

Facing Technology: Legal Ethics Developments in 2021 and 2022

Speakers:

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

Hon. Leo M. Gordon, United States Court of International Trade

Elizabeth Rogers, Partner, Michael Best & Friedrich LLP

(c) 2022 Lexeprint Inc. All Rights Reserved.

Speakers



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



Hon. Leo M. Gordon
United States Court of International Trade



Elizabeth Rogers
Partner
Michael Best & Friedrich LLP

(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

- Cyber Attacks on Law Firms
- Ethics Rules
- Bar Associations' Ethics Opinions
- Real-World Examples
- Key Takeaways

(c) 2022 Lexeprint Inc. All Rights Reserved.



Cyber Attacks on Law Firms

(c) 2022 Lexeprint Inc. All Rights Reserved.



The Numbers

- According to PwC Law Firm's Survey in 2020, cyber risk is the second greatest threat to law firms since 2020 after Covid-19.
- An ABA Report from 2020 showed that 29% of law firms reported a security breach, and 36% reported malware infections.
- 71% of the Top 100 firms said they were "somewhat concerned" or "extremely concerned" about cybersecurity threats.
- **The problem is only 22% of Top 100 firms have a Cybersecurity Committee.**

(c) 2022 Lexeprint Inc. All Rights Reserved.



It is Critical that Law Firms Follow Ethical Guidelines

- Law Firms are specific targets for cyber hacks.
- Failure to respond properly to a cyber incident can open a firm to serious ethical issues.
- **Firms are ethically obligated to protect this sensitive data, offering cybercriminals the opportunity for a quick payout**.
- Law firms are also managed by attorneys who usually have little to no background and experience with cybersecurity matters.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Why are Law Firms Major Targets for Cyber Attacks?

- Law firms have money, house valuable, confidential client information, and are usually not prepared for a cyber attack.
- In July 2021, Campbell Conroy & O'Neil announced that their "network was impacted by ransomware, which prevented access to certain files on the system."
- The firm could not confirm whether the bad actors viewed or accessed their client files, however, they did note that the "system included certain individuals' names, dates of birth, driver's license numbers / state identification numbers, financial account information, Social Security numbers, passport numbers, payment card information, medical information, health insurance information, biometric data, and/or online account credentials (i.e., usernames and passwords)."

(c) 2022 Lexeprint Inc. All Rights Reserved.



Security Measures that Firms Should Implement

- As technology continues to evolve, firms must implement robust security measures, as not doing so means easier access to sensitive information for adversaries.
- Law Firms tend to implement weaker security measures, which provides hackers increased accessibility to sensitive information.
- As a result, law firms are increasingly targeted by hackers seeking client information.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Who Attacks Firms?

- There is a wide variety of hackers with their own skill-sets and motivations
- Examples of distinct groups include:

1. Nation States
2. Non-state organizations, including criminal enterprises, terrorist groups, and sophisticated hacker communities
3. "Lone-wolf" hackers and insiders.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Firm Liability

- Law firms may be increasingly liable for client's damages resulting from a cyber attack.
- Statutes can vary widely from state to state on issues such as notification to law enforcement, and Congress has yet to pass a national data breach notification law.
- This means law firms and other businesses that possess private client information on firm networks must be prepared to meet the data breach notification requirements of any jurisdiction in which they do business, including internationally.

(c) 2022 Lexeprint Inc. All Rights Reserved.



ABA 2021 Report on Cybersecurity

- The ABA produced a 2021 Legal Technology Survey Report that 'explores security threats and safeguards that reporting attorneys and their law firms are using to protect against them.'
- Some key takeaways from the report:

1. Consequences of data breaches included: downtime/loss of billable hours (36 %); consulting fees for repair (31 %); destruction or loss of files (13 %); replacement of hardware/software (18 %).
2. 24% of firms noted that they had to notify a client or clients of the breach.
3. 42% of firms noted that they had cyber liability insurance.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Ethics Rules

(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."

(c) 2022 Lexeprint Inc. All Rights Reserved.

Example

A lawyer would have difficulty providing competent legal services in today's environment without knowing how to efficiently use email or create an electronic document.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Model Rule 1.4 - Communications

- Model Rule 1.4(a)(3)
  - "A lawyer shall keep the client reasonably informed about the status of the matter."
- Model Rule 1.4(a)(4)
  - "A lawyer shall promptly comply with reasonable requests for information."
- 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.



Model Rule 1.4 - Communications

- Comments:
  - [1]: Reasonable communication between the lawyer and the client is necessary for the client effectively to participate in the representation.
  - [4]: When a client makes a reasonable request for information, however, paragraph (a)(4) requires prompt compliance with the request.
  - [5]: The client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued, to the extent the client is willing and able to do so.
  - [7]: In some circumstances, a lawyer may be justified in delaying transmission of information when the client would be likely to react imprudently to an immediate communication...A lawyer may not withhold information to serve the lawyer's own interest or convenience or the interests or convenience of another person.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Model Rule 1.6 – Confidentiality of Information

- 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 non-exclusive 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.
- Comment [19]
  - When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients.
  - This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Model Rule 1.9 (c) – Duties to Former Clients

- 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.



Model Rule 4.4 – Respect for Rights of Third Person

- Model Rule 4.4(b)
  - "A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender."
    - Comment [2]: Paragraph (b) recognizes that lawyers sometimes receive a document or electronically stored information that was mistakenly sent or produced by opposing parties or their lawyers… If a lawyer knows or reasonably should know that such a document or electronically stored information was sent inadvertently, then this Rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures."
    - Comment [3]: Some lawyers may choose to return a document or delete electronically stored information unread, for example, when the lawyer learns before receiving it that it was inadvertently sent.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Bar Associations' Ethics Opinions

(c) 2022 Lexeprint Inc. All Rights Reserved.



"Cloud computing" while keeping client information confidential

- "Cloud computing" is where remote servers are networked so data storage can be shared within large groups. Lawyers need to take reasonable precautions and must ensure that there is "adequate access" to the client's information where it is stored remotely, the service provider has "adequate security," and the confidentiality of the client's information is maintained.
- Florida Bar Ethics Opinion 12-3 (2013).

(c) 2022 Lexeprint Inc. All Rights Reserved.



Using the Internet as a Means to Transmit Information Relating to the Representation of a Client

- Under Model Rule 1.1, a lawyer has a duty to understand the "benefits and risks associated with relevant technology."
- Model Rule 1.6(c) states that a lawyer must make "reasonable efforts" to prevent unauthorized access or disclosure of a client's information.
- Under Model Rule 1.4, a lawyer may be required to inform the client of security safeguards. A lawyer can use the internet to transmit client information as long as reasonable efforts were made to prevent unauthorized access to said information.
- American Bar Association Formal Opinion 477R (2017).

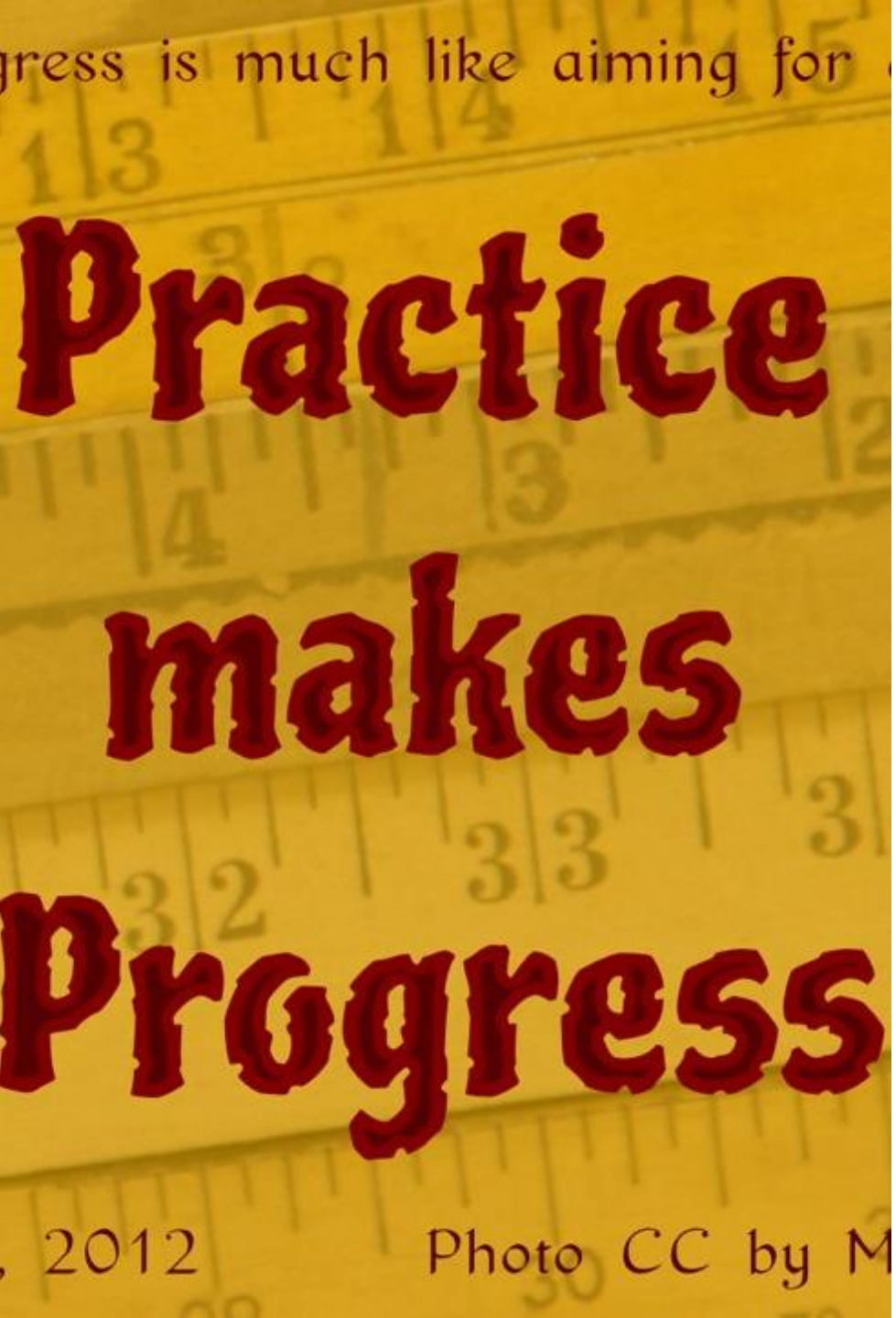
(c) 2022 Lexeprint Inc. All Rights Reserved.



Lawyer's Obligations After an Electronic Data Breach or Cyberattack

- "Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers. In one highly publicized incident, hackers infiltrated the computer networks at some of the country's most well-known law firms, likely looking for confidential information to exploit through insider trading schemes. Indeed, 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."
- ABA Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 17, 2018)

(c) 2022 Lexeprint Inc. All Rights Reserved.

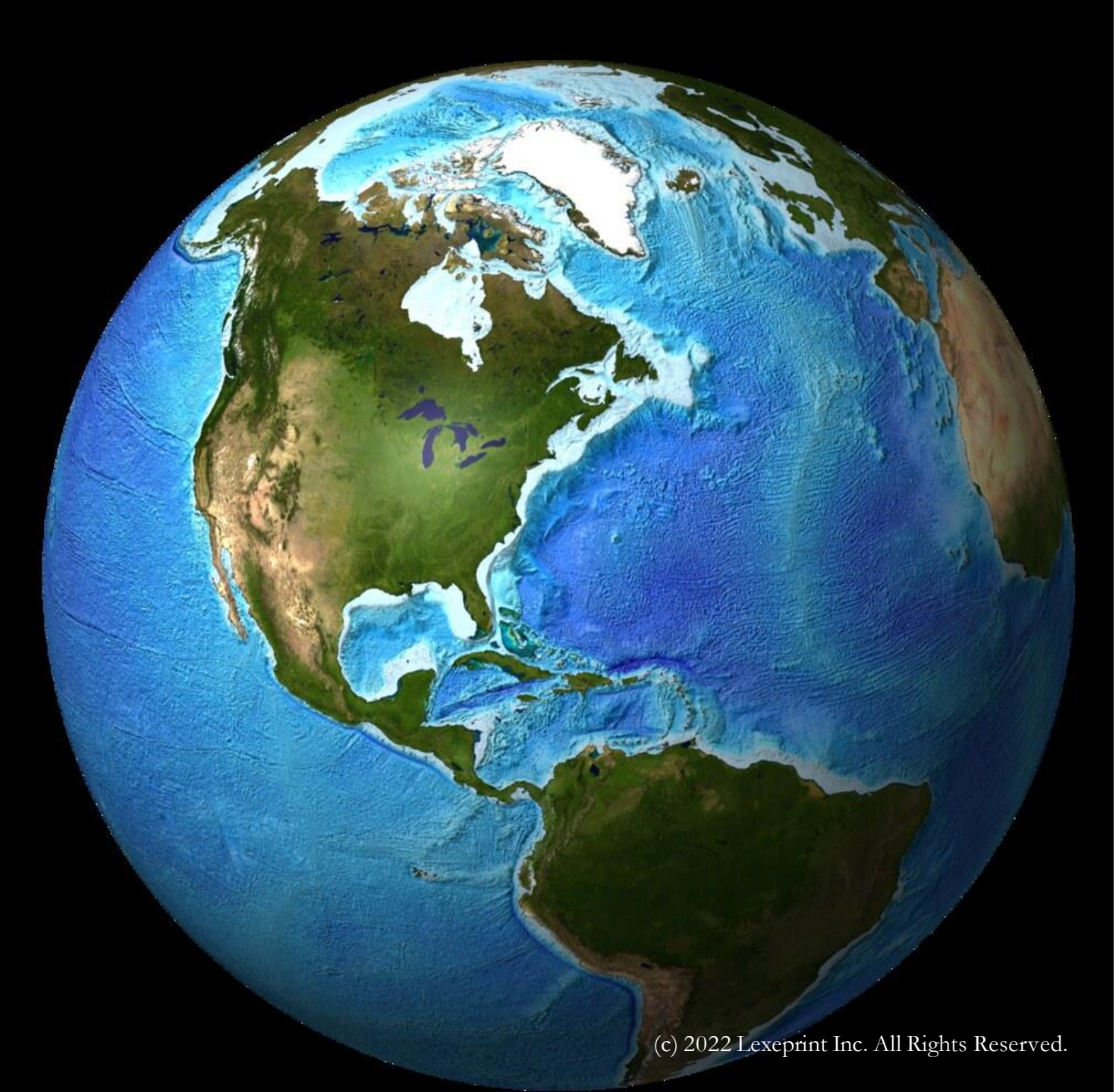


Virtual Practice

- The opinion states that "...w*hen practicing virtually, lawyers must particularly consider ethical duties regarding competence, diligence, and communication, especially when using technology. In compliance with the duty of confidentiality, lawyers must make reasonable efforts to prevent inadvertent or unauthorized disclosures of information relating to the representation and take reasonable precautions when transmitting such information. Additionally, the duty of supervision requires that lawyers make reasonable efforts to ensure compliance by subordinate lawyers and nonlawyer assistants with the Rules of Professional Conduct, specifically regarding virtual practice policies."*
- Attorneys have ethical and common law duties, and contractual and regulatory duties that require them to take competent and reasonable measures to safeguard information relating to clients.

- ABA Formal Opinion 498 (February 2021)

(c) 2022 Lexeprint Inc. All Rights Reserved.



Real-World Examples

(c) 2022 Lexeprint Inc. All Rights Reserved.



Targeted Attacks are Increasing

- Last year, 80% of law firms reported phishing attempts. (InfoSecurity North America)
- The FBI has reported that law firms are often viewed as "one-stop shops" for attackers (with information on multiple clients), and it has seen hundreds of law firms being increasingly targeted by hackers. (American Bar Association)
  - Law firm breaches have ranged from simple (like those resulting from a lost or stolen laptop or mobile device) to highly sophisticated (like the deep penetration of a law firm network, with access to everything, for a year or more).

(c) 2022 Lexeprint Inc. All Rights Reserved.



Seyfarth Shaw LLP & Fragomen, Del Rey, Bernsen & Loewy LLP

- Both BigLaw firms announced security incidents, involving a malware attack that risked clients' sensitive information.
- In the Seyfarth case, the ransomware attack involved criminals freezing the victims out of the network and demanding payment to restore access. The firm reported it had restored all critical systems and that no client/firm data was accessed.
- In the Fragomen data breach, an "unauthorized third party" gained access to a file with the employment eligibility data of Google staffers. This breach was most likely caused by credential compromise rather than malware.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Cadwalader, Wickersham & Taft

- This firm issued a notice that stated that one of its third-party vendors, TBG West Insurance, suffered a ransomware attack on March 27, 2020.
- What happened?
  - The attack encrypted files within its system.
  - In July 2020, the vendor informed Cadwalader that some of its current and past employee social security numbers might have been exposed.
  - However, the firm also stated that "the vendor breach did not impact their firm's systems or any client data.
- What was the result?
  - In the end, the vendor "paid the ransom to regain access to their data."
- What did the vendor and firm do?
  - The vendor made changes that would boost their security
  - All residents that were potentially affected were sent notices by July 30, 2020.
  - Additionally, Cadwalader noted that they were evaluating their own assessments of vendor security in response to the attack.

(c) 2022 Lexeprint Inc. All Rights Reserved.

Key Takeaways

- Reasonable diligence to secure the confidentiality of confidential client information should be practiced by lawyers working remotely.
- Portable electronic devices should not contain client information, or the devices should be able to be remotely deactivated and scrubbed.
- The laws of the jurisdictions in which you practice, and your clients do business should be consulted.
- “Different states may vary in their interpretation of lawyers' professional responsibilities regarding data breaches.”

(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



Hon. Leo M. Gordon
Email: leo_gordon@cit.uscourts.gov
URL: htt https://www.cit.uscourts.gov



Elizabeth Rogers
Email: earogers@michaelbest.com
Phone: (512) 640-3164
URL: https://www.michaelbest.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, cyrptocurrency, 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.

© 2022 Lexeprint Inc. All Rights Reserved.



Hon. Leo M. Gordon
United States Court of International Trade
Contact:
E: leo_gordon@cit.uscourts.gov
URL: https://www.cit.uscourts.gov

Judge Leo M. Gordon has served as a judge of the United States Court of International Trade since March 2006. Judge Gordon is responsible for resolving judicial disputes involving challenges to the administration and enforcement of the federal customs and international trade laws by principally U.S. Customs and Border Protection, the U.S. Departments of Commerce, Agriculture, and Labor, and the U.S. International Trade Commission. In addition to his judicial duties, Judge Gordon has chaired, at different times, the Court's Rules, Budget, Public Affairs/Education, and Strategic Planning Committees. Judge Gordon began his career in 1977 as Assistant Counsel at the Subcommittee on Monopolies and Commercial Law, Committee on the Judiciary, U.S. House of Representatives. In that capacity, Judge Gordon was the principal attorney responsible for the Customs Courts Act of 1980 that created the U.S. Court of International Trade. He also had responsibilities involving a wide range of antitrust and other commercial law legislative projects.

Judge Gordon is a member of the Board of Directors for the Federal Judges Association ("FJA"), serves on its Executive Committee, and co-chairs the Association's Benefits Committee. Judge Gordon is also a member of the Board of Directors for the Federal Judges Association ("FJA"), serves on its Executive Committee, and co-chairs the Association's Benefits Committee.

Judge Gordon is a Fellow (Miembro de Numero) of the International Customs Law Academy ("ICLA"). He has addressed the annual meeting of the ICLA in 2012 in Cancun, Mexico speaking on the "Resolution of Customs Disputes in the United States in the Digital Age," and in 2014 in New York speaking on "The U.S. Court of International Trade and Its Role in U.S. Customs Law." Judge Gordon is also a Director of the Academia de Intercambio y Estudios Judiciales ("AIEJ") (The Academy for the Interchange and Study of Judicial Matters) based in Buenos Aires, Argentina. Since 2013, he has conducted several judicial training programs for AIEJ in the United States and Argentina. He also played a principal role in the development of AIEJ's training program for 2017 and 2018.

Judge Gordon attended the University of North Carolina – Chapel Hill, graduating Phi Beta Kappa. He received a J.D. degree from Emory University School of Law. Judge Gordon is a member of the New Jersey, Georgia, and District of Columbia Bars.



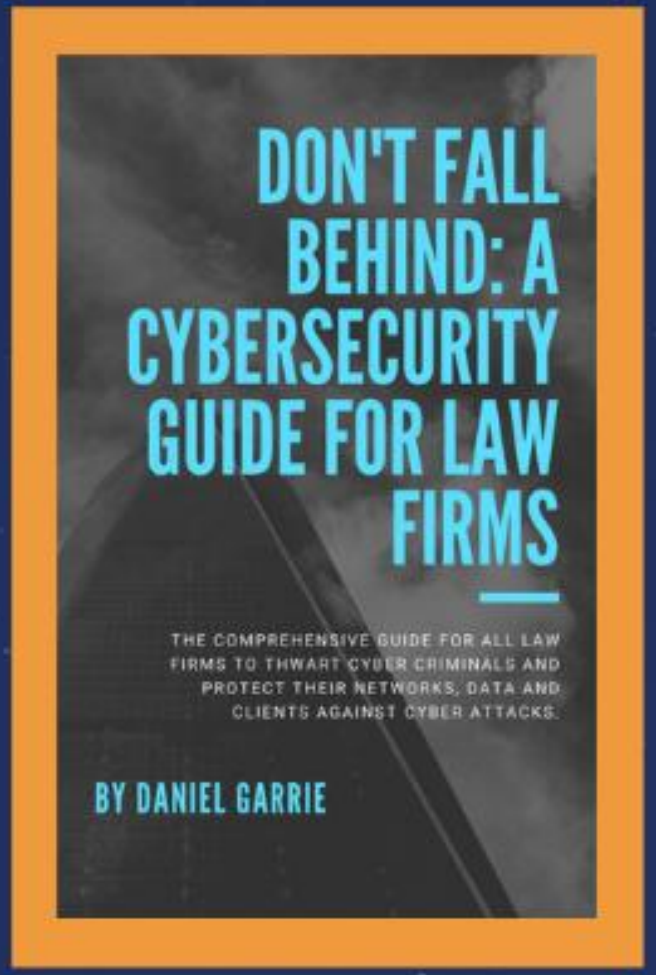
Elizabeth Rogers
Michael Best & Friedrich LLP – Partner
Contact:
E: earogers@michaelbest.com
W: (512) 640-3164
URL: https://www.michaelbest.com/

Elizabeth focuses on issues including breach responses, privacy risk assessments, and enterprise-wide cybersecurity compliance frameworks across industries such as retail, health care, financial services, retail electric providers, education, and state and local governments. She devotes a significant portion of her practice to the energy sector, leading an internal cross-team of energy and cybersecurity attorneys, to assist the firm's clients in the utility industry with their unique cybersecurity concerns.

During her tenure with Texas state government, Elizabeth worked with executive leadership and other stakeholders to develop the state's first official privacy division. In her role as Chief Privacy Officer, Elizabeth provided practical compliance counsel on cybersecurity and privacy requirements, served on the breach response team, and created and implemented policies, procedures, and employee privacy and security awareness training.

Outside of her law practice, Elizabeth teaches cybersecurity and privacy law topics for the University of Texas School of Information's Master's Program in Identity Management and Security. She is a thought leader on privacy and cybersecurity matters facing businesses, and frequently speaks and is published on emerging trends in these areas.

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.