Philanthropy — who focuses on “investing well, not quickly” — has put together a fund for recovery from the hurricanes.

More specifically, *Houstonia* magazine compiled a list of local charities to help in the coming months, covering everything from food banks to wildlife orphaned by the storm. Global Giving also has set up sites dedicated to helping those devastated by Hurricanes Irma and Maria. Additionally, Nate Hendricks, an ALA member with the Suncoast Chapter, helped start the Puerto Rico Legal Project, a nonprofit law firm that assists lower-income individuals and families on the island. They are currently collecting and delivering aid to some of the hardest hit areas in Puerto Rico. To help their efforts, visit www.prlegalproject.org.

And it's not just hurricanes that are upending lives — Mexico is coping with the aftermath of a devastating earthquake. *The New York Times* compiled a list of ways you can help the ongoing rebuilding efforts there. Additionally, many regions have been hit by wildfires in recent months. The Red Cross has information on how to aid in areas hit hard by these fires. If you are aiming to help a specific region, Googling “wildfire donations + the region” will bring up local charities.

Please remember — before you donate, you can vet many charities using Charity Navigator. Search through nearly 9,000 charities for an unbiased rating to make sure your dollars are being used as you intend.

And checking in with your ALA friends can mean a lot. Let them know that you are still thinking of them, and there to help if they need anything. As Valerie Hayes notes, gestures like that provide comfort and go a long way.

“The outpouring of support from all of you has been overwhelming and we appreciate it more than words could ever express,” she says.



WILL YOUR COMPANY'S BACKGROUND CHECKS LAND YOU HERE?



FAILURE TO COMPLY WITH FEDERAL, STATE AND LOCAL PRIVACY LAWS COULD MAKE YOU A TARGET FOR A LAWSUIT

If your firm conducts pre-employment background investigations, you may be at risk. Over the past few years, employers have been bombarded by lawsuits, based upon violations of federal, state and local laws.

RAI specializes in providing professional service firms with the in-depth background information they need to make informed hiring decisions. Our proprietary compliance platform reduces risk by seamlessly managing all legally required documentation, providing an easy-to-use client and applicant experience.

Contact us at **800-255-9693** to receive a free demonstration of our compliance platform, or visit **[ResearchAssociatesInc.com](https://www.ResearchAssociatesInc.com)** to learn more.

TRUST RAI FOR ALL YOUR INVESTIGATIVE NEEDS



Don't Assume Your Data Isn't at Risk

Data privacy breaches are a growing concern for firms of all sizes. Find out what you need to know to keep information secure.



ERIN BRERETON
Owner, Chicago Journalist Media

Law firms are no stranger to data breaches — nearly half of the firms that technology services provider LogicForce assessed in a recent study had been targeted for potential client data in the past year.

Roughly 40 percent, however, didn't know they'd been breached.

When attackers considered potential targets, LogicForce found firm size and revenue didn't really matter. If hackers can't get information from companies in other industries, law firms that have client data may seem like the next best option, according to LogicForce Chief Information Officer Jordan McQuown.

"Corporations are spending millions on cybersecurity; that's why we're seeing a shift to firms being targeted," McQuown says. "Hackers are going down the food chain to who has the data they want. M&A intellectual property is an easier target."

WHAT'S AT STAKE

In recent years, clients, particularly ones in regulated industries, have begun to pay more attention to how law firms are housing and exchanging information, according to Fernando M. Pinguelo, Partner and Chair of the Cyber Security and Data Protection Group at the 60-attorney East Coast firm Scarinci Hollenbeck.

"You've got insurance policies to protect you from financial penalties, but the biggest concern is the loss of client confidence. Law firms pride themselves on protecting that. You can't put a value on it."

"More and more, we're seeing clients issue questionnaires to verify the vendors they use are protecting data they are obligated to protect themselves," Pinguelo says. "Law firms traditionally fall under that vendor umbrella."

More than a third of firms reported getting a security and systems audit in 2016, according to LogicForce.

Firms that experience a breach can see a number of repercussions. Thirty-seven percent suffered downtime and a loss of billable hours, according to a 2016 ABA survey; 28 percent incurred hefty correction fees.

In addition, if word gets out about a breach, the damage to a firm's reputation could be considerable, says Heather Haughian, Founder and Managing Partner at business law firm Culhane Meadows, whose practice focuses on privacy- and security-related issues.

"You've got insurance policies to protect you from financial penalties, but the biggest concern is the loss of client confidence," Haughian says. "Law firms pride themselves on protecting that. You can't put a value on it."

RISKS FIRMS FACE

Even with safety controls in place, the way employees now work may expose firms to potential breaches, according to Darragh Fitzpatrick, Partner with Tabush Group, a virtual workspace, private cloud and managed IT service provider.

"In the last five years, mobile technologies have opened up the network both in ways companies want and don't necessarily want to happen," Fitzpatrick says. "It's a great way for attorneys and administrative people to be productive, but it opens up all sorts of questions from a security perspective."

Logging in through an unsecure Wi-Fi network when working remotely, for example, could expose data. Employees may unwittingly be the victim of a spear-phishing attack, in which cybercriminals transpose a letter or two to make a phony email address seem legitimate, to lure recipients to log in to a fake system that steals their credentials.

Once criminals have access to the system, they can install malicious software, as three hackers did two years ago to obtain ongoing mergers and acquisition deal updates for insider-trading purposes.

Cybercriminals may also try to trick firm members into making a fraudulent wire transfer by pretending to be a firm official and asking them to deposit funds to a known partner in a new bank account.

"Hackers are going for the path of least resistance; transfers are becoming an easy target," McQuown says. "You send two emails, someone sends \$30,000 and you're done in two minutes, instead of a day of understanding what your firewall is and [figuring out how] to bypass it."

Another type of malware — ransomware — traditionally locks a firm out of its system and holds the network hostage until a fee is paid. In June, global law firm DLA Piper was the victim of a multiple-day ransomware attack.

"They can encrypt it so you can't access it, although we're seeing that changing a little bit," McQuown says. "Rather than encrypting data and firms having the ability to pay to recover it, they're taking a few sensitive files and posting them online as blackmail — saying 'Hey, we're on your network, pay us X amount and we won't expose the rest of it.'"

SAFEGUARDING DATA

To ensure client and firm data is as secure as possible, law firms need to examine how they treat information internally. Technology can reinforce some elements; employees may need to be responsible for others.

The following steps may help correct potential weaknesses:

Put policies into practice. "You find a lot are basically just shelf material," McQuown says. "They're great in practice, but there's no real follow-up or appropriate technical control on how it's executed."

Don't, for example, let some firm members opt out of using the firm email system because they prefer Gmail.

“In the last five years, mobile technologies have opened up the network both in ways companies want and don’t necessarily want to happen.”

“If there are procedures around technology that are burdensome for employees, we’ve seen some come up with ways to work around whatever protections the company thinks it has in place,” Pinguelo says. “Companies need to be mindful of how the policy impacts productivity; it can’t be so restrictive that it does.”

Educate employees about potential threats. “So many data breaches are employee negligence- or error-related — when most could have been avoided with proper training,” Haughian says. “If partners, attorneys and staff are not trained, and it isn’t in the forefront of their minds, all it takes is one person making a mistake.”

Fraudulent wire transfer schemes, for example, typically exploit human — not technological — weaknesses.

“Technology really has nothing to do with preventing a wire transfer breach; good training and best practices do,” Fitzpatrick says. “It’s important to give examples of social engineering to get people educated about being diligent when reviewing who they received an email from.”

Increase password security. Fitzpatrick recommends enacting a policy that supports the use of complex passwords — containing a combination of upper- and lowercase characters, numbers and symbols — and recommends people change their passwords every 90 days.

Using the same password for multiple accounts can also be problematic, according to Haughian.

“If a hacker gets into one system, now they’re in all the systems because you didn’t use a different password for your bank account or home mortgage,” she says. “They can pull all the data.”

Add extra login levels to mobile devices. Haughian suggests securing your phone or other portable devices as you would a computer.

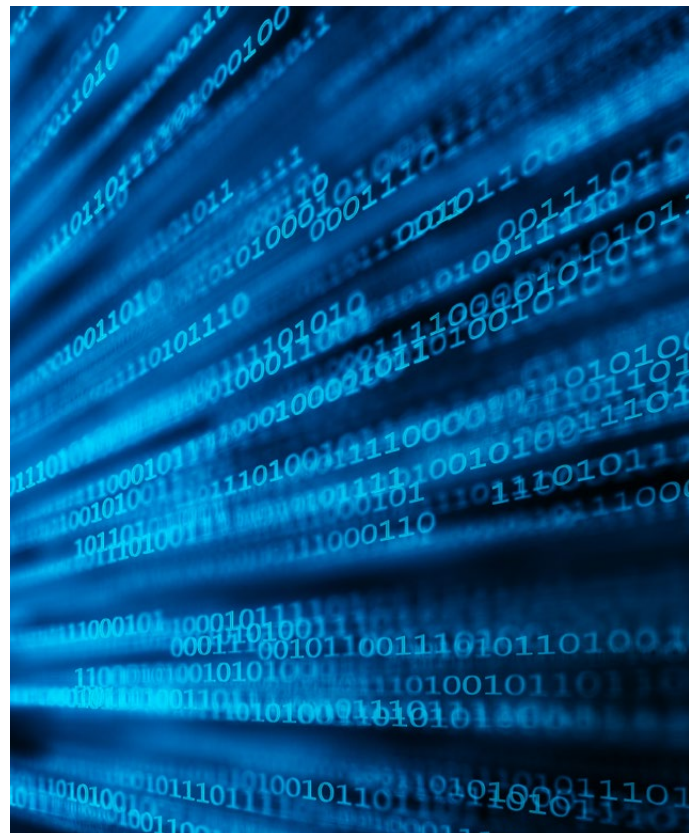
“Your phone really is a small computer; people overlook that,” she says. “Enforce biometric readers; most phones

now have one. Or make sure you have a strong password and passcode. Make sure BYOD [bring your own devices] have antivirus and malware software on them. Require firm members to do upgrades.”

McQuown says firms can also proactively prevent executions in certain directories to safeguard against ransomware attacks.

“Basically, email comes in and goes into a temporary directory — you’re doing malware detection called sandboxing; you put it in a box to see what it will do,” he says. “[You can also use] application whitelisting. A firm may have 30 software packages, but you know what they all are, so you request only those systems can execute on any end-user PC.”

Vary permission levels as much as possible. Firms sometimes view written content as a firm-wide product that should be generally accessible so others can borrow language



“So many data breaches are employee negligence- or error-related — when most could have been avoided with proper training.”

from documents, according to McQuown. However, setting different permission levels can help protect data.

“[Consider giving] only people who need to have access to the data access,” he says, “possibly restricting it to practice areas or some people who work on a project.”

ADOPTING MULTIPLE METHODS

For a more robust protection level, Fitzpatrick says, firms should take a layered approach to security.

“It’s the same way to secure a house: a gate, doors, locks, an alarm system,” he says. “You don’t just put one door with a lock in it; you know someone could break the lock.”

One of those layers should include ensuring your IT infrastructure is being managed properly.

“Cloud services evolved so well in recent years that firms may not always need an IT professional on staff now — however, some firms, particularly smaller ones, don’t really engage correctly with their IT partner,” Fitzpatrick says. “If your IT partner isn’t looking at the data or alerting anybody to potentially malicious activity, it’s opening up the chance the firm has been compromised significantly.”

According to Fitzpatrick, to guard against ransomware and other potential threats, at minimum, firms need to have a system in place that includes internal and external backups — specifically, backing data up on-site and replicating it on-site using a cloud service.

“It’s more of an investment; people sometimes see that as an extra expense,” he says. “But when you’re talking about business continuity and how you make infrastructure function, it’s the safest thing to do. If some of the largest and most secure government entities can be compromised, any business can be.” ■

ABOUT THE AUTHOR

Erin Brereton is a legal industry marketing consultant and freelance journalist who has written about the legal industry, finance, business and other topics for more than 50 legal associations, magazines, websites and other publications.

 breretonerin@gmail.com

 twitter.com/erbrer09

 www.chicagojournalist.com

Get the Education You Need, When You Need It

Planning to become a Certified Legal Manager (CLM)[®]? Need continuing education credits to meet state requirements? Interested in expanding your skill set? Keep up with new trends and build toward a certification with ALA's arsenal of on-demand online education, which comes in several forms including:



Conference Recordings
alanet.org/recordings



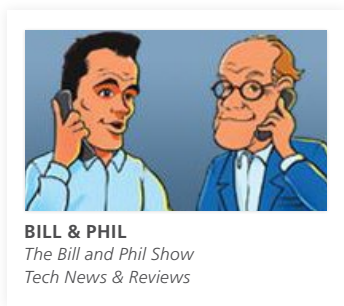
ALA Webinars
alanet.org/webinars



Legal Management CE Courses
alanet.org/legalmgmt



Check out all the available online education opportunities: alanet.org/education/online-learning



Amazon Echo Show Brings a Nice Touch

A couple of years ago, when we first purchased the Amazon Echo, we predicted that Amazon had a hit with this new voice-activated digital assistant and smart speaker. We were not wrong.

“

But the touchscreen interface on the Echo Show is what intrigued us and seduced us into forking over \$230 for yet another Echo device.”

In the past two years Amazon has not only sold millions of Echos but also expanded the Echo device franchise to include the Echo Dot, Amazon Tap, Echo Look and now the Echo Show. If you guessed that we had purchased all of these, you would be correct. Our latest purchase was the Echo Show, which offers the biggest upgrade to date.

The Echo Show's most distinguishing feature is its 7-inch LCD touchscreen. All the previous Echo devices are simply speakers of different sizes and shapes that only take input via voice commands or a linked smartphone app. Of course, the Echo Show is always listening for voice commands just like the other Echo devices, and it features a very good speaker that can fill a room with music or other audio content. But the touchscreen interface on the Echo Show is what intrigued us and seduced us into forking over \$230 for yet another Echo device.

WHAT'S NEW WITH ECHO

After we took the device out of the box, the first thing we noticed is that the Echo Show is not cylindrical like the other Echo devices. It is more of a square and sits nicely on your desktop or countertop with the 7-inch touchscreen aligned atop the speaker base. So why would we want a touchscreen on our smart speaker? For starters, the touchscreen makes the device setup much more user-friendly. We were able to configure our new Echo Show very easily using the touchscreen controls.

Another touted benefit of the Echo Show video screen is the ability to conduct video calls with other Echo Show owners (since the Echo Show also has a built-in camera). Think of this as Amazon's answer to Apple iPhone's popular FaceTime app. As we tested, we found

that it is quite easy to “call” another Echo user (whether they have the Echo Show or some other Echo device). If the other user has Echo Show or the Alexa app on their smartphone, you can video chat hands-free. If the user you are calling just has the screen-less Amazon Echo, you can make a voice call.

We really like this sort of private phone network capability of the Echo ecosystem. If you have family or business associates that you regularly communicate with, and they have an Echo in their home or office, it is very easy to initiate a chat with them by simply issuing a voice command to Echo. The quality of both the audio and video is pretty good.

Other uses for Echo Show’s screen are nice but not necessarily overwhelming. You can play YouTube videos, view Amazon Video content, see weather forecasts, stream music lyrics to your favorite songs, etc. Of course, all this content can be viewed by issuing a voice command — if you can remember what to say. We had to keep our voice command cheat sheet near our Echo Show so we could remember the various commands available.

As with the other Echo devices, we expect that third-party products will begin to create integrations (or skills) that take advantage of the Show’s video screen. For example, while we do not have this integration, we understand there are home

security systems that integrate with Echo Show to allow you to view your home security cams remotely. However, at the time of our testing, there were no dramatic video integrations that we observed besides the video-chat capability.

So while we are generally thrilled with our newest gadget, we tend to only use the Echo Show for the same functions we use our less expensive Amazon Echo, Tap and Dot for. We’re not sure why, but we have found it difficult to find anyone who wants to video chat with us. (Alas, that is not actually an Amazon problem.) So until we get some video-chat partners or we see some really cool video integrations from third-party vendors, we’ll just continue to use our Echo Show as a pretty expensive smart speaker that obeys our every command. ■

ABOUT THE AUTHOR

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

 twitter.com/billandphil



ALA's 2017 Compensation and Benefits Survey

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

-  **Data from more than 1,000 law offices' questionnaires included in the final results**
-  **Results encompass data for more than 6,000 professionals**


Association of Legal Administrators



ORDER YOUR REPORT TODAY!
alanet.org/compsurvey

idea
AWARDS

Innovators Wanted for **ALA's IDEA Awards!**

Submissions are now being accepted for the 5th Annual Innovation, Development, Engagement, and Advancement (IDEA) Awards.

Continually interested in striving for excellence, ALA encourages its membership to develop new practices that deliver great value and transformational impact to the rest of the Association and the legal industry at large. Do you know of a ...

- Member • Chapter • Region • Committee • Firm • Business partner



... that has developed unique or innovative programs, services or events that improve the legal community and advance the legal management profession. If so, ALA wants to recognize them and promote their good works!

Past winners created a millennial-focused YouTube channel, an Adopt-a-Chapter initiative and a program to leverage talented female attorneys to attract valuable female decision-makers as clients. Recipients will be announced at the 2018 Annual Conference & Expo in National Harbor, Maryland.



Enter your submissions! alanet.org/awards
Send questions to awards@alanet.org

Can Your Firm Win the War Against “Wares”?

By Marco Maggio



I speak with ALA chapters throughout the country a few times a month on various technology topics. In the last few years, these conversations have been predominantly about cybersecurity and compliance.

I used to ask the audience if anyone had been victimized by an intrusion. Although I wouldn't get any verbal responses, I would lose eye contact with 10 to 20 percent of the audience every time. When I ask the same question today, it's almost a badge of honor for participants to openly discuss their latest attack — and how quickly their firm was able to recover.

Education is generally the best defense against the current onslaught of nefarious attacks. Let's review some common definitions and actions your firm can take to understand the threat and wage the war against malicious software. The following are abbreviated definitions of common types of malware:

Adware: Typically these advertisements appear in the form of pop-ups, but are commonly coupled with spyware to track browsing behavior.

Bot-nets: Get planted on your PC — and usually on many other computers — then sit and wait for orders from a command-and-control server. They're commonly used in distributed denial of service (DDoS) attacks, in which a number of computers send simultaneous traffic to a single point, thereby overloading it to cause chaos or ultimately a crash.

Keyloggers: Software used to either monitor or capture keystrokes to obtain private data, such as passwords or credit card and banking information. Other malware can act as a keylogger, including viruses, Trojans and even worms.

Malware: Malicious software designed to disrupt your computer's normal functions or to invoke chaos and destruction.

Rootkits: Malicious and stealthy software planted deep down on your computer to avoid being noticed by administrators, users and security programs. The intent of rootkits can be to take control of your computer, adjust system configurations, or remotely access or steal data.

Ransomware: Menacing malware — typically delivered through phishing — that has recently become very popular. It takes control of your data or computer through locking you out of your system or through encryption. It demands a ransom, most commonly in the form of Bitcoin, to regain access to your computer or data.

Spyware: Just as it sounds, spyware is developed to spy on your activity and gather information without you knowing. Sometimes coupled with downloaded software, adware and even Trojans. It can capture keystrokes or simply monitor your online behavior.

Trojans: One of the most notorious pieces of malware, Trojans are traditionally camouflaged as run-of-the-mill software that sneak a package such as a keylogger, a bot or ransomware onto your system. Trojans are notorious as they come in the guise of legitimate software.

Worms: Like a virus, a worm is known for its ability to multiply and spread through networks, sometimes at a very

End-user awareness coupled with preventive measures can serve as a first line of defense in your firm's battles against the "wares."

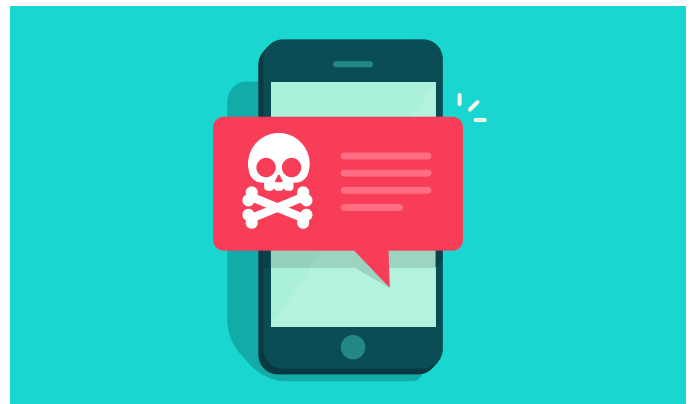
rapid pace. The key difference is that a virus infects files that a user spreads and a worm travels freely across a network, destroying everything in its path.

Viruses: Stealthy software that has an uncanny ability for reproduction. A virus grows by infecting other files and spreading across computers. They can hide on USBs and in many places on a computer. However, their ability to be spread is what makes them so dangerous.

How do you prevent your firm from getting acquainted with one of these troublesome "wares"? While there is no magic bullet to stop them, there are common best practices you can use at your firm to prevent unwanted infections, including:

- Train and educate the end-user to be diligent. Continuous online training is both very effective and practical.
- Educate and test your users on phishing.
- Deploy email spam and antivirus prevention; configure additional phishing protections.
- Patch your systems in a timely manner.
- Install managed antivirus on all workstations and servers to provide automated antivirus definition updates.
- Install managed malware prevention.
- Use DNS filtering for office and remote users.
- Perform monthly internal and external vulnerability scans of your critical systems to identify known technical vulnerabilities on the LAN and public-facing side of your network, respectively. If you aren't performing monthly scans, you should perform an annual project-based scan at minimum.
- Get a firewall with unified threat management (UTM) capabilities; deploy and configure the advanced security features (IDS/IPS, gateway antivirus, gateway antispymware, geoblocking, application control, etc.).
- Back up and verify critical data.

- Enable network traffic analysis and look for anomalies.
- Keep and review device and system logs. For advanced security event monitoring and alerting, explore managed security incident and event management (SIEM) offerings.



End-user awareness coupled with preventive measures can serve as a first line of defense in your firm's battles against the "wares." Although there is no way to truly win the war, you can fight a good fight by employing these reasonable efforts to reduce the risk to your clients and your firm — that way, you can remain focused on the practice of law. ■

ABOUT THE AUTHOR

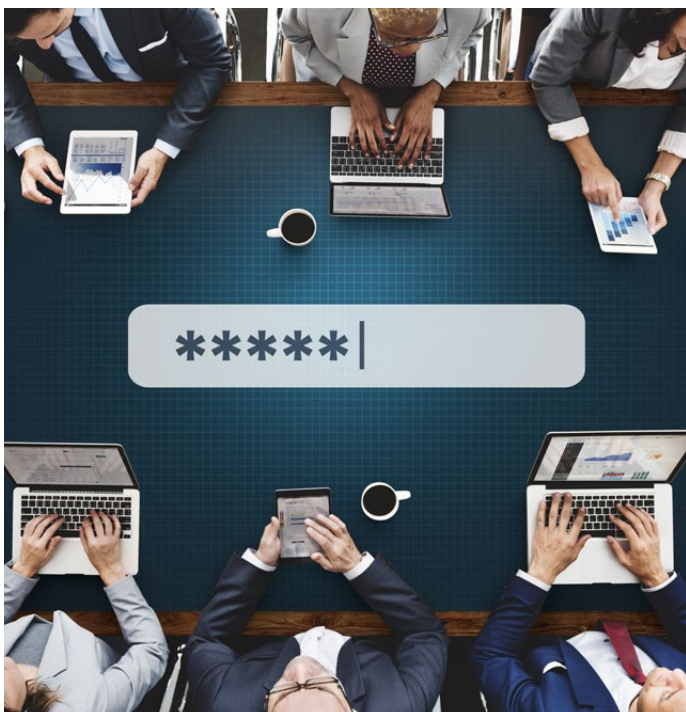


Marco Maggio is the U.S. Legal Practice Director of All Covered's legal practice and is responsible for the strategy, marketing and education of the national legal practice at Konica Minolta. He owns the legal vertical portfolio and holds the vendor relationships for a myriad of legal applications. Maggio also is a regular speaker for industry associations and a regularly published author for technology relevant to the legal industry.

 twitter.com/acmarcomaggio

Corporate Clients Are Zeroing In on Outside Counsel Cybersecurity

By Augustin Cal



More than ever, corporate legal departments across industries are focused on cybersecurity. The almost daily barrage of news stories about data breaches and ransomware attacks has corporate leaders feeling uneasy and compelled to take urgent action to contain risk. Unfortunately, at many companies, the legal function has not kept pace with procurement areas on cybersecurity defense, particularly regarding third parties, such as outside counsel law firms and other legal vendors.

Many corporate legal departments leverage information sharing and automation technologies that increase their operational efficiency and improve collaboration with outside counsel. These partners are frequently engaged for the most sensitive work and given access to confidential information. It's no wonder that events like the Panama Papers release and the WannaCry and Petya ransomware attacks have corporate legal and law firm leaders losing sleep.

CLIENTS AND LAW FIRMS HAVE WORK TO DO

The growing cybersecurity threat has prompted advice from professional corporate and law firm industry associations. The American Bar Association released guidelines to help firms understand and meet their professional responsibilities regarding cybersecurity. Meanwhile, the Association of Corporate Counsel (ACC) issued model security controls with a list of suggested security measures for legal departments to require of their vendors. It's critical to take the advice in these documents on board when establishing a third-party cybersecurity program.

In addition, I suggest that legal departments take the following steps:

- **Take a tiered approach.** Legal teams have limited resources, so risk mitigation efforts should focus on those vendors with the greatest quantity of the most business-critical data.
- **Develop security guidelines.** Base them on current best practices and bring in IT to make sure guidelines are aligned with internal security efforts.
- **Require vendor self-assessments.** Provide a standard template so that all providers address your particular concerns. This process can even alert firms to gaps they previously did not know about.

Both clients and law firms should also:

- **Develop and track action plans.** Based on self-assessments, corporate legal staff and law firms should build corrective and preventive security plans and integrate them into the relationship management process.
- **Develop formal incident response plans.** Having predefined responses ready for the most likely incident types allows for quick reaction when problems occur.
- **Keep up with best practices.** Regularly research evolving accepted practices and update policies and

A good legal cybersecurity solution will allow the client to specify requirements and service providers to show how they meet each requirement.

plans accordingly. For example, the National Institute of Standards and Technology recently updated its Digital Identity Guidelines, which no longer suggest routine password changes and instead recommend forcing password changes only when there is risk that passwords have been compromised.

PUTTING THE PLANS INTO MOTION

Many legal departments have begun a formalized effort to ascertain the security levels of their outside counsel and then address gaps. Most legal departments don't have a dedicated, automated tool to track third-party cybersecurity and often start by leveraging the general administrative tools they already have, using email and spreadsheets to gather and track security information. This is good — I recommend that legal departments quickly establish a formal third-party risk management program because breaches strike without warning.



However, this manual approach has serious limitations in terms of both security and efficiency. Therefore, legal departments should also immediately begin seeking a dedicated tool that automates the tracking of legal service provider cybersecurity. Solutions of this type deliver better value because they are built to support third-party security needs. When evaluating these tools, look for:

- **A central repository for self-assessments:** Email is inherently insecure and often relatively easy to hack. To avoid the vulnerability of email, look for a system with

a secure shared space where law firms and legal service providers can inform the client about their security measures.

- **The ability to track requested and submitted information:** A good legal cybersecurity solution will allow the client to specify requirements and service providers to show how they meet each requirement.
- **Dashboards and reports:** Quick, easy views into each firm's or provider's status are essential. This is useful when conducting security audits, approaching annual law firm reviews, or reporting to senior corporate management on legal department security.

Most importantly, both legal departments and law firms need to be sure that they approach security as an ongoing effort. Cybersecurity needs and technology are constantly evolving, and as a result, third-party security must be addressed as a continuing collaboration between client and firm.

Clear requirements help outside counsel understand how they can meet their clients' specific cybersecurity needs. Most law firms and other service providers are already working hard to improve cybersecurity and are eager to team up with their clients on these critical efforts. ■

ABOUT THE AUTHOR



Augustin Cal is the Product Line Director, Growth Markets at Wolters Kluwer ELM Solutions where he is responsible for determining how ELM Solutions can best serve new markets, defining strategy and executing those plans. He works closely with customers to understand their needs and find ways to help them overcome challenges that are not yet addressed by their existing solutions.

 augustin.cal@wolterskluwer.com

 www.wkelmsolutions.com

Anniversaries, Awards and Appointments

MEMBERS ON THE MOVE >>>>



Elizabeth Lee Davis, CLM



Barbara Fisher



Brian Formagus



Chas Hipp



Jennifer Irish



Kerri Lawrence



Dennis Mapes



John T. Podbielski Jr.



Anne Scott



Shelley Strong

Elizabeth Lee Davis, CLM, member of the Florida Capital Chapter, is now Office Manager at Holland & Knight in Tallahassee, Florida.

Barbara Fisher, member of the Ottawa Chapter, is now Manager, Ottawa Office, at Osler, Hoskin & Harcourt LLP in Ottawa, Ontario.

Brian Formagus, member of the Capital Chapter, is now Director of IP Services at Sughrue Mion PLLC in Washington, D.C.

Chas Hipp, an independent member in Region 4, is now Firm Administrator at Naman, Howell, Smith & Lee, PLLC, in Waco, Texas.

Jennifer Irish, a member of the Maryland Chapter, is now Director of Human Resources at Goodell, DeVries, Leech & Dann, LLP, in Baltimore, Maryland.

Kerri Lawrence, member of the Capital Chapter, is now Chief Financial Officer at Traub Lieberman Straus & Shrewsbury LLP in St. Petersburg, Florida.

Dennis Mapes, an independent member from Region 4, is now Firm Administrator at Ritsema & Lyon PC in Denver, Colorado.

John T. Podbielski Jr., member of the Greater Chicago Chapter, is now Director, Client Account Team, at Hinshaw & Culbertson LLP in Chicago.

Anne Scott, member of the Capital Chapter, is now Deputy General Counsel at Covington & Burling LLP in Washington, D.C.

Shelley Strong, member of the Silicon Valley Chapter, is now Office Administrator at Littler Mendelson PC in San Jose, California.

IN MEMORY

ALA mourns the passing of two members. **Jerome Bello** was an independent member from Region 1. The longtime member recently passed away at the age of 71. Jerry joined ALA in 1987 and remained a member through 2015; he served as a Legal Administrator at Boston law firms, including his most recent workplace, Hartley Michon Robb, LLP.

Kevin Tracey, an independent member from Region 3, recently passed away at the age of 60. Kevin joined ALA in 2005 and had worked at Faegre Baker Daniels LLP in Minneapolis.



HELP US BE YOUR CHEERLEADER!

If you have a recent accomplishment that you'd like to share with other members in *BOLD Bites* or *Legal Management's* "Member Spotlight," send us an email at publications@alanet.org.

CONGRATS ARE IN ORDER

David H. Oxley, CLM, and **Kelly A. Thiemert, CLM** — both members of the Minnesota Chapter — were named two of 2017's Unsung Legal Heroes by *Minnesota Lawyer* magazine. The honor is reserved for the state's most talented and dedicated legal support professionals who consistently go above and beyond in their roles. David serves as Director of Information Technology at Messerli & Kramer PA. Kelly is the Firm Administrator at Hellmuth & Johnson PLLC.

And kudos to **Tanya M. Russell**, a member of the Greater Los Angeles Chapter! She was honored at the Century City Chamber of Commerce's 2017 Women of Achievement Annual Awards Dinner. Tanya is the Director of Office Administration for Katten Muchin Rosenman LLP and serves as a mentor for high schoolers in a corporate work study program at her firm and as a City of Los Angeles-approved visitation monitor.

Jerry Brown, ALA Visionary, Passes Away



Carol Phillips provided this photo from when several ALA Past Presidents gathered. From left to right, front row: Norma Lee, Dodie Stewart; middle row: Elizabeth Kalb, Carol Phillips, Beverlee Johnson, John Moore; back row: Jerry Brown, Nancy Siegel, Douglass Boyd, Donald Akins, Harold Doherty, William Bachman.

In June, ALA lost another one of its early visionaries. Former ALA President (1986–1987) Jerry Brown passed away at the age of 80.

Jerry served on the Board of Directors at a time when the industry was expanding and facing different kinds of challenges than we are experiencing today. Firms were starting to branch out to other locations, notes Nancy J. Siegel, ALA President from 1990 to 1991.

“It was a dynamic time for ALA,” recalls Nancy, who served on the Board with Jerry. “West Coast firms were opening offices on the East Coast; East Coast firms opening offices on the West Coast; Midwest firms opening offices on both coasts. This rapid growth and decentralization of law firms meant new management positions — high-level functional managers and remote office administrators.”

As a result, Nancy says ALA altered the membership criteria to allow this broader group of managers to become voting

members of the association. “Jerry handled this change with his ever open, calm and steady approach to leadership.”

But that was the way Jerry approached life. He had a drive that enabled him to oversee all those changes. He was Director of Finance and Administration at Van Cott, Bagley, Cornwall & McCarthy in Salt Lake City for 31 years. During that time, he worked with others to form the Utah Chapter and served as its first President.

Jerry was the Past President when Carol Phillips, CLM, became President-Elect. She notes Jerry was there to provide support when her 1988–1989 term began a bit sooner than expected. “During the first few months of my term, the ALA President, David Vogels, learned that he had a serious illness that would limit his involvement with ALA. Jerry stepped in to work with David and me, and provided support to David, and at the same time provided me with historical knowledge and advice on handling my new position,” says Carol. “He was an ALA leader in its early years ... working to provide members with educational opportunities to develop their skills and abilities to meet the changing role of the legal administrator.”

Carol — who notes Jerry was foremost a proud family man to his wife and two sons — also saw ALA as an extension of his family. She found a quote from Jerry from 1996, the year ALA turned 25. She says it sums how much the Association meant to him:

“ALA is like a family, where each of us is driven by a sense of something bigger than ourselves, and where contributions of time and talent are given unselfishly for the benefit of the whole.” ■