Cyber Attacks and Ethical Obligations of In-House and Outside Counsel



Speakers:

Daniel B. Garrie, Esq., Co-Founder, Law & Forensics, Mediator, Arbitrator, and e-Discovery Special Master, JAMS

James Vinocur, Partner, Goldberg Segalla

Melanie Phillips, Cybersecurity Associate, Orrick, Herrington & Sutcliffe LLP

Dr. Peter Kamminga, Mediator & Arbitrator, JAMS

(c) 2022 Lexeprint Inc. All Rights Reserved

Speakers



Daniel B. Garrie, Esq.
Co-Founder, Law & Forensics
Mediator, Arbitrator,
and Special Master, JAMS



James Vinocur
Partner
Goldberg Segalla



Melanie Phillips,
Cybersecurity Associate
Orrick, Herrington & Sutcliffe
LLP



Dr. Peter Kamminga,
Mediator & Arbitrator
JAMS

(c) 2022 Lexeprint Inc. All Rights Reserved

Disclaimer

- This is not legal advice, nor should it be considered legal advice.
- This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients.
- This presentation is offered for educational and informational uses only.



(c) 2022 Lexeprint Inc. All Rights Reserved

Agenda

- Overview
- Duty of Competence
- Obligation to Monitor for Data Breach
- Stopping the Breach and Restoring Systems
- Duty of Confidentiality
- Attorneys Obligations to Provide Notice of Data Breach
- Key Takeaways

(c) 2022 Lexeprint Inc. All Rights Reserved



Overview

(c) 2022 Lexeprint Inc. All Rights Reserved



Data Breach Threat

- Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession.
- The data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.

(c) 2022 Lexeprint Inc. All Rights Reserved



Ethical Obligations and Other Statutory Framework

- Each Statutory scheme may have different post-breach obligations, including different notice triggers and different response obligations.
- Attorneys who have experienced data breaches should review all potentially applicable legal response obligations and remember compliance with statutes does not necessarily achieve compliance with ethics obligations.

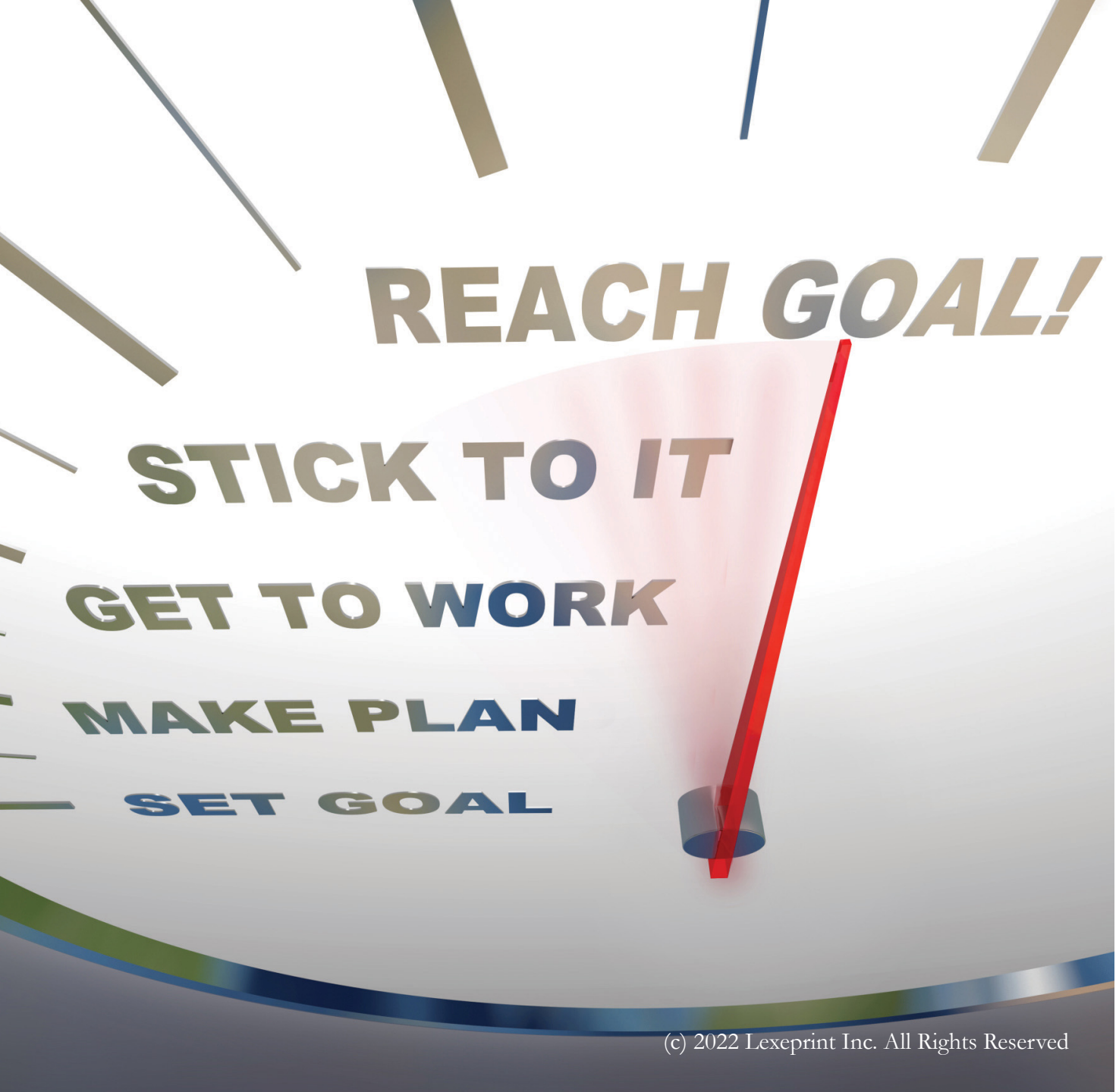
(c) 2022 Lexeprint Inc. All Rights Reserved



Ethical Obligations and Other Statutory Framework

- Compliance with the obligations imposed by the Model Rules of Professional Conduct depends on the nature of the cyber incident, the ability of the attorney to know about the facts and circumstances surrounding the cyber incident, and the attorney's roles, level of authority, and responsibility in the law firm's operations.

(c) 2022 Lexeprint Inc. All Rights Reserved



Duty of Competence

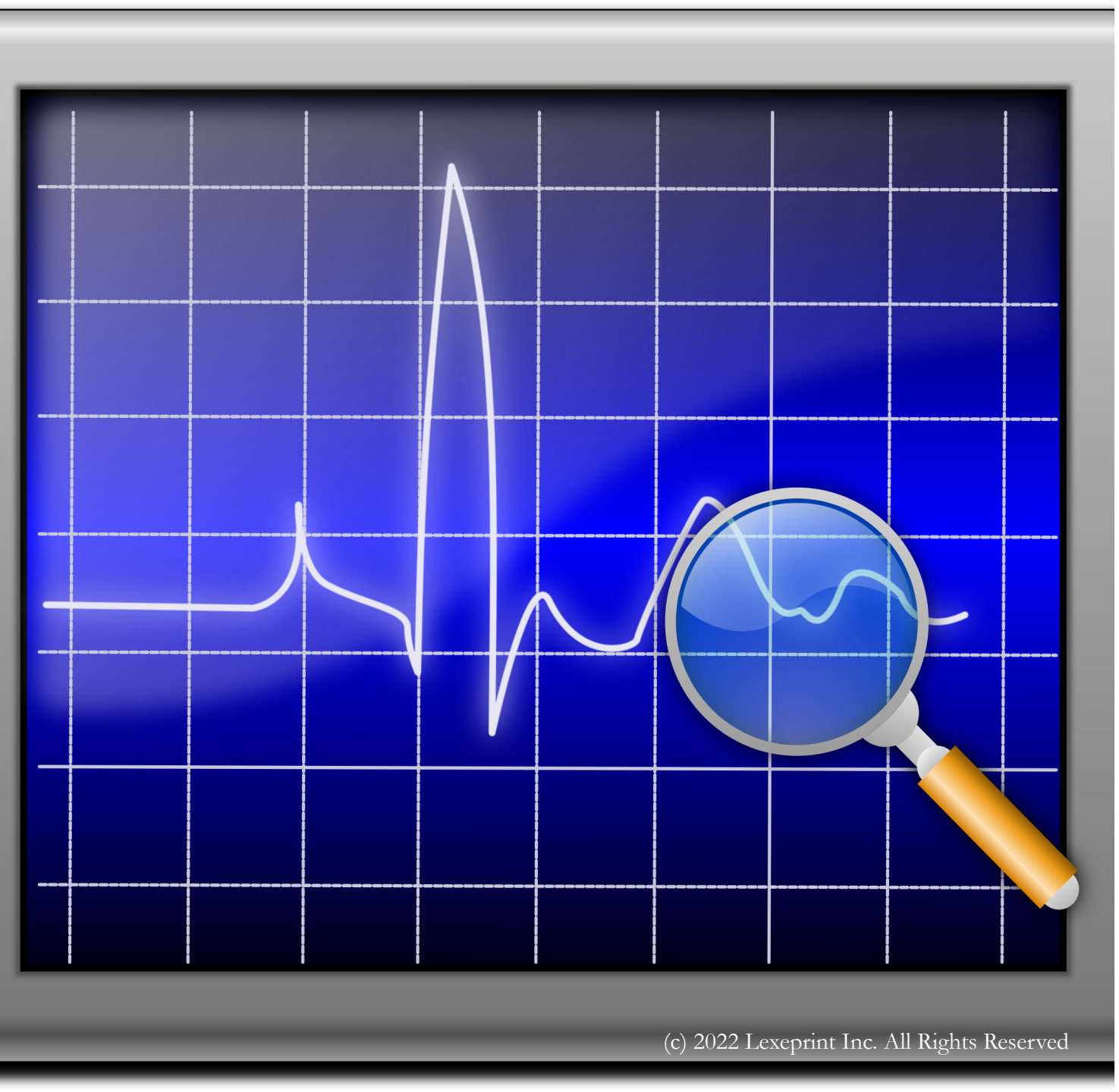
(c) 2022 Lexeprint Inc. All Rights Reserved



Model Rule 1.1- Duty of Competence

- Model Rule 1.1
  - " A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."
- Comment [8]
  - "To 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, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."
- Example: A lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document.

(c) 2022 Lexeprint Inc. All Rights Reserved



Obligation to Monitor for Data Breach

(c) 2022 Lexeprint Inc. All Rights Reserved



Data Breach Definition

- For the purpose of the American Bar Association's (ABA) opinion they defined data breach to be:

  "a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode."

(c) 2022 Lexeprint Inc. All Rights Reserved



Scope of Ethical Violation

- An ethical violation does not necessarily occur if a cyber-intrusion or loss of electronic information is not immediately detected, because cyber criminals might successfully hide their intrusion despite reasonable or extraordinary efforts by the lawyer.
- The potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach.

(c) 2022 Lexeprint Inc. All Rights Reserved



Stopping the Breach and Restoring Systems

(c) 2022 Lexeprint Inc. All Rights Reserved



Incident Response Plans

- When a breach is suspected or detected Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate resulting damage.
- As a matter of best practices lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach.
- Incident response plans help personnel to minimize loss or theft of information and disruption of services caused by incidents.

(c) 2022 Lexeprint Inc. All Rights Reserved



Common Features of Incident Response Plans

- The incident response process should promptly:
  - Identify and evaluate any potential network anomaly or intrusion;
  - Assess if any data or information may have been accessed or compromised;
  - Quarantine the threat or malware;
  - Prevent the exfiltration of information from the firm; eradicate the malware;
  - And restore the integrity of the firm's network;
  - Identify the team members and their backups;
  - Provide the means to reach team members at any time an intrusion is reported;
  - And define roles of each team member.

(c) 2022 Lexeprint Inc. All Rights Reserved



Restoring Service

- Whether or not the lawyer has an incident response plan in place, after taking prompt action to stop the breach, a competent lawyer must make all reasonable efforts to restore computer operations and start servicing the needs of their clients.
- A lawyer can do so on their own, if qualified, or through association with experts.
- Allowing the lawyer an opportunity to evaluate what occurred and how to prevent a reoccurrence. Consistent with obligations under Model Rule 1.6 (c).

(c) 2022 Lexeprint Inc. All Rights Reserved



Post Breach Investigation

- A post- breach investigation requires that the lawyer gather sufficient information to ensure the intrusion has been stopped and then, to the extent reasonably possible, evaluate the data lost or accessed.
- The information gathered in a post-breach investigation is necessary to understand the scope of the intrusion and to allow for accurate disclosure to the client consistent with the lawyer's duty of communication and honesty under Model Rules 1.4 and 8.4 (C).

(c) 2022 Lexeprint Inc. All Rights Reserved



Duty of Confidentiality

(c) 2022 Lexeprint Inc. All Rights Reserved



Model Rule 1.6

- Model Rule 1.6(a)
  - "A lawyer shall not reveal information relating to the representation of a client unless certain circumstances arise."
- Model Rule 1.6(c)
  - "Lawyers must make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client."
    - Comment [18]: The unauthorized access to, or the inadvertent disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

(c) 2022 Lexeprint Inc. All Rights Reserved



"Reasonable Efforts" Definition

- Comment [18] includes nonexclusive factors as a guide for lawyers in making a "reasonable effort"
  - 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, and
  - The extent to which the safeguards adversely affect the lawyer's ability to represent clients.

(c) 2022 Lexeprint Inc. All Rights Reserved



“Reasonable Efforts” in Practice

- These reasonable efforts could include:
  - Restoring technology systems as practical,
  - The implementation of new technology or new systems, or
  - The use of no technology at all if the task does not require it, depending on the circumstances.

(c) 2022 Lexeprint Inc. All Rights Reserved



Scope of Monitoring for Breaches of Client Confidentiality Standard

- The legal standard for "reasonable" security rejects requirements for specific security measures (i.e., firewalls or passwords) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updates in response to new developments.

(c) 2022 Lexeprint Inc. All Rights Reserved



Permitted Disclosure

- Model Rule 1.6 allows a lawyer to reveal information relating to the representation of a client if the lawyer reasonably believes that disclosure:
  - Is impliedly authorized and will advance the interests of the client in the representation, and
  - Will not affect a material interest of the client adversely.

(c) 2022 Lexeprint Inc. All Rights Reserved



Permitted Disclosures Cont.

- In exercising discretion to disclose information to law enforcement about a data breach, a lawyer must consider:
  - Whether the client would object to the disclosure;
  - Whether the client would be harmed by the disclosure; and
  - Whether reporting the theft would benefit the client by assisting in ending the breach or recovering stolen information
- Even then, without consent, the lawyer may disclose only such information as is reasonably necessary to assist in stopping the breach or recovering the stolen information.

(c) 2022 Lexeprint Inc. All Rights Reserved



Attorneys Obligations to Provide Notice of Data Breach

(c) 2022 Lexeprint Inc. All Rights Reserved



Current Clients

- Model Rule 1.4 generally addresses communications between a lawyer and current client. Under this rule, an obligation exists for a lawyer to communicate a data breach to current clients.
- Model Rule 1.4(a)(3)
  - A lawyer "must keep the client reasonably informed about the status of the matter"
- Model Rule 1.4(b)
  - "A lawyer shall " explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."

(c) 2022 Lexeprint Inc. All Rights Reserved



Disclosure of a "Serious Breach"

- The ABA Formal Ethics Committee advised in Opinion 95-398 that under Model Rule 1.4(b) for a "serious breach"
  - A disclosure may be required where the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation.

(c) 2022 Lexeprint Inc. All Rights Reserved



“Serious Breach” Defined

- The committee defined a serious breach as, the misappropriation, destruction or compromise of client confidential information, or a situation where a lawyer’s ability to perform the legal services for which the lawyer was hired is significantly impaired by the event.
- A breach in which the client's interests have a reasonable possibility of being negatively impacted.

(c) 2022 Lexeprint Inc. All Rights Reserved



Former Clients

- Model Rule 1.9 (c) addresses lawyers' duties to former clients.
- When electronic information relating to the representation of a former client is subject to unauthorized access, disclosure or destruction, the Model Rules provide no direct guidance on a lawyer's obligation to notify the client.
- Lawyers should recognize that in the event of a data breach involving former client information, data privacy laws, common law duties of care, or contractual arrangements with the former client relating to records, may mandate notice to former clients of a data breach.

(c) 2022 Lexeprint Inc. All Rights Reserved



Model Rule 1.9(c)

- Model Rule 1.9 (c)
  - "A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter. . . Reveal information relating to the representation except as these Rules would permit or required with respect to a client."

- The rule fails to provide what steps, if any should be taken if such information is revealed.

(c) 2022 Lexeprint Inc. All Rights Reserved



Current Clients Property

- Model Rule 1.15(a) provides that a lawyer shall hold "property" of clients "in connection with a representation separate from the lawyer's own property."
- An open question exists whether Model Rule 1.15's reference to "property" includes information stored in electronic form.
- Jurisdictions that have addressed the issue agree that client files may be maintained in electronic form, with client consent, but that lawyers must take reasonable precautions to safeguard the data under the duty imposed in Rule 1.15.

(c) 2022 Lexeprint Inc. All Rights Reserved



Former Clients Property

- Model Rule 1.6(d) directs that lawyers should return "papers and property" to clients at the conclusion of the representation, which has commonly been understood to include the client's file, in whatever form it is held.
- The rule has also been interpreted as permitting lawyers to establish appropriate data destruction policies to avoid retaining client files and property indefinitely.

(c) 2022 Lexeprint Inc. All Rights Reserved



Minimum Disclosure Requirements

- 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 under Rule 1.4 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.

(c) 2022 Lexeprint Inc. All Rights Reserved



State and Federal Law Obligations

- If personally identifiable information of clients or others is compromised as a result of a data breach, the lawyer should evaluate the lawyer's obligations under state and federal law.
- All fifty states, the District of Columbia, Guam, Puerto Rico, and Virgin Islands have statuary breach notification laws.
- Most breach notification laws specify
  - who must comply with the law,
  - Define “personal information”
  - Define what constitutes a breach, and
  - Provide requirements for notice

(c) 2022 Lexeprint Inc. All Rights Reserved

Key Takeaways

- Conduct regular reviews of your systems and processes to understand where potential risks may lie.
- Conduct regular cyber security awareness training for all employees.
- Create, implement and regularly test an Incident Response Plan.
- Annually review your cyber insurance policy. Review coverage for incidents including; ransomware payments, credit monitoring, business interruption, digital forensic consultants, etc.
- There is no impenetrable shield to completely prevent a cyber-attack. However, firms can and should take all possible steps to make it harder for bad actors to infiltrate.

(c) 2022 Lexeprint Inc. All Rights Reserved



Questions?

(c) 2022 Lexeprint Inc. All Rights Reserved

Contact Us



Daniel B. Garrie
Email: daniel@lawandforensics.com
dgarrie@jamsadr.com
Phone: 855-529-2466
URL: www.lawandforensics.com



Melanie Phillips
Email: mphillips@orrick.com
Phone: (206) 839-4323
URL: https://www.orrick.com/



James Vinocur
Email: jvinocur@goldbergsegalla.com
Phone: (646) 292-8719
URL: https://www.goldbergsegalla.com/



Dr. Peter Kamminga
Email: pkamminga@jamsadr.com
Phone: (212) 607-2758
URL: https://www.jamsadr.com/

(c) 2022 Lexeprint Inc. All Rights Reserved



Daniel B. Garrie, Esq.
Law & Forensics – Co-founder
JAMS – Mediator, Arbitrator, eDiscovery Special Master
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: www.lawandforensics.com

LAW & FORENSICS
A Global Legal Engineering Firm

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie is the Co-Founder of Law & Forensics LLC, Head of Computer Forensics and Cyber Security Practice Groups and has been a dominant voice in the computer forensic and cybersecurity space for over 20 years. Prior to Daniel's legal career, he successfully built and sold several technology start-up companies. Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engineering firms in the industry. Daniel has both a Bachelor's and a Master's Degree in computer science from Brandeis University, as well as a J.D. degree from Rutgers Law School. Daniel has led forensic teams in some of the most visible and sensitive cyber incidents in the United States.

Daniel regularly testifies as an e-discovery, cybersecurity and computer forensic expert witness, authoring forensic expert reports on multi-million-dollar disputes. His ability to perform complex investigations and effectively communicate the results to a jury has made him one of the most sought-after experts in the country. His testimony has been pivotal in a number of cases. Since 2008, Daniel has served as a Neutral and Special Master and in 2016, he joined JAMS as one of the organization's youngest Neutrals. At JAMS, Daniel serves as an Arbitrator, Forensic Neutral, and technical Special Master with a focus on cybersecurity, cryptocurrency, and complex software and technology related disputes.

Daniel is well-published in the cybersecurity space, Editor-in-Chief of the Journal of Law & Cyberwarfare, author of more than 200 articles and books including, "Understanding Software, the Internet, Mobile Computing, and the Cloud. A guide for Judges", published by the Federal Judicial Center. He has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and a thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

(c) 2022 Lexeprint Inc. All Rights Reserved



James Vinocur
Partner – Goldberg Segalla
Contact:
W: (646) 292-8719
E: jvinocur@goldbergsegalla.com
URL: https://www.goldbergsegalla.com/

James E. Vinocur is a highly experienced litigator with more than 10 years of experience handling matters in New York courts. His extensive experience includes data privacy litigation, cyber and white-collar fraud, including institutional and corporate cyber intrusions and theft, international money laundering schemes, business email compromise fraud, international identity theft rings, SIM swapping schemes, and complex cryptocurrency fraud.

Before joining Goldberg Segalla, James spent 12 years at the New York County District Attorney's Office, including as deputy chief of the Cybercrimes and Identity Theft Bureau, where he investigated domestic and international money laundering, financial crimes, corporate theft, and cyber intrusions. During his time at the District Attorney's office, he gained invaluable trial experience, which included taking more than 50 hearings and trials to verdict—including the 1979 murder and kidnapping of Etan Patz—and presenting over 150 cases to the Grand Jury.

James provides thought leadership on current trends and developments in cyber and financial crime both internally and to outside multinational companies, nonprofit organizations, and business groups. He has also authored internal memoranda and policy positions on the application of Fourth and Fifth Amendment law to emerging technologies and cyber-forensic techniques.

Additionally, James spent two years as a special assistant U.S. attorney in the U.S. Attorney's Office for the District of New Jersey, where he investigated and prosecuted an elite foreign target engaged in cybercrimes against businesses in the United States, leading to his arrest and conviction.

(c) 2022 Lexeprint Inc. All Rights Reserved



Melanie Phillips
Cybersecurity Associate – Orrick, Herrington & Sutcliffe LLP
Contact:
W: (206) 839-4323
E: mphillips@orrick.com
URL: https://www.orrick.com/

Melanie Phillips works with clients to create practical solutions for their data collection, management, and security practices.

Melanie advises clients in various critical areas, including incident response planning, incident response, consumer breach litigation, and regulatory enforcement actions. She has worked on cybersecurity incident and data breach investigations for a range of clients, including enterprise-wide network intrusions. Melanie also assists clients with digital crime investigations. With more than a decade of litigation experience, including in key areas of trade secret, employment, and consumer protection matters, she has a holistic understanding of the key drivers of privacy and security in organizations big and small.

Melanie has dedicated countless hours to pro bono work over her career, focused on issues relating to domestic violence. She was awarded the Honorable Benjamin Aranda III Outstanding Public Service Award in 2014 in recognition of her work with the Los Angeles County Bar Association Domestic Violence Clinic. She also earned the Pro Bono Award at Orrick for her outstanding commitment to pro bono work in 2007 relating a complicated VAWA petition on behalf of an Iraqi interpreter working for the United States military.

(c) 2022 Lexeprint Inc. All Rights Reserved



Dr. Peter Kamminga
Mediator & Arbitrator– JAMS
Contact:
W: (212) 607-2758
E: pkamminga@jamsadr.com
URL: https://www.jamsadr.com/

JAMS® Local Solutions. Global Reach.®

Dr. Peter Kamminga, Esq., Ph.D. is a full-time JAMS panelist with more than 20 years of experience as mediator, arbitrator, and resolver of complex disputes in the U.S., Europe and globally. Peter has successfully mediated and co-mediated hundreds of complex civil and commercial disputes involving multiple parties, sophisticated questions of law, global jurisdictional issues and aggregate values of millions or billions of dollars. Years of experience resolving highly technical and complex, bet-the-company cases, have yielded a nuanced acumen in driving to resolution a wide variety of matters often involving cross-border aspects.

He mediates and arbitrates a range of disputes including matters involving professional liability claims against professional service firms and disputes arising from cybercrime, data breaches, computer fraud, hacking, ransomware, and internet scams, and their insurance coverage aspects.

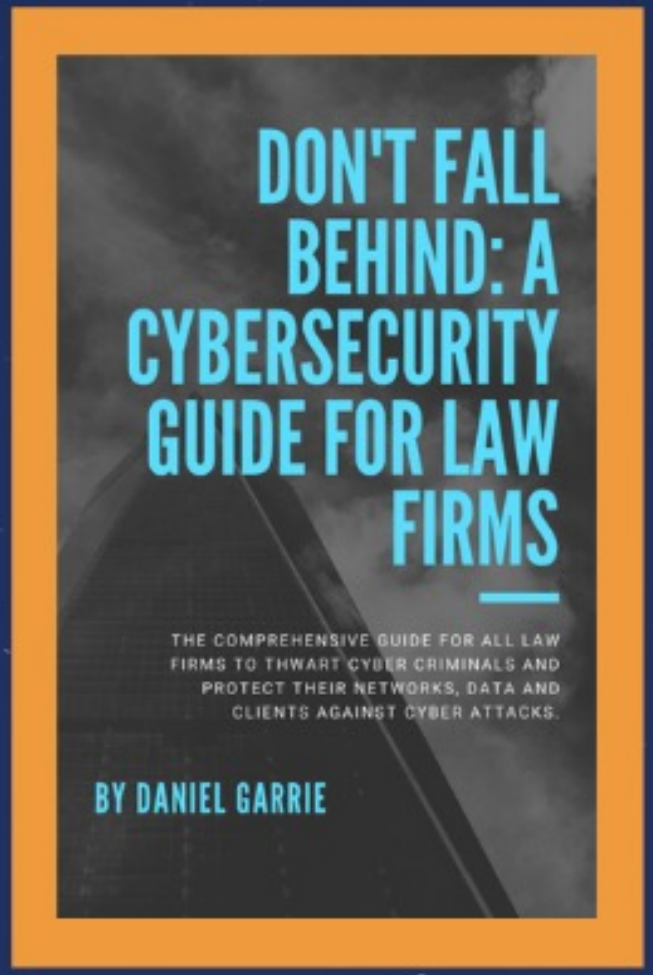
Clients value him for being an "excellent listener" who "can study up on new issues quickly" and is "persistent and able to ask the tough questions and push parties to find solutions that make good legal and business sense."

Educated both in the U.S. and in Europe, Dr. Kamminga is fluent in English, Dutch, French and has an excellent working knowledge of German.

In addition to his full-time work as a neutral, Dr. Kamminga is an associate professor of law and an internationally recognized legal expert and scholar. As a thought leader on ADR and mediation he has initiated ADR initiatives in the U.S. and abroad and frequently speaks for Fortune 500, universities, governments, and other organizations around the world. He has authored several books and dozens of articles on contract law and dispute resolution.

(c) 2022 Lexeprint Inc. All Rights Reserved

A CYBERSECURITY GUIDE FOR LAW FIRMS



"NO ONE IS IMMUNE TO A CYBERSECURITY INCIDENT. EVERY INDUSTRY AND BUSINESS SECTOR—INCLUDING THE LEGAL PROFESSION—IS A TARGET FOR HACKERS AND CYBER CRIMINALS. AS EARLY AS 2009, THE FBI FLAGGED THE LEGAL INDUSTRY AS A GROUP THAT WAS VULNERABLE TO CYBER ATTACKS, ISSUING AN ADVISORY THAT HACKERS WERE INCREASINGLY TARGETING LAW FIRMS."



AVAILABLE ON:

amazonkindle AND PAPERBACK!

Buy Now

(c) 2022 Lexeprint Inc. All Rights Reserved