PROGRAM MATERIALS
Program #3230
February 8, 2022

Vendor Risk Management: What Lawyers Need to Know

- Michelle A. Schaap, Esq. - Chiesa Shahinian & Giantomasi PC
- Ryan M. Beeck, Esq. - Chiesa Shahinian & Giantomasi PC

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

Vendor Risk Management: What Lawyers Need to Know

Michelle A. Schaap, Esq. and Ryan M. Beeck, Esq.

February 2022

CHIESA SHAHINIAN & GIANTOMASI PC

csglaw.com

This outline has been prepared for a presentation regarding vendor cyber risk management. Ms. Schaap and Mr. Beeck are admitted to practice law in the State of New Jersey. This outline is for informational purposes only and is not intended to constitute legal advice. Every matter has specific facts and special circumstances requiring its own analysis by legal counsel. References to websites, resources or publications in this outline are not intended, and should not be interpreted, as an endorsement by the authors of any product or opinion set forth therein. Website and resource addresses are provided for reference only and the authors make no guarantee as to their accuracy or reliability.

Law Firms Are A Growing Target

✓In 2019, we knew of several New Jersey firms that experienced compromise of their systems allowing bad actors to inject rules into their email systems to redirect client traffic.

✓In January, 2020, already five law firms reported that they were victims of the Maze ransomware gang

✓And in 2021, the third party breaches….Microsoft, Solar Winds, Kaseya and others

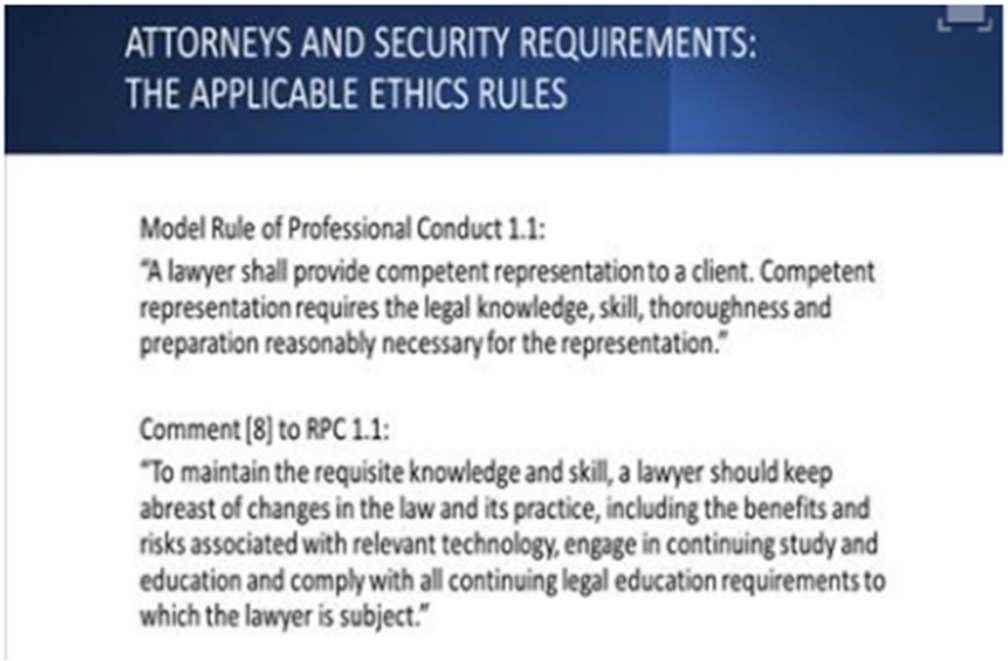
CSG law

Rules Of Ethics That Come Into Play

- Rule 1.1: Duty of Competence
- Rule 1.6: Duty of Confidentiality
- Rule 5.1 and 5.3: Duty of Supervision

CSG law

Client Confidentiality – PRC



ABA Opinion 477R: Securing Communication Of Protected Client Information

- A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken **reasonable efforts** to prevent inadvertent or unauthorized access. However, a lawyer may be required to take **special security precautions** to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

Do You Know What You Don't Know?

- Michael Witt and Nicholas Goldworthy posed the following in the Michigan Bar Journal's March 2021 question:

- "Do I know enough about technology to communicate sensitive information and am I doing enough to uphold my ethical duty to maintain client confidence?"

http://www.michbar.org/file/barjournal/article/documents/pdf4article4127.pdf

Ethical Considerations

- Attorneys have a duty to keep informed of best practices in IT security and how to best protect client data.
- Ethics rules require attorneys to protect client data and their IT infrastructures from bad actors:
  - PRC 1.6 provides:
    (a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).
  - (c) A lawyer shall make **reasonable efforts** to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.
- Some state bar associations have already issued advisory opinions as to whether an attorney violates the duties of confidentiality and competence by using technology which may be susceptible to unauthorized access by third parties

Unintended Consequences….

- PDF redaction tool…. If not used properly can result in disclosure
  - Florida School District with the Parkland Shooter
  - NY Times revealed the name of an NSA agent
- File sharing Sites and the law

In response to a discovery request, plaintiff's counsel sent defense counsel electronic copies of all documents and information it had received from Harleysville, including a copy of the September 22, 2015, email from Cesario to Rowe containing the hyperlink to the Box Site.

Harleysville Insurance Company v. Holding Funeral Home, Inc., Case No. 1:15cv00057, United States District Court, W.D. Virginia, Abingdon Division. February 9, 2017.

NJ Advisory Opinion 701

- The availability of sensitive client documents in an electronic medium that could be accessed or intercepted by unauthorized users … raises issues of confidentiality under RPC 1.6."
- "The obligation to preserve client confidences extends beyond merely prohibiting an attorney from himself making disclosure of confidential information without client consent . . .It also requires that the attorney take reasonable affirmative steps to guard against the risk of inadvertent disclosure."
- The attorney must "*exercise reasonable care*" to guard against unauthorized access
- "when client confidential information is entrusted in unprotected form, even temporarily, to someone outside the firm, it must be under a circumstance in which the outside party is aware of the lawyer's obligation of confidentiality, and is itself obligated, whether by contract, professional standards, or otherwise, to assist in preserving it. . . The touchstone in using "reasonable care" against unauthorized disclosure is that: (1) the lawyer has entrusted such documents to an outside provider under circumstances in which there is an enforceable obligation to preserve confidentiality and security, and (2) use is made of available technology to guard against reasonably foreseeable attempts to infiltrate the data. If the lawyer has come to the prudent professional judgment he has satisfied both these criteria, then "reasonable care" will have been exercised
- Footnote: "In the specific context presented by the inquirer, where a document is transmitted to him by email over the Internet, the lawyer should password a confidential document (as is now possible in all common electronic formats, including PDF), since it is not possible to secure the Internet itself against third party access.

Acting Competently To Preserve Confidentiality

- Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to:
  - the sensitivity of the information
  - the likelihood of disclosure if additional safeguards are not employed
  - the cost of employing additional safeguards
  - the difficulty of implementing the safeguards
  - the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).
- A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule.

➢IF A CLIENT DIRECTS YOU **NOT** TO USE SECURE MEASURES, DOCUMENT IT!

In Addition To The Rules Of Ethics

- Proactive State Laws
  - California Consumer Privacy Act
    - A business that relies on a service provider to process personal information must have a written agreement with the service provider prohibiting the entity from retaining, using, collecting, selling or disclosing the personal information for any purpose (including a commercial purpose) other than performing the services specified in the contract.
- Sectoral Laws
  - Are you a business associate and subject to HIPAA
- What does your website say about vendors?
  - FTC Act Section 5
- Client billing guidelines (have you been designated the “data controller”?)

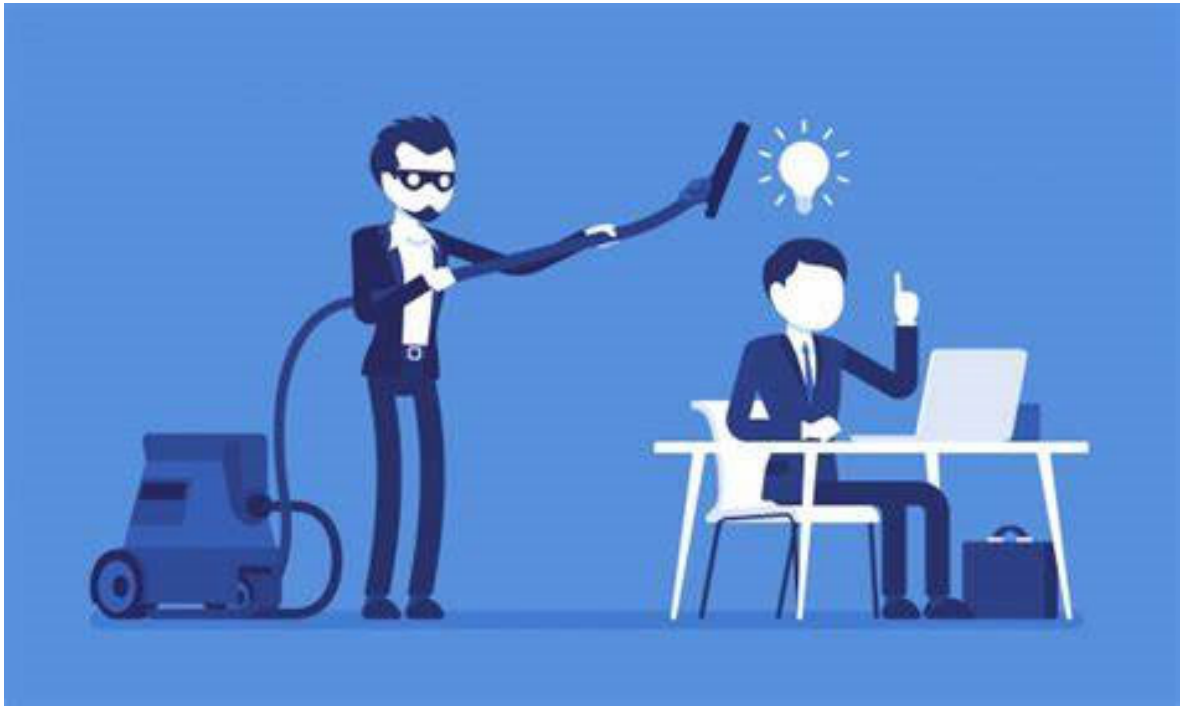
Attorney Vendor Management

- Have a detailed written vendor risk management program that includes:
  - Thorough analysis of the types of data, systems, and environments used and/or accessed by each vendor.
  - Process of vetting vendors, including whether the vendor has suffered any technological or physical breaches of security.
- Vet new *and* existing vendors
- Manage the relationship from onboarding to disengagement
- Maintain an inventory of your vendors

Before Engaging A Vendor

- Ask detailed questions about the vendor's security programs and procedures.
  - Does the vendor back-up its data?
  - Is the data encrypted (at rest and in motion)?
  - What is the training and level of access of the vendor's employees?
  - Does the vendor have written policies, such as a tested incident response plan and disaster recovery plan?
  - Does the vendor conduct annual risk assessments and penetration tests, an annual employee cyber mindfulness training program?
  - Does the vendor implement "least privilege" concepts when assigning access credentials to its personnel to internal and external systems and data.
  - Consider whether SOC 2 reports should be required and/or external certifications should be provided.

Remember that vendors are not just software providers….



Contractual Provisions – Ownership of the Data

- What type of data is being provided to, and/or accessed by, each vendor?
  - Does the vendor truly need the information to carry out its intended function?
- Can the vendor use/repurpose aggregated data?

Assess The Vendor

- SOC Reports (SOC 2, Type II preferred)
- ISO Certification
- Compliance with Sectoral Laws (e.g. HIPAA for health benefit providers)
- PCI-DSS compliance for payment processing vendors
- Third Risk Assessments
- Penetration Tests

Your Vendors Have Been (And May Still Be) Working Remotely, Too!

- Is that work force properly trained?
- Are vendors' personnel using personal devices to access and process your data?
- **Even if you undertook a risk assessment of any given vendor, it probably did not address remote operations.**
- **Risk Assessments are NOT one and done**

You may still be working remotely

- Your vendor may be too….
  - Have they accounted for this in their practices?
- What are there video conferencing polices
  - Are they your video conference provider?....

Contractual Provisions – Confidentiality

- Be wary of standard terms and conditions that allow for disclosure of electronically stored information to third parties well below the standard that attorneys must employ to protect client information.
- ***Example Dropbox:***
  - "*Law & Order*. We may disclose your information to third parties if we determine that such disclosure is reasonably necessary to (a) comply with the law; (b) protect any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or our users; or (d) protect Dropbox's property rights."
- Agreeing to these terms of service could lead to a waiver of the attorney-client and/or work product privileges.
- Vendors should also be required to provide timely notice if they suffer a data breach
  - Timely notification is critical because notification may be required to clients, law enforcement, and/or regulatory agencies.
- Vendors should be required to notify the attorney if they receive a request for data (from a subpoena or otherwise).
  - Attorney can then seek a protective order.

➢ Watch out for user "click through" acceptance

Contractual Provisions – Insurance

- Does the vendor have cyber and/or business interruption insurance.
- Vendor should be required to maintain certain levels of insurance and name the attorney or law firm as an additional insured.
- The amount of coverage should be reviewed periodically!
- Vendor should be required to give notice if more than have of agreed limits are eroded due to a claim in any coverage period.

➢Ask to see policy exclusions

Contractual Provisions – Indemnification and Limits of Liability

- If a breach occurs, who is monetarily responsible for any losses?
  - How are losses/damages defined?
    - Does it include the costs of notifying law enforcement, state regulatory agencies, and impacted persons/entities?
  - What types of damages are excluded?
    - Consequential, incidental, or other special damages.
- Caps on indemnities?

Vetting is an Ongoing Process

- Conduct risk assessments at least once annually to ensure compliance with the agreement and satisfactory technological infrastructure
- Reevaluate the types of data the vendor has and reassess the need for such vendor to have that information.
- Review any risk assessments and penetration tests that were conducted by the vendor
- Require updated insurance certificates
- Require evidence of annual industry-specific certifications

Repeatable and Adaptive

Vendor assessment and management programs should be repeatable and adaptive

Your company is not stagnant!

It expands and grows

Access To Your Data

- Your data is not a bargaining chip
  - Your data should NEVER be held hostage
    - Whether in a contract dispute or otherwise

The End Of The Relationship

- All confidential information should be returned or destroyed.
- If information is in an archive and cannot be returned or destroyed, the vendor should ensure that safeguards are in place to maintain the confidentiality and security of the information, and data will be destroyed in accordance with documented retention/destruction policies.
- If equipment is renting or otherwise sourced, data should be wiped prior to return of the equipment.
- All access credentials, whether technological or physical, should be reset or deactivated

Resources

- National Institute of Standards and Technology www.nist.gov/
- International Standards Organization (www.27000.org)
- CIS Controls
- SANS Institute
- V. Zamora's Illinois Bar Journal Article: "Cloud Cover", 109 Ill. B.J. 30, 2021, Illinois State Bar Association.

In Summary

- Know the rules
- Understand your legal and contractual requirements with regard to clients and vendors
- Vet vendors
- Negotiate contracts
- Ongoing monitoring and assessing
- Data breach response
- Vendor offboarding
- Document your practices

Michelle A. Schaap
Member, Privacy & Data Security and Corporate & Securities Groups

Michelle regularly advises on cybersecurity preparedness, counsels when data security incidents arise and trains companies on best practices for security procedures addressing both their business operations and their customers' concerns. Michelle assesses risk management practices and security incident preparedness in developing proactive security incident response and recovery plans. Additionally, she works with clients in contract review, drafting and negotiation in critical areas of privacy and security.

Michelle counsels clients on incident and breach response – often serving as quarterback to the incident response team, working closely with her client's senior executives, forensics, law enforcement and other critical members of the team.

She is a Certified Information Privacy Professional, awarded from the International Association of Privacy Professionals, with a concentration on U.S. private-sector law (CIPP/US), and recognized by Best Lawyers

Ryan M. Beeck
Associate, Corporate & Securities Group

Ryan M. Beeck is an associate in CSG's Corporate & Securities Group.

Prior to joining the firm, Ryan was a law clerk for the Honorable Joseph L. Yannotti, P.J.A.D., New Jersey Superior Court, Appellate Division.

Ryan earned his J.D. from Rutgers Law School where he was elected to the Order of the Coif, an Executive Editor for the *Rutgers University Law Review*, a student attorney for the Rutgers Community and Transactional Lawyering Clinic and was awarded the Morris Gann Prize in Evidence. During law school, he served as a judicial intern for the Honorable Vicki A. Citrino, J.S.C., of the New Jersey Superior Court. Ryan received his B.A. in Political Science, *cum laude*, from Loyola University Maryland and was a member of the Pi Sigma Alpha Honors Society.

Michelle A. Schaap, Esq.
Member, Privacy & Data Security and Corporate & Securities
Chiesa Shahinian & Giantomasi PC
973.530.2026
mschaap@csglaw.com

Ryan M. Beeck
Associate, Corporate & Securities
973.530.2382
rbeeck@csglaw.com