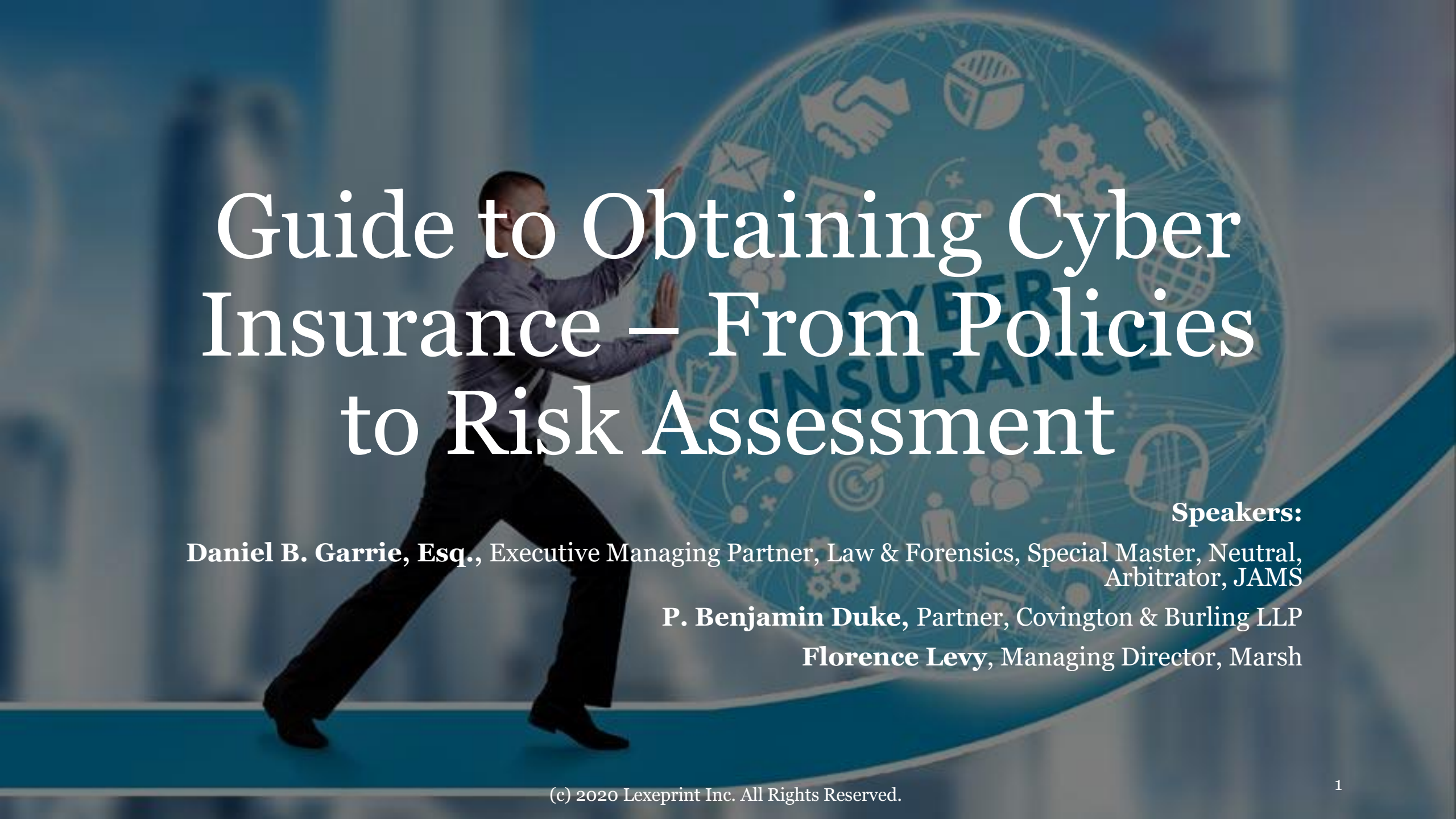



# Guide to Obtaining Cyber Insurance – From Policies to Risk Assessment

**Speakers:**

**Daniel B. Garrie, Esq.**, Executive Managing Partner, Law & Forensics, Special Master, Neutral, Arbitrator, JAMS

**P. Benjamin Duke,** Partner, Covington & Burling LLP

**Florence Levy**, Managing Director, Marsh

(c) 2020 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) 2020 Lexeprint Inc. All Rights Reserved.

# Speakers



**Daniel B. Garrie, Esq.**
Co-founder, Law & Forensics
Special Master,
Neutral, Arbitrator, JAMS



**Florence Levy**
Managing Director,
Marsh



**P. Benjamin Duke**
Partner,
Covington & Burling LLP

(c) 2020 Lexeprint Inc. All Rights Reserved.

# Agenda

1. Cyber Insurance Overview
2. Types of Policies
3. Assessing the Risk
4. Current Policy Issues
5. Key Takeaways

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Cyber Insurance Overview

(c) 2020 Lexeprint Inc. All Rights Reserved.




# What is Cyber Insurance?

- Cyber insurance generally covers your business' liability for a data breach, identity theft, personal data theft, or loss of other data involving sensitive customer information.
- Cyber insurance can help you recover from a data breach or identity theft by offsetting costs that pile up in the aftermath of an attack, as well as mitigate your cyber risk.
- Cyber insurance can reimburse for costs associated with business interruptions and extra expenses due to a cyber attack

(c) 2020 Lexeprint Inc. All Rights Reserved.



# What does Cyber Insurance cover?

- First-Party and Third-Party risks
- Respond to “bad actors” both inside and outside the insured corporation
- Provide cover for fines & penalties (where allowed by law)
- Cover intangible risks – loss and damage to non-physical “property”
- Costs associated with operational disruptions due to a cyber-attack; including Ransomware attacks
- Include costs associated with Media/Electronic content liability

(c) 2020 Lexeprint Inc. All Rights Reserved.



# What services can cyber insurance offer?

- Insurers also provide access to risk control, governance, compliance and technical services as part of the offering

(c) 2020 Lexeprint Inc. All Rights Reserved.




# Potential Threats that Cybersecurity Insurance Covers

- Threats within an organization may include:
  - Social engineering
  - Lost mobile devices
  - Improper handling of PII
  - Unintentional disclosure
  - Rogue employees
  - Coding inaccuracies
  - Human error

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Additional Potential Cyber Threats Cybersecurity Insurance Can Cover

- Threats from outside an organization may include:
  - Hackers
  - DDOS attacks
  - Criminals
  - Vendors
  - State sponsored espionage

(c) 2020 Lexeprint Inc. All Rights Reserved.




# Other Cyber Liability Coverage

- Policies may also cover liability arising from:
  - Business interruption
  - Data loss/destruction
  - Computer fraud
  - Business email compromise
  - Ransomware threats, publications costs, and reputational harm due to a cyber attack

(c) 2020 Lexeprint Inc. All Rights Reserved.




# Types of Policies

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Types of Cyber Policies

- Cyber Insurance is split between First Party Coverage and Third-Party Coverage types.
- Policies can either be purchased as a basic endorsement added onto a general liability policy, or they can be purchased as a “stand-alone” policy.

(c) 2020 Lexeprint Inc. All Rights Reserved.



# First-Party Coverage

- Usually will cover forensic investigations or remediation
- Covers costs of determining (but not always eliminating) the cause of loss of data.
- FPC will sometimes, but not always, cover the repair or replacement cost of the lost data.
- Most policies will NOT cover damage to other property/equipment resulting from loss of data or network downtime.

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Third-Party Coverage

- Will cover:
- Regulatory actions arising from breaches
  - Privacy notification costs
  - Costs of notifying third parties potentially affected by breach
  - Civil litigation including defense costs

(c) 2020 Lexeprint Inc. All Rights Reserved.




# Third-Party Coverage

- Often includes costs of call centers and credit/identity monitoring
- Often includes costs of retaining privacy counsel
- Payment card industry fines and penalties
    - Sometimes, but not always, covered

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Endorsement v. Stand-Alone

- A “stand-alone” insurance product is one that is designed to provide insurance protection for a specific risk or cost and afford an insured coverage for a particular concern.
- Stand-alone policies usually provide the broadest coverage.

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Endorsement v. Stand-Alone

- Cyber Risk “Endorsements” are insurance policies that may be purchased along with traditional insurance and provide coverage specifically geared toward cyber risks.
- Cyber endorsements are not as comprehensive as a true separate cyber policy, but they are more cost effective

(c) 2020 Lexeprint Inc. All Rights Reserved.




# When Advising a Client on Cyber Insurance, look for the following:

- Policy Type: Is it stand-alone or an extension of existing policy?
- Deductibles: compare
- Beware of applicability of coverage and potential sublimits
- Attack Scope: any attack affecting company or only targeted attacks
- Attack Vectors: network vs. social engineering
- Time Frames: APT's and spear phishing take time; is there time period for applicable coverage
- Consider cross-over with other policies such as crime, K&R and Property; address potential Silent Cyber Issues

(c) 2020 Lexeprint Inc. All Rights Reserved.




# Assessing the Risk

(c) 2020 Lexeprint Inc. All Rights Reserved.




# How does an insurance company assess risk for a cyber underwriting?

- Remember COPE:
  - Construction
  - Occupancy
  - Protection
  - Exposure

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Construction

- When an underwriter is assessing the Construction of a company's cyber network, they are looking at:
- How is the information security program structured?
- What are the organization's strengths and opportunities for improvement in the areas of:
- General technology policies and procedures
- Incident response and crisis management policies and procedures
- Organizational staffing and employee training
- Senior management and leadership cyber security awareness

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Occupancy

- When an underwriter is assessing the Occupancy of a company's cyber network, they are looking at:
- How does your organization handle data processes such as:
- Classification policies
- How do you manage data?
- Data retention policies
- Backup and recovery policies

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Protection

- When an underwriter is assessing the Protection of a company's cyber network, they are looking at:
- How well is your organization protected from advanced cyber attacks? Areas include:
- Current and planned technology deployment
- In-house and external personnel
- Functional capabilities, such as threat visibility, operational security, incident response, monitoring and detection capabilities

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Exposure

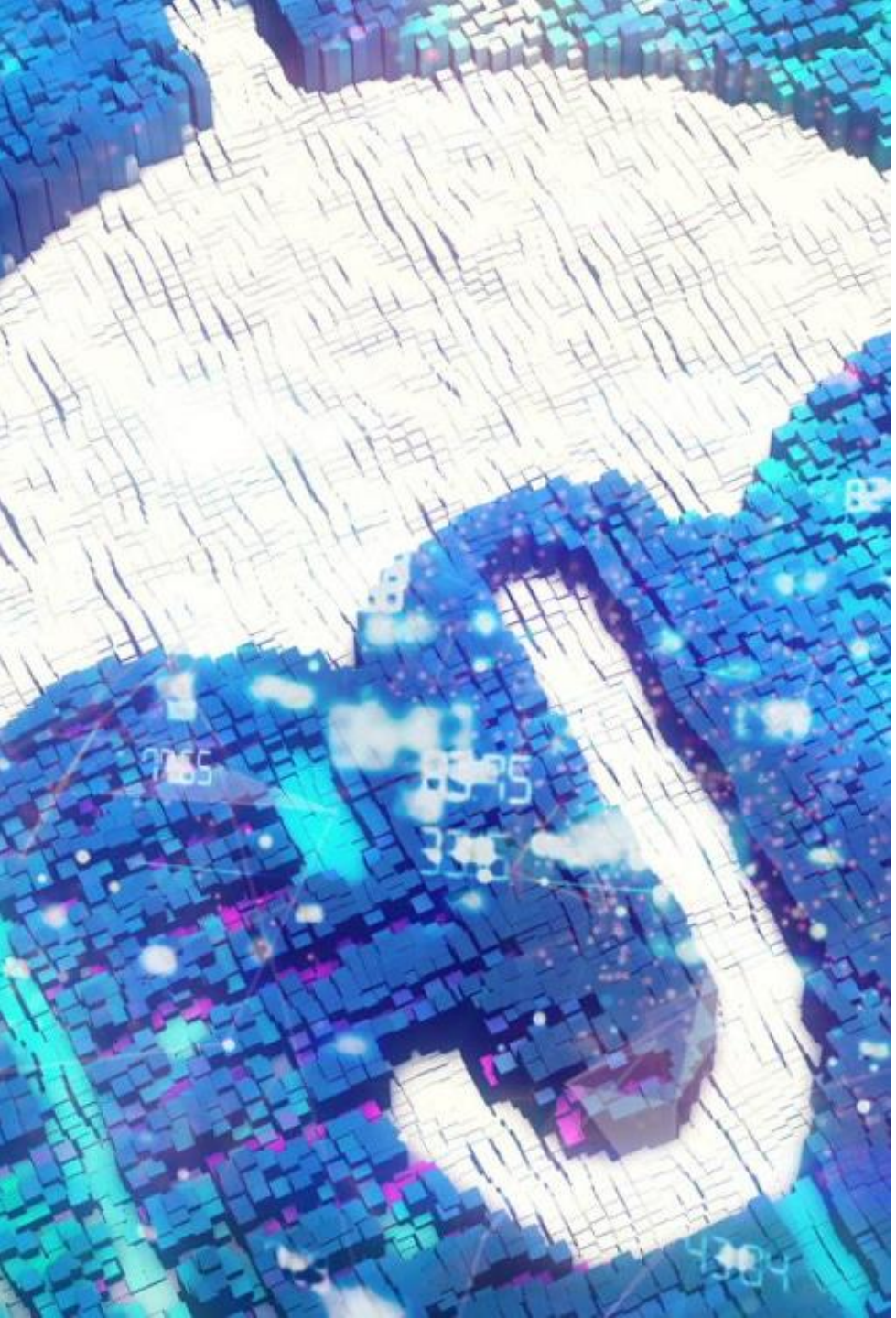
- When an underwriter is assessing the Exposure of a company's cyber network, they are looking at:
- What is the potential for risk based on your industry and your location?
- Additionally, the following areas may be important:
  - Processes and policies used by the organization to identify business and information security risks
  - Any history of attacks within the industry or company.
  - What is the value of the company's information assets?

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Current Cyber Policy Issues

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Uniformity

- Unlike traditional insurance industries, the Cyber Insurance field suffers from a severe lack of uniformity and industry standards.
- As cyberthreats evolve and proliferate, more insurers are expanding options to help law firms mitigate loss.
- Without industry standards, coverage and cost vary from plan to plan, sometimes causing gaps in potential coverage.

(c) 2020 Lexeprint Inc. All Rights Reserved.



# War Exclusions

- An escalating issue with cyber policies is that they exclude coverage for losses that stem from acts of war, such as invasions, insurrections, revolutions, military coups, and terrorism.
- In an insurance contract, a war exclusion clause refers to the protection of an insurer who will not be obligated to pay for losses caused by war-related events.

(c) 2020 Lexeprint Inc. All Rights Reserved.



# War Exclusions and Cyber Terrorism

- Cyber insurers are increasingly willing to modify war exclusions so that they don't apply to "cyber terrorism."
- While definitions of cyber terrorism differ, they generally include acts perpetrated electronically by any party to cause harm, intimidate the public, or for political, religious or ideological purposes.

(c) 2020 Lexeprint Inc. All Rights Reserved.




# War Exclusions and Cyber Terrorism

- “An act of war, invasion, acts of foreign enemies, hostilities, civil war, rebellion, revolution, insurrection, military or usurped power or the seizure and nationalization of the Insured's Critical System or information assets by order of any governmental authority. Provided, however, this exclusion shall not apply to Cyber Terrorism.”

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Key Takeaways

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Key Takeaways

- Cyber insurance is increasingly needed to cover liability for business interruption, data breaches and losses stemming from ransomware attacks.
- Remember the different types of policies and the difference between an endorsement and a stand-alone policy.

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Key Takeaways

- How does an underwriter assess a company's risk? Remember COPE.
- Pay attention to current cyber insurance policy issues, such as a lack of uniformity leading to coverage gaps, and war exclusions.

(c) 2020 Lexeprint Inc. All Rights Reserved.



# Questions

(c) 2020 Lexeprint Inc. All Rights Reserved.

# Contact Us




**Daniel Garrie**
Email: daniel@lawandforensics.com
Phone: (855) 529-2466
URL: www.lawandforensics.com



**P. Benjamin Duke**
Email: pbduke@cov.com
Phone: (212) 841-1072
URL: https://www.cov.com



**Florence Levy**
Email: florence.levy@marsh.com
URL: https://www.marsh.com


(c) 2020 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. In particular, Daniel recently located and recovered deleted files in both private and public cloud computing environments using his patented software, Forensic Scan. This investigation took less than forty-eight hours to clean and recover the data from the servers of a cloud-hosting provider that was compromised by a malicious cyber-attack. Thanks to the Forensic Scan technology, that Daniel co-invented and patented (US9990498B2 and US9990497B2), and his own expertise, Daniel and his team was able to identify the source of the breach and remediate the problem in record time.

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, including one involving the embezzlement of millions of dollars from a large non-profit. Daniel was able to perform a thorough analysis of the alleged embezzlers' phone and computer, despite the embezzlers' attempts to wipe them, and identify concrete evidence of the embezzlement to a jury. 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. Some of the major cases for which he has served as an e-discovery special master, or forensic neutral include: *Hougan vs. City of Newport Beach, No. 30-2012-00582855* (Super. Ct. Cal. 2014)*; Small v. University Medical Center of Southern Nevada, 2014 WL 4079507*(D. Nev. 2014)*; C.D.S. Inc. v. Zelter and Amazon Web Services, Inc.*, (S.D.N.Y. 2016); *Jawbone, Inc. v. Fitbit Inc.* et al (Super. Cal., S.F. County 2018). In addition to his vast litigious experience, 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) 2020 Lexeprint Inc. All Rights Reserved.



**P. Benjamin Duke**
Covington & Burling LLP – Partner
**Contact:**
W: (212) 841 1072
E: pbduke@cov.com
URL: https://www.cov.com

COVINGTON
COVINGTON & BURLING LLP

Ben Duke advises and advocates for insurance policyholders in a broad range of complex litigation, arbitration and other matters involving all types of insurance, from general liability to D&O, professional liability, fidelity bond, and other specialized coverages.

Mr. Duke has helped obtain significant insurance recoveries on behalf of clients in many industries, including the financial services, technology, energy, and pharmaceutical industries. He is currently handling major coverage litigation in New York courts and has nationwide experience litigating in state and federal courts and in numerous arbitration forums. As co-lead trial and appellate litigation counsel, Mr. Duke recently helped a major technology company recover over $150 million in coverage for a massive government-mandated environmental remediation in Wisconsin's Fox River.

Representative Matters

- Represent futures commission merchant in $140 million fidelity bond litigation arising from illegal employee trading.
- Counsel for major integrated oil company in asbestos coverage litigation.
- Special insurance coverage counsel for Chapter 11 Trustee in bankruptcy proceedings involving multi-billion dollar liquidation of multinational commodities firm.
- Counsel for major technology manufacturing company in litigation against multiple insurance companies, for coverage of historical PCB contamination of a major river system.
- Litigated and co-tried $450 million bondholder dispute on behalf of major energy company.

(c) 2020 Lexeprint Inc. All Rights Reserved.



**Florence Levy**
Marsh – Managing Director
**Contact:**
E: florence.levy@marsh.com
URL: https://www.marsh.com/

Florence Levy focuses in the complex and dynamic risk environment of Cyber and Commercial E&O insurance. She advises clients as a member of Marsh's Cyber Center of Excellence (CoE), drive growth, particularly in the Western Zone, and leads innovative development of new and existing Cyber and E&O products as an integral part of thier product development team.

She also partners with key markets in Cyber and E&O insurance to advocate on her clients' behalf to obtain the best terms, conditions, coverage and pricing. She is a frequent speaker and contributor at various industry events and create original content for a variety of trade publications.

(c) 2020 Lexeprint Inc. All Rights Reserved.