KEY TAKEAWAYS
FROM THE
CYBERSECURITY THOUGHT LEADERSHIP CONFERENCE
OF THE
TECHNOLOGY AND THE LEGAL PROFESSION COMMITTEE
OF THE
NEW YORK STATE BAR ASSOCIATION

February 3, 2020

Opinions expressed are those of the Committee preparing these Key Takeaways and do not represent those of the New York State Bar Association unless and until the report has been adopted by the Association's House of Delegates or Executive Committee.

TECHNOLOGY AND THE LEGAL PROFESSION COMMITTEE

CO-CHAIRS

Mark A. Berman
Ganfer Shore Leeds & Zauderer LLP

Gail L. Gottehrer
Law Office of Gail Gottehrer LLC

COMMITTEE MEMBERS

Seth Agata
Mark A. Berman
Alison Arden Besunder
Shoshanah V. Bewlay
John D. Cook
Hon. Fern A. Fisher
Parth N. Chowlera
Tracee E. Davis
Sarah E. Gold
Gail L. Gottehrer
Maura R. Grossman
Ronald J. Hedges
Shawndra Jones
James B. Kobak, Jr.
Glenn Lau-Kee
Ronald C. Minkoff
David P. Miranda
Mauricio F. Paez
Marian C. Rice
Kevin F. Ryan
Prof. Roy D. Simon
Sanford Strenger
Ronald P. Younkins

CYBERSECURITY THOUGHT LEADERSHIP MEETING ATTENDEES AND CONTRIBUTORS

Seth Agata
Christina Ayiotis
Karim Beldjilali
Eric Burke
Patrick Burke
Sasha Carbone
Sarah Cole
Todd Daubert
Ariel Evans
Emma Greenwood
David Horrigan
Laurie Kamaiko
Mary Kavaney
Erez Lieberman
Dr. Andrea Matwyshyn
Michael Mooney
Mauricio Paez
Fernando Pinguelo
Debbie Reynolds
Marc Roman
Elizabeth Roper
Jay Shapiro

LAW SCHOOL VOLUNTEERS

Nicole Cardascia
Aishwarya Minochia

JUDICIAL REVIEWERS

Hon. Timothy Driscoll
U.S. Magistrate Judge James C. Francis IV (ret.)
Hon. Saliann Scarpulla

SPECIAL THANKS TO

Dentons US LLP
Ronald J. Hedges
Todd Daubert
Salvatore Imperati
Molly Watson

TABLE OF CONTENTS

Page

INTRODUCTION FROM THE CO-CHAIRS

Given the rash of ransomware attacks on, and phishing attacks directed at, lawyers and law firms in recent years, the Technology and the Legal Profession Committee deemed it appropriate to look for a new way to provide concise, practical, understandable cybersecurity resources to NYSBA members. The Committee sought to reach two groups in particular: (1) solo practitioners and attorneys practicing in small law firms who do not have the assistance of the specialized IT departments found at larger law firms, and (2) law students and new lawyers, who may be comfortable with technology but unaware of the ethical issues associated with it. It is the Committee's hope that by familiarizing them with the importance of cybersecurity to their practice of law, and demonstrating NYSBA's focus on issues that are relevant to law students and new lawyers, we can encourage them to become active members of NYSBA.

Recognizing that many attorneys may not be attending cybersecurity-focused CLE programs, the Committee decided to experiment with a new, non-traditional approach to legal education. We invited cybersecurity professionals with expertise in the cybersecurity issues affecting the legal community to participate in a thought leadership conference at the offices of Dentons US LLP in New York City. The thought leaders were divided into groups, with each group focusing on a topic of critical importance. The members of each group worked together to identify the key points on their topic that attorneys need to know and to provide tips for attorneys on that cybersecurity issue. Each group presented their work to all the attendees, who provided additional feedback.

The document that follows is the result of this collaboration of cybersecurity thought leaders. The *Key Takeaways* from the collective work of our thought leaders are set forth in five sections, each consisting of bullet pointed lists. It is concise and easy to read, and at the same time, packed with relevant information about incident response, ransomware, risk management, corporate disclosures, and cyber insurance. We chose this non-traditional format, rather than a formal report with paragraphs and case citations, in order both to increase the chances of busy attorneys and law students reading it and to make the document readable in one sitting. We are confident that after reading the *Key Takeaways*, attorneys and law students will be better able to have conversations with cybersecurity vendors, insurance providers, and clients about cybersecurity issues, and to take steps to improve their cybersecurity defenses and ensure that they are complying with their ethical duties. It is meant to be a living document that will be updated regularly to help NYSBA up to date as cybersecurity threats evolve and new challenges emerge.

The Committee thanks the Cybersecurity Thought Leaders, whose names are listed on the preceding page, for volunteering their time and talent, and sharing their considerable knowledge and experience. We also thank Dentons US LLP, including Ronald J. Hedges, Todd Daubert, Salvatore Imperati, and Molly Watson, for hosting the Cybersecurity Thought Leadership Conference and for their continued support of NYSBA and the Technology and the Legal Profession Committee.

Section 1
Incident Response

A minimal level of cybersecurity competence requires practitioners to understand basic cyber risk management concepts, and industry standard approaches to managing this risk. The basic elements include (i) cyber threat literacy; (ii) pre-incident planning; (iii) incident response; and (iv) iteration.

- Cyber Threat Literacy:
    - Refers to understanding the cyber risks that legal practitioners face, such as financial fraud through phishing, ransomware, cloud denial of service, remote computing hacking, data theft, and inadvertent data breaches, among other things.
    - Requires an understanding of who the bad actors are; what their mode of operations that contributes to cyber incidents experienced by legal practitioners is; what their motives and common methods for orchestrating attacks are; what types of information are at risk; how information is compromised; and/or how financial fraud takes place.
    - Also relevant is understanding the technology resources used by the practitioner that could either facilitate these attacks or make them more likely to succeed.
- Pre-Incident Planning:
    - Requires the adoption of best practices for developing a cyber-incident response and compliance program covering all major areas of the legal practice.
    - At its core, pre-incident planning requires that the practitioner take a proactive approach to planning for incident response, which includes defining technical and administrative response and investigation protocols, communications protocols, external resource engagements, internal ownership, client notice obligations, and a containment/reinstatement approach.
    - This needs to be done prior to the incident, and should be based on reasonable crisis management approaches and techniques.
    - Another important key element is incident response training for all lawyers and staff. It is essential that the law firms are cyber secure so that the cyber risk to a firm is not passed on to a client.
- Incident Response Plan:
    - Requires formal written guidelines and steps for investigating, responding, and reporting cyber incidents.

- Should take into consideration the ethical obligation of the practitioner, while ensuring an effective and efficient response to the incident.
    - This includes effective coordination with third party service providers, particularly if the incident originated with the third party.
    - Contracts with third parties should address notification issues, as well as the forensic collection of evidence and the respective insurance coverages.
- Incident response plans should be consistent with industry best practices and standards, taking into consideration the size of the practice. *See, e.g.*, National Institute of Standards and Technology (NIST) Special Publication 800-61, Revision No. 2 (Computer Security Incident Handling Guide), at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.
- A well written response plan directs an attorney or law firm in how to:
    - contain the incident;
    - safeguard evidence;
    - engage third party support (*e.g.*, forensics);
    - identify and comply with the relevant state and federal data breach notification laws;
    - consider notification to relevant law enforcement agencies to coordinate data breach notification procedures with any potential criminal investigations;
    - estimate the number of affected individuals and determine notification obligations;
    - notify any relevant insurance carrier to determine scope of possible coverage, services available and any consent requirements;
    - keep appropriate written records of the investigation steps and findings; and
    - maintain diligence on basic cyber hygiene
        - use strong passwords
        - backup systems regularly
        - only install application that are necessary for the job function
        - update/upgrade systems and application regularly

        - educate users quarterly or annually on info security policy and incident response plan, and
        - restrict users' access and privileges.
    - **Practice pointer**: Be sure to have at least one printed copy of your incident response plan and for it to be in a safe place should your office be inaccessible and/or your computer systems compromised.

- Iteration:
    - Refers to having an adaptive and dynamic cyber incident response approach.
        - As the firm's technology evolves, so will the risk profile.
        - Also, bad actors constantly change their tactics, approaches and tools, so response plans need to consider the evolving cyber threat landscape.
    - This requires that the response approach be reviewed and updated as necessary to reflect these changes. This is particularly true after an incident. The legal practitioner should adjust the plan based on "lessons learned" from responding to the incident (as well as the results of any root cause analysis performed).

Section 2
Ransomware

- Ransomware has become one of the most significant threats to lawyers and the data they possess. It is one of the most lucrative methods of extortion on the Internet. Here's an example of one method used to deliver the infection:

    - An email is received, indicating that you need to review a web link that is relevant to something you're actively working on. Since hackers often study their targets in advance, they can craft quite convincing emails. The email may seem like it originated inside your organization, usually from another staff member.

    - You open the link and connect to a site that performs basic interrogation of your web browser, looking for known vulnerabilities. The site leverages one of these vulnerabilities to push a copy of the ransomware package to your machine.

    - The ransomware silently loads in the background, identifying local and networked hard drives that are attached to your device. It often replicates itself to other locations, enabling it to reload when your machine restarts.

    - The ransomware may leverage tools within the operating system to limit your recovery options, deleting prior copies of data (shadow copies) that may be of value.

    - Tasks are spawned that begin the encryption process. Many of these tasks start by inspecting network-connected drives, knowing they're often a more significant source of value than what's stored directly on your machine.

    - The keys used to encrypt the data are delivered over the Internet to a command and control server using multiple layers of obfuscation to prevent you from identifying its location.

    - Depending upon the variant of ransomware, data may be exfiltrated, the contents of which are evaluated to determine the value of what was encrypted. A countdown timer starts, and should you choose not to pay the ransom, the encryption keys on the server are deleted once that timer expires.

    - **Practice Pointer**: Having an offsite backup of your data is the only sure way for a business to recover from a ransomware attack.

- How do I protect myself and my organization?
    - ***Non-technical considerations***
        - **Awareness and Education**
            - Education is one of the most critical factors in protecting yourself from an attack. Hackers prey on many aspects of human nature; our desire to help others and to respond quickly in times of trouble. The emails may try to convey a level of urgency or sensitivity, sparking these hard-to-control, subconscious responses.
        - By educating yourself and your staff about the risks, you will learn to spend more time reviewing and less time reacting to likely threats. Commercially available security awareness tools should be utilized to simulate real threats, identifying those at a higher risk of clicking through suspicious links or attachments.
            - Note that email is ***not*** the only method of delivery.
            - Any site can link (knowingly or unknowingly) to malicious content. Minimizing access to "high-risk" sites is a good strategy toward protecting your data.
            - However, attorneys are often tasked with research which requires access to sites that others can more easily avoid. In this case, it's essential to use separate, isolated and locked-down machines for this research.
            - For those more traditional use cases, simple Domain Name System (DNS) protection services like Quad9, Cisco Umbrella (OpenDNS), Webroot DNS, and others provide excellent content filtering to block unwanted content and help keep you away from bad sites that could lead to a malicious attack.
        - **Make people accountable**
            - Make sure that people know they're personally on the hook for maintaining a high level of security consciousness. Requiring your staff to sign their names in acceptance of a security policy tends to hold more weight than a casual or even regular discussion about security awareness.
            - Knowing you're the potential source of a ransomware infection or a data breach can be embarrassing. Many will keep it to themselves, avoiding the issue until it's too late. Time is of the essence, and quick reporting is essential. Your policy should clearly define how someone should react to such a threat. Perhaps

in a larger organization, they call the IT department as the first step. But what next? Do they leave the machine powered on? Disconnect it from the network? Should they notify their boss? Clients? Colleagues? The authorities? Having a plan in advance eliminates a lot of the confusion and stigma associated with a security event.

- **Know what you have**
    - Many organizations don't know what the impact of an attack is; they don't have a clear understanding of what applications and data they hold in the first place.
    - It's difficult to prove you are keeping information confidential when you don't know where all of it is. It is especially important when you use third parties to perform business functions. In larger organizations, this can be improved through thorough and frequent documentation. If you're forced to rebuild a system from scratch, can you easily replicate the settings from before the attack? Are your most business-critical data easily identifiable so that they can be recovered or made accessible more easily?
    - You'll often find that restoring from backups is your only recourse. If that's the path you're forced to take, would your IT staff or partner know where to start, including which applications have dependencies on one another?
- **Implement an incident response plan**
    - As discussed in Section 1, no matter how large or small your organization is, a response plan is critical in helping you to make the right decisions at a time where you're working under substantial duress.
- **Carry the appropriate insurance**
    - As discussed in Section 5, cyber insurance is an important tool for protecting against the significant losses likely to be encountered during a ransomware attack, and providing access to service providers needed to respond to such incidents, such as forensic consultants.
    - Not only will you incur costs related to the recovery effort, but data may also be lost which impacts clients or other outside organizations. You may have to prove that data was not exfiltrated during the attack, incurring significant fees for technologists specializing in forensic data loss investigations. If you discover that data has been stolen, you may be required to

issue a breach notification. You may incur data replacement costs and business interruption losses.

- Many of these costs are not covered by general liability or professional liability policies, but coverage can often be obtained through appropriate cyber insurance.

- ***Technical Considerations***
    - **Have the right tools in place beforehand**
        - There are many steps you can take to limit your exposure from a technology perspective. Some of these straddle the line between technical and non-technical, the first of which is employing the principle of least privilege (PoLP). PoLP suggests that you never log in with a level of security above what's necessary to do your job.
        - By default, most Windows machines assign full administrator rights to the first account created on the device.
          This behavior presents an extremely high risk, as anything executed (in this case, a malicious payload) runs with the same level of access rights. Once run, the ransomware has unfettered access to all of your most critical data. Removing administrative rights from your regular, daily login account is a crucial step.
        - Another critical step is the collection of logs from all possible sources, literally every device in your network.
        - Firewall and network switch logs can help to show when an attack started or, better yet, can provide insight into attempted attacks before they succeed. Server logs can show failed login attempts, helping your IT staff identify which account(s) may be compromised. These logs should be sent to a location that is isolated from your environment.
        - There are several cloud services designed solely around the collection of logs and the identification of potential threats (Papertrail, Loggly, Splunk & Graylog are examples).
    - **Create a data intake procedure**
        - You're always going to need to share data amongst clients and colleagues. Many users never think twice about plugging a USB storage device into their computer or inserting a CD/DVD into their computer, especially when it's handed to them by a person they trust.

        - The process of bringing data into the organization should occur on an isolated, intermediary workstation. The data should be scanned for malware, migrated to the isolated machine, then transferred into production through a separate, trusted storage device. The copied data must then be removed from the intermediate workstation, eliminating any risk of future exfiltration should it become compromised.

    - **Eliminate low-hanging fruit opportunities**

        - Exploiting known vulnerabilities is how many of these attacks occur in the first place. Keeping all aspects of your environment up-to-date (patching) is a fundamental step toward preventing a ransomware infection. Holding on to outdated operating systems or platforms is extremely risky. Attackers are always looking for ways to bypass a system's inherent protections. When a vendor stops providing security patches for these platforms, the likelihood of compromise increases significantly over time.

        - In addition to patching, a layered defense strategy also helps to mitigate your risk.

            - Ensure that a properly equipped firewall protects the edge of your network. Use a "Next Generation" firewall and implement advanced features such as "encrypted traffic inspection." Nearly 75% of all internet traffic is encrypted, meaning that the firewall never sees threats contained within that traffic. Inspecting encrypted traffic enables the firewall to intercept the session, decrypt and inspect it, then forward it on to the intended recipient.

        - Deploying a reputable anti-virus/anti-malware application may seem like an obvious requirement, but many fail to renew their annual maintenance for these products.

            - In the past, organizations would rely on a vendor who provided updated virus definitions for the life of the product. The threat landscape changes so often that this no longer provides sufficient protection. The product itself will usually be found to have known vulnerabilities over time, requiring that it be upgraded in its entirety.

    - **The end-all, be-all requirement…**

        - The likelihood of being compromised, despite all of the efforts put forth, is still high. There is a never-ending battle between the good guys and the bad guys. Unfortunately, the good guys are often a

step behind the bad. In cases where ransomware takes hold, the only option for recovery (other than paying the ransom, which comes with an entirely separate set of risks), is to restore the data from a recent backup.

- The backups themselves are the target of ransomware encryption, with many newer threats seeking out known backup file formats to prevent recovery.
    - Backups should be stored in a way that protects them from compromise, with at least three full copies of the data in separate locations.
    - You may see references to the "3-2-1" backup model recommended by US-CERT (three copies, two on-premise in different formats and one offsite), or even the "3-1-2" model (three copies, one on-premise backup and two copies in isolated cloud locations).
    - The point is to make sure you have multiple copies of your backup data in various places.
- Consider moving files from a traditional fileserver or local machine to a cloud-based file storage repository like Microsoft Sharepoint/OneDrive, Google Drive, Box, etc.
    - Pick a platform that has built-in recovery and rollback options as files encrypted locally can be inadvertently replicated over the data in the cloud.
    - Large cloud vendors offer levels of protection that are prohibitively expensive to deploy on your own.

- **This all sounds expensive!**
    - There are great options available for a relatively low cost. The GCA Cybersecurity Toolkit (toolkit@globalcyberalliance.org) contains a list of tools that can help with the inventory process (knowing what you have), patch management, email protection, DNS filtering, Antivirus, and backup. It also provides guidance on strong authentication (not explicitly related to ransomware, but another "must-have" for protecting your credentials and limiting your exposure early on). Finally, it contains information related to better securing your email communications with others through the proper implementation of industry standards such as SPF and DMARC (Sender Policy Framework and Domain-based Message Authentication, Reporting & Conformance, respectively).

- You can expect to spend more on the firewall and backup platforms (relative to the size of your organization).
    - Many companies now offer advanced “firewall as a service” options, providing next-generation firewalls for a monthly fixed fee. A quick Google search using those terms should help you to identify someone in your area.
    - We suggest staying away from retail “big-box” and “office supply” stores when it comes to firewalls and network switch purchases. While they may carry one or two “prosumer” class devices, the majority of them do not possess the advanced features needed to provide adequate levels of protection.
- For the technically advanced, open-source products may be layered together to provide a robust security foundation. The downside of these products is that they often require manual configuration of the more advanced features, something that commercial vendors expose through simple checkbox-style configuration screens.
- On a related note, you’ll find that several commercial backup vendors offer free versions of their products. They won’t provide the same feature set of the commercial product, and they often have limits on the number or size of devices they’ll protect; however, they may be an excellent first step for an organization that does not have a reliable solution in place.

Section 3
Risk Management

Here are your options for risk management:

Risk Avoidance	Risk Mitigation	Risk Transfer	Risk Acceptance
What you can do: ● stop doing business ● discontinue a risky business operation after assessing risk and reward	What you can do: ● training & monitoring ● due diligence in business processes (people, vendors, etc.) ● The rest of this presentation	What you can do: ● insurance ● Indemnification clauses in contracts	What you can do: ● no risk assessment ● minimize risk via other means (avoid, mitigate, transfer) to a residual level[1] that is acceptable

Risk Management

https://www.globalcyberalliance.org/gca-cybersecurity-toolkit/

Information or devices are stolen, lost, or compromised:

- Know what you have so that you know what to protect: https://gcatoolkit.org/smallbusiness/know-what-you-have/
    - knowledge and data
    - business processes
    - physical devices
    - third and nth party vendors
- Stay on top of what's going on with your technology
    - Take your vitamins: update your systems
    - Be notified of changes to systems and vendors

[1] The residual level is the remaining potential risk after all IT security measures are applied.

- Secure networks & internet connection
    - Connect to a known and trusted network or safely connect using privacy protecting DNS filtering like Quad9. https://www.globalcyberalliance.org/quad9/
    - Encrypt all firm and client data and communications, saved or transmitted
    - Use systems that require multiple ways of proving you are who you are
- Be carefully curious
    - Don't open attachments or click on links
    - Report any suspicious or out of the ordinary email to IT or outside service
    - Don't always trust every email you get-consider using DMARC email authentication
    - Safe surfing and use protection
- Make security a priority at leadership level
    - Change the way you work - update policies and enforce them
    - Change the way you interact with technology
    - Deepen training to be ongoing, relevant, and interactive

Section 4
Cybersecurity and Corporate Disclosures

Steps to Take Before a Possible Breach

- Organizations should consider having general cyber security disclosures without or regardless of a breach.
- There should be a crisis communications plan (along with incident response team) in place.
- Internal publications should address disclosure protocols in the event of a breach.
- Consider whether engagement letter should address.
- Also consider disclosures if a breach is reasonably anticipated.

Steps in Addressing Possible Breach

Step #1: Determine the nature of incident - what it involves and who, or what, was impacted.

- Details of occurrence (was it a hack? breach? Simply an "event"?)
- Whose data was impacted
- What categories of data
- Are third parties involved such as entities that maintain or store the data
- Determine which insurance is implicated and when the earliest notice must be given to insurer

Step #2: Determine your duties/obligations.

- Jurisdictions impacted
    - Location of impacted parties and possible varying obligations to each
    - Laws
    - Regulations
- Contractual obligations
    - Engagement letter
    - Contracts with 3rd party vendors

- Insurance

- Ethical obligations

- Court order/ "matter dependent" factors (i.e., matters under seal)

Step #3: Determine notice requirements.

- ABA Formal Opinion 483, *Lawyers' Obligations After an Electronic Data Breach or Cyberattack*, Oct. 17, 2018 (https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf)

- SEC

- FTC- Data Breach Response Guide for Business

- Law enforcement investigation will impact timing

- State law

- International sources of law

- Industry guidance and practice

Step #4: Determine who *must* receive, and who *should* receive, disclosure.

- Mandatory and/or Discretionary Disclosure

  - Government regulators, agencies

  - Opposing counsel

  - Court

  - Shareholders/investors/partners

  - Internal [corporate officers, board, employees, shareholders, *et al.*]

  - Law enforcement

    - The incident may, as an initial matter, be brought to an entity's attention by law enforcement.

    - Even if it not, there may be a legal obligation to disclose such incidents to law enforcement, depending on the jurisdiction(s) implicated (including those outside of the United States); there

may be a duty to cooperate should an investigation and/or prosecution result.

- Law enforcement may have better resources to identify the source of such incidents and may be more cognizant of the impact beyond that of the specific entity that is contacting it; indeed, there may be other victims.
    - If a crime has been committed by an employee of the organization, there may be a need to identify that sooner rather than later.
- An organization may choose to delay notifying law enforcement (either because of relationships with law enforcement or for other corporate/cultural reasons)
    - This strategy could create risk if the wrongdoer is then able to cause additional damage to the law firm or to others.
- An organization may find that law enforcement is discouraging dissemination of information about the breach while it is conducting its investigation
    - This position may conflict with lawyers' ethical obligation to notify clients.
- Regardless, these decisions should, if possible, be decided at a senior, policymaking level and considered in advance of any breach.

- Contractual parties
- Data subjects [employees, current/former clients, potential clients, *et al.*]

Step #5: Determine what should be disclosed.

- Rollout
    - First, general "holding statement" (if appropriate)
- More specific communication
    - Resource dependent on how accomplished (*i.e.*, need external vendor, dark website)

- ABA Standard (Ethics Opinion 483)
    - The disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything.
    - In a data breach scenario, the minimum disclosure required to all affected clients is that there has been unauthorized access to or disclosure of their information, or that unauthorized access or disclosure is reasonably suspected of having occurred.
    - Lawyers must advise clients of the known or reasonably ascertainable extent to which client information was accessed or disclosed.
    - If the lawyer has made reasonable efforts to ascertain that extent of information affected by the breach but cannot do so, the client must be advised of that fact.
    - In addition, and as a matter of best practices, a lawyer also should inform the client of the lawyer's plan to respond to the data breach, from efforts to recover information (if feasible) to steps being taken to increase data security.
    - The Committee concludes that lawyers have a continuing duty to keep clients reasonably apprised of material developments in post-breach investigations affecting the client.
- Statutorily/regulatory mandated contents
    - New York SHIELD Act instructive – disclosure must include:
        - Contact Information for the person or business making the notification;
        - Telephone numbers or websites of relevant state and federal agencies that provide information regarding security breach response and identify theft prevention and protection information; and
        - Description of the categories of information that were, or are reasonably believed to have been accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, accessed or acquired.
- All dependent on nature of breach
- Consider preparing, in advance, a generic disclosure statement.

Step #6: Determine method of disseminating disclosure.

- Resource dependent
- Stakeholder dependent
- Consider third party involvement either because of third party involvement with the breach or to retain a third party to assist in dissemination of disclosure. Very often, insurance companies provide this as a service (in order to keep costs down).

Step #7: Determine if there are, or should be, ongoing disclosure obligations.

- Ethical obligations (must keep client reasonably informed)
- Legally- statutory obligation
- Circumstances that might warrant alteration/amendment of disclosure
- Related issues on business continuity

Step #8: Address other post-breach/disclosure issues.

- Reputational damage ("damage control")
- "Lessons learned" – disclose
- Any internal investigation or review of procedures (taking into account possible involvement by law enforcement and relationship of such procedures to prosecutions or civil liability)
- Mitigation efforts – disclose
- Additional communications that depend on parties harmed by breach (vendors, public, customers, clients)

Section 5
Cyber Insurance

Do you know how much you can lose from a cyber incident?

- Small firms that have a cyber incident will be unsustainable without insurance resources
    - Ransomware attacks / Denial of Service Attacks
    - Data breaches
    - Fund Transfer scams

Do you realize that your lawyer's liability insurance does not cover your cyber exposure?

- #1 Business Risk
- 85% of business is digital
- All are in Scope
- Liability insurance does not cover all your cyber exposure
    - sublimit on your professional liability policy is not enough

Do you know what to do if you are the victim of a cyber incident?

- Cyber incidents require immediate response.
- Cyber insurance can provide you access to service providers that specialize in cyber incident response

Example: Small company (5-attorney shop)

- Chart illustrates the return on investment in a cyber insurance policy, comparing the price of a policy based on revenue versus being self-insured and having to pay for a loss out of pocket:

Cyber Stand Alone Policy

$	1,000,000	Revenue
$	1,000,000	Limit
	$1,000	Policy Cost
$	30,000	Cost per record - 500
$	20,000	Legal
$	500,000	Privacy Fines
$	**550,000**	Total
	549000%	ROI

Coverage Afforded on a Stand Alone Cyber Policy

- Chart lays out the stand-alone coverages afforded in a cyber insurance policy, and shows that having a sublimit on Lawyers Professional Liability (LPL) policy does not provide lawyers with sufficient coverage:

Third Party Liability Insuring Agreements		
Multimedia Liability	$1,000,000 Each Claim	$1,000,000 Aggregate
Security and Privacy Liability	$1,000,000 Each Claim	$1,000,000 Aggregate
Privacy Regulatory Defense and Penalties	$1,000,000 Each Claim	$1,000,000 Aggregate
PCI DSS Liability	$1,000,000 Each Claim	$1,000,000 Aggregate
Bodily Injury Liability	$350,000 Each Claim	$350,000 Aggregate
Property Damage Liability	$100,000 Each Claim	$100,000 Aggregate
TCPA Defense	$75,000 Each Claim	$75,000 Aggregate
First Party Liability Insuring Agreements		
Breach Event Costs	$1,000,000 Each Claim	$1,000,000 Aggregate
Post Breach Event Remediation Costs	$75,000 Each Claim	$75,000 Aggregate
BrandGuard®	$1,000,000 Each Claim	$1,000,000 Aggregate
System Failure	$1,000,000 Each Claim	$1,000,000 Aggregate
Dependent System Failure	$1,000,000 Each Claim	$1,000,000 Aggregate
Cyber Extortion	$1,000,000 Each Claim	$1,000,000 Aggregate
Cyber Crime Aggregate Limit (A, B and C combined)		$100,000
A. Financial Fraud Sub-Limit	$100,000 Each Claim	$100,000 Aggregate
B. Telecommunications Fraud Sub-Limit	$100,000 Each Claim	$100,000 Aggregate

Cyber Policies Provide:

- Loss Transfer
    - Pay for good portion of costs and expenses
- Immediate Response Capabilities
    - Hot lines
    - Breach Coaches
- Services / Expertise
    - Forensics / IT
    - Legal
    - Vendors for Notification if required

How to get lawyers to buy an adequate limit

ROLF model for limits adequacy – Tool - $50 for the analysis

Reputational – based on case law
Operational – DoS and Ransomware (based on revenue and on-premise systems)
Legal – based on case law
Financial - # of records (Aggregate Limit)

Be aware of how much you could lose, and how much cybersecurity insurance could save you.