Best Cybersecurity Practices for Boards



Speakers:

Daniel B. Garrie, Esq., Founder, Law & Forensics; Neutral, JAMS; Adjunct, Harvard

Jennifer Deutsch, Director, Cybersecurity and Privacy, Law and Forensics

(c) 2023 Lexeprint Inc. All Rights Reserved

This Photo by Unknown author is licensed under CC BY-SA

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, as spoken and do not reflect those of their employers or clients.



This presentation is offered for educational and informational uses only.



Soliciting speakers is strictly prohibited.

(c) 2023 Lexeprint Inc. All Rights Reserved.

Speaker



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



Jennifer Deutsch
Director,
Cybersecurity and Privacy
Law and Forensics

(c) 2023 Lexeprint Inc. All Rights Reserved

Agenda

- Cyber Risk Landscape
- Attorney Role in Cyber Risk Management and Incident Response
- Regulatory Guidance and Requirements: SEC & FTC
- Prevention Over Cure: Cyber Risk Assessment

(c) 2023 Lexeprint Inc. All Rights Reserved.



Cyber Risk Landscape

(c) 2023 Lexeprint Inc. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-ND

What is a data breach?

- A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve Personally Identifiable Information (PII), trade secrets or intellectual property.

*National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*

(c) 2022 Lexeprint Inc. All Rights Reserved


This Photo by Unknown Author is licensed under CC BY-ND

What is a cyber attack?

- Deliberate action to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks.

**National Research Council*

(c) 2022 Lexeprint Inc. All Rights Reserved



Questions To Consider When Assessing Threat of a Data Breach

- Threats – Who is attacking?
- Vulnerabilities – What weaknesses can be attacked?
- Impacts – What the attack does – what is the financial damage of any breach?
- Value – What is the value of the data to the business, or does it contain PII?

(c) 2022 Lexeprint Inc. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-NC

What is Cybersecurity?

- Cybersecurity is the act of protecting information and communications technology (ICT) systems and their contents.
- A broad and arguably somewhat fuzzy concept, cybersecurity can be a useful term but tends to defy precise definition. It usually refers to one or more of three things:
  - A set of activities and other measures intended to protect—from attack, disruption, or other threats—computers, computer networks, related hardware and devices software and the information they contain and communicate, including software and data, as well as other elements of cyberspace.
  - The state or quality of being protected from such threats.
  - The broad field of endeavor aimed at implementing and improving those activities and quality.

(c) 2022 Lexeprint Inc. All Rights Reserved



What are some weapons?

- Social Engineering
- Unpatched Vulnerabilities
- Bypassing Security
- Denial of Service Attacks (DoS)
- Group Phishing
- Spear Phishing
- Viruses/Worms
- Trojan Horse
- Zero Day Exploit
- Website Exploit
- Spyware, Malware, Ransomware

(c) 2023 Lexeprint Inc. All Rights Reserved



Legal, Business, and Technical Issues to Consider at the Board Level

(c) 2022 Lexeprint Inc. All Rights Reserved



Board Duties

- Board duties generally fall within seven categories:
  - Governance
  - Strategy
  - Risk
  - Talent
  - Compliance
  - Culture
  - Insurance
- With respect to cybersecurity, the board's duties in each of these categories play a critical role in effective oversight of the cybersecurity program.

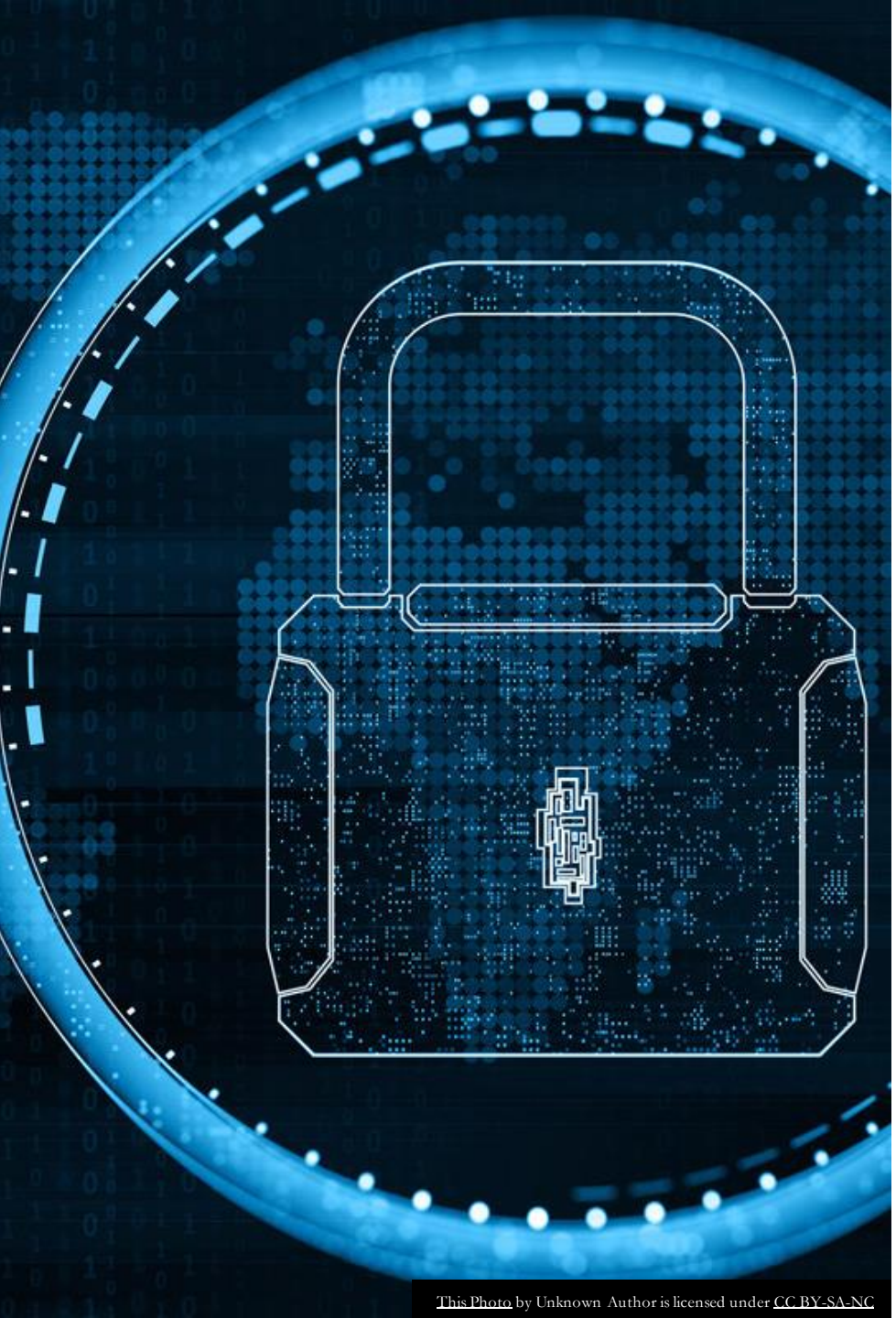
(c) 2022 Lexeprint Inc. All Rights Reserved



Cyber Risk Mitigation Model for the Board of Directors

- HR & Compliance
  - Provide training and education
- Business Units/Operations
  - Implement and drive conformance with the cyber strategy
- Government Affairs & Communications
  - Help shape policy (including crisis management plan) and assure good communications with regulations
- Finance
  - Assure maximum efficiencies with limited dollars
- Internal Audit & Compliance
  - Assure accountability and effective systems and controls

(c) 2022 Lexeprint Inc. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-SA-NC

Cyber Risk Mitigation Model for the Board of Directors

- Acquisitions & Growth
  - Adopt strategies to decrease risks in entering into new markets
- Procurement
  - Protect against third party intrusions
- Legal/Regulatory & Privacy
  - Assure compliance with applicable cyber and privacy laws
- IT & Security
  - Evaluate cyber risks and drive implementation of cyber strategy and ERM

(c) 2022 Lexeprint Inc. All Rights Reserved



Board Compliance

- In general, boards rely on the general counsel, internal audits and ERM, among other functions, to provide independent risk assessments and to confirm risk management processes are in place.
- For the foreseeable future, cyber risks are potentially more consequential than other enterprise-significant risks.
- It is important that the general counsel, internal audits and ERM give cybersecurity a high priority. Boards should undertake regular, proactive discussions with these functions to ensure their leaders recognize that cyber risk is dynamic and requires continuous external screening for new forms of threat mitigation.

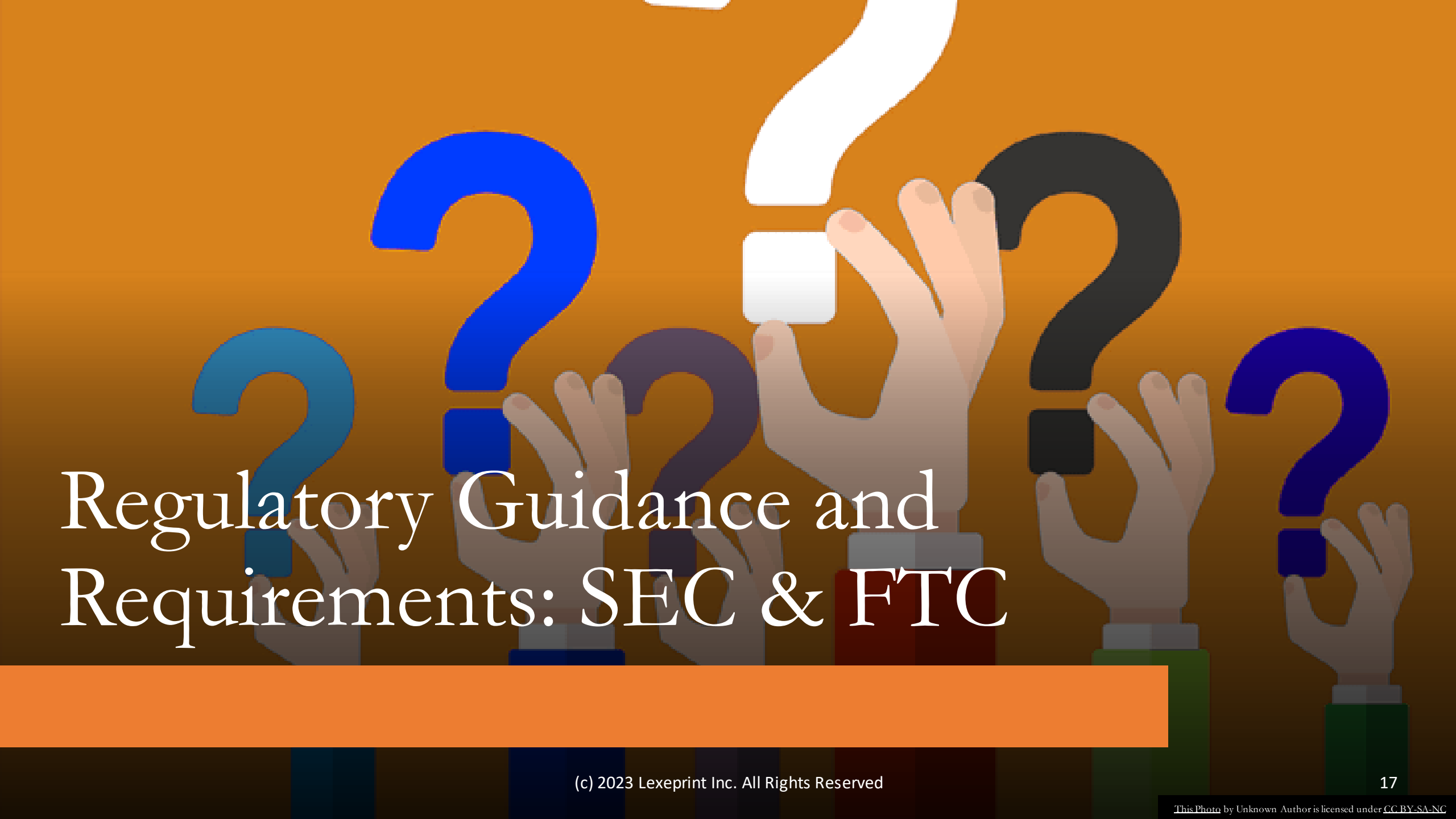
(c) 2022 Lexeprint Inc. All Rights Reserved



Potential Impacts And Possible Implications For The Board

- Loss of IP
- Regulatory Risk
- Reputational Risk
- Legal expenses

(c) 2022 Lexeprint Inc. All Rights Reserved



Regulatory Guidance and Requirements: SEC & FTC

(c) 2023 Lexeprint Inc. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-SA-NC


This Photo by Unknown Author is licensed under CC BY

SEC on Board Responsibility

The SEC has stated:

- A director is expected to attend the Company's annual meeting of members. A director who is unable to attend any meeting (which it is understood will occur on occasion) is expected to notify the Chairman of the Board or the Chairman of the appropriate committee in advance of such meeting. In addition, directors are expected to act in the best interests of the Company, maintain independence and integrity, develop and maintain a sound understanding of the Company's strategies, industries and businesses, review management development and succession planning, endeavor to be available on reasonable notice, attend and prepare for meetings, and provide active, objective and constructive participation at meetings of the Board and its committees.

(c) 2022 Lexeprint Inc. All Rights Reserved



SEC 2020 Cybersecurity and Resiliency Observations

The following guidelines were released by the Office of Compliance Inspections and Examinations:

- **Senior Level Engagement.** Devoting appropriate board and senior leadership attention to setting the strategy of and overseeing the organization's cybersecurity and resiliency programs.
- **Risk Assessment.** Developing and conducting a risk assessment process to identify, manage, and mitigate cyber risks relevant to the organization's business. This includes considering the organization's business model, as part of defining a risk assessment methodology, and working to identify and prioritize potential vulnerabilities, including remote or traveling employees, insider threats, international operations and geopolitical risks, among others.
- **Policies and Procedures.** Adopting and implementing comprehensive written policies and procedures addressing the areas discussed below and identified risks.

(c) 2023 Lexeprint Inc. All Rights Reserved



SEC 2020 Cybersecurity and Resiliency Observations

- **Testing and Monitoring.** Establishing comprehensive testing and monitoring to validate the effectiveness of cybersecurity policies and procedures on a regular and frequent basis. Testing and monitoring can be informed based on cyber threat intelligence.
- **Continuously Evaluating and Adapting to Changes.** Responding promptly to testing and monitoring results by updating policies and procedures to address any gaps or weaknesses and involving board and senior leadership appropriately.
- **Communication.** Establishing internal and external communication policies and procedures to provide timely information to decision makers, customers, employees, other market participants, and regulators as appropriate.

(c) 2023 Lexeprint Inc. All Rights Reserved


This Photo by Unknown author is licensed under CC BY-NC.

2023 Proposed Cybersecurity Rules

- On March 15, 2023, the SEC published long-anticipated proposed cybersecurity and consumer information protection rules.
- The SEC stated that the proposed amendments would:
  - Address the cybersecurity risks for 'Market Entities,'
  - Enable the U.S. securities markets, which part of the critical infrastructure Financial Services Sector, to mitigate risk from cyber incidents through protective measures.

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-NC.

Structure of 2023 Proposed Cybersecurity Rules

- The proposal is threefold:
  - An Amendment to Regulation S-P,
  - Proposed Rule 10, and
  - Amendments to Regulation Systems Compliance and Integrity (SCI).
- In according with its rulemaking process, the public comment periods for the proposals will remain open for 60 days after they are published in the Federal Register.

(c) 2023 Lexeprint Inc. All Rights Reserved.

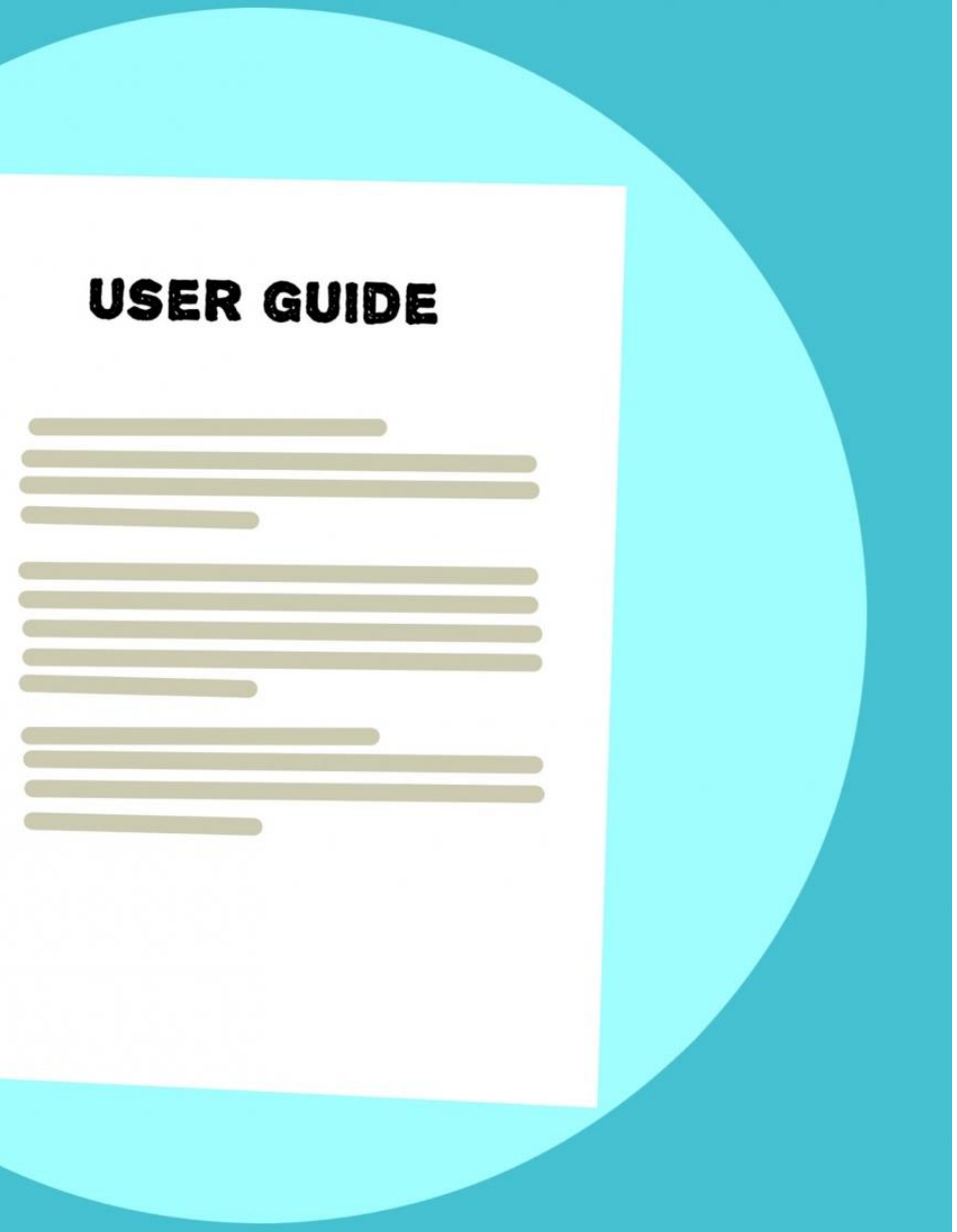


FTC's Health Breach Notification Rule

- The FTC Breach Notification Rule for Electronic Information (16 CFR Part 318) "requires vendors of personal health records and related entities to notify consumers following a breach involving unsecured information."
- Service providers to one of these vendors experiencing a data breach must notify the entity which must then notify consumers.

**Federal Trade Commission, Legal Library*

(c) 2023 Lexeprint Inc. All Rights Reserved.



FTC Data Breach Response Guidance

- The FTC provides the "Data Breach Response: A Guide for Business" in its Business Guidance Resources.
- The key elements of the guidance include
  - Secure operations,
  - Fix vulnerabilities,
  - Notify appropriate parties, and
  - Model letter for informing individuals whose information has been stolen.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Essential Questions for the Board

(c) 2022 Lexeprint Inc. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-SA-NC



What to Ask Fellow Board Members?

- General Questions
  - Does your insurance cover the Board if there is a cyber - attack?
  - Does your insurance cover the C-Suite if there is a breach?
  - Is there a Board committee assigned to address cybersecurity?
- Technology Specific Risks
  - Who has board ownership of the operational management of IT?
  - Are you confident that the organization has identified the key systems and information assets and assessed their vulnerability to attack?

(c) 2022 Lexeprint Inc. All Rights Reserved



What to Ask Fellow Board Members?

- Operational Cyber Risks
  - Do the outsourced providers and contractors have controls and policies in place and do they align with our company's expectations?
  - Is there a written security policy which is supported by regular testing and training?
  - Are you confident employees understand and follow this?

(c) 2022 Lexeprint Inc. All Rights Reserved



What to Ask the C-Suite?

- CISO and CIO
  - How confident are you that your organization's most important systems and information are being properly managed?
  - How confident are you they can withstand cyberattacks from internal and external actors?
  - Does your IT strategy adequately reflect cyber risk?

(c) 2022 Lexeprint Inc. All Rights Reserved


This Photo by Unknown Author is licensed under CC BY-SA

What to Ask the C-Suite?

- CFO and General Counsel
  - Is legal involved in the incident response plan?
  - Do you know who your incident response vendor?
  - Do you know who your contact is with the federal and local law enforcement?
  - Have you identified your publication relations/crises management firm?
  - Do you have a law firm retained?
  - Does your company have cyber insurance?
- Everyone
  - Do you have a full and accurate picture of the impact on your organization following a successful cyber-attack, from a financial, operational, and reputational perspective?

(c) 2022 Lexeprint Inc. All Rights Reserved



Prevention Over Cure: Cyber Risk Assessment

(c) 2023 Lexeprint Inc. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY

Framework for Cybersecurity

- In 2018, the National Institute of Standards and Technology (NIST) issued a 'Framework for Improving Critical Infrastructure Cybersecurity.' It was designed to help improve cybersecurity risk management.
- It can be a guide or model to international cooperations on how to strengthen their cybersecurity in critical infrastructure as well as other sectors and communities.
- The framework consists of three parts:
  - The Framework Core,
  - The Implementation Tiers, and
  - The Framework Profiles.

(c) 2023 Lexeprint Inc. All Rights Reserved



This Photo by Unknown author is licensed under CC BY-ND.

What is a Cyber Risk Assessment?

- The NIST defined cyber risk assessments as:
  - "*risks assessments that are used to identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.*"
- This assessment is used to inform decision-makers and support proper risk responses. It also helps to provide an executive summary to help executives and directors make informed decisions about security.
- According an ABA survey, only 35% of respondents report that their firm has had a full security assessment performed by a third party.

(c) 2023 Lexeprint Inc. All Rights Reserved


This Photo by Unknown author is licensed under CC BY-SA-NC.

What is a Tabletop

- Cyber Risk Assessments can take the form of audits, workshops, or tabletops.
- A cybersecurity tabletop is a simulated or hypothetical cyber event that tests an organization's ability to respond to a cyber incident.
- Tabletops generally include stakeholders from departments and teams across an organization, including IT, legal, HR, and senior management.
- Tabletops are used to test an organization's existing cyber risk management and identify weak points or gaps.
  - The risks identified through a tabletop are not only technical; they also identify legal and regulatory risks.
- Resource: Tabletop.ai

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-SA-NC.

Why Should Your Law Firm Do a Tabletop?

- Ensure Sensitive Information is Protected
  - Tabletop exercises provide a critical opportunity for law firms to measure their cybersecurity risk management as a business but also as the custodian of highly sensitive client information.
- Better Counsel
  - By participating in this exercise, attorneys can not only protect their business but also gain valuable experience and knowledge in incident response, which can help them provide better legal advice to clients.
- Mitigate Technical and Regulatory Threats
  - Participating in a tabletop allows organizations to receive actionable mitigation strategies and demonstrate compliance and active risk management to regulators and other stakeholders.

(c) 2023 Lexeprint Inc. All Rights Reserved.

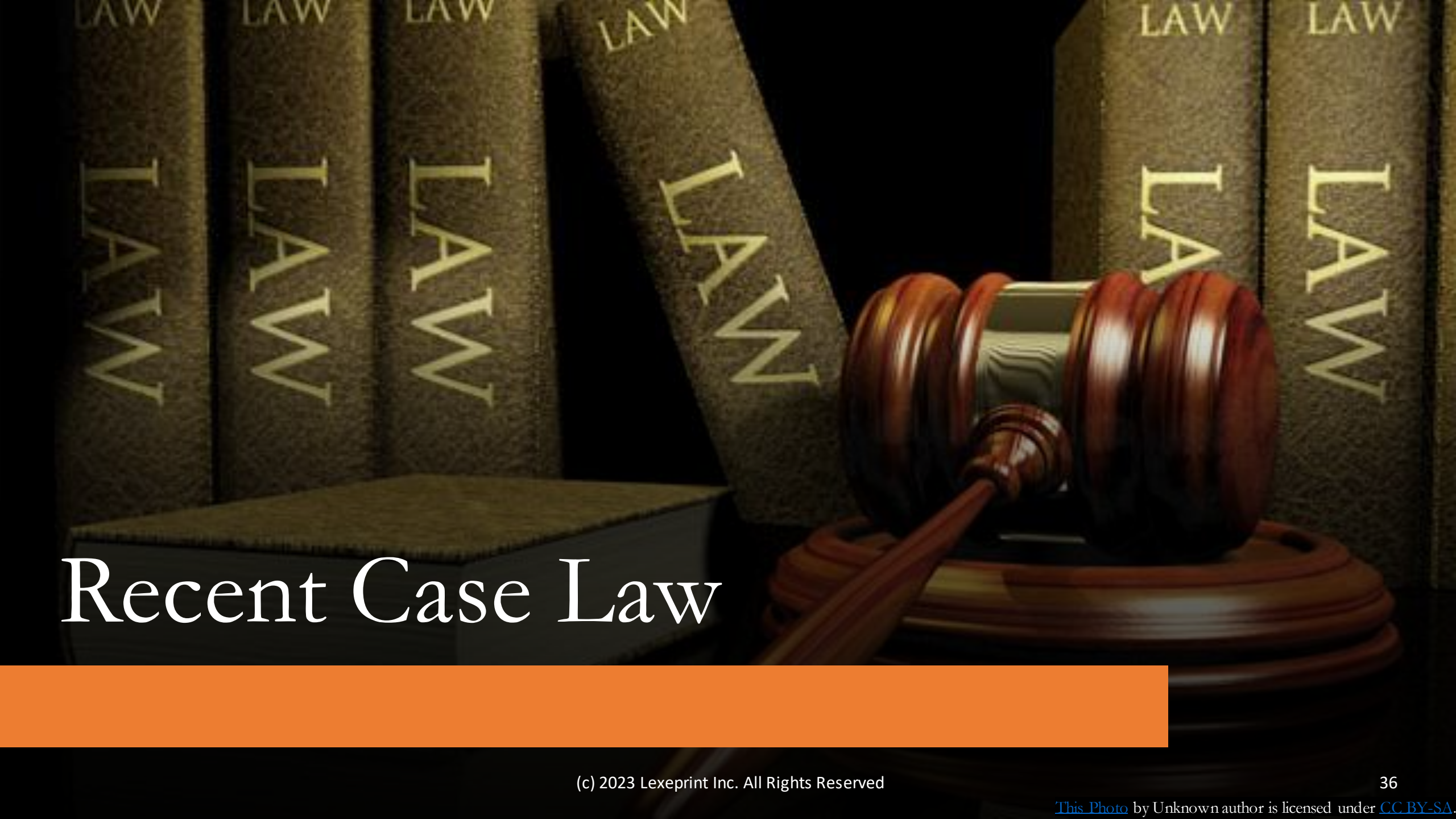


This Photo by Unknown author is licensed under CC BY-SA-NC.

Why Should Your Law Firm Do a Tabletop? (cont.)

- Training and awareness
  - The exercises can also serve as a training and education opportunity for attorneys and staff, raising awareness of the importance of cybersecurity and data protection and promoting a culture of security within the firm.
- Competitive Edge
  - Finally, conducting cybersecurity tabletop exercises can help law firms differentiate themselves from competitors by demonstrating their proactive approach to cybersecurity, which can be a significant factor in client retention and acquisition.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Recent Case Law

(c) 2023 Lexeprint Inc. All Rights Reserved

This Photo by Unknown author is licensed under CC BY-SA.


This Photo by Unknown author is licensed under CC BY.

Re: Blackbaud Inc, Customer Breach Litigation, (SC) 2022

Third-party businesses may be liable to parties they do not have direct contact with or a contract.

- **Facts:** Blackbaud is a cloud company that provides data collection and software solutions for non-profit organizations and healthcare entities, among others. The company was hacked, and their client's data, which included the PII of children, was exfiltrated and then held for ransom, which Blackbaud paid in exchange for the commitment that the hackers would destroy the data. The vendor notified its clients months later.
- **Issues:** Did Blackbaud's behavior constitute negligence for not complying with industry and regulatory security standards? Did Blackbaud have a duty to the customers of its clients against the unlawful conduct of a third-party criminal actor?

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-SA-NC

Re: Blackbaud Inc, Customer Breach Litigation, (SC) 2022 (cont.)

- **Ruling:**
  - The court ruled that Blackbaud owed the plaintiffs a duty based off of "Blackbaud's alleged creation of the risk" and the special circumstances of its contracts with Social Good Entities.
  - Following South Caroline law, the court ruled that despite security decisions being made in SC by Blackbaud, injury occurred where the servers were attacked, in Massachusetts. Even though Blackbaud's servers were located across the country, the plaintiffs' data was solely housed in MA.
- **Observations:** Most organizations store data in multiple jurisdictions. Third parties may change the location of their information during the time they are contracted, potentially affecting companies' legal exposure.

(c) 2023 Lexeprint Inc. All Rights Reserved.

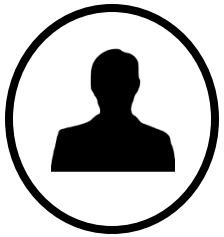

This Photo by Unknown Author is licensed under CC BY-ND

Vash v. T-Mobile US, Inc (GA) 2021

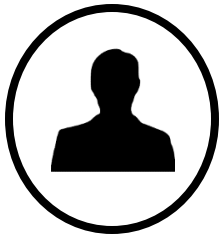
- **Facts:** Plaintiff Stephen J. Vash filed a suit seeking compensation for a T-Mobile data breach that compromised the personal data of more than 50 million people. T-Mobile includes a clause to arbitrate disputes as part of the terms and conditions in the agreements when opening an account.
- **Issue:** Should the court support T-Mobile's forced arbitration clause? Did T-Mobile's negligence lead to the data breach?
- **Ruling:** The Court ruled that a settlement would be appropriate in this case, which resulted in a $350 million payout that will fund claims by class members, plaintiffs' legal fees, and administrative costs.
- **Observation:** If the named plaintiffs have opted out of the arbitration clause, it is possible for a settlement case to proceed.

(c) 2023 Lexeprint Inc. All Rights Reserved.

Contact Us



Daniel B. Garrie
Email: daniel@lawandforensics.com
URL: www.lawandforensics.com



Jennifer Deutsch
Email: jennifer@lawandforensics.com
URL: www.lawandforensics.com

(c) 2023 Lexeprint Inc. All Rights Reserved.



Daniel B. Garrie, Esq.
Law & Forensics – Founder
JAMS – Neutral
Harvard – Faculty
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.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Daniel B. Garrie, Esq.
Director, Cybersecurity and Privacy – Law and Forensics
Contact:
E: jennifer@lawandforensics.com
URL: www.lawandforensics.com

LAW & FORENSICS
A Global Legal Engineering Firm

Jennifer Deutsch is an accomplished privacy professional, currently serving as the Director of Privacy Services at Law & Forensics, LLC. In this role, she is responsible for providing comprehensive privacy solutions and ensuring alignment with the latest data security and privacy standards. Her work also involves conducting cybersecurity audits, compliance assessments, and digital forensics investigations.

Jennifer is a licensed attorney, admitted to the Florida State Bar. Jennifer holds the distinguished certification of the International Association of Privacy Professionals (IAPP) for both the United States and the European Union. This globally recognized credential underscores her deep understanding of privacy and data protection laws and principles. She is currently furthering her expertise in the field of cybersecurity by pursuing a Master's degree in Cybersecurity Risk Management from Georgetown University.

(c) 2022 Lexeprint Inc. All Rights Reserved.