SUFFOLK ACADEMY OF LAW
The Educational Arm of the Suffolk County Bar Association
560 Wheeler Road, Hauppauge, NY 11788
(631) 234-5588

INTRODUCTION TO CYBERSECURITY, PRIVACY & DATA PROTECTION FOR ATTORNEYS

FACULTY:

Eric B. Stern, Esq., Partner
Kaufman Dolowich Voluck
Co-Chair of the Data Privacy and Cybersecurity Practice Group

January 12, 2023
Suffolk County Bar Association, New York

Like us on:

"The opinions, beliefs and viewpoints expressed herein are those of the authors and do not necessarily reflect the official policy, position or opinion of the Suffolk County Bar Association, Suffolk Academy of Law, their i Board of Directors or any of their members"

There's a whole new way to obtain your CLE certificate! It's fast, easy and best of all you can see the history of courses that you've attended!

Within 10 days of the course you attended, your CLE Certificate will be ready to view or print. Follow the instructions below:

1. Go to SCBA.org
2. Member Log In (upper right corner)
3. If you **do not** know your username or password, click the area below and enter your email that is on file with SCBA. Follow the prompts to reset your username and password.
4. After you log in, hover over your name and you will see "Quick Links". Below that you will see:
   a. My SCBA
   b. My CLE History
   c. Update My Information
   d. Update My Committees
5. Click on **My CLE History**, you will see the courses you have attended. Off to the right side you will see the Icon for certificates. You are now able to download the certificate, print it or save it. You may go to your history and review the courses you have taken in any given year!
6. **CLE certificates will no longer be mailed or emailed**. Certificates will be available within 10 days after the course.

Eric B. Stern, Esq. – Kaufman Dolowich Voluck, LLP

Eric B. Stern, Esq. is a partner and co-deputy chair of the data privacy and cyber security practice group at Kaufman Dolowich Voluck, LLP, with decades of experience representing clients in all aspects of insurance coverage litigation. He is an aggressive trial lawyer who has experience litigating cases at both the trial and appellate levels, over many types of insurance coverage issues. These include, but are not limited to:

- D&O liability,
- Professional liability,
- Commercial general liability,
- Uninsured/underinsured motorist liability, and
- Homeowners' liability.

Mr. Stern's insurance coverage experience includes litigation and coverage opinions in matters arising from claims of asbestos and lead paint poisoning, as well as the interplay of pollution exclusions with claims of environmental pollution. He represents both insurance carriers and other private companies, advising them on many types of insurance matters. Additionally, Mr. Stern provides counsel on cybersecurity matters to help ensure client's policies are in compliance with complex cybersecurity laws, such as NY SHIELD compliance. He lead the start-up of the Firm's Data Privacy and Cybersecurity Practice and continues to mentor other lawyers in this ever-changing and crucial area of the law.

As a published author and well-known speaker, Mr. Stern frequently presents various topics regarding insurance coverage for cyber losses, additional insurance coverage, and New York Insurance Law 3420 (d). He has contributed to many articles in these areas including publishing in the *Insurance Journal*, *New York Law Journal*, *Insurance Coverage Law Center*, and *Healthcare Risk Management*, among other sources.

Mr. Stern is passionate and enthusiastic about the law and has always been an adept writer, thinker, and speaker, utilizing these gifts both inside and outside of the workplace. In his free time, Eric serves his community through work with several non-profits, including his local house of worship.

KEY TAKEAWAYS

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

January 20, 2022

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

Gail L. Gottehrer
Law Office of Gail Gottehrer LLC

Ronald J. Hedges
Dentons US LLP

COMMITTEE MEMBERS

Jennifer V. Abelaj
Paul H. Aloe
Mark A. Berman
Robert M. Brill
Patrick J. Burke
Sasha A. Carbone
Ada Chan
Bryan Daniels
Zoe L. Davidson
Craig H. Effrain
Daniel H. Erskine
Matei Foit
William S. Friedlander
Shawndra G. Jones
Kenneth A. Krajewski
Anthony Tze Cheung Lam
Glenn Lau-Kee
Christian P. Levis
Erica L. Ludwick
Dan Feng Mei
Marissa J. Moran
Mauricio F. Paez
Alexander Paykin
Debbie Reynolds
Effie Silva
Enet Somers-Dehaney
Sanford Strenger
David Titus
Ryan M. Torino

CYBERSECURITY THOUGHT LEADERS AND CO-AUTHORS

Nicole Cardascia
Daniel H. Erskine
Gail L. Gottehrer
Thomas Grillo
Ronald J. Hedges
Erez Liebermann
Laurie Kamaiko
Mary Kavaney
Christian P. Levis
Dan Feng Mei
Aishwarya Minocha
Debbie Reynolds
Elizabeth Roper
Enet Somers-Dehaney
James Vinocur

SPECIAL THANKS TO

Dentons US LLP
Bryan Cooper
Molly Watson

TABLE OF CONTENTS

Page

INTRODUCTION FROM THE CO-CHAIRS

Technology continues to play an increasingly significant role in the practice of law. The evidence is indisputable – a major law firm recently announced that its attorneys can work from anywhere indefinitely; the New York State Supreme Court's Commercial Division issued rules endorsing the use of virtual depositions; and courts across the country have indicated that remote judicial proceedings are here to stay.

The widespread adoption of technology has the potential to transform the legal profession. The shift to remote work and virtual court proceedings could increase diversity, equity, and inclusion; improve access to justice; and reduce the costs of litigation and practicing law. As attorneys and courts become more dependent on technology, however, the profession and our legal system become more vulnerable to cyberattacks. Accordingly, it is crucial for attorneys to go beyond just satisfying their ethical obligation of technological competence and to understand and prioritize cybersecurity.

We held our Third Annual Cybersecurity Thought Leadership Conference virtually in October 2021 and are happy to share this Report on the Key Takeaways from that conference. We focused on four topics that are relevant to all attorneys, whether they work in government agencies, public interest organizations, educational institutions, in-house, or law firms: Insider Threats, Phishing, Cloud Technology Best Practices, and Security Assessment Vendors. The Report provides practical guidance to attorneys who are new to cybersecurity and to those who, already familiar with cybersecurity, are interested in learning more.

We thank the Cybersecurity Thought Leaders, whose names are listed on the preceding page, for their commitment to cybersecurity education and to the Cybersecurity Subcommittee. We also thank Bryan Cooper and Molly Watson for sharing their expertise and to Dentons US LLP for its continued support of the Technology and the Legal Profession Committee and the Cybersecurity Subcommittee.

Gail Gottehrer and Ron Hedges

Co-Chairs, NYSBA Technology and
the Legal Profession Committee

INSIDER THREATS

Introduction

- "Insider" threats, whether intentional or inadvertent, are a significant percentage of cybersecurity events. Insiders can be involved in breaches of personally identifiable information, often are a conduit to credentials that allow threat actors access to a firm or company's computer systems, and can be unknowing participants in funds transfer frauds.

- As direct bad actors, unknowing tools of bad actors, or simply through lack of knowledge of basic cybersecurity preventative procedures, insiders can be the cause of a cybersecurity incident that results in loss of business, financial damages, and reputational harm to the company for which they work.

- The scope of such threats, and the role insiders can play in their occurrence, are constant and everchanging. As discussed below, however, there are basic steps that all companies can take to minimize their occurrence and their effect.

- All entities, whether small or large, public or private, can and should take reasonable steps to anticipate such threats in their environments, prepare in advance as to how they will respond to threats that have been executed, and educate employees at all levels on how to recognize and avoid insider threats. Many of those steps are relatively low cost and require a commitment to a culture of cybersecurity rather than significant financial expenditures.

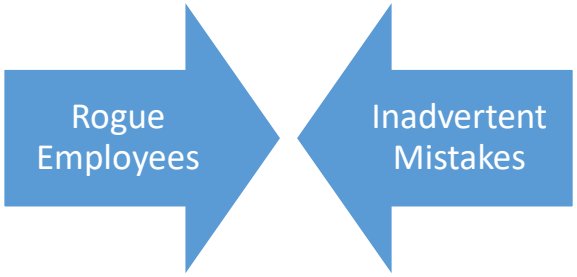
What is an Insider Threat?

- An insider threat is "the potential for an individual who has or has had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization." https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated.

- The Department of Homeland Security advises that insider threats include sabotage, theft, espionage, fraud, and improper acquisition of competitive advantage that are often carried out through abusing access rights, theft of materials, and mishandling physical devices.

- DHS notes that such threats can also result from employee carelessness or policy violations that allow malicious outsiders access to company computer systems. https://www.cisa.gov/instider-threat-cyber.

Who Are Insiders?



- Insider threats can be caused by the intentional conduct of a rogue employee. They can also be the result of inadvertent mistakes such as an employee clicking on an attachment to an unsolicited email that sends malware into the firm's computer system or an employee who mistakenly believes they are responding to the directions from a senior executive when they send gift cards or make a payment to an account of someone they believe to be a legitimate vendor.
    - For an example of the latter, imagine an assistant who receives an email from the CEO of their company in which the CEO directs the assistant to wire a substantial sum to an account outside the organization.
    - The assistant does so without any inquiry and, to their (and the entity's) horror, learns that they have been the victim of a phishing scam.
- Sometimes, the threat is due to a deliberate action that the employee actor may not even realize constitutes a data breach for which they, as well as their company, may be liable.
    - In a recently reported case, a law firm has contended that the attorney defendants who left the firm secretly downloaded and removed files.
    - Other reported incidents involve attorneys who transferred client funds held in trust without checking that the email with instructions as to the account to which to transfer funds actually came from the client.
- "Insiders" are not only employees.
    - An "insider" can also be a consultant, contractor or outside administrator to whom services are delegated, such as an IT vendor.
    - Often, such vendors are provided credentials that allow them access to their client's (namely, your company's) computer network.
    - If the vendor shares those credentials, or does not reasonably protect them, or if the vendor is subject to a cyber attack that results in a bad actor obtaining those credentials, wrongful access to their client company's computer network can occur.

Risks Presented by Insider Threats

Whatever the nature of the insider threat, the risk that insider threats can present to an entity include:

- Theft of intellectual property, including trade secrets;
- Unauthorized access to personal data that can constitute a data breach that triggers a company's statutory obligations to provide notice to affected individuals;
- Regulatory scrutiny due to failure to comply with state, federal or other governmental or regulatory data security requirements, including ones that apply to law firms;
- Fines or other sanctions by one or more regulator;
- Cyberattacks that affect a company's operating systems or computer networks;
- An award of damages and other relief, including attorneys' fees, in civil actions brought under applicable privacy laws or common law by affected individuals or entities;
- Harm to business reputation; and
- Loss of consumer, customer, or public trust.

Steps to Take to Minimize Insider Threats

Business entities can take steps before an incident occurs to minimize the risk of a successful threat, to reduce the damages that can occur if there is an incident, and to comply with applicable legislative and regulatory cybersecurity requirements.

Some of the basic steps include:

- Developing policies and procedures to plan for and respond to insider threats and their aftermath;
- Instituting multi-factor authentication for access to computer networks, particularly for mobile devices and for remote access to systems (**Note:** Do not allow opt outs or exceptions!);
- Taking steps to ensure that patches are promptly applied and monitoring applications to make sure they are timely applied;
- Adopting "zero trust," meaning have all personnel operate on the assumption that there is always a threat (*e.g.*, assume emails with attachments from unknown sources are not safe until verified);
- Conducting security audits of personnel and systems on a regular basis, including periodic testing;

- Engaging in "tabletop" exercises to plan for and develop responses to threats and their aftermath;

- Obtaining cyber insurance, which may offer services to plan for and respond to an incident as well as help defray some of the costs and damages resulting from an incident;

- Educating all personnel, including those at the board or governing body level, in cybersecurity awareness and procedures, from recognizing phishing emails to encouraging physical data security (*e.g.*, not keeping passwords in plain sight);

- Instituting practices that identify unusual account activity, or when an insider is acting in an unusual way;

- Limiting the access of vendors and employees to only systems they need to do their jobs and terminating access when it is no longer needed (especially when an insider's employment is terminated!);

- Monitoring policies and procedures on a regular basis and revising them in response to recognized shortcomings and to incorporate new threats; and

- Cultivating a culture of awareness of the need for cybersecurity.

Resources

Numerous resources are available to assist in the education and awareness of threats. A few recently issued ones are:

- A Fact Sheet on Rising Ransomware Threat to Operational Technology Assets, issued on June 9, 2021, by the Cybersecurity and Infrastructure Security Agency of the United States Department of Homeland Security (CISA) available at Ransomware Threat to OT | CISA, which includes "several recommended actions and resources that critical infrastructure entities should implement to reduce the risk of ransomware."

- "Ransomware risk: 2 preventive steps for your small business," released on November 5, 2021, by the Federal Trade Commission," available at Ransomware risk: 2 preventive steps for your small business | Federal Trade Commission (ftc.gov).

    - These steps are:

        - ***Step #1. Make sure your tech team is following best practices to fend off a ransomware attack.***

            - One key protective step is to set up offline, off-site, encrypted backups of information essential to your business.

            - Furthermore, share the CISA Fact Sheet with your IT staff.

        - Underline, *italicize*, CAPITALIZE just how important it is for them to stay current on the latest word from the leading federal agency on defending against these threats and on updates from other trustworthy public-private partnerships.

        - CISA's ransomware resources – including its Ransomware Guide – should be required reading. This isn't something to save for a slow day at the office.

        - Your IT team should immerse themselves in the latest advice from CISA and other authoritative experts.

    - ***Step #2. Schedule a security refresher for your employees.***

        - Ransomware isn't just an issue for IT professionals.

        - Bad actors often use email to your staff as their entryway into your computer system.

        - By clicking on a link or downloading an attachment, a distracted staffer could inadvertently hand a computer criminal the keys to your corporate kingdom.

        - As companies up their defensive game, the bad guys have responded. Some use publicly available information or stolen data about an employee to craft a more personal message.

        - Rather than a misspelled mess that screams scam from the start, the email – or phone call, text, etc. – may appear at first glance to be legitimate business correspondence or even a message from a colleague.

        - A small business's best defense is a workforce trained in the tricks that cybercriminals are likely to use.

        - Other important protections are: 1) rigorous authentication procedures; and 2) a company policy that requires passwords for employee credentials and administrative functions to be l-o-n-g and complex.

        - In addition, educate your staff on the folly of using the same password on different platforms, and consider the many benefits of multifactor authentication.

These steps can be readily reviewed and incorporated into any entity's policies and procedures.

Other government websites also identify resources available for organizations to better understand, detect, and deter insider threats. *See, e.g.*, Department of Homeland Security National Cybersecurity and Communications Integration Center's website, at https://www.cisa.gov/insider-threat-cyber.

Key "Takeaways" on Insider Threats

- Every entity, public or private, including law firms, faces insider threats;
- Entities should develop policies and procedures that allow for appropriate monitoring of activities that are unusual or suspicious;
- Entities should become familiar with laws and regulations that address unauthorized access and data breach;
- Entities should utilize resources provided by cyber insurers, government and regulatory agencies, and specialized privacy and cybersecurity counsel; and
- All personnel at all levels of the organization should be educated about insider risks and compliance with cybersecurity procedures on a regular basis – no opt outs!

Every organization faces cybersecurity risks. Making sure you and everyone in your organization are aware of those risks and of the ways in which insiders can perpetuate – and minimize – them, is critical to mitigating the cybersecurity risks and potential losses your organization faces.

Phishing, and the Many Forms It Takes

Phishing affects everyone.

What is Phishing?

Phishing is the fraudulent attempt to obtain sensitive information by disguising oneself as a trustworthy entity in a communication. Phishing scams range in sophistication, from a shotgun approach to a highly targeted approach. Phishing is widespread and appears in text messages, robocalls, and emails.

There are different types of phishing, including email phishing, spear phishing, whaling, vishing, and smishing.

Phishing emails tend to induce or trick recipients into clicking on a link and/or opening an attachment in an email. Popular phishing tactics include messages such as:

- "We have noticed some suspicious activity on your account," and
- "We have noticed there's an issue with your payment information."

Phishing emails often include fake invoices and links to make payments.

Spear Phishing

- Spear phishing often relates to an employee, who is responsible for money transfers, receiving a seemingly legitimate email instructing a transfer of funds.
- These are targeted scams and the purported "sender" of the transfer-request-email is often a high-level executive within the company.
- Spear phishing attackers often gather and use personal information about their target.

Whaling

- Whaling is often directed specifically at senior executives and other high-profile targets.
- The contents will likely be created to be of interest to the person or role targeted, such as a subpoena or customer complaint.

Vishing

- Vishing uses the telephone to conduct phishing attacks.
- The attacker-caller dials a large quantity of telephone numbers and plays automated recordings to the victim-callee. These automated recordings include false claims of fraudulent activity on the victim's bank accounts or credit cards. The victim is directed to call a number controlled by the attackers. These calls will prompt victims to enter sensitive information to "resolve" the supposed fraud.

Smishing

- Smishing is an attack with the intent to gather personal information, including social insurance and/or credit card numbers.
- Common smishing examples include bank notifications, package updates, act-now coupons, and urgent warnings. Everyone should be suspicious of any such request, especially if they are from unknown numbers.

Some Statistics

In 2019, one third of all data breaches involved phishing. Phishing is the most common way to penetrate a system.

- Phishing has become a gateway for ransomware, malware, and other cyberattacks. It is the delivery mechanism of choice for ransomware and other malware.
- Usually, phishing emails are sent by seemingly friendly contacts with attachments and/or links that can lead to the installation of malware, which is then used to give the bad actor access to the computer or network. The phishing emails may also allow the bad actor to use the computer to launch malicious attacks or even use the computer to perpetrate fraud campaigns.

If there has been a phishing attack, there are remediation steps that can be followed to prevent the extent of the attack.

- If funds have been mistakenly wired, the organization(s) or individual(s) should contact their bank immediately and consider contacting law enforcement, filing a complaint with the FBI's Internet Crime Complaint Center (IC3), and filing a complaint with local police, the United States Secret Service, or the local FBI office.

- If data has been breached via a phishing attack, the organization or individual should consider contacting law enforcement and a cyber-security specialist/analyst.

Phishing has been so prevalent in all industries that 75% of organizations around the world experienced some kind of phishing attack in 2020. The successful efforts to reduce phishing come from establishing a culture of cybersecurity within the organization. Regular training and phishing tests can help users become the front-line defense for any of these attacks.

- To establish a culture of being cyber aware, organizations must require frequent data security and social engineering training. Knowledge is the best prevention method that helps everyone learn the signs of malicious emails or the indications of an attack.

- 2019 statistics show that 38% of untrained users fail phishing tests. Therefore it is crucially important to maintain good cyber hygiene practices in the organization.

FBI Internet Crime Complaint Center (IC3) 2020 statistics report that IC3 received 791,790 complaints for about $4.1 billion in losses.

- According to the FBI, phishing was the most common type of cybercrime in 2020.

- Phishing incidents more than doubled in frequency, from 114,702 incidents in 2019 to 241,324 incidents in 2020.

- These trends indicate that phishing and other cyberattacks are getting more sophisticated and organizations need to establish their front-line defense.

Why Lawyers Should Care About Phishing

There are a number of practical, ethical, and legal considerations posed by phishing attacks of which all attorneys should be mindful.

- From a practical perspective, the majority of cyber attacks are perpetrated via phishing schemes.

    - Nearly three-quarters of all organizations reported sustaining a successful phishing attack in 2020, according to one survey.

    - These attacks, which can lead to the execution of ransomware, network intrusion, or even business email compromises to name but a few, are the linchpin for a majority of cyber incidents.

- As victims range from solo practitioners to international law firms, all attorneys should be mindful of the damage caused by phishing schemes.

- Potential fallout from a cyber attack can include loss of productivity, remediation costs, breach notification, regulatory scrutiny, litigation, and insurance coverage issues.

- One reason why bad actors continue to target lawyers and law firms is that they are rich sources of the type of information sought by the attackers Bad actors often seek out clients' and employees' personal information, including social security numbers, contact information, and financial account information. Lawyers' involvement in high-value transactions also make them targets for bad actors seeking to intercept and manipulate banking information.

- In addition to these practical considerations, attorneys are ethically required to ensure that their clients' and employees' personal information are reasonably safeguarded.

    - Comment 8 to Rule 1:1 of the Model Rules of Professional Conduct requires that "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . ."

    - In addition, NYSBA Opinion 842 states that Rule 1.6 requires that lawyers take affirmative steps to protect their clients' confidential information. (It should also be noted that NYSBA recommended in June 2020 that lawyers be mandated to obtain a CLE credit on the topic of cybersecurity.)

    - Separately, the American Bar Association declared in Ethics Opinion 477R that lawyers are "required to make reasonable efforts to ensure their communications are secure and not subject to inadvertent or unauthorized cyber security breaches."

- Beyond ethical requirements, there are legal requirements to be aware of in the context of a phishing attack.

    - New York's Shield Act, https://www.nysenate.gov/legislation/bills/2019/s5575, imposes affirmative duties on attorneys who hold and store personal information to ensure that there are reasonable administrative, technical, and physical safeguards in place to protect that information. Any entity that sustains a data breach of this type of personal information has an obligation under the Shield Act to notify those affected and, in some cases, the New York Attorney General's office.

    - The Health Information Technology for Economic and Clinical (HITECH) Act and the Gramm-Leach-Bliley (GLBA) Act impose, respectively, additional safeguards on the storage and handling of patients' medical data, and on financial institutions that handle personal information.

- Law firms of any size that collect personal information from existing and potential clients must ensure that they are compliant with various consumer privacy laws.
    - In the United States, California (California Consumer Privacy Act), Colorado (Colorado Privacy Act), and Virginia (Virginia Consumer Data Protection Act) require businesses of any type to notify residents at or before the time of collection of their data, and of the business's use of that data.
    - The European Union's General Data Protection Regulation (GDPR) places similar restrictions on the collection and use of its residents' data. Failure to abide by these regulations can result in significant fines, litigation, and regulatory action.

Multi-Factor Authentication (MFA)

One step all attorneys should take to mitigate the risk of a cyber incident is to implement multi-factor authentication across both device and account usage.

- Stealing passwords is now the top aim of individuals perpetrating cyber attacks.
- According to Microsoft, implementing MFA can decrease the risk of a successful account breach by 99%.
- There are number of options, including SMS-based MFA, voice-call MFA, and app-based MFA.

The Global Cyber Alliance (GCA)

- GCA is a global not-for-profit created to make the internet safer globally. Former New York County District Attorney Cyrus Vance Jr. created GCA utilizing asset forfeiture funds. GCA now has over 180 member entities from 18 sectors and 33 countries. www.globalcyberalliance.org
- GCA, when it was created in 2015, gave thought and consideration as to how to reduce the risk of phishing, .and created tools to better ensure that users would be safer from this type of cyberattack.

Quad9

The first tool was launched in November of 2017 and called Quad9.

- This name is derived from the IP address of 9.9.9.9.
- Quad9 is a protective DNS infrastructure.
- DNS stands for Domain Name System, which is essentially the phone book of the internet.
    - When a user tries to go to the website of buycatfood.com, DNS translates the website into a numerical IP address that is recognized globally and the user is taken to that address.
- Quad9 takes numerous commercial threat feeds that have been donated by intelligence providers to this free global resource. There are now millions of malicious websites on a block list that are known to contact malicious code like malware. If a user unknowingly tries to go to a website containing malware or other malicious code, the search does not resolve and the user is protected from going to that unsafe site. https://www.globalcyberalliance.org/quad9/
- Quad9 is different from other DNS services in that it does not sell the users' data so it is privacy protecting.
- In 2021, Quad9 made between 60-100 million blocks a day globally.
- In 2017, New York City began to use Quad9 to protect all its guest WIFI.
- Quad9 is now used on every continent.

DMARC

While DNS protects users leaving their organizations and going out to surf on the internet, GCA wanted to promote a tool that would better protect users from receiving fraudulent emails, especially "spoofing" emails, where the bad actor's attempts imitate a legitimate entity and fool the user into giving up his or her personally identifiable information.

- To further this effort, GCA examined why the DMARC (Domain Message Authentication Reporting and Conformance) tool that stops spoofing was not more widely deployed around the world.
- In speaking to partners, GCA learned that a major factor in the limited deployment of DMARC was the difficulties of such deployment.
- To address this concern, GCA created a wizard or a toolkit that is now available in 17 languages and has been deployed worldwide. https://www.globalcyberalliance.org/dmarc/
- While DMARC is not the silver bullet in protecting any organization, it has provided major security benefits to organizations that have deployed it, like Aetna, which stopped 60 million fraudulent emails after deploying DMARC.

- GCA has created a video that explains DMARC and its benefits. https://vimeo.com/221659402

Small Business Toolkit

GCA has created a cybersecurity tool kit for small and medium businesses (including law firms) that can assist with compliance with the SHIELD Act, which mandates certain administrative, physical, and technical safeguards.

- The toolkit can be found at: https://www.globalcyberalliance.org/gca-cybersecurity-toolkit-for-small-business
- The toolkit contains 6 toolboxes that include free and vetted tools.
- The toolkit is linked to the Center for Internet Security (CIS) top five Critical Controls.
- These Controls have been shown to improve the online security posture of users by 85%.

Cloud Technology Best Practices

What Is Cloud Computing?

Cloud computing is a delivery model for information technology (IT) services, permitting users the right to use computing and data storage services (both hardware and software) to access and store information and/or software functionality on remote servers owned or operated by third parties, usually through the internet or private networks.

- The remote servers are hosted in data centers worldwide, permitting cloud vendors to sell computing power, storage capacity, and data across such centers dynamically for fast delivery and on-demand bandwidth.

- Largely all or any IT supply may be delivered as a cloud service, *e.g.*, software applications, branded databases, data retrieval/storage, network configuration and software design tools.

- The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Delivery Options

1. **IaaS: Infrastructure as a Service**

    - Hardware infrastructure (*e.g.*, servers and storage) for remote use permitting users to install, implement, and maintain operating systems and software selected. *E.g.*, Amazon Elastic Compute Cloud (Amazon EC2), Rackspace, Microsoft® Azure® cloud.

2. **SaaS: Software as a Service**

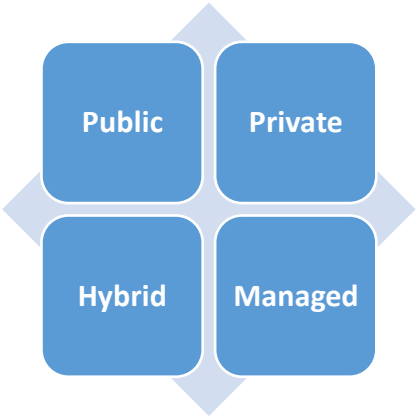
    - Third-party provider manages hardware and software for software applications (no copy on user computer) accessed via a browser/internet permitting user to run,

add, review, sort and manipulate data. *E.g.*, Google's Gmail, DropBox, iCloud, Westlaw.

3. **PaaS: Platform as a Service**
    - Remote computing environment provided for software developers/programmers to develop or extend and run new or existing applications. *E.g.*, Heroku Cloud Application Platform, Google App Engine.

4. **XaaS: Anything as a Service**
    - "X" means anything/any solution. The "aaS" means the business model of third-party providers describing how/method user both receives and pays for solution.

Service Options



Ways in which Cloud Technology Services are provided to users include:

1. **Public clouds**
    - Shared, self-service, "pay as you go" basis.

2. **Private clouds**
    - Dedicated hardware environment for the user.

3. **Hybrid clouds**
    - Combination of public and private clouds, private cloud for proprietary/sensitive information with public cloud for cost savings and less crucial information.

4. **Managed clouds**
    - Managed by a third-party provider, owned by user.

Cloud Computing Security Issues

Key threats to be mindful of when entering into a cloud computing agreement:

- Account Takeovers
- Malware
- Insider Threats
- Data Breaches

Account Takeovers

- Threat actors can leverage user credentials to gain access to cloud storage services.
- From there, they can:
    - Access sensitive data
    - Launch additional attacks
    - Impersonate users
- Credentials can be obtained via:
    - Social engineering
        - Use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes
    - Remote Desktop Protocol access
        - Provides access to a desktop or application hosted on a remote host
    - Phishing

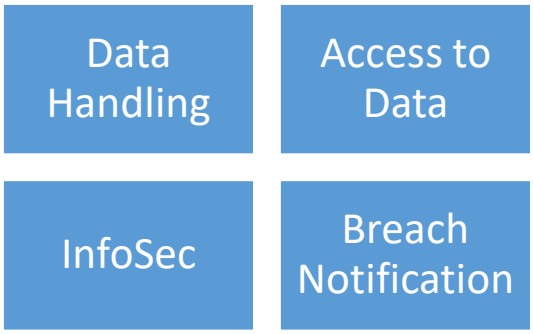
Malware

- Cloud storage services are also used by criminals to host malware.
    - In 2020, over half of malicious code deliveries happened using cloud apps.
- Threat actors will compromise cloud accounts belonging to one user/organization, and then move laterally within the command and control servers.
- Supply chain attacks: malware is deployed in the software development phase, then spreads downstream

Insider Threats

- Users within the organization can misuse cloud access to:
    - Steal proprietary or confidential data
    - Interfere with operations

Factors to consider when evaluating cloud vendors



Data Handling

- Use of, and access, to data.
- Confirm that vendor is only accessing the data necessary to provide its services to the client.
- Confirm that any use of necessary data is only used to provide a specific service to the client and not for any other purpose.
- Confirm that vendor will not give third-party access to client data.
- Exception:
    - Vendor may disclose data as required by applicable law or governmental authority.
    - However, vendor must give client prompt notice of such a demand and cooperate with client in any effort to contest disclosure or seek a protective order.

Vendor Access to Data

- Who has access to client data? Does vendor limit access to client data within its own company?

- Confirm that vendor will not permit any of its employees, subcontractors, or subcontractor employees to access client data unless the individual or company needs access to perform the agreed upon scope of work.

- How does the vendor vet employees who handle sensitive client data?

- Do employees have a clean work and education history and no criminal records?

Cybersecurity Practices

- Does the vendor maintain, implement, and comply with a written data and information security program?

    - An Information Security (InfoSec) Program should:

        - Protect the security and confidentiality of client.

        - Protect against anticipated threats or hazards to the security or integrity of client data.

        - Protect against unauthorized access to or use of client data.

    - What to Look for in an InfoSec Program:

        - Guidelines on the proper disposal of client data after it is no longer needed to carry out services.

        - Access controls on electronic systems used to maintain, access, or transmit client data.

        - Access restrictions at physical locations containing client data.

        - Encryption of electronic client data consistent with then-current, nationally recognized encryption standards.

        - Least privilege principles for access to client data, supplemented either by dual control procedures or segregation of duties.

        - Regular testing and monitoring of electronic systems accessing or storing client data.

        - Procedures to detect actual and attempted attacks on or intrusions into the systems containing or accessing client data.

        - Regular, annual review of the program to ensure that it complies with applicable laws, regulations, technology changes, and best practices.

Breach Notification

- Confirm that vendor will exercise reasonable efforts to prevent unauthorized exposure or disclosure of client data.
- Confirm that vendor has a protocol in play in case of a "Data Incident" in which vendor is responsible for the unauthorized disclosure of, access to, or use of client data.
- In the event of a Data Incident, vendor should notify the client within 48 hours and cooperate with client and law enforcement agencies to investigate and resolve the Data Incident.
- Confirm that vendor will aid in notifying injured third parties.
- Confirm that vendor will compensate client for any reasonable expenses related to notification of injured parties.
- Confirm that vendor will provide one year of credit monitoring to any affected individual.
- Confirm that vendor will provide client access to confidential information (*e.g.* non-public information, trade secrets, confidential records, sensitive information) if it relates to the Data Incident.

See also, Illinois State Bar Ass'n Professional Conduct Advisory Opinion No. 16-06 (Oct. 2016), https://www.isba.org/sites/default/files/ethicsopinions/16-06.pdf (listing factors to consider when evaluating cloud vendors).

Key Laws

- Sarbanes−Oxley Act of 2002, Pub. L. 107-204 (Public companies email retention, data security and integrity, and oversight)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191 (Use and disclosure of protected health information)
- Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. 113-283. Federal agencies to develop and implement information security programs. Executive Order 14208, "Improving the Nation's Cybersecurity" (May 12, 2021)
- Data privacy and security laws, including laws concerning the cross-border transfer of personal information.
- N.Y. General Business Law § § 899-aa, 899-bb
- For state agencies N.Y. State Technology Law § 208
- N.Y. Department of Financial Services (NYDFS) Cybersecurity Regulations for Financial Services companies (23 NYCRR 500.0 through 500.23)

- N.Y. Gen. Bus. Law § 349(a) and N.Y. Exec. Law § 63(12) (deceptive acts and practices)
- Federal Trade Commission Act, Section 5 (15 U.S.C. § 45)
- Federal Trade Commission's Red Flags Rules issued under the Fair and Accurate Credit Transactions Act (FACTA)
- Gramm-Leach-Bliley Act (GLBA) (Pub. L. No. 106-102, 113 Stat. 1338 (1999)
- Telephone Consumer Protection Act (TCPA)
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (a/k/a the "Patriot Act")
- Children's Online Privacy Protection Act of 1998 (COPPA)
- Fair Credit Reporting Act (FCRA) as amended by FATA
- Electronic Communications Privacy Act of 1986 (ECPA)
- Computer Fraud and Abuse Act (CFAA)
- Video Privacy Protection Act of 1988 (VPPA)
- GDPR (Regulation (EU) 2016/679)
- UK Data Protection Act 2018

Confidentiality of Business, Personal or Privileged Information

- N.Y. Rules of Prof. Conduct, Rule 1.0(c)
- N.Y. Rules of Prof. Conduct, Rule 1.6
- N.Y. Gen. Bus. Law § 399-ddd (Social Security Numbers)
- N.Y. Gen. Bus. Law §§ 399-h, 899-aa(1)(b), and § 899-bb (data disposal)
- N.Y. Penal Law §§ 250.00 to 250.05 (eavesdropping law)
- N.Y. Lab. Law § 203-c (employee privacy protection)
- N.Y. Gen. Bus. Law § 395-b (unlawfully installing or maintaining viewing devices)
- N.Y. Lab. Law § 203-d (employee personal identifying information)

- N.Y. Lab. Law § 704 (surveillance as an unfair labor practice)
- N.Y. Pub. Health Law § 2781 (HIV and AIDS information)
- N.Y. Comp. Codes R. and Regs. tit. II, ch. XIX, § 420.0 to 420.24 (Privacy of Consumer Financial and Health Information)
- N.Y. Gen. Bus. Law § 380 (Credit Reporting)
- N.Y. Gen. Bus. Law § 520-a (Restriction on Collecting Addresses on Credit Card Transactions)
- N.Y. Pub. Off. Law §§ 91-99 (Government Data Banks)
- N.Y. Pub. Off. Law § 89(2)(b)(i) (Employment and Medical Information Records)
- N.Y. Lab. Law § 201-a (Employment Records)
- N.Y. Pub. Off. Law § 89(2)(b)(iii) (State Mailing Lists)
- N.Y. Pub. Off. Law § 521-C (Credit Card Lists)
- N.Y. Pub. Health Law § 17 (Medical Records)
- N.Y. Gen. Bus. Law art. 39-F §§ 899-aa et seq. (Notification of Unauthorized Acquisition of Private Information)
- N.Y. Exec. Law § 718
- N.Y. C.P.L.R. 4502(b) (Spousal privilege); *see also* N.Y. C.P.L. Article 250
- N.Y. C.P.L.R. 4503 (Attorney-client)
- N.Y. C.P.L.R. 4504 (Physician, dentist, chiropractor, nurse)
- N.Y. C.P.L.R. 4505 (Clergy)
- N.Y. C.P.L.R. 4507 (Psychologist)
- N.Y. C.P.L.R. 4508 (Social worker)
- N.Y. C.P.L.R. 4509 (Library circulation records)
- N.Y. C.P.L.R. 4510 (Rape crisis counselor)
- Civ. Rights Law § 79-h (Journalist Shield Law)
- Jud. Law § 499 (Member or authorized agent of a lawyer assistance committee)

eDiscovery

- Federal Rules of Civil Procedure
    - Rule 16
    - Rule 26
    - Rule 37 (data retention)
- N.Y. Commercial Division Rules 22 New York Codes, Rules and Regulations (NYCRR) § 202.70(g)
    - Rule 1(b)
    - Rule 11-e(f)
    - Rule 11-g
    - Appendices A, B, E
    - N.Y. C.P.L.R.
        - Rule 3103
        - Rule 3120
        - Rule 3122(b)
        - Rule 2301
        - *See also, generally,* 22 NYCRR §§ 202.1 to 202.69

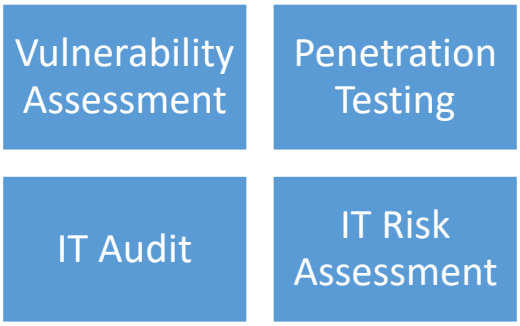
Security Assessment Vendors

- N.Y. Rule of Professional Conduct ("Rule") 1.1 addresses competence of attorneys.
- Rule 1.6 deals with the obligation of attorneys to take reasonable measures to protect confidentiality.
- Taken together, these rules require attorneys to have sufficient technical knowledge to engage in the practice of law and to maintain the confidentiality of information.

What Are Security Assessments and Security Assessment Vendors?

- Security assessments are periodic exercises that allow companies, including law firms, to test their data security systems.
- Security Assessment Vendors are contractors who are retained by organizations to conduct assessments to test the organization's security preparedness.
    - These vendors should be expected to know and follow industry standards in undertaking security assessments and reporting the results of assessments.
    - Attorneys should know enough to be able to satisfy themselves that the vendors they select to conduct security assessments are qualified and that the assessment is done in accordance with industry standards.

Types of Security Assessments



- Vulnerability Assessment:
    - This type of assessment is intended to map vulnerabilities in an organization's IT systems.
    - It seeks to identify and "fix" vulnerabilities as a first step toward a more comprehensive security environment.

- Penetration Testing (Pen Test):
    - This assessment is focused on a particular "target."
    - It attempts to penetrate the target's IT system and allows the vendor who is "attacking" the target to evaluate the system's functionality, management, and security.
    - There are three levels of information that a tester could have about the IT system it is attacking:
        - White = the tester has full access to the system.
        - Grey = the tester has some knowledge about the system but not enough to assure access.
        - Black = the tester has no information about the system and is essentially acting as an external hacker.
- IT Audit:
    - Purpose is to test whether an existing IT system follows a governing compliance standard which might have technical as well as documentation requirements.
    - The intent of the audit is not to test a system's security but, rather, to demonstrate that it is in compliance with certain standards or requirements.
- IT Risk Assessment:
    - Purpose is to address risks that are known or are foreseeable to an organization.
    - Use is to identify the assets of the organization, the impact of risks on those assets, enable the organization to define acceptable levels of risk, and protect assets against identified risks.

Who Performs Assessments and When Are They Performed?

- There are vendors that specialize in one or more of the assessments described above and can be retained to conduct these assessments.
- These vendors may also provide incident response services, investigate an incident, and address the vulnerabilities that enabled the incident.
- Taken together, vendors can be retained to, among other things:
    - Identify risks
    - Advise on how to improve existing security measures and implement new ones

- Detect cyber threats and breaches (actual or attempted)
- Respond to cyber threats and breaches
- Return operations to "normal"

What to Consider When Retaining a Vendor

- Cost (initial contract amount and potential subsequent charges).
- Nature of the assessment to be performed and its scope.
- Nature of the data that the attorney has:
    - Personal health information that might be protected under sectoral privacy laws like HIPAA.
    - Personally identifiable information that might be subject to privacy or cybersecurity laws like the CCPA and NY SHIELD Act.
- Policies and procedures that the vendor will follow, and technologies that the vendor will use, in performing the assessment. (This enables the attorney to discharge her duty to supervise under Rule 5.3.)
- The vendor's understanding of the attorney's ethical obligations and the vendor's agreement to conduct itself in accordance with those obligations.

Reasons to Have a Written Retainer Agreement

- Sets forth compliance with legal obligations (*e.g.*, if protected health information subject to HIPAA is involved).
- Creates a record of:
    - Scope of work to be performed.
    - Milestones, deliverables, and deadlines vendor agrees to meet.
    - Allocation of risk should the vendor fail to perform and/or third parties are adversely affected during the course of the vendor's performance.
    - Vendor's indemnification obligations for any damages or penalties imposed by reason of the vendor's performance or lack thereof.
    - Selection of the method for resolving any disputes that arise out of the agreement.
    - Selection of venue for any litigation arising out of the agreement.

Additional Provisions to Consider Including in a Retainer Agreement

- Reasonable notice of actual or threatened breach of data held by the vendor.
- Requirement that vendor obtain written confirmation before conducting any work beyond that specified in the scope of work section.
- Duration of the retention agreement.
- Requirement that vendor secure specific amount of insurance for the benefit of the organization in connection with the work to be performed under the agreement.
- Prohibition on vendor assigning work to be performed under the agreement to another entity unless agreed to in writing prior to the assignment.
- When applicable, an acknowledgement by the vendor that it has been retained for purposes of assisting counsel to provide legal advice and that attorney-client privilege will apply to any communications made for those purposes.
    - Two Types of Privilege
        - Attorney-Client Privileged Communication. Four elements of attorney-client communication:
            - contains confidential information;
            - between attorney and client;
            - with the intent that the information be kept confidential;
            - for the primary purpose of obtaining legal advice.
        - Attorney-Client Privilege is not automatic and each element can be challenged.
        - Privilege protects the communication and not the underlying facts.
        - Attorney Work Product Protection. An attorney's work product, which may include work product created by an attorney's agent, may not be discoverable if the product is:
            - A document or tangible thing;
            - that was prepared in anticipation of litigation or for trial;
            - by or for a party or its representative (including the party's attorney, consultant, surety, indemnitor, insurer or agent).
        - Protection is not automatic.

- When determining if protection applies, courts may examine the timing between the retainer agreement, work production creation, litigation holds, litigation and the assertion of privilege.

Recommendations

- Recommendations for increasing chances that communications and work product will be considered privileged and survive challenges

  - Purpose

    - To trigger privilege protection it should be counsel, preferably outside counsel, who retains the vendor as counsel's agent to "translate" the information about the client's system for "the purpose of rendering legal advice" to the client.

    - Include a statement of the purpose in the retainer agreement.

    - If in-house counsel retains the vendor, be mindful of in-house counsel's dual role as both business risk advisor and legal counsel.

  - Scope

    - Explicitly define the scope of vendor's work.

    - Consider tying the scope of work to anticipated litigation for work product protection or tying the scope to compliance with statutes, regulations, privacy laws, notification laws, or consent decrees for attorney-client protection.

    - Consider the time vendor is given to perform the work to mitigate the risk of a challenge that the vendor's work was not in anticipation of litigation.

  - Fee

    - Limit application of the fee to a specific task and do not allow the fee to shift to varying scopes of work that depend on the evolution of events.

    - For example, a retainer fee applied to a data breach in anticipation of litigation that shifts to risk assessment and training if a data breach does not occur will make the vendor's work vulnerable to a challenge on privilege.

  - Maintain Confidentiality

    - To maintain privilege, the vendor's work and vendor's communications with counsel must be kept confidential.

    - Counsel should direct the vendor's work assignments and control the communications between vendor and the client company.

    - Counsel and vendor should establish protocols for keeping information confidential.

- Investigation/Risk Assessment Reports

    - Report's purpose must be to assist attorney in providing legal advice and not merely relate information about client company's systems.

    - If the ultimate work product co-mingles legal advice with business risk, then it may be vulnerable to a challenge on privilege.

    - Consider drafting reports that point out potential legal issues and request legal advice, or creating two versions of the report: one that remains confidential for the purpose of giving legal advice and a second one that does not contain characterizations of facts and can be widely distributed in the client organization or made public.

- Investigation in Two Tracks

    - To maintain privilege and mitigate the risk against co-mingling legal counsel and business risk advice, consider running data breach investigations and post-breach activities on separate tracks.

    - Have outside counsel run a legal track that focuses on legal matters and litigation and in-house counsel manage the ordinary-course investigation, risk-related matters, and the day-to-day legal issues.

    - Keep the two tracks separate.

- Legal Advice

    - Counsel must provide client with legal advice for privilege to attach.

- Vet Public Statements

    - Ensure company's public statements about its data security system and/or the results of vendor's risk assessments do not waive privilege.

    - Ensure company's public statements do not misrepresent anything about its data security system.

Staff Memorandum

HOUSE OF DELEGATES
Agenda Item #9

REQUESTED ACTION: Approval of the report and recommendations of the Committee on Technology and the Legal Profession.

Attached is a report from the Committee on Technology and the Legal Profession recommending that NYSBA support amendment of the mandatory continuing legal education rule be amended to require one credit in cybersecurity. The credit would be included within the "ethics and professionalism" category and would not add to the minimum 24-hour biennial rule for experienced attorneys or the 32-hour biennial requirement for new attorneys. The amendment would be effective for four years and revisited after that time.

The committee notes that New York ethics rules require lawyers to keep up with technology and to exercise reasonable care in preventing disclosure of confidential information. Accordingly, educating attorneys regarding cybersecurity has taken on increased importance. Both Florida and North Carolina have added a technology requirement to their CLE requirements. Rather than recommend a general technology requirement, the committee believes cybersecurity protection is a pressing issue for lawyers and should be emphasized through a one-credit requirement.

This report was published in the Reports Community February 2020. The Local and State Government Law Section has indicated that it opposes the proposal, and the Trusts and Estates Law Section indicates that it supports.

The report will be presented at the June 13 meeting by committee co-chair Mark A. Berman.

REPORT RECOMMENDING THAT THE ATTORNEY CONTINUING LEGAL EDUCATION BIENNIAL REQUIREMENT BE MODIFIED TO REQUIRE THAT THE ETHICS AND PROFESSIONALISM REQUIREMENT INCLUDE FOR FOUR YEARS ONE CREDIT ON CYBERSECURITY

COMMITTEE ON TECHNOLOGY AND THE LEGAL PROFESSION

OF THE

NEW YORK STATE BAR ASSOCIATION

January 27, 2020

Opinions expressed are those of the Committee preparing the Report 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.

COMMITTEE ON TECHNOLOGY AND THE LEGAL PROFESSION

CO-CHAIRS

Mark A. Berman

Ganfer Shore Leeds & Zauderer LLP

Gail L. Gottehrer

Law Office of Gail Gottehrer LLC

COMMITTEE MEMBERS

Seth Agata
Alison Arden Besunder
Shoshanah V. Bewlay
John D. Cook
Hon. Fern A. Fisher
Parth N. Chowlera
Tracee E. Davis
Sarah E. Gold
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

EXECUTIVE SUMMARY

The Committee on Technology and the Legal Profession (the "Committee") of the New York State Bar Association ("*NYSBA*") proposes to the Executive Committee of *NYSBA* that it recommend that the biennial, twenty-four hour credit requirement for attorney continuing legal education requirement ("CLE") contained in the CLE Board Rules and Regulations be modified to require one credit on the topic of cybersecurity. The credit would be considered under "*Ethics and Professionalism*" and it would be included within the existing biennial "*Ethics and Professionalism*" requirement. The one credit would not add to the already-required thirty-two (32) credit hours for new attorneys or the twenty-four (24) hours for more experienced attorneys. The requirement would exist for four years and would be revisited thereafter and potentially be extended depending on the state of the legal profession at the time regarding cybersecurity, including the "hacking" of law firm electronically stored information.

INTRODUCTION

NYSBA has a long history of being on the cutting edge of CLE requirements for lawyers. *NYSBA* considers technological competence in the practice of law to be essential to respond effectively to the needs of our changing society and a CLE requirement designed to educate lawyers on how to protect confidential and proprietary client and law firm electronic assets relates directly to legal competency.

Mandatory CLE was initially conceived, supported and implemented as a way to enhance both lawyer competence and public trust in the profession. The ABA's 1992 MacCrate Report, entitled "*Law Schools and the Profession: Narrowing the Gap*," provided a platform for states considering whether to mandate CLE requirements and identified four basic values of professional responsibility. As described by one commentator in 1998, the four values are: "1) providing

competent representation; 2) striving to promote justice, fairness and morality; 3) striving to improve the profession; and 4) professional self-development." Including a mandatory cybersecurity component will help advance those values by providing attorneys with ongoing education in this critical area and increasing public trust that their confidential and proprietary information will be secure when in the possession of attorneys.

THE LANDSCAPE OF HACKING IN THE LEGAL PROFESSION

The *New York Law Journal* ("*NYLJ*") reported in an October 2019 article, entitled "Eight NY Law Firms Reported Data Breaches as Problems Multiply Nationwide," that the number of law firm data breaches in New York State doubled in 2018 and that "[d]espite a number of high-profile breaches putting firms on notice of cyber risks in recent years, there are indications that law firm breaches are occurring more frequently, not less." The article also reported that some cybersecurity lawyers and consultants said the numbers "likely represent a tiny fraction of the breaches affecting the legal industry. Law firms, like other privately held businesses, don't often publicize when their data is breached, and many may not report it to state officials, depending on the law." The *NYLJ* also reported in an October article entitled, How Vendor Breaches Are Putting Law Firms at Risk, that "[e]xternal breaches, including phishing and hacking as well as vendor incidents, were the most commonly identified source of data exposure events reports by law firms."

Also, in an October 2019 article, entitled "As Hackers Get Smarter, Can Law Firms Keep Up?," the *NYLJ* reported that "large and small law firms can do much better in preventing and reacting to data breaches" and "cautioned that the legal sector may risk falling behind other industries." The *NYLJ* noted that "[w]hile hackers are getting smarter, it's also the case that some law firms aren't keeping up with security guidelines developed inside the industry and in other

professional fields, according to legal industry surveys and interviews with security consultants and law firm leaders." The article quoted Austin Berglas, former head of the FBI's cyber branch in New York, as stating that "he would rate law firm cybersecurity as 'middle of the road' now, as firms juggle the competing interests of access and security."

The article then quoted Logicforce, an IT law firm consulting company that had surveyed midsize law firms, which noted that the legal industry "remains very vulnerable to cyberattacks." The article noted that, according to the survey, "fewer firms in 2019 compared with last year's survey reported implementing prevention techniques such as multifactor authentication and data loss prevention technology, which can scan and block the transmission of personally identifiable information." Critically, the *NYLJ* article made clear that "[e]thics laws require lawyers to keep pace with technology to protect client information. Still, some observers point to a slow pace of budding ethics rules on cybersecurity questions."

NEW YORK'S ETHICAL FRAMEWORK

NYSBA Committee on Professional Ethics Op. 950 provides:

> A fundamental principle in the client-lawyer relationship "is that, in the absence of the client's informed consent or except as permitted or required by the Rules of Professional Conduct (the "Rules"), the lawyer must not knowingly reveal information gained during and related to the representation, whatever its source." Rule 1.6, Cmt. [2]. The attorney not only has an obligation to refrain from revealing such information, but also must *exercise reasonable care* to prevent its disclosure or use by "the lawyer's employees, associates, and others whose services are utilized by the lawyer." (emphasis added).

NYSBA Committee on Professional Ethics Op. 1019 provides that the duty of "reasonable care"

> does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered to determining the reasonableness of the lawyer's expectation of confidentiality

> include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.

In fact, NYSBA Committee on Professional Ethics Op. 842 provides that a lawyer must take reasonable care to *affirmatively* protect a client's confidential information. It further provides that:

> [c]yber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks. That is particularly true where there is outside access to the internal system by third parties, including law firm employees working at other firm offices, at home or when traveling, or clients who have been given access to the firm's document system. See, e.g. Matthew Goldstein, "Law Firms Are Pressed on Security For Data," N.Y. Times (Mar. 22, 2014) at B1 (corporate clients are demanding that their law firms take more steps to guard against online intrusions that could compromise sensitive information as global concerns about hacker threats mount; companies are asking law firms to stop putting files on portable thumb drives, emailing them to non-secure iPads or working on computers linked to a shared network in countries like China or Russia where hacking is prevalent)
>
> In light of these developments, it is even more important for a law firm to determine that the technology it will use to provide remote access (as well as the devices that firm lawyers will use to effect remote access), provides reasonable assurance that confidential client information will be protected. Because of the fact-specific and evolving nature of both technology and cyber risks, we cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients, including the degree of password protection to ensure that persons who access the system are authorized, the degree of security of the devices that firm lawyers use to gain access, whether encryption is required, and the security measures the firm must use to determine whether there has been any unauthorized access to client confidential information.

New York ethics opinion make clear that lawyers have an affirmative duty to protect confidential and proprietary client and law firm information and to stay current on cybersecurity threats, including the risk of being electronically compromised and what anticipatory or counter-measures should be reasonably implemented in order to appropriately safeguard client and law firm confidential and proprietary information.

The education of lawyers on the issue of cybersecurity has become even more imperative now that New York has enacted the "*Stop Hacks and Improve Electronic Data Security*" or "*SHIELD Act*," which applies to all law firms, even to solo practitioners and small firms. The *SHIELD Act* creates, for the first time, substantive security requirements for persons or businesses that hold the "private information" of New York residents, and it: (1) expands the types of data that may trigger data breach notification to include user names or e-mail addresses, and account, credit or debit card numbers; (2) broadens the definition of a breach to include unauthorized "access" (in addition to unauthorized "acquisition"); and (3) creates a new reasonable security requirement for companies to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of" private information of New York residents. Safeguards may include designating employees to coordinate a security program, conducting risk assessments and employee training on security practices and procedures, selecting vendors capable of maintaining appropriate safeguards and implementing contractual obligations for those vendors, and securely disposing of private information within a reasonable time.

The *SHIELD Act*, as it applies to solo practitioners and small law firms, requires those persons and entities to ensure that there "are reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."

OTHER STATES NOW MANDATE TECHNOLOGY CLE CREDIT

The Florida Supreme Court approved a rule requiring Florida lawyers to take a minimum of three hours of technology-related CLE courses during a three-year cycle. In addition to adding the three-hour requirement, the Court amended a comment to its rule on lawyer competence to

state that lawyers could retain nonlawyer advisers with "established technological competence in the relevant field." The Court added that competent representation may also involve cybersecurity and safeguarding confidential information. The Court also noted that "in order to maintain the requisite knowledge and skill, a lawyer should engage in continuing study and education, including an understanding of the risks and benefits associated with the use of technology."

The North Carolina Supreme Court also recently approved a mandatory CLE rule. It provides that:

> "Technology training" shall mean a program, or a segment of a program, devoted to education on information technology (IT) or cybersecurity (see N.C. Gen. Stat. §143B-1320(a)(11), or successor statutory provision, for a definition of "information technology"), including education on an information technology product, device, platform, application, or other tool, process, or methodology. To be eligible for CLE accreditation as a technology training program, the program must satisfy the accreditation standards in Rule .1519 of this subchapter: specifically, the primary objective of the program must be to increase the participant's professional competence and proficiency as a lawyer. Such programs include, but are not limited to, education on the following: a) an IT tool, process, or methodology designed to perform tasks that are specific or uniquely suited to the practice of law; b) using a generic IT tool process or methodology to increase the efficiency of performing tasks necessary to the practice of law; c) the investigation, collection, and introduction of social media evidence; d) e-discovery; e) electronic filing of legal documents; f) digital forensics for legal investigation or litigation; and g) practice management software. See Rule 1602 of this subchapter for additional information on accreditation of technology training programs.

THE COMMITTEE'S APPROACH

The Committee considered recommending that a general technology component be added as a required subject under New York Bar's CLE requirement, as did Florida and North Carolina; however, the Committee agreed that such a general requirement may result in attorneys not actually focusing on what the Committee believes to be one of the most pressing and urgent issues facing our legal profession: cybersecurity protection of confidential and proprietary client and law firm electronic information and assets, which includes protecting client and law firm monies

maintained in escrow and operating accounts, all of which are subject to phishing, scams, impersonation, fraud and other wrongful artifices. The Committee believes that requiring attorneys to take one credit in cybersecurity will sensitize and educate lawyers on how to secure confidential and proprietary client and law firm electronic information, and when and how to notify clients and/or law enforcement, as appropriate, in the event of a cyber incident.

Lastly, notwithstanding reporting by the press on data breaches and, more importantly on law firm breaches, the Committee has been surprised by the relative lack of attendance at *NYSBA* CLEs on cybersecurity, whether in person or over webinars.

CONCLUSION

Accordingly, we request that the Executive Committee of the NYSBA support this important initiative by voting in support of the Committee's recommendation.

To: Committee on Technology and the Legal Profession
From: Trusts & Estates Law Section, CLE Committee
Date: May 8, 2020
Re: Proposed Modification of MCLE Requirements

The Committee on Technology and the Legal Profession of the New York State Bar Association has proposed a modification of the New York State CLE Board Regulations & Guidelines (*see* "Report Recommending that the Attorney Continuing Legal Education Biennial Requirement Be Modified to Require that the Ethics and Professionals Requirement Include for Four Years One Credit on Cybersecurity," January 27, 2020). The proposed modification is that, for a period of four years — two biennial registration periods — one of the credit-hours of continuing legal education already mandated in the area of ethics and professionalism (*see* 22 NYCRR §1500.12 [a] [1] and 22 NYCRR §1500.22 [a]) be devoted to cybersecurity. At the end of the four-year period, the Committee on Technology and the Legal Profession would evaluate whether to extend the requirement. We recommend that the proposal be approved. Safeguarding client information in electronic form is a timely and important ethics issue for attorneys practicing in New York State.

COMMENTS ON THE REPORT OF THE COMMITTEE ON TECHNOLOGY AND THE LEGAL PROFESSION BY THE LOCAL AND STATE GOVERNMENT LAW SECTION

These comments are respectfully submitted by the Local and State Government Law Section (the "Section") on the report of the Committee on Technology and the Legal Profession (the "Committee") entitled "Report Recommending that the Attorney Continuing Legal Education Biennial Requirement Be Modified to Require that the Ethics and Professionalism Requirement Include for Four Years One Credit on Cybersecurity" dated January 27, 2020.

While the Section agrees with the Committee that cybersecurity for law firms is of critical importance, and agrees that this subject should be offered as an option to fulfill the required continuing legal education ("CLE") ethics credits, we disagree with the recommendation that it be mandatory that one credit of the four required CLE ethics credits be on this topic for the following reasons:

1. It has not been demonstrated that cybersecurity is a topic over which most attorneys have control. Many attorneys, particularly those employed by larger law firms and government entities, have little, if any, ability to control or influence their employer's cybersecurity policies and do not typically handle escrow funds. Similarly, they do not control the choice of vendors to be used by their employers, or those vendors' cybersecurity choices or protections. While the Section recognizes that phishing emails and hacking attempts may be sent to any attorney, and that attorneys should be educated about how to avoid such attempts, this topic does not require an hour of CLE for every attorney for every biennial reporting period. The first line of defense is the email software utilized by the attorney's employer, whether firm or governmental entity, and the majority of attorneys have no control over those choices.

2. Enacting this requirement effectively limits the amount of CLE programming that the Section can provide on ethical subjects specific to Section members during Section meetings. One of the Section's goals has been to provide, during its in-person Fall and Annual Meetings, sufficient CLE opportunities for the members to satisfy their CLE requirements. Given the finite time available for programming during Section meetings, particularly the annual meeting in New York City, the imposition of this requirement will mean, as a practical matter, that a portion of the time otherwise devoted to Section-specific ethical education will be replaced with this more general CLE instruction in order to fulfil the requirement, thereby diluting the member benefit of providing Section-specific information. While it is true that the Section could offer additional substantive and ethical programming via webinars throughout the year to make up for this change, it is not as optimal as engaging in the ethical discussions of municipal law subjects that typically occur at the in-person meetings.

3. As a corollary to the second point, the assertion may be made that the Section (or another entity) could provide the cybersecurity requirement via webinar or at a separate meeting. While technically correct, this also raises concerns. For example,

Section attorneys are not typically cybersecurity experts, and the Section likely would need to locate outside sources to provide this education to their members. Some governmental entities typically provide their attorneys with in-house CLE. The City of New York is an example. If this requirement is imposed, the City will be burdened with either developing new courses to satisfy this requirement or obtaining the materials from outside sources, neither of which is optimal because, as noted in item 1 above, few of their employees would have any decision-making authority concerning cyber-security.

In sum, the goal of sensitizing attorneys to cybersecurity issues is laudable. However, it can be achieved by methods other than making training a mandatory hour of education for every attorney.

Tannenbaum Helpern
Syracuse & Hirschtritt LLP

900 Third Avenue New York, NY 10022-4775
Tel: (212) 508-6700 | Fax: (212) 371-1084
www.thsh.com | @THSHLAW

Vincent J. Syracuse
Direct Dial: (212) 508-6722
Fax: (212) 371-1084.
E-mail: Syracuse@thsh.com

June 5, 2020

Mark A. Berman, Esq.
Ganfer Shore Leeds Zauderer LLP
360 Lexington Avenue
New York, New York 10017

Re: Report Recommending that the Attorney Continuing Legal Education Biennial Requirement Be Modified to Require that the Ethics and Professionalism Requirement Include for Four Years One Credit on Cybersecurity (the "Cybersecurity Report")

Dear Mark:

I am a member of the NYSBA Committees on Attorney Professionalism and Continuing Legal Education and a former Chair of the Commercial & Federal Litigation Section. I have also authored over 75 Attorney Professionalism Forums in the NYSBA Journal since January 2012.

I write to support the adoption of the Cybersecurity Report by the House of Delegates at tomorrow's meeting. I endorse the proposal that for a period of four years one of the credit-hours of continuing legal education already mandated in the area of ethics and professionalism (*see* 22 NYCRR §1500.12 [a] [1] and 22 NYCRR §1500.22 [a]) be devoted to cybersecurity with an evaluation whether to extend the requirement to take place at the end of the four years. As emphasized in our June/July Forum, which discusses the ethical and professional challenges that we have all been facing practicing law during the pandemic, the protection of client information from cybersecurity threats is an ethical issue of paramount importance to all attorneys practicing in New York State and should be make a part of the continuing legal education ethics requirement.

Sincerely,

s/Vincent J. Syracuse

Vincent J. Sryacuse

[1127761-1]

NEW YORK STATE BAR ASSOCIATION
One Elk Street, Albany, New York 12207 PH 518.463.3200 www.nysba.org

To: Mark Berman & the Committee on Technology and the Legal Profession

From: Young Lawyers Section

The Young Lawyers Section supports the proposed modification to the MCLE requirements contained in the Report your Committee prepared. We agree that it is critical for all lawyers in New York State to fully understand and appreciate the necessity of cybersecurity. Including cybersecurity as part of the MCLE requirements would ensure that law firms are better equipped to practice law in 2020 and beyond. Especially as we work from home, relying on digital technology to engage with our clients, our colleagues, the courts and others, it is imperative that we practice securely.

Reprinted with permission from: New York State Bar Association *Journal*, June/July 2020, Vol. 92, No. 5, published by the New York State Bar Association, One Elk Street, Albany, NY 12207.

The Attorney Professionalism Committee invites our readers to send in comments or alternate views to the responses printed below, as well as additional hypothetical fact patterns or scenarios to be considered for future columns. **Send your comments or questions to: NYSBA, One Elk Street, Albany, NY 12207, Attn: Attorney Professionalism Forum, or by email to journal@nysba.org.**

This column is made possible through the efforts of the NYSBA's Committee on Attorney Professionalism. Fact patterns, names, characters and locations presented in this column are fictitious, and any resemblance to actual events or to actual persons, living or dead, is entirely coincidental. These columns are intended to stimulate thought and discussion on the subject of attorney professionalism. The views expressed are those of the authors, and not those of the Attorney Professionalism Committee or the NYSBA. They are not official opinions on ethical or professional matters, nor should they be cited as such.

TO THE FORUM:

I am the managing partner of a general practice law firm of approximately 40 lawyers and 20 staff members. In response to the ongoing pandemic, all firm employees are required to work from home. While the safety of the firm's employees is always a top priority, our management team has concerns about how our employees remain in compliance with their ethical obligations during this time. Specifically, with many of our attorneys working in close quarters to other family members, how can they best ensure they are safeguarding client's confidentiality?

Additionally, our firm has implemented a number of practices to facilitate a seamless transition when working from home. For example, we provide secure remote access protected with two-factor authentication for access to our work applications. We also provide a firm-hosted cloud-based file sharing service so that our employees can transfer multiple and high-volume files to clients as well as one another throughout the workday. Are there any specific ethical obligations we should be aware of with respect to the technology and working from home? How can our firm ensure that we are using technology safely, effectively and in compliance with our ethical obligations?

Separately and surprisingly, we have reached out to adversaries requesting extensions of deadlines, and one adversary in particular was obstinate refusing to give us an extension, despite the fact that my client was one of the many individuals who had become sick because of the pandemic, forcing us to make an application to the court. Is our adversary's conduct ethical? What principles of ethics should we adhere to when dealing with unreasonable adversaries?

Lastly, given that face-to-face communications are severely limited and individual accessibility is uncertain, what are our ethical obligations with respect to the supervision of subordinate attorneys and staff?

Sincerely,
Patty Partner

DEAR PATTY:

The global pandemic has undoubtedly forced us to steer a course through uncharted professional territory. It has created many professional and ethical challenges as lawyers have been compelled to practice law primarily in a remote work environment.

One of the most fundamental challenges that lawyers face when working from a remote location is the necessity to protect client confidences. As discussed in prior Forums, RPC 1.6 governs a lawyer's duty of confidentiality, and this duty applies in all settings and at all times.

When working at home, it is easy to adopt casual practices. Attorneys should be wary of falling into that trap. Working remotely often creates unique circumstances of having to work in close proximity to other family members. As a result, attorneys must take extra precautions to safeguard client confidences. For example, your "remote office" should be as autonomous as possible. It is best practice to avoid working in commonly used areas of your home such as the kitchen table or the living room.

However, we understand that this might not be feasible in every situation, especially for attorneys with younger children engaging in remote learning. If your circumstances do not permit you to create a designated and private workspace within your home, you should endeavor to set clear boundaries with children, partners and other members of your household as to how they should treat your workspace and work files. You also may want to consider investing in a locked filing cabinet to store sensitive information. If you do not have locked storage, we suggest that you store your work-related materials somewhere only you can access them. Attorneys should also consider practical efforts, such as not letting children or significant others access work devices for personal use and setting up a private, password-protected, Wi-Fi network specifically for your professional work. At a minimum, your work devices (laptops, tablets, phones) should always be password-protected with strong and unique passwords.

We also suggest that you do your best to become "tech-savvy" or competent in the technology you will need when working remotely. The NYSBA Committee on Professional Ethics (the "Committee") has opined that an attorney should only use technology that he or she is competent to use. See NYSBA Comm. on Prof'l Ethics, Op. 1025 (2014). Accordingly, a law firm should take appropriate steps to ensure that its attorneys are familiar with the firm's operating systems and computer programs and the firm's policies concerning the use of those systems/programs before transitioning to a fully remote work environment.

But, that is only half the battle. Attorneys also should be cognizant of the heightened risk of cybersecurity threats when working remotely. Comment [8] to RPC 1.1 states: "to maintain the requisite knowledge and skill, a lawyer should . . . keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information." As addressed in a prior Forum, attorneys and law firms have an ethical obligation to institute and maintain sound cybersecurity protocol, and to ensure that third-party vendors do the same. See Vincent J. Syracuse, Maryann C. Stallone, Richard W. Trotter & Carl F. Regelmann, Attorney Professionalism Forum, N.Y. St. B.J., June 2017, Vol. 89, No. 5.

Phishing scams are an example of a common cybersecurity threat to law firms. These scams include fraudulent emails that appear to be sent from a genuine source, such as a colleague, family member or personal banking institution, for the purpose of obtaining personal information, such as passwords and banking details, and defrauding attorneys or their firms. For this reason, attorneys should be extra vigilant when reviewing emails and downloading files. It is always a best practice to double check the email address of the sender and confirm the email is legitimate, as many hackers will create fake email accounts with only slight variations to that of the individual the hacker is purporting to impersonate. Attorneys also should avoid downloading files or clicking on links from an email that they are not expecting, and immediately bring emails that appear to be suspicious to the attention of the firm's IT department for further investigation.

Furthermore, we recommend that attorneys access their firm networks remotely through a Virtual Private Network (VPN), an encrypted connection over the internet from a device to a network. The encrypted connection

helps ensure that sensitive data is safely transmitted over the internet. Firms should always keep their VPNs current and deploy all patches with updated security configurations. Moreover, it is critical to maintain proper multi-factor authentication for all VPN access to networks.

Cybersecurity threats also arise with the use of cloud-based file-sharing services to send and receive confidential client documents. A 2014 report by the Department of Homeland Security recognized that "online tools that help millions of Americans work from home may be exposing both workers and businesses to cybersecurity risks." Michael Roppolo, Work-from-home remote access software vulnerable to hackers: Report, CBS News (July 31, 2014).

In two ethics opinions issued in 2014, the Committee concluded that giving lawyers remote access to client files was not unethical, as long as the technology used provides reasonable protection to confidential client information, or the law firm informs the client of the risks and obtains informed consent from the client to proceed. See NYSBA Comm. on Prof'l Ethics, Op. 1019 (2014) and NYSBA Comm. on Prof'l Ethics, Op. 1020 (2014). In Opinion 1019, the Committee noted that "because of the fact-specific and evolving nature of both technology and cyber risks, we cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients." Id. However, Comment [17] to RPC 1.6 instructs us that "[t]he key to whether a lawyer may use any particular technology is whether the lawyer has determined that the technology affords reasonable protection against disclosure." RPC 1.6, Comment [17].

To meet the reasonable care standard set forth in RPC 1.6, attorneys should consult with their firm's IT department or service provider to investigate whether their firm's file-sharing services implement reasonable security measures to protect client confidence. Where possible, the firm should implement two-factor authentication to access its work applications and software. If after speaking with your IT provider/personnel you continue to have doubts as to security, you should obtain the client's consent before sharing any files or documents. The failure to employ basic data-security measures can have severe consequences, including civil liability for professional malpractice.

A security measure that law firms should consider implementing to protect client confidences is the encryption of files and emails sent both inside and outside the firm. Encryption is the process of converting digital information into a code, to prevent unauthorized access by outside parties

Additional best practices in addressing cybersecurity risks include: (1) understanding and using reasonable security measures, such as secure internet access methods; when accessing files remotely, attorneys should avoid logging on to unsecured Wi-Fi networks or "hotspots," which can expose both the attorney and the firm's files to malware – software designed by hackers that can infiltrate remote desktops and whose capabilities include logging keystrokes, uploading discovered data, updating malware and executing further malware; (2) training non-lawyer support staff in the handling of confidential client information and to report suspicious activity; (3) clearly and conspicuously labelling confidential client information as "privileged and confidential"; (4) conducting due diligence on third-party vendors providing digital storage and communication technology; (5) creating and implementing a data breach incident response plan; and (6) assessing the need for cyber insurance for data breaches. See ABA Standing Committee on Ethics and Professional Responsibility, Formal Opinion No. 477 (May 2017).

Using secure internet access is of critical importance to avoid a man-in-the-middle attack, or "MITM" attack, which occurs when the communication between two systems is intercepted by a third party, i.e., a Man-in-the-Middle. This can happen in any form of online communication, such as email, web-browsing, and even social media. The MITM can use a public Wi-Fi connection to gain access to your browser, or even compromise your entire device. Once the MITN gains access to your device they have the ability to steal your credentials, transfer data files, install malware, or even spy on the user. To avoid the potentially significant and disastrous effects of a MITM attack, you should work off a secure Wi-Fi network and avoid using "hotspots."

Additionally, when using video-conferencing platforms such as Zoom, make sure that your meetings are password-protected to avoid a type of cyberattack called "Zoom-bombing," where strangers hijack a private Zoom teleconferencing chat and draw offensive imagery onscreen, such as pornographic images, personal information of the individuals in the chat, and even taunting them with hate speech and threats.

Turning to the part of your question regarding the civility (or lack thereof) of your adversary, the pandemic is certainly no excuse for bad behavior. As discussed in a recent Forum, RPC 3.4 governs "fairness to opposing party and counsel" and provides that when dealing with an opposing party and the opposing party's counsel, an attorney must act with fairness and candor. See RPC 3.4; see also Vincent J. Syracuse, Maryann C. Stallone, Carl F. Regelmann & Alyssa C. Goldrich, Attorney Professionalism Forum, N.Y. St. B.J., April 2020, Vol. 92, No. 3. The commentary to Rule 1.2 further provides that in

accomplishing the client's objectives, the lawyer should not be offensive, discourteous, inconsiderate or dilatory. RPC 1.2 Comment [16]. And, while the RPC does not specifically address an attorney adversary's obligations under Rule 3.4 or 1.2 in the wake of a global pandemic, it is axiomatic that lawyers should be particularly sensitive to reasonable requests for extensions under such circumstances.

While your adversary's refusal to grant you a reasonable extension is not a per se violation of the RPC or a basis for a report to the Disciplinary Committee, such conduct may violate the New York State Standards of Civility (the "Standards"), particularly if this is the first time you are asking for an extension on the motion. See 22 N.Y.C.R.R. § 1200, App. A. As discussed in a prior Forum, the Standards of Civility were adopted as a guide for the legal profession, including lawyers, judges and court personnel, and outline basic principles of behavior to which lawyers should aspire. See Vincent J. Syracuse, Maryann C. Stallone & Hannah Furst, Attorney Professionalism Forum, N.Y. St. B.J., March/April 2016, Vol. 88, No. 3.

The language of the Standards of Civility is clear – in the absence of a court order, a lawyer should agree to reasonable requests for extensions of time when the legitimate interests of the client will not be adversely affected. See 22 N.Y.C.R.R. § 1200, App. A. An adversary who refuses to provide a reasonable extension during the global pandemic in order to gain some tactical advantage is not just exhibiting bad form, but is creating a negative reputation and relationship with their adversary that may ultimately adversely affect their position in the litigation. By way of example, an uncooperative attorney is unlikely to get a professional courtesy in the future. Moreover, judges and juries generally do not look kindly upon attorneys that do not extend professional courtesies. In the ordinary course, reasonable requests for extensions of time should be handled by the attorneys in the case, not by the courts.

The flip side to this scenario, which is also likely to occur, is attorneys using the pandemic as an excuse for their dilatory tactics to delay the case and frustrate your client's ability to recover. As is the case with many ethical rules, the deciding factor in whether to grant or deny a request for an extension is the reasonableness of the request.

Separately, your obligations with respect to the supervision of subordinate attorneys remain unchanged. RPC 5.1 sets forth the responsibilities of law firms, partners, and managers over other lawyers. Lawyers serving in a managerial or supervisory role are required to make reasonable efforts to ensure that all attorneys comply with their ethical obligations. This duty becomes even more important in a time of disaster or emergency. See RPC 5.1. Specifically, RPC 5.1(b) requires lawyers with management or direct supervisory authority over other lawyers in the firm to establish internal policies and procedures designed to provide reasonable assurance that all lawyers in the firm will conform to the RPC such as identifying dates by which actions must be taken in pending matters and ensuring that inexperienced lawyers are appropriately supervised. See RPC 5.1, Comment [2].

There are no bright line rules governing supervision. Comment [3] to RPC 5.1 tells us that each law firm should carefully consider the structure and nature of its practice when adopting policies governing the supervision of subordinate attorneys. See RPC 5.1, Comment [3]. For example, if the firm is relatively small and consists of mostly experienced lawyers, informal supervision and periodic review of compliance with the required policies will ordinarily suffice. Conversely, if the firm is much larger, and employs numerous junior attorneys, more elaborate measures may be necessary to place the firm in compliance with RPC 5.1. Id.

The degree of supervision required also varies on a case-by-case basis and is generally judged by what is reasonable under the circumstances. Factors that should be considered include: (i) the experience of the person whose work is being supervised, (ii) the amount of work involved in a particular matter, and (iii) the likelihood that ethical problems might arise while working on the matter. See id.

Generally speaking, it is best practice for supervising attorneys to remain apprised of subordinate attorneys' workload, implement a system for review of the subordinate attorney's work product and ensure that the subordinate attorney understands that system. In our experience, requiring subordinate attorneys to submit weekly status reports detailing the matters they are working on is a good first step to guarantee that no matter falls through the cracks.

Supervising attorneys also should establish an open line of communication with subordinate attorneys. In today's age, there are many mediums that allow for regular communication in this remote work environment, including video conferencing (via Zoom or Skype), telephone calls, email and even text messages. Therefore, in addition to communicating via email, a supervising attorney should schedule regular calls (via Zoom, Skype or telephone) with subordinate attorneys to check on their progress and review and discuss their work product and workload. How often you communicate with the individuals under your supervision will depend on the complexity of the matter and issues, and the upcoming deadlines in those matters. This too is a matter of the lawyer's reasonable judgment and care.

Notably, RPC 5.1(d) articulates a general principle of personal responsibility for acts of other lawyers in the law firm and imposes such responsibility on a lawyer who orders, directs or ratifies wrongful conduct and on lawyers who are partners or who have comparable managerial authority in a law firm who know or reasonably should know of the conduct. See RPC 5.1(d). Thus, lawyers acting in a supervisory or managerial role should be aware that their failure to exercise diligence in reviewing the work of subordinate attorneys may result in personal liability under RPC 5.1(d).

Whether you are working in the office or remotely, attorneys should always use their best efforts so that client communication and diligent representation continues uninterrupted. One of our prior Forums referred attorneys to RPC 1.4, which governs an attorney's obligations with respect to communicating with clients. RPC 1.4 states that attorneys are ethically obligated to promptly comply with reasonable requests for information from clients. RPC 1.4(a)(4); see Vincent J. Syracuse, Maryann C. Stallone & Carl F. Regelmann, Attorney Professionalism Forum, N.Y. St. B.J., July/August 2016, Vol. 88, No. 6. To avoid noncompliance with RPC 1.4 while working remotely, attorneys should inform clients of the best way to reach them. If, for example, an attorney is able to forward calls from the office line to a personal cell phone, the attorney can tell clients that they may still use the office number. If attorneys do not have this ability, they need to advise their clients what alternate number they can be reached at (whether a cell phone number or home landline). In addition, attorneys should regularly check their office voicemail and email and avoid large gaps in response time.

Finally, attorneys must continue to maintain their professionalism and decorum despite working from the comfort of their homes. We have previously talked about the importance of dressing appropriately when appearing in front of a tribunal; proper dress is part of basic professionalism and a sign of respect. See Vincent J. Syracuse & Matthew R. Maron, Attorney Professionalism Forum, N.Y. St. B.J., May 204, Vol. 86, No. 4. That standard still applies when participating in a virtual court conference, as well as video arbitrations and mediations. Judge Dennis Bailey of Broward County Florida recently expressed his dismay that attorneys appeared inappropriately on camera for virtual court hearings: "It is remarkable how many attorneys appear inappropriately on camera," Bailey said. "We've seen many lawyers in casual shirts and blouses, with no concern for ill-grooming, in bedrooms with the master bed in the background, etc. One male lawyer appeared shirtless and one female attorney appeared still in bed, still under the covers. And putting on a beach cover-up won't cover up that you're poolside in a bathing suit. So, please, if you don't mind, let's treat court hearings as court hearings, whether Zooming or not." Debra Cassens Weiss, Lawyers are dressing way too casual during Zoom court hearings, judge says, ABA Journal (Apr. 15, 2020), https://www.abajournal.com/news/article/lawyers-are-dressing-way-too-casual-during-zoom-hearings-judge-says.

As always, the devil is in the details. What is deemed appropriate can be subjective, and there may not always be agreement on what should be worn when in a virtual court or ADR proceeding. Certainly, going shirtless, wearing a bathing suit or video conferencing from your bed is never appropriate. You should use common sense, and when in doubt, it is best to err on the side of caution and overdress to avoid facing the risk of having your choice of clothing overshadow the needs of your client or what you might be saying.

Sincerely,
The Forum by
Vincent J. Syracuse, Esq.
(syracuse@thsh.com)
Maryann C. Stallone, Esq.
(stallone@thsh.com) and
Alyssa C. Goldrich, Esq.
(goldrich@thsh.com)
Tannenbaum Helpern Syracuse & Hirschtritt LLP

QUESTION FOR THE NEXT ATTORNEY PROFESSIONALISM FORUM:

DEAR FORUM:

I am an attorney in private practice focusing on personal injury law here in New York. I also do a bit of matrimonial law. My clients come from underserved communities, and many face extreme financial hardships. I've always known that Rule 1.8(e) prohibits giving financial assistance to clients in connection with a pending litigation and, as much as I have wanted to, I never gave anyone a dime. Rather, over the years, I developed a nice Rolodex with contacts at public service associations to refer these clients to so they could get their needs met. But with all this Covid-19 stuff going on it has gotten way worse and so many have now found themselves without a paycheck and are simply unable to meet their day-to-day needs. The public service organizations have been inundated, and my clients are unable to get desperately needed help. I was recently approached by a client, a young parent of two preschool-aged children, who is unable to buy groceries. And while I know that I probably shouldn't have, I figured that it would be okay to give him a few bucks for a couple of bags of groceries. He's a good kid and I know the money is going to his children. I am concerned I may have done something wrong but it really was so little to me and so much to him. What should I have done?

Sincerely,
Justa Bene Mensch

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.