

The Who, Why, How and Where of Cybersecurity Insurance for Law Firms

Speakers:

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

Anthony Dagostino, Executive Vice President, Global Cyber and Technology Practice, Lockton Companies

Tamara Snowdon, Cyber Coverage Leader, Marsh

(c) 2021 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) 2021 Lexeprint Inc. All Rights Reserved.



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



Anthony Dagostino
Executive Vice President, Global
Cyber and Technology Practice,
Lockton Companies



Tamara Snowdon
Cyber Coverage Leader, Marsh

(c) 2021 Lexeprint Inc. All Rights Reserved.

Agenda

1. Increased Need for Cyber Insurance in 2021
2. Significance of Cyber Insurance for Law Firms
3. The State of Cybersecurity in 2021
4. Cyber Insurance Policy Considerations
5. Key Takeaways

(c) 2021 Lexeprint Inc. All Rights Reserved.



Increased Need for Cyber Insurance in 2021

(c) 2021 Lexeprint Inc. All Rights Reserved.



Surge in Cybercrime

- With the COVID-19 pandemic still forcing many to continue working remotely, cybercrime has been raging out of control. Thus, many businesses including firms are seeking the best ways to protect themselves and their firms via cyber insurance.
- According to 'Finaria, it', the global cyber insurance market is predicted to grow by 21% over last year and reach $9.5 billion this year. Statistics indicate that by 2025, the cyber insurance market will exceed $20 billion.

(c) 2021 Lexeprint Inc. All Rights Reserved.



Significance of Cyber Insurance for Law Firms

(c) 2021 Lexeprint Inc. All Rights Reserved.



Why is Cyber Insurance important?

- To understand the gravity of why law firms needs cyber insurance, the understanding of what these policies are and what they cover will help.
- Cyber insurance is 'intended to assist companies and other organizations with the financial aspects of data recovery and other activities in the unfortunate event of a cyber breach.'
- Attorneys cannot afford to suffer these types of losses and continue to operate.

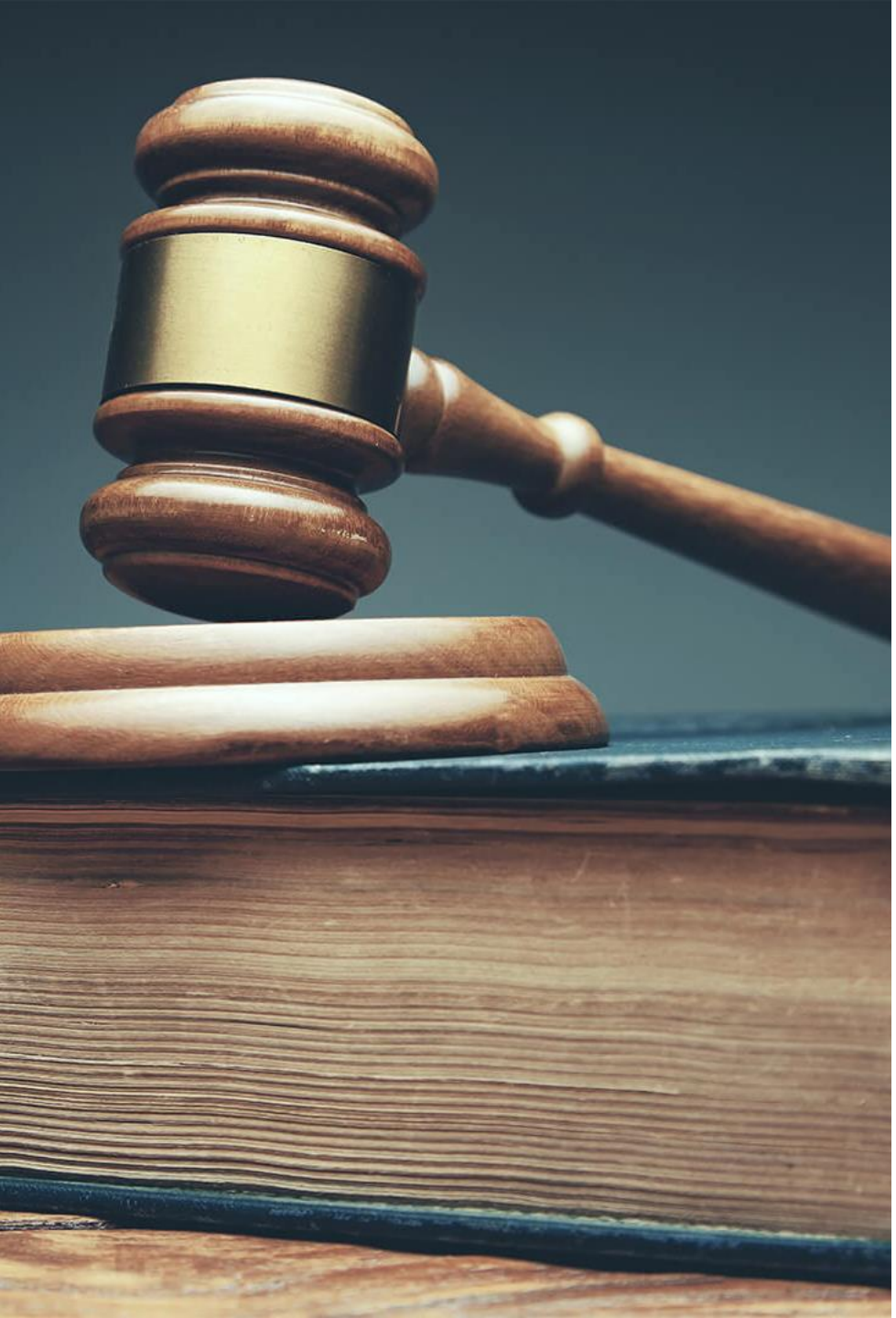
(c) 2021 Lexeprint Inc. All Rights Reserved.



Current State of Cyber Insurance

- It has been estimated that premiums on insurance policies are as high as $7.5 billion in 2020.
- Only 1/3 of all companies hold these types of policies.
- Roughly ¼ of all law firms experience breaches.
- The 2019 Hiscox Cyber Readiness Report indicated that 41% of firms from Europe and the US have already adopted cyber insurance. Also, 30% more were planning to adopt cyber insurance in 2020.

(c) 2021 Lexeprint Inc. All Rights Reserved.



Consequences of Cybercrime for Law Firms

- Loss of access to work product and documents creates business interruptions;
- It can be very expensive to regain access and repair damaged systems;
- Payment of ransom to cybercriminals; and
- Malpractice, ethics, governmental, and other third-party claims arising from data breaches.

(c) 2021 Lexeprint Inc. All Rights Reserved.



The State of Cybersecurity in 2021

(c) 2021 Lexeprint Inc. All Rights Reserved.



New Opportunities for Hackers

- There are a number of different cyber exposures that the coronavirus could present. Cyber criminals are already preying on the widespread fear that the coronavirus has created.
- It is a perfect opportunity for hackers, adept when it comes to identifying vulnerabilities in infrastructure and defenses, to spread ransomware infections, malware and launch other cyber threat campaigns.
- Malicious infections in the name of coronavirus have already been reported to be in circulation in the U.S. and U.K.
- Ankura consulting has found malicious .pdf, .mp4 and .docx files disguised as documents relating to the coronavirus.
- Although the file names suggest that they include virus protection instructions, current threat developments and virus detection techniques, they actually contain a number of malware samples, such as Trojans and worms that could damage or encrypt data.

(c) 2021 Lexeprint Inc. All Rights Reserved.



Work from Home Leads to Increased Vulnerability

- In addition to an organization being more susceptible to a cyber attack due to employees' coronavirus fears, it is also possible that an organization's technological defenses will be more vulnerable than usual.
- As the coronavirus is causing more employees to work remotely, it is possible that those individuals are logging in remotely from a less secure network and perhaps using less secure hardware.
- High volumes of employees logging in remotely may make it easier for cyber criminals, infiltrating a network through remote desktop services, to stay hidden in an attempt to identify and access systems with sensitive data.

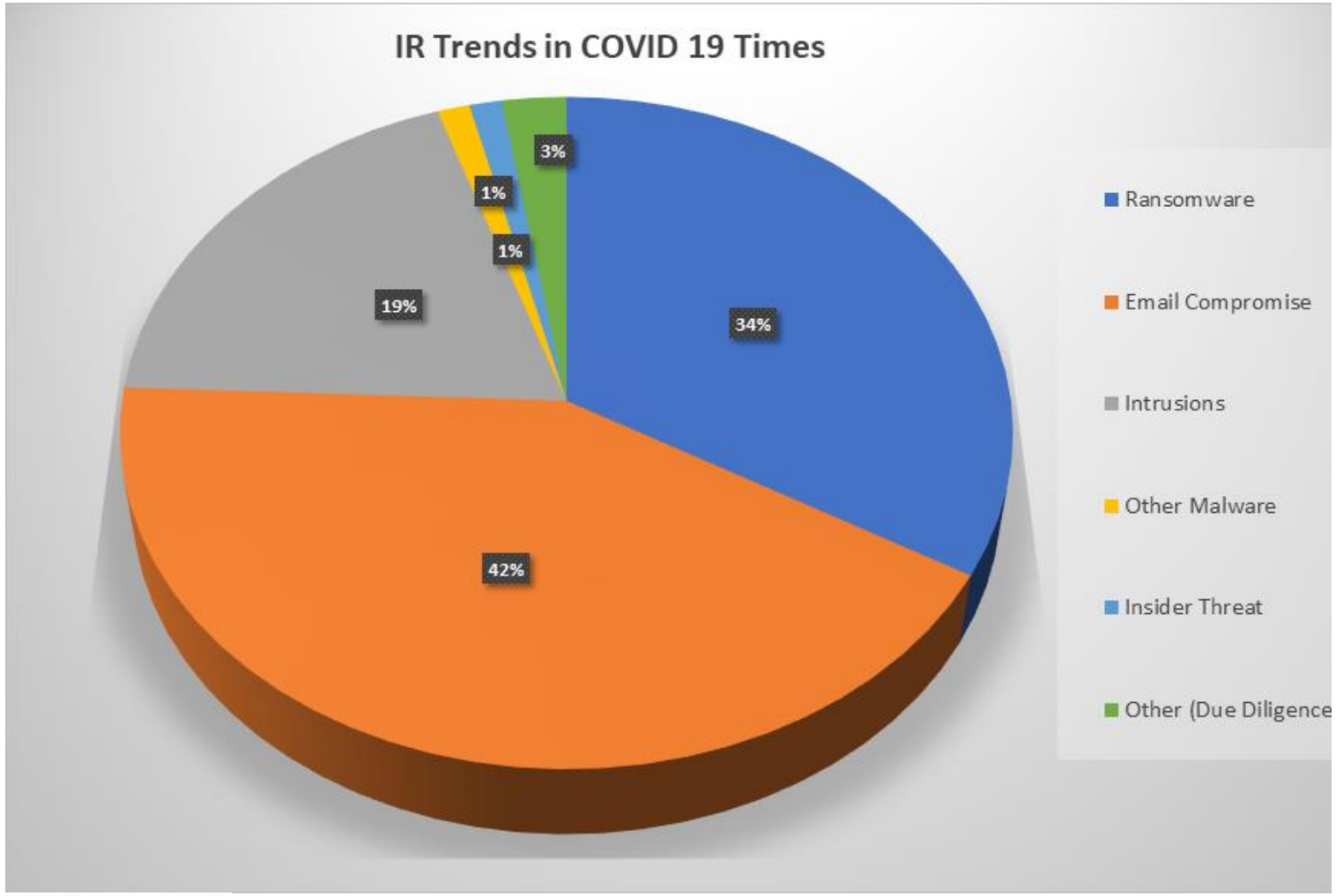
(c) 2021 Lexeprint Inc. All Rights Reserved.



2021 Cyber Threat Observations

- Attackers Using **COVID-19 Alerts** and **Tracking Maps** to Hide Spyware or Phish Information
- Ransomware Research Shows **Window of Opportunity** For Attackers
- **Heightened Situational Awareness** Increasing in Unprecedented Ways
  - Alert levels for a variety of cyber threats were already at all time highs.
  - Critical services and corporations working to maintain service levels and come online in new (for them) and potentially vulnerable ways.
- **Disruptive and Destructive** attacks continue to be prevalent with a focus on **Critical Services**
- **Extortion** activity on the rise
- **System vulnerabilities** are being monetized

(c) 2021 Lexeprint Inc. All Rights Reserved.



ankura

Cyber Incident Response Trends – Q2 2020

(c) 2021 Lexeprint Inc. All Rights Reserved.

A New Form of Extortion – Exfiltration

SOME Ransomware threat actors are now exfiltrating data from victims before encrypting their data

- Goal is to create more leverage to force victims to pay ransom demands by threating to leak stolen data and **doing** it
  - First, attackers leak samples of the data on either the internet or the dark web
  - If the victim does not comply the attackers may leak everything they took as a malicious way to "teach the victims a lesson"
  - Victims now are forced to deal with a ransomware attack and a data breach at the same time which often carries strict legal notification obligations

Maze, Sodinokibi and Nemty Ransomware Threat Actors

- Started the trend of creating a dedicated website to list victims that have yet to pay in an attempt to shame the victims into compliance
  - Threat actors have even notified victims in advance of extortion demands, that the victims have been breached
  - The "steal then encrypt" business model is popular but unknown if it is more profitable than traditional encryption-only attack
  - Noticing the data being taken prior to the deployment of the ransomware, could result in fewer successful attacks
  - Reporting the breach immediately and notify the victims, also minimizes the threat of the attack and damage the company's reputation

(c) 2021 Lexeprint Inc. All Rights Reserved.



Cyber Insurance Policy Considerations

(c) 2021 Lexeprint Inc. All Rights Reserved.



Why You Should Purchase Cyber Insurance

- Data is critical to any corporation. The value of your data is more likely worth more than the equipment in which it is stored. Cyber policy can offer coverage for data restoration in the event of a loss.
- Third-party data is essential to many corporations. However, it belongs to your suppliers and customers. If you lost it, it is highly probable that you will be the one to pay. Most commercial contracts and non-disclosure agreements address the security of third-party data that could trigger claims if your business experiences a data breach.

(c) 2021 Lexeprint Inc. All Rights Reserved.



Should a Client Buy Cyber Insurance?

- Everyone should buy cyber insurance. It is cheap and certainly pays.

(c) 2021 Lexeprint Inc. All Rights Reserved.



Do you rely on your CGL for cyber protection?

- CGL and other traditional liability policies provide limited coverage, at best, for cyber-related risks
  - Most CGL, D&O and traditional E&O policies now contain specific exclusions aimed at cyber-related losses

(c) 2021 Lexeprint Inc. All Rights Reserved.



Do you rely on indemnity agreements to manage your cyber risk?

- Indemnity agreements typically have limitations, and are only as good as the entity providing the indemnity

(c) 2021 Lexeprint Inc. All Rights Reserved.



If you decide to recommend buying cyber insurance, you should discuss the following questions with your clients:

- ✓What security controls can you put into place that will reduce the premium?
- ✓Will you have to undertake a security risk review of some sort?
- ✓What is expected of you to reduce or limit the risks?
- ✓The security/protection industry is very fast changing, how can the insurance ensure that your policy is current?

(c) 2021 Lexeprint Inc. All Rights Reserved.



If you decide to recommend buying cyber insurance, you should discuss the following questions with your clients:

- ✓ Do all portable media/computing devices need to be encrypted?
- ✓ What about unencrypted media in the care or control of your third-party processors?
- ✓ Are all and any court attendances to defend claims from others covered?
- ✓ Are malicious acts by employees covered?

(c) 2021 Lexeprint Inc. All Rights Reserved.



Items to Consider

- Adequate limits
- Separate limit of coverage for first party breach response coverage
- Coverage for your vendors' breaches involving your information
- Coverage for a *suspected* incident
- Coverage for ransomware
- Modified Intentional Acts Exclusion / Rogue Employee Coverage

(c) 2021 Lexeprint Inc. All Rights Reserved.



Items to Consider

- Unencrypted data exclusion
- Safeguard exclusion
- Coverage that only extends to *personally* identifiable information
- Failure to follow your own privacy policy exclusion
- Professional services or legal services exclusion
- Prior Acts exclusion

(c) 2021 Lexeprint Inc. All Rights Reserved.



Policy Variance

- US Centric Policies
  - Stand-alone cyber policies, created in 1999, only started to take off in 2007 and to date, only 35% of businesses purchase coverage – and that estimate may be overstated
  - Will usually only cover US based risks (on a global basis)
  - Coverages for Bodily Injury/ Property Damage usually not available
  - Bigger focus on First Party Coverages
  - Prior to new European data privacy guidelines, notification requirements were a focus more in US based policies

(c) 2021 Lexeprint Inc. All Rights Reserved.



Policy Variance

- Most policies contain the same basic coverage; specific enhancements and industry – related coverages must be negotiated into the policies on a case by case basis
- Global Policies
  - Address new concerns brought about by GDPR
  - Can extend over US or EU operations
  - Generally broader terms and conditions are available in the UK or EU, although US policies are catching up.

(c) 2021 Lexeprint Inc. All Rights Reserved.



Key Takeaways

(c) 2021 Lexeprint Inc. All Rights Reserved.



Key Takeaways #1

- Use a broker experienced in placing cyber coverage.
- Shop aggressively and get multiple quotes.
- Always ask for specimen policy forms (promotional materials may not be consistent with actual policy language).
- Review policy language carefully and ask questions.

(c) 2021 Lexeprint Inc. All Rights Reserved.



Key Takeaways #2

- Consider seeking advice from policyholder counsel experienced in cyber policies.
- Negotiate, negotiate, negotiate.
- When claims arise, be skeptical of any denial of coverage.
- You paid for the coverage, so go get it!

(c) 2021 Lexeprint Inc. All Rights Reserved.

Questions?

(c) 2021 Lexeprint Inc. All Rights Reserved.

Contact Us



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



Anthony Dagostino
Email: adagostino@lockton.com
Phone: (646) 572-7314
Website: https://www.lockton.com



Tamara Snowdon
Email: Tamara.Snowdon@marsh.com
Phone: (212) 345-7033
Website: https://www.marsh.com

(c) 2021 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) 2021 Lexeprint Inc. All Rights Reserved.



Tamara Snowdon
Marsh – Cyber Coverage Leader
Contact:
E: Tamara.Snowdon@marsh.com
W: (212) 345-7033
URL: https://www.marsh.com

Tamara Snowdon is a Cyber Coverage Leader with Marsh's Cyber, Media & E&O Practice in New York as part of FINPRO's Center of Excellence. Tamara manages a book of business focusing on primarily on security, privacy, technology, media and professional liability insurance products.

Tamara's day to day focus is on evaluating data privacy and security exposures, and placing complex cyber programs through the use of gap analysis, cyber risk modeling, benchmarking and manuscripting of policy language. She implements insurance programs for a variety of companies including technology, media, healthcare, financial institutions, manufacturers, retailers and telecommunications. Tamara has written extensively on the subject of cyber security during her career.

(c) 2021 Lexeprint Inc. All Rights Reserved.



Anthony Dagostino
Lockton Companies – Executive Vice President
Contact
E: adagostino@lockton.com
W: (646) 572-7314
URL: https://www.lockton.com

Anthony is executive vice president and Global Cyber & Technology Practice leader for Lockton, the world's largest privately held, independent insurance broker and consultant. Anthony oversees Lockton's cyber strategy focusing on delivering innovative and effective solutions to clients across the globe through risk transfer solutions, analytics and risk consulting.

Prior to joining Lockton in July 2019, he led Willis Towers Watson's global cyber risk consulting and insurance brokerage practices. He brings nearly two decades of experience in cyber, technology, and financial lines insurance underwriting and brokerage through an array of leadership positions. Prior to joining the insurance industry, Anthony was a research analyst in the venture capital space focusing on early-stage emerging technology companies.

Anthony serves on numerous advisory boards helping start-up companies and also participates in various public-private sector working groups. He is a regular contributor to news media and is active in his hometown community through a number of charities.

(c) 2021 Lexeprint Inc. All Rights Reserved.

A new book by Daniel Garrie...

"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."

Don't Fall Behind: A Cybersecurity Guide for Law Firms

As cybersecurity attacks continue to rise, the legal sector has been identified as one of the primary targets of cyber criminals. While studies show cybersecurity is considered a significant threat, survey respondents have indicated their companies are not taking proper measures to combat these threats. This concise guide offers steps all law firms should take to protect their networks and data against cyber attacks.

(c) 2021 Lexeprint Inc. All Rights Reserved.