Contents

COMPUTER AND TECHNOLOGY SECTION

September 28, 2017

Promotion: With Technology and Justice for All CLE on 12/1

Sponsored by the Computer & Technology Section, State Bar of Texas

Friday, December 1, 2017 from 9 a.m. to 2 p.m.

Texas Law Center, 1414 Colorado Street, Austin, TX 78701

Register Online Here or View the Full Program

Cost (Includes electronic materials, continental breakfast and lunch):

$0 – Legal Aid and Texas Opportunity & Justice Incubator Attorneys

$100 – Members of the Computer and Technology Section

$125 – All others**

Overview. Leading practitioners will discuss a wide range of technology-related topics, including laws dealing with technology, security issues and recommendations, issues related to use of social media, latest developments in eDiscovery, tips and tricks to increase efficiency and realize cost savings, and more.

Topics include:

- Welcome and Opening Remarks by Chief Justice Nathan Hecht of the Supreme Court of Texas
- 15 Tech Laws to Protect Your Clients: Cases and Codes for the Courtroom: Shawn Tuma, Lisa Angelo, Pierre Grosdidier (45 Minutes)
- Improving Your Posture: How to Increase the Security of Your Practice and Protect Client Confidentiality: Elizabeth Rogers, David Coker (45 Minutes, 15 Minutes Ethics)

- #NoTweetingAfterMidnight: Ethical Use of Social Media for You and Your Clients: John Browning (30 Minutes, 30 Minutes Ethics)
- On Sale Now: eDiscovery for Low or No Cost: Craig Ball (30 Minutes)
- The Princess Bride: Mobile Lawyering and Using Low Cost Tech for Client Communication: Rick Robertson, Mark Unger (30 Minutes)
- 60 Apps in 60 Minutes: Tips, Tricks, and Technology to Improve Your Practice: Kristen Knauf, Joseph Jacobson, Shannon Warren, Al Harrison (60 Minutes)

Join us the evening before for a reception. Attendees and Section Members are invited to a reception from 5 to 7 p.m. on Thursday, November 30, 2017 at WeWork University Park located at 3300 N. Interstate 35, 7th Floor, Austin, TX 78705. Click to RSVP: evite.me/A59nRZwEwY

This event will sell out! Sign up soon to secure your spot. Approximately 50 seats only are expected to be sold for this exciting CLE. You will earn 4 hours of **CLE credits** while you learn the latest developments in technology and law, plus you get the chance to network with colleagues from around the state.

******Join the section*** *for an annual fee of $25 on your My Bar Page and get all the additional benefits of membership in addition to saving money on this CLE.*

CLE Event Program

With Technology and Justice For All

Sponsored by the Computer and Technology Law Section
Friday December 1, 2017
Texas Law Center, 1414 Colorado Street, Austin, Texas

9:00 Welcome and Opening Remarks
Chief Justice Nathan Hecht
Supreme Court of Texas

9:15 15 Tech Laws to Protect Your Clients: Cases and Codes for the Courtroom
.75 hr (.25 ethics)

Shawn Tuma,
Frisco Scheef & Stone, L.L.P.

Lisa Angelo,
Houston Angelo Law Firm PLLC

Pierre Grosdidier,
Houston Haynes and Boone LLP

10:00 #NoTweetingAfterMidnight: Ethical Use of Social Media for You and Your Clients .5 hr ethics

John Browning,
Rockwall Passman & Jones

10:30 Break

10:45 Improving Your Posture: How to Increase the Security of Your Practice and Protect Client Confidentiality
.75 hr (.25 ethics)

Elizabeth Rogers,
Austin Greenberg Traurig, LLP

David Coker,
Fort Worth Coker & Associates

11:30 On Sale Now: eDiscovery For Low to No Cost .5 hr

Craig Ball,
New Orleans Craig D. Ball, P.C.

12:00 Lunch provided

12:15 Luncheon Presentation:

The Princess Bride: Mobile Lawyering and Using Low Cost Tech for Client Communication .5 hr

Rick Robertson,
Plano Koons Fuller, P.C

Mark Unger,
San Antonio The Unger Law Firm PC

12:45 Break

1:00 60 Apps in 60 Minutes: Tips, Tricks, and Technology to Improve Your Practice 1 hr

Kristen Knauf,
Dallas Infogroup

Joseph Jacobson,
Dallas Law Offices of Joseph Jacobson

Shannon Warren,
Houston Law Office of Shannon Warren, PLLC

Al Harrison,
Houston Harrison Law Office PC

2:00 Adjourn

MCLE Course # 928013796
This course has been approved for 4 hours of continuing legal education, including 1 hour of ethics credit

With Technology and Justice For All

December 1, 2017 | 9 a.m. – 2 p.m.
Texas Law Center | 1414 Colorado Street, Austin, Texas 78701

☐ $100 Section Member
☐ $125 Non Section Member
☐ $0 Legal Aid Providers or Justice Incubators

Join the section for an annual fee of $25 on your My Bar Page and get all the additional benefits of membership in addition to saving money on this CLE.

Name:_____
Address:_____
City, State, Zip:_____
Telephone:_____
Bar Number:_____
Email:_____

TO REGISTER ONLINE, visit: https://statebaroftexasections.redpodium.com/with-technology-and-justice-for-all

Make checks payable to Computer and Technology Law Section.
Please return completed form and payment to:
Rhonda.bridges@texasbar.com or
State Bar of Texas
Attn Rhonda Bridges – Sections Accountant
P.O. Box 12487 Austin,
Texas 78711

Parking

There is no parking available at the Texas Law Center. The nearest public parking is the **Moody Bank Building Parking Garage** at 400 W. 15th Street. The entrance to the garage is at 16th and Guadalupe streets. Telephone number is 512-320-8900. Parking is approximately $15 per day. Handicap parking is available at the Texas Law Center on a first-come, first serve basis. Please notify Security upon arrival that you need to use the handicap parking.

Special Accommodations:

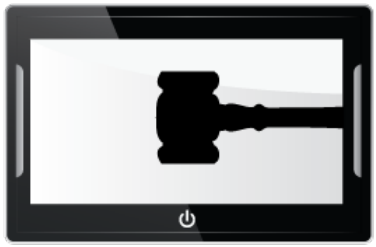
Please email sections@texasbar.com or call 512.427.1420 if you need accommodations for a disability, and we will do our best to assist you.

Refund Information:

If you register and are unable to attend, full refunds will be provided for requests received on or before November 24, 2017. After that date, you will be e-mailed a copy of the course materials and no refund will be available. To request a refund, please contact Rhonda Bridges at the State Bar of Texas Section Accounting Department by phone at (512) 427-1428 or by email at rhonda.bridges@texasbar.com.

Materials:

Bring your wireless electronic device! Materials will be made available to registrants on a secure webpage prior to, and during the CLE conference.



COMPUTER AND TECHNOLOGY SECTION

Letter from the Chair

By Michael Curran

Thank you for being a member of the Computer & Technology Section! We appreciate your support, and we have exciting updates to share with you in this issue of *Circuits*.

1. We are holding a new legal tech CLE. On December 1, the Section is sponsoring With Technology and Justice for All. This CLE will focus on legal tech issues relevant to all Texas attorneys including data security, social media, law office technology, and more! Section members can enroll at a discount. As usual, we will also be co-sponsoring the Adaptable Lawyer CLE Track during the State Bar of Texas Annual Meeting next June.

2. The Section is hosting a membership reception the evening of November 30, the night before the legal tech CLE. The reception will be held from 5 PM to 7 PM at the Texas Opportunity & Justice Incubator offices, which is located in the hipster co-working space WeWork near the University of Texas campus.

3. Another benefit started last year under Chair Shannon Warren is the Section's free online video tips. Many thanks to Michael Peck for directing the TechBytes initiative.

The Computer & Technology Section welcomed four new council members this past summer: Kristen Knauf and Rick Robertson of Dallas; Lisa Angelo of Houston; and, Eddie Block of Austin. All four new council members are working to improve the Section during their three year terms, and it is my pleasure to introduce Kristen Knauf as the new editor of our ***Circuits*** newsletter!

We hope that our many Section members who were impacted by Hurricane Harvey are recovering. Some of the Section's past Chairs and council members were amongst the hundreds of Texas lawyers who were displaced from their homes and offices. The Section made a monetary contribution to Lone Star Legal Aid after their technology and offices were destroyed in the storm, and we have spoken with leadership of the Bar regarding legal technology assistance needs during other potential recovery initiatives.

Again, thank you for being part of the Computer & Technology Section. We hope to see you at the upcoming CLE and reception, and we look forward to sharing legal technology insights that you may find valuable throughout the year. I can be reached at michaelcurranpc@gmail.com with any questions or suggestions that you may have.

Letter from the Editor

By Kristen Knauf

The cooler weather is not the only thing sending shivers down our spines here at the Computer & Technology Section. It is becoming more difficult to turn on the news and not hear about another data breach or cyber-attack. Cyber criminals are becoming more sophisticated, and protecting your firm's security has never been more important. In this issue of *Circuits*, we reflect on the ever-increasing importance of protecting your client's data:

- Al Harrison and Joseph Jacobson discuss the role of engagement agreements in securing client data, and ethical obligations that you may not have previously considered.
- Craig Ball focuses on the overlooked consequences of failing to protect your firm from hackers and data thieves: Are you ready to be denied discovery because your firm isn't "Cybersecure"?
- Lisa Angelo provides a practical overview of cyber insurance, including provisions to consider adding to your policy.

More information on all things computer and technology, including additional cybersecurity resources, can be found on the State Bar's technology resources page. Check out our award-winning TechBytes series: short videos on a wide variety of technology-related topics. You will also find tips, courses, information from TexasBarCLE, and current and past technology columns featured in the *Texas Bar Journal*.

As always, we encourage you to help us make *Circuits* the best publication that it can be by contributing your own articles and/or providing feedback and suggestions to Kristen Knauf at Kristen.knauf@infogroup.com.

Clarifying Cloud Computing

By Al Harrison and Joseph Jacobson

In contemporary law practice, the phenomenon known as "cloud computing" is virtually unavoidable. As evidenced by the prevalent practice among lawyers of relying on such web-based infrastructure as Google Gmail and Google Drive, Yahoo!, Microsoft Outlook, and such popular social media websites as Facebook, Twitter, and LinkedIn, practitioners should appreciate that cloud computing has become integral to the practice of law. Accordingly, attorneys must comprehend the ramifications of engaging in cloud computing while simultaneously complying with the applicable ABA Model Rules of Professional Conduct for safeguarding the privacy and security of client proprietary information.

Cloud Computing

What is meant by "cloud computing"? And, indeed, what is the "cloud"? As its name implies, the cloud corresponds to an amorphous, far-reaching aggregation of geographically dispersed hardware and software resources designed to be remotely accessed on an on-demand basis. All cloud use means that implicated hardware, software, and data are out of attorneys' immediate physical control. Whenever attorneys invoke the Internet, the underlying infrastructure manifests itself as a huge collection of file servers, massively networked myriad computers and storage devices, and operational software applications devolve to a seemingly omnipresent cloud.

Engaging in cloud computing does not necessarily require reliance on the Internet at large but can involve limited aggregations of resources in the form of different cloud formations. For instance, a "private cloud" affords the benefit of an exclusive intranet of limited scope and, importantly, having only limited authorized access to its built-in resources. Such a private intranet may be accessed by authorized personnel within a particular brick-and-mortar physical location, such as lawyers or support staff accessing a law firm's private intranet; or it may be accessed remotely, similar to accessing the Internet, but, of course, only by authorized personnel. Other examples of private clouds on a fee or subscription basis are offered by third-party providers such as Uptime Practice (uptimepractice.com) and Online Tech (onlinetech.com). Private clouds such as these are geared to a sole user, such as a small law firm or a sole practitioner, and all the infrastructure is dedicated to this user; security and compliance issues are rigorously controlled throughout the upload, storage, and download phases.

In contrast, a "public cloud" affords the benefit of a freely available intranet provided as a service to customers or clients, but such service is provided neither solely to a single law firm nor to the public at large. Such public clouds allocate and share hardware resources among several users (e.g., many law firms, many sole practitioners, and myriad other users from diverse fields). Privacy, security, and compliance issues are addressed, but the implementation varies with the service provider and pricing tier. These public clouds are owned by third-party providers like Amazon Web Services (aws.amazon.com), Google Drive (cloud.google.com), Dropbox (dropbox.com), and Microsoft OneDrive (onedrive.live.com).

Yet another cloud platform is a "hybrid cloud," which is composed of a combination of private clouds and public clouds that link together rather than merge their respective resources. That is, each of these private and public cloud formations retains its separate and distinct infrastructure while nevertheless offering users extended resources online.

Regardless of which cloud computing platform is invoked, it should be obvious that relying on a cloud is the antithesis of invoking local law office hard drives and other storage devices and initiating applications only from software stored locally.

Ethically Engaging the Cloud

Whatever the nature of their cloud use, attorneys have a profound professional responsibility to safeguard the integrity and confidentiality of client data. As any business, a law firm must comply with applicable state, federal, and international statutes, regulations, and treaties that govern data privacy—augmented, of course, by applicable rules of professional responsibility. We will explore in greater depth the particulars of attorney cloud computing conduct, including participation in social media activities, in a series of articles to appear online in the *GPSolo eReport* (americanbar.org/publications/gpsolo_ereport). Please join us to keep abreast of the latest cloud computing trends and potential impact upon your attorney-client relationships and ongoing professional responsibilities.

Al Harrison is a patent attorney, concentrating on oil and gas and software and practicing intellectual property law in Houston, Texas. He is chair of the GPSolo Division's Resource Center Committee and a senior advisor to the Book Publishing Board. He is chair of the Data Privacy and Security Committee of the Business Law Section and a past chair of the Computer and Technology Section of the State Bar of Texas; serves on the Advertising Review and the Professionalism Committees; and is a board member of the Texas Bar College.

Joseph Jacobson is a transactional attorney practicing various aspects of business law and commercial real estate. He has represented businesses having operations in Europe and Asia. He was a board member of the Japan American Society of Dallas and a founder of the e-Commerce Committee of the Dallas Bar Association. He was an adjunct professor at Southern Methodist University Dedman Law School. He is vice-chair of the Data Privacy and

Security Committee of the Business Law Section and a past chair of the Computer and Technology Section of the State Bar of Texas.

Are You Ready to be Denied Discovery Because Your Firm isn't Cybersecure?

By Craig Ball

Cybersecurity and personal privacy are real and compelling concerns. Whether we know it or not, virtually everyone has been victimized by a data breach. Law firms are especially tempting targets to hackers because, they hold petabytes of sensitive and confidential data. Lawyers bear this heady responsibility despite being far behind the curve of information technology and arrogant in dismissing their need to be more technically astute. Cloaked in privilege and the arcana of law, litigators in private practice have proven obstinate when it comes to adapting discovery practice to changing times and threats, rendering them easy prey for hackers and data thieves.

Corporate legal and risk management departments better appreciate the operational, regulatory and reputational risks posed by lackluster cybersecurity. Big companies have been burned to the point that, when names of giants like Sony, Target or Anthem are publicly discussed, people might think "data breach" before "electronics," "retail," or "health care." The largest corporations operate worldwide and, as such, are subject to stricter data privacy laws. In the United States, we assume if a company owns the system, it owns the data. Not so abroad, where people have a right to dictate how and when their personal information is shared.

Headlines have forced corporate clients to clean up their acts respecting data protection, and they have begun dragging their lawyers along, demanding that outside counsel do more than pay lip service to protecting, *e.g.*, personally-identifiable information (PII), protected health information (PHI), privileged information and, above all, information lending support to those who would sue the company for malfeasance or regulators who would impose fines or penalties.

Corporate clients are making outside counsel undergo security audits and requiring their internal legal team members to institute operational and technical measures to protect company confidential information. These measures include encryption in transit, encryption at rest, access controls, extensive physical security, incident response capabilities, cyber liability insurance, industry (*i.e.*, ISO) certifications and compulsory breach reporting. For examples of emerging "standards," look at the Model Information Protection and Security Controls for

Outside Counsel Possessing Company Confidential Information recently promulgated by the Association of Corporate Counsel.

Forcing outside counsel to harden their data bulwarks is important and overdue; but, it is also disruptive and costly. Many small firms will find it more difficult to compete with legal behemoths. Savvier small firms, nimbler in their ability to embrace cybersecurity, will frame it as a market differentiator. At the end of the day, firms big and small must up their game in terms of protecting sensitive data.

Enhanced cybersecurity is a rising tide that lifts all boats.

Well, maybe not *all* boats. Let me share who is likely to get swamped by this rising tide: requesting parties (or, as corporations call them "*plaintiffs' lawyers*"), and their *experts* and *litigation support providers*. Requesting parties and others in the same boat will find themselves grossly unprepared to supply the rigorous cybersecurity and privacy protection made a condition of e-discovery.

Again, *cybersecurity and personal privacy are real and compelling concerns*, but these security concerns will also be used tactically to deflect and defer discovery. They will serve as hurdles and pitfalls tending to make plaintiffs' lawyers think twice before pursuing meritorious cases. If you have not run into this, you soon will, and your instinct may be to resist. Don't.

Fighting to be cavalier about data security is a battle that requesting parties cannot win and should not fight. Requesting parties must instead be ready to put genuine protections in place and articulate them when challenged.

I know some will say, "all we have to do is sign a protective order." What they do not see is the trap set by executing protective orders without the ability (and sometimes without the intention) to meet the obligations of the order. High profile gaffes will follow, and the failure of a few will be the undoing of many.

A protective order is not the answer if it is an empty promise. Requesting parties cannot agree to employ stringent data protection and then go about business as usual: e-mailing confidential data, storing it on unencrypted media and failing to ensure that all who receive confidential data from counsel handle it with requisite caution.

Here is an example of how it could go down for a firm with an inadequate cybersecurity framework:

1. Producing parties will demand protective orders imposing stringent-but-appropriate data protection practices and breach reporting requirements.
2. Requesting parties will sign these orders because—let's be frank—requesting parties will agree to almost anything if they believe it will get them "the smoking gun." Plus, how do you persuade a judge that she shouldn't issue a protective order when all the other side wants are sensible measures like access controls, encryption and breach reporting to protect sensitive data and PII?
3. Requesting parties will treat information produced in discovery with the same care they bring to their own confidential information, which is to say, not much and less than that protective orders typically require.
4. Confidential data will be mishandled, probably with so little actual prejudice as to prompt requesting counsel to ignore the breach reporting obligation in the order, reasoning "no harm, no foul."
5. The breach will ultimately come to light, opening counsel's mishandling of produced data to scrutiny and prompting discovery-about-discovery. The failure to set up secure systems, establish policies, train employees, test and audit processes and require contractors and experts to do the same will be gleefully dissected in court.
6. The producing party will beat its chest in lamentations of irreparable harm. The legal press will have a field day. The judge will be wrathful. The requesting party's counsel will look like a clown and might lose his ability to serve on plaintiffs' steering committees.
7. Producing parties will ceaselessly argue the now-proven hazard of e-disclosure, and requesting parties everywhere will be tarred with the same brush, challenged to prove they aren't going to be the next ugly breach. Judges will be less willing to grant full and fair discovery and more willing to impose arduous conditions for access.

A cynical and dystopian prediction? Perhaps. But it is t's already happening now.

The way to keep this in check is for requesting parties to act now to prepare to receive and protect confidential data sought in discovery.

Requesting parties cannot expect to be held to a lesser standard of cybersecurity than the producing parties compelled to surrender confidential data to them. A grizzled trial lawyer once warned me, "*Defendants are forgiven several lies. Plaintiffs get none.*" So, a party can be incautious with its own data because it is theirs; but attorneys who fail to protect an opposing

party's confidential data will be harshly judged. They do not just hurt their clients and opponents; they undermine the very foundations of discovery.

So, what must counsel for requesting parties do? Here are a dozen suggestions:

1. Take cybersecurity duties seriously. This is not someone else's job: it is your job. You are the gatekeeper. This is Rule One, not by accident.
2. Don't just treat an opponent's confidential data with the care you afford your own; treat it better. It's like money in your trust account. You don't treat client monies/data like your own. You don't commingle client monies/data with yours, and you don't use that money/data for anything but permissible purposes with careful recordkeeping.
3. If there is a protective order, read it closely and be sure that you fully understand what it requires you to do in terms of the day-to-day conduct of any who access confidential information.
4. A proper chain of custody is essential. You must be ready to establish who received confidential data and the justification for its disclosure. You must be able to prove you had a good faith basis to believe that the person receiving confidential data understood the need to protect the data and possessed the resources, training and skill to do so. This obligation encompasses anyone who gets the data from you, including experts, clerical staff, associated counsel and service providers. Anyone with access to confidential data must be well-prepared to protect the data because their failure is your failure.
5. Proceed with caution when disclosing confidential data to experts. Industry experts serve multiple masters and may seek to exploit confidential data obtained in one matter in other engagements. Secure the expert's written commitment not to do so, and enforce it. As well, don't supply confidential data to an expert without first obtaining the expert's consent to receive and protect it. People who appreciate the burden of protecting other people's sensitive data want to hold as little of it as possible.
6. Recognize that you don't get to decide what data warrants protection. The designation rules. If you think something isn't properly designated as confidential or sensitive, challenge the designation; but, until the other side concedes or the Court rules, the designation sets the duty.
7. Confidential data should be encrypted in transit and at rest. This means that none of the confidential data gets attached to an e-mail, moved to portable media (*e.g.*, a thumb drive or a portable hard drive) or uploaded to the cloud *unless it is encrypted*.

No exceptions. No excuses. By the way, if you store or transmit the decryption keys alongside the encrypted data, it does not count as encrypted.

8. Perimeter protection is not enough. The biggest risks to confidential data are internal threats, that is, from craven or careless members of your own team. Trust but verify. Access to confidential data should be afforded only on an as-needed/when-needed basis.
9. Access to confidential data must be monitored and logged. Remote access and after-hours access should be audited. Safeguard the other side's confidential data in much the same manner as banks protect the contents of safety deposit boxes: There is adequate physical security (walls, doors, alarm systems and guards) and monitoring of the perimeter (cameras and key cards). There is a vault to keep all contents safe when the perimeter is breached, and access controls to make contents available only to authorized persons (dual-keyed boxes and ID/signature scrutiny). Data protection also incorporates elements of perimeter security (limiting physical access to the devices and systems), monitoring (logging and auditing), a vault (strong encryption with sound key management) and access controls (two- factor log in credentials and electronic access controls).
10. Have a written data security and incident response policy and protocol in place and *conform your practice to it*. Be sure all employees with access to sensitive and confidential data agree to be bound by the policy and train everyone in leading industry cybersecurity practices. You must first recognize a risk to be prepared to meet it. "No one told me to do that" is not the testimony you want to hear when your staff take the stand.
11. Be wary of oppressive obligations to destroy or "return" data after a case concludes. Confidential case data tends to seep into mail servers, litigation databases, document management tools and backup systems. Are you prepared to shut down your firm's e-mail and destroy its backup media because you failed to consider what an obligation to eradicate data would really entail? Have you budgeted for the cost of eradication and certification when the case concludes?
12. As an alternative, consider cloud-based storage and review tools that integrate encryption, two-factor authentication and access logging. The cloud's key advantage lies in a user's ability to shift many of the physical and operational burdens of cybersecurity to a third-party. It's not a complete solution, but it serves to put a secure environment for confidential data within reach of firms of all sizes.

If this sounds like a big, costly pain, then you have been paying attention. It is a headache. It slows you down, and the risks grow and change as fast as the technology. But if requesting parties do not put adequate protections in place on their own, courts will allow producing parties to dictate what hoops requesting parties must jump through to obtain discovery–if, indeed, courts do not deem the risk so disproportionate that they deny access altogether.

E-discovery is hard enough. Don't make it harder by giving opponents the ability to claim you can't be trusted to protect their information.

Checklist for Cyber Insurance

By Lisa Angelo

This article is for those considering purchasing their own cyber insurance policy, advising clients about cyber insurance, or working on behalf of the insurer. This article presents a checklist to help facilitate a more positive transaction that will hopefully result in more accurate coverage.

What is cyber insurance?

You have heard about "cyber breaches" and "cyber-attacks.". The ongoing theme is that companies use technology to conduct business, and are therefore vulnerable to having their data compromised. The effects of these cyber events are expensive and long-lasting. Cyber insurance policies purport to offset some of these expenses and offer aid to the targeted companies. The evolving nature of the cyber-attacks and the technical terminology complicate these types of policies.

Consider that we are continuously developing new technology. With new technology also comes new vulnerabilities to discover, exploit, and hopefully patch. This process is on a loop that makes it difficult to precisely capture the essence of cyber risks for the purpose of underwriting insurance policies, let alone selecting adequate coverage.

What follows are two checklists that may be handy when considering the purchase of cyber insurance.

CHECKLIST 1: The Basics

Before you embark on your cyber insurance shopping spree, it is helpful to evaluate your company's security needs, and possibly beef-up some of the more obvious and easily remedied vulnerabilities. The following is a checklist of basic security measures every company can benefit from incorporating.

- ☐ **Password Protected Devices**
- ☐ **Multi-Factor Authentication**
- ☐ **Encryption**
- ☐ **Firewall**
- ☐ **Anti-Virus**
- ☐ **Backups**
- ☐ **Updated Software**

☐ **User Training Program**

The user training program referenced in the checklist above is commonly referred to as an employee training program, but it is more appropriately labeled as a "user" training program because all users of technology can benefit from training. Employees are not the only group requiring training. Training programs should be part of continuing education and updated in accordance with new technology, new vulnerabilities, new laws and regulations, and the general technical landscape of the company (*i.e.* changes to infrastructure).

Topics to cover in a training program might include:

- appropriate use of social media;
- education about cyberattacks;
- how to identify and avoid phishing attacks;
- how to identify suspicious activity on the computer;
- steps for reacting to suspicious activity (what to do, who to call);
- proper passwords;
- tips for responsible internet use;
- securing mobile devices.

CHECKLIST 2: Provisions to Consider Including in Your Policy

☐ **Definitions**

Definitions are particularly important because the policies include technical terms and while the terms might be used loosely in day to day life, they have very specific meanings in any insurance policy. For instance, it is extremely important to understand what events constitute a breach. Must a breach stem from the act of an outsider breaking in, or may a breach also include the act of an employee clicking on phishing email? Are these scenarios different?

☐ **Notice Requirement**

Understand what triggers the insured's duty to notify the carrier of a claim, and when notice must be given. It is not always intuitive. For example, the policy could require notice at the time of the breach or at the time of discovery of the breach. Of course, you will also need to understand the meaning of "breach" to know when to provide notice. Missing this deadline could be fatal to your coverage.

☐ **Currency**

It is common for cyberattacks such as a ransomware attack to demand payment in

cryptocurrency like Bitcoin. The first question is, are you expected to pay the ransom? There are different opinions as to whether the ransom should be paid. Second, do you have coverage for the ransom? Third, does your policy make payments in various types of currency that include crypto-currency? Fourth, does the policy reference a process for obtaining crypto-currency? Unlike a typical money-exchange, cryptocurrency could take a long time to gather. Compared to other types of insurance, this may seem like a strange consideration. However, it drives home the point that innovative technology complicates these insurance products.

- ☐ **Wait Period**

  If your policy includes a waiting period before there is coverage, consider what it might look like to cease all business for that duration of time. Could your business comfortably survive five hours of five days? It is important to understand the ramifications of a wait period on your business. Perhaps it is a policy provision you can afford to be flexible with or else need to tighten up.

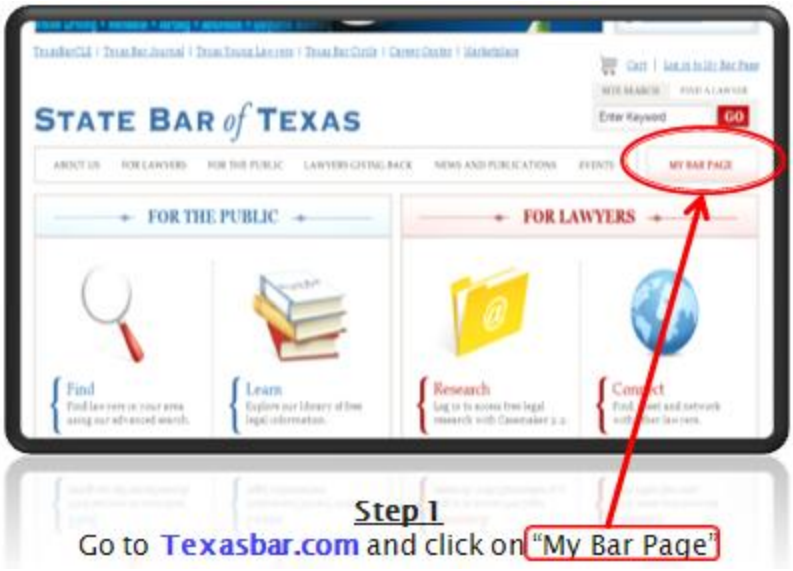
- ☐ **Breach Response Plan**

  If you have a detailed breach response plan, does the insurance policy create any conflicts? For instance, the policy might identify the forensics team or lawyer you must use in the event of a covered breach. Consider if this complies with your current breach response plan or if you need to update your plan accordingly, assuming you approve those identified in the policy.

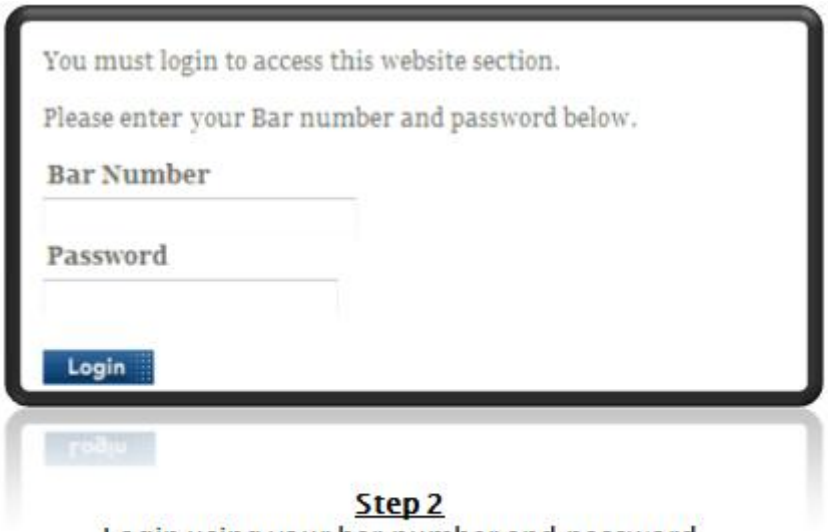
While these checklists are far from being comprehensive guides, they are a great way to get the wheels turning when thinking about what might be the right cyber insurance coverage. Consider expanding these checklists to include additional items that address industry regulations and company procedures. Remember that there is no one-size-fits-all when it comes to cyber policies. This also might mean that there is more room for negotiation and you will want to be prepared.

How to Join the State Bar of Texas Computer & Technology Section

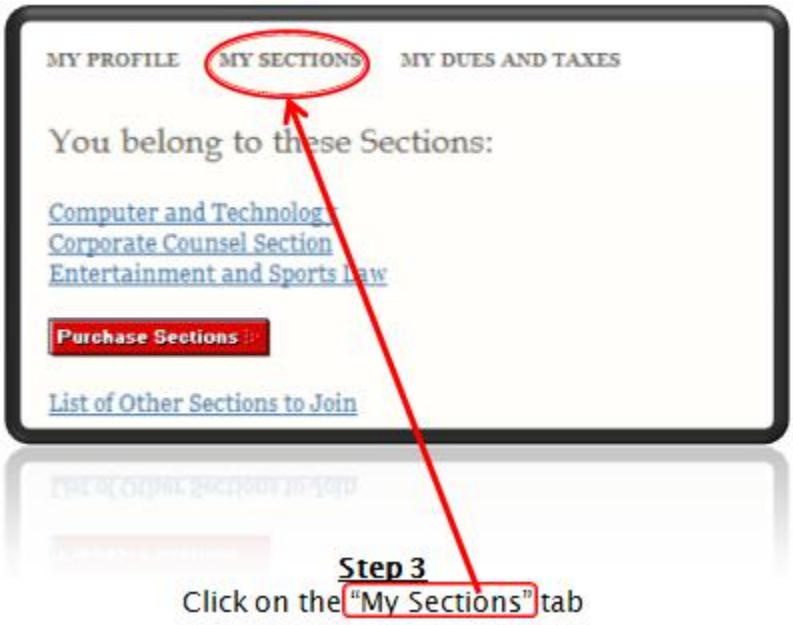
Joining the State Bar of Texas Computer & Technology Section is easy. You can join online by visiting the State Bar of Texas Website at www.Texasbar.com. Please follow these instructions to join the Computer & Technology Section online.



Step 1
Go to Texasbar.com and click on "My Bar Page"



Step 2
Login using your bar number and password
(this will be the same information you'll use to login to the Section website)



If you see "Computer and Technology", congratulations, you're already a member.

If not, click the "Purchase Sections" button and follow the instructions to add the Computer and Technology Section. **Please note: It may take several days for the State Bar to process your section membership and update our system.**

You can also complete this form and mail or fax it in.

State Bar of Texas Computer & Technology Section Council

Officers

Michael Curran – Austin – Chair
Sammy Ford IV – Houston – Chair-Elect
John Browning – Dallas – Treasurer
Shawn Tuma – Dallas – Secretary
Shannon Warren – Houston – Past Chair

Term Expiring 2018

Pierre Grosdidier – Houston
David Coker – Dallas
Laura Leonetti – Houston
Reginald Hirsch – Houston

Webmaster

Elizabeth Rogers– Austin

Term Expiring 2019

Sanjeev Kumar– Austin
Judge Xavier Rodriguez– San Antonio
Judge Scott J. Becker– McKinney
Eric Griffin– Dallas

Term Expiring 2020

Kristen Knauf – Dallas
Lisa Angelo – Houston
Rick Robertson – Plano
Eddie Block– Austin

Chairs of the Computer & Technology Section

2017-2018: Michael Curran
2016-2017: Shannon Warren
2015-2016: Craig Ball
2014-2015: Joseph Jacobson
2013-2014: Antony P. Ng
2012-2013: Thomas Jason Smith
2011-2012: Ralph H. Brock
2010-2011: Grant Matthew Scheiner
2009-2010: Josiah Q. Hamilton
2008-2009: Ronald Lyle Chichester
2007-2008: Mark Ilan Unger
2006-2007: Michael David Peck
2005-2006: Robert A. Ray
2004-2005: James E. Hambleton
2003-2004: Jason Scott Coomer
2002-2003: Curt B. Henderson
2001-2002: Clint Foster Sare
2000-2001: Lisa Lynn Meyerhoff
1999-2000: Patrick D. Mahoney
1998-1999: Tamara L. Kurtz
1997-1998: William L. Lafuze
1996-1997: William Bates Roberts
1995-1996: Al Harrison
1994-1995: Herbert J. Hammond
1993-1994: Robert D. Kimball
1992-1993: Raymond T. Nimmer
1991-1992: Peter S. Vogel
1990-1991: Peter S. Vogel