Cyber Insurance Ransomware

Speakers:

Daniel B. Garrie, Co-founder, Law & Forensics; Neutral and Discovery Referee JAMS

Peter Halprin, Partner, Pasich LLP

Tamara Snowdon, Cyber Coverage Leader, Marsh

Aarti Soni, Cyber Director & Product Innovation Counsel, McGriff, Seibels & Williams

Lou Botticelli, Senior Director, Markel

(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

Speakers



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



Peter Halprin
Partner
Pasich LLP



Tamara Snowdon
Cyber Coverage Leader
Marsh



Aarti Soni
Cyber Director & Product
Innovation Counsel,
McGriff, Seibels & Williams

(c) 2021 Lexeprint Inc. All Rights Reserved

Agenda

- Ransomware Attacks in 2021
- State of Cyber Insurance
- State and Federal Ransomware Guidance
- Cyber Insurance Case Trends in the last year
- Key Takeaways

(c) 2021 Lexeprint Inc. All Rights Reserved



Ransomware Attacks in 2021

(c) 2021 Lexeprint Inc. All Rights Reserved



Accenture $50M Ransomware Threat

- In August, the global consulting firm Accenture suffered a ransomware attack by the LockBit ransomware gang.
- LockBit reported the theft of 6 terabytes worth of Accenture's data and demanded the firm pay a $50 million ransomware payment, without which they would release volumes of private data to the public.
- Exactly how the hackers infiltrated Accenture's network remains to be determined. However, it appears to be an inside job from preliminary evidence. The LockBit website displayed the message "these people are beyond privacy and security. I really hope that their services are better than what I saw as an insider. If you're interested in buying some databases, reach us."

(c) 2021 Lexeprint Inc. All Rights Reserved



How Accenture Succeeded in Handling this Crisis

- Initial reports suggested that Accenture had backup protocols in place and moved swiftly to isolate their affected servers, once identified.
- Companies must not only retain clean backups but should also ensure that their restore point is clean from any type of potential compromise or external access.
- It is essential for every business to ensure that adversary access is removed, and compromised systems are not put back into your environment. Security gaps through which adversaries may enter must be promptly addressed.

(c) 2021 Lexeprint Inc. All Rights Reserved



Colonial Pipeline

- One of the nation's largest pipelines, which carries refined gasoline and jet fuel from Texas up the East Coast to New York, was forced to shut down after being hit by ransomware in a vivid demonstration of the vulnerability of energy infrastructure to cyberattacks.
- The operator of the system, Colonial Pipeline, was forced to shut down its 5,500 miles of pipeline, which carries 45 percent of the East Coast's fuel supplies, in an effort to contain the breach.

(c) 2021 Lexeprint Inc. All Rights Reserved



Colonial Pipeline

- Gas stations across the east coast were forced to shut down and average national gas prices to rose above $3 for the first time since 2014.
- Colonial Pipeline confirmed it paid the hackers $4.4 million ransom.
  - Colonial Pipeline's CEO told the Wall Street Journal he authorized the payment because the company didn't know the extent of the damage and wasn't sure how long it would take to bring the pipeline's systems back.

(c) 2021 Lexeprint Inc. All Rights Reserved



Colonial Pipeline Ransomware Attack Could Raise Cyber Insurance Bar

- The ransomware attack on Colonial Pipeline Co., one of the most recent high-profile examples of a growing threat may make it harder for companies to negotiate cyber insurance policies without first bolstering their technological defenses.
- The hackers' attack caused Colonial Pipeline to temporarily halt fuel operations extending from Texas to New Jersey and it took down aspects of the company's IT systems.
- The incident has renewed interest in cyber insurance policies, even as insurers raise the bar for policyholders to qualify for coverage.

(c) 2021 Lexeprint Inc. All Rights Reserved



State of Cyber Insurance

(c) 2021 Lexeprint Inc. All Rights Reserved



State of Cyber Insurance

- Victims of ransomware attacks have paid at least $350 million in 2020, according to the cryptocurrency data firm Chainalysis, but that total could be larger given the unknown number of unreported incidents.
- As a result, insurers have reportedly pulled back on their willingness to pay a company's losses and have introduced exclusions into the hardest hit sectors, according to experts. Policyholders can expect an increase in premiums — in fact, data from insurance broker Marsh has already shown such a rise.
- In May, Marsh reported that the U.S. cyber insurance market experienced a 35% price rise, the largest annual increase for the product since 2015.

(c) 2021 Lexeprint Inc. All Rights Reserved



Insurers Set Limits on Risky Sectors Amid Cybercrime Spike

- The U.S. Government Accountability Office ("GAO") found that the mushrooming pace of cyberattacks has led many insurance providers to set coverage limits on sectors like health care and education that are known to be a common target for hacks.
- In a report released in May, the watchdog agency added that more than half of insurance brokers polled in recent months said that their clients saw premiums rise between 10% and 30% in late 2020, as cyberattacks became more common and more severe.
- The agency concluded that "the extent to which cyber insurance will continue to be generally available and affordable remains uncertain."

(c) 2021 Lexeprint Inc. All Rights Reserved



Insurers Set Limits on Risky Sectors Amid Cybercrime Spike

- Amid the spike in cybercrime, more and more insureds continue to elect to enroll in cyber insurance coverage, the GAO found, citing data from the global insurance broker Marsh McLennan, which told the agency that 47% of its clients signed up for cyber insurance in 2020, compared to just 26% in 2016.
- The GAO's report also found that the increasing pace of cyberattacks — particularly ransomware attacks, in which attackers demand ransoms in exchange for regaining access to frozen networks — has spurred insurers "to reduce cyber coverage limits for certain riskier industry sectors, such as health care and education, and for public entities and to add specific limits on ransomware coverage."
- Both the health care and education industries are known to have an exceptionally high interest in keeping patient or student data confidential. Cybersecurity experts state that many public entities do not make the same levels of investment in data security that private companies do.

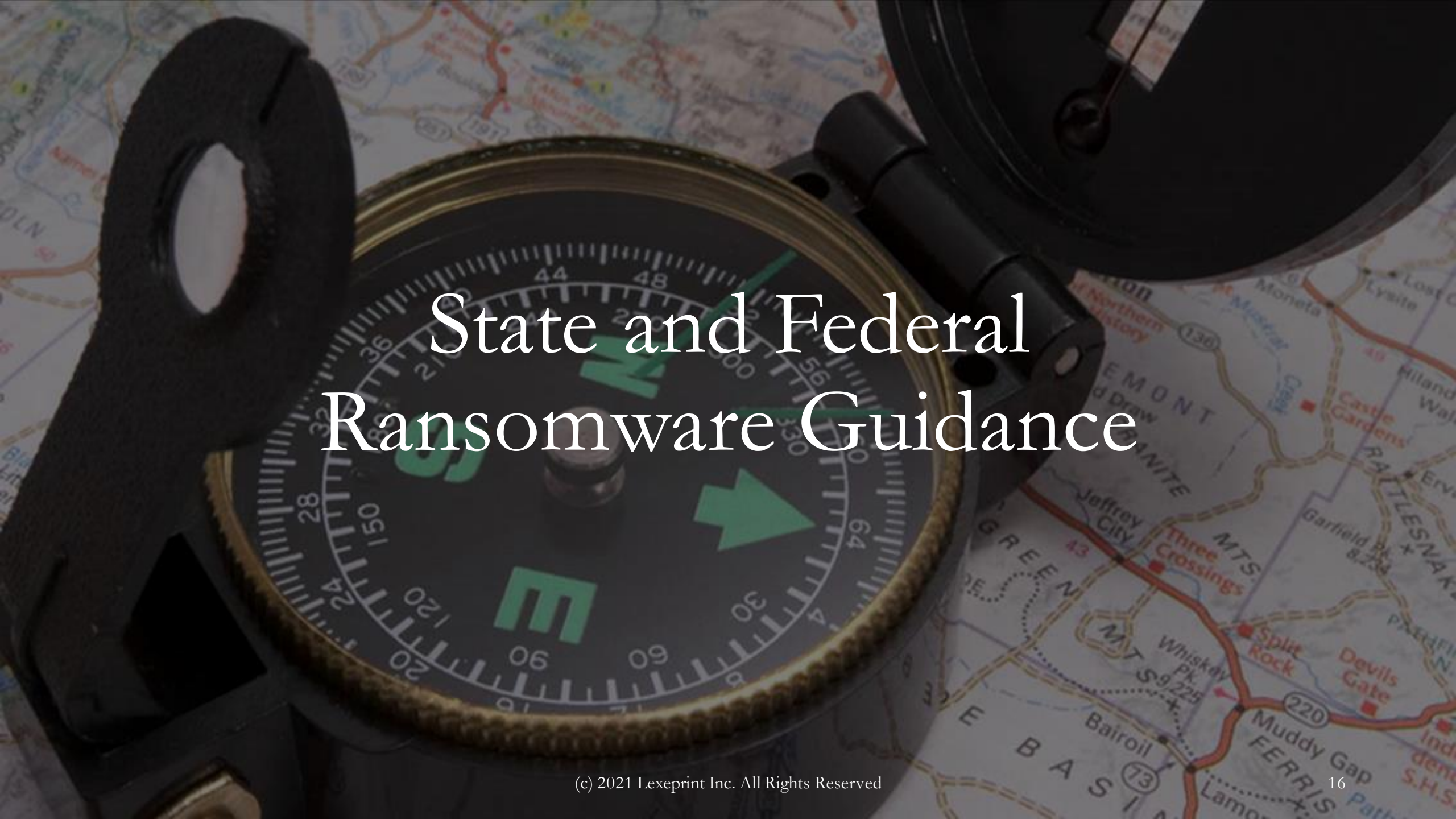
(c) 2021 Lexeprint Inc. All Rights Reserved



Insurers Set Limits on Risky Sectors Amid Cybercrime Spike

- The GAO also found that industry stakeholders reported a lack of clarity around different terms that appear on cyber insurance policies, leading to confusion between clients and insurers about what types of incidents are covered. Watchdog stated that the definition of policy terms such as "cyberterrorism" are defined differently by different companies and suggested that Federal and State governments work with the insurance industry to set a common set of definitions on disputed terms.
- GAO anaylzed data from the National Association of Insurance Commissioners between January and May, interviewed two industry associations representing cyber insurance providers, and spoke to one large cyber insurance provider and officials at the U.S. Department of Treasury, in order to compile its report.

(c) 2021 Lexeprint Inc. All Rights Reserved



State and Federal Ransomware Guidance

(c) 2021 Lexeprint Inc. All Rights Reserved



Department of Financial Services' Cyber Insurance Risk Framework

- On Feb. 4, 2021, the New York State Department of Financial Services ("DFS") issued new guidance concerning cyber risks (Insurance Circular Letter No. 2 (2021) (the "Circular Letter")).
- The Circular Letter provided guidance to property-casualty insurers operating in New York and what they should consider in their underwriting, claims and related practices on cyber risks.

(c) 2021 Lexeprint Inc. All Rights Reserved



Department of Financial Services' Cyber Insurance Risk Framework

- DFS created a Cyber Insurance Risk Framework to foster the growth of a robust cyber insurance market that maintains the financial stability of insurers and protects insureds. It outlines best practices for managing cyber insurance risk (the "Framework").
- The Framework applies to all authorized property/casualty insurers that write cyber insurance. However, property/casualty insurers that do not write cyber insurance should still evaluate their exposure to "silent risk" and take appropriate steps to reduce that exposure.
- DFS recommends against making ransom payments. Ransom payments fuel the vicious cycle of ransomware, as cybercriminals use them to fund ever more frequent and sophisticated ransomware attacks.

(c) 2021 Lexeprint Inc. All Rights Reserved



OFAC Ransomware Advisory

- In October 2020, the U.S Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued an advisory reinforcing that payments made to cyber actors are considered to be a violation of the law.
- OFAC issued this advisory to "highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities."

(c) 2021 Lexeprint Inc. All Rights Reserved



OFAC Ransomware Advisory

- The demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that companies rely on to continue conducting business.
- This advisory describes the sanctions risks and provides information for contacting relevant U.S. government agencies, including OFAC, if there is a reason to believe that the cyber actor is demanding ransomware payment.
- The advisory indicated that the payer will be subject to civil penalties and specifically stated that it applies to cyber insurance companies, digital forensic, incident response companies, and financial services companies.

(c) 2021 Lexeprint Inc. All Rights Reserved



OFAC Penalties

- OFAC has imposed, and will continue to impose, sanctions on actors and others who materially assist, sponsor, or provide financial, material, or technological support for ransomware activities.
- Criminal penalties include a fine of up to $1 million and/or up to 20 years in prison for each violation.
- Civil penalties include a fine of up to $55,000 for each violation.

(c) 2021 Lexeprint Inc. All Rights Reserved



CISA & FBI Advisory

Preventing an Attack

- In May, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) released a joint advisory ("Advisory"), considering the recent DarkSide ransomware attack on the U.S. Pipeline operator. The Advisory encourages critical infrastructure (CI) asset owners and operators to "adopt a heightened state of awareness."
- The Advisory includes several recommendations for businesses to mitigate the risk of ransomware attacks. A few of these recommendations include:
  - requiring multi-factor authentication (MFA) for remote access to company networks;
  - enabling strong spam filters to block phishing emails;
  - conducting user training on phishing attacks;
  - regularly updating software and
  - conducting security patches.

(c) 2021 Lexeprint Inc. All Rights Reserved



CISA & FBI Advisory

Reducing Impact of an Attack

- The Advisory also contains mitigation recommendations for CI entities to reduce the risk of severe disruptions in the event of successful ransomware attacks.
- These recommendations include:
  - implementing and ensuring robust network segmentation between IT and operational technology (OT) networks;
  - organizing OT assets into logical zones;
  - identifying OT and IT network inter-dependencies and
  - developing workarounds or manual controls.

(c) 2021 Lexeprint Inc. All Rights Reserved



Cyber Insurance Case Trends in the Last Year

(c) 2021 Lexeprint Inc. All Rights Reserved



Policyholders May be Entitled to Coverage under a Property Policy for Losses Incurred Due to a Ransomware Attack

- *National Ink and Stitch, LLC v. State Auto Property and Casualty Ins. Co., No.SAG-18-2138* (Mem. Op. Jan. 23, 2020, D. Md.)
- Issue: Does a business owner's property insurance policy, which covers, among other things, "direct physical loss or of damage to Covered Property," include the replacement of an entire computer system due to a ransomware attack?
- Ruling: The court held among other things, that "loss of use, loss of reliability, or impaired functionality" were types of "damage to" covered property sufficient to trigger coverage.
  - The court stated that "[h]ere, not only did Plaintiff sustain a loss of its data and software, but Plaintiff is left with a slower system, which appears to be harboring a dormant virus, and is unable to access a significant portion of software and stored data."

(c) 2021 Lexeprint Inc. All Rights Reserved



National Ink and Stitch, LLC v. State Auto Property and Casualty Ins. Co., No.SAG-18-2138 (Mem. Op. Jan. 23, 2020, D. Md.)

- Observations:
- Policyholders should consider the potential for coverage under a wide array of policies when facing loses arising from social engineering or ransomware attacks.
- Policyholders should also review any current policies or proposed renewed policies to evaluate the extent of such policies. When evaluating these policies, policyholders should consider other products or endorsements that may be related to such risks.

(c) 2021 Lexeprint Inc. All Rights Reserved

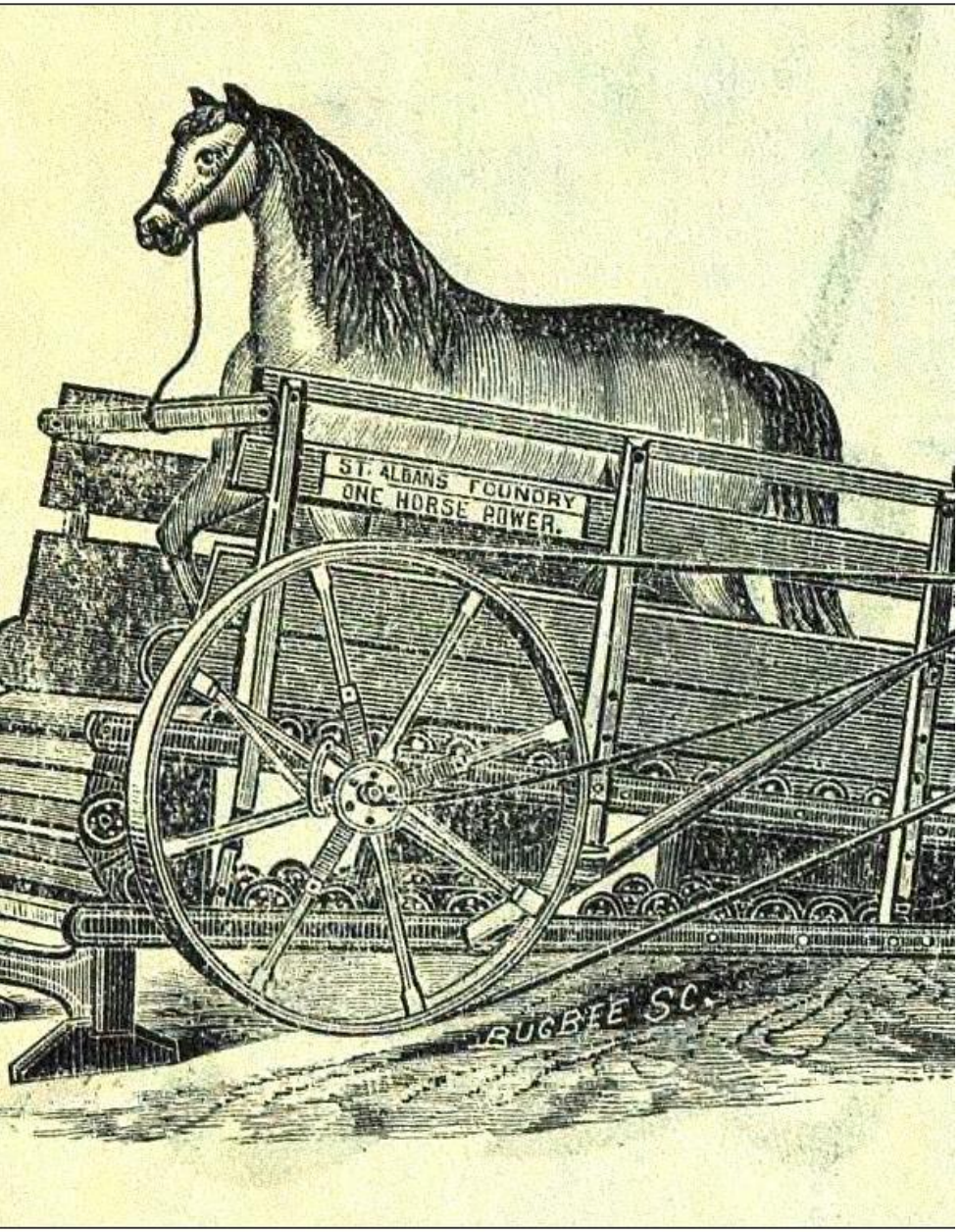


Indiana Ransomware Attack Coverage Bout

G&G Oil Co. of Indiana v. Continental Western Insurance Co, 145 N.E. 3d 842 (Ct. App. Ind. March 31, 2020)

- In November 2017, G&G suffered a ransomware attack that restricted the company from accessing its servers and most of its workstations.
- The company paid the hijacker's initial bitcoin demand. However, the hijacker refused to restore the company's control over its computer servers unless an additional payment was made.
- G&G made 3 more bitcoin payments before the hijacker gave the company the passwords to enable the decryption of their computers and regain access to their servers.

(c) 2021 Lexeprint Inc. All Rights Reserved



ONE HORSE POWER
ST. ALBANS FOUNDRY

Indiana Ransomware Attack Coverage Bout

G&G Oil Co. of Indiana v. Continental Western Insurance Co, 145 N.E. 3d 842 (Ct. App. Ind. March 31, 2020)

- Issue: Is an insurance company required to indemnify a company for their losses suffered as a result of a ransomware attack under a Policy's Computer Fraud Provision?
  - This case was a National first impression among appellate courts in the area of cybercrime.
- Ruling: The Indiana courts ruled that the bitcoin payments were not the result of fraudulent use of a computer.
- Observations: The crime was characterized by the court as theft. They found that there was no deception involved. Losses incurred as a result of a ransomware attack are not covered under the commercial crime coverage part of a multiperil commercial common insurance policy.

(c) 2021 Lexeprint Inc. All Rights Reserved



Indiana Supreme Court Reverses G&G Decision

- The Indiana Supreme Court ruled unanimously on March 18, 2021, reversing a lower court's ruling that Continental Western Insurance Co. doesn't have to cover a series of bitcoin ransom payments that policyholder G&G Oil Co. made to a hacker to restore access to the company's computer systems.
- The decision is the first by a state top court to weigh in on the applicability of crime insurance to a ransomware attack.

(c) 2021 Lexeprint Inc. All Rights Reserved

Key Takeaways

As cyber-attacks grow more frequent, companies should start to demonstrate very strong security systems, practices and policies as a precondition for obtaining insurance.

As insurers get comfortable with the idea of allocating capital to this unique sector, companies need to invest in their protection while working with their insurers to increase the different types and amount of insurance available to them.

There is no substitute for having a robust plan in place before incidents occur.

(c) 2021 Lexeprint Inc. All Rights Reserved

Contact Us



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



Peter Halprin
Email: PHalprin@PasichLLP.com
Phone: (646) 974-6470
Website: https://pasichllp.com/



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



Aarti Soni
Email: aarti.soni@mcgriff.com
Phone: (470) 332-8367
Website: https://www.mcgriff.com/



Phillip Jackman
Email: pjackman@cdas.com
Website: https://cdas.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.



Peter Halprin
Pasich LLP – Partner
Contact:
W: (646) 974-6470
E: PHalprin@PasichLLP.com
URL: https://pasichllp.com/

Peter A. Halprin is a partner in Pasich LLP's New York office. Peter represents commercial policyholders in complex insurance coverage matters with a focus on recovery strategies in relation to captive insurance, cyber crime, natural disasters, professional services and technology disputes, and regulatory investigations. Over the course of his career, Peter has arbitrated, litigated, and mediated claims involving a broad range of insurance policies and recovered hundreds of millions of dollars in insurance proceeds for policyholders.

Peter has advised clients regarding insurance coverage under an array of forms and policies including Boiler & Machinery, Builder's Risk, Commercial Crime, Cyber, Directors & Officers (D&O), Employment Practices Liability (EPLI), Errors & Omissions (E&O), Fidelity, General Liability (GL), Kidnap & Ransom (KKR), Media Liability, Pollution Legal Liability (PLL/EIL), Products Liability, Property, Technology E&O, Trade Credit, and Workers' Compensation.

Peter acts as counsel for U.S. and foreign companies in domestic and international arbitrations, including both ad hoc (ARIAS, Bermuda Form, London) as well as institutional (AAA, ICC, ICDR, JAMS, LCIA) arbitration forums. He has served as both party-appointed and sole arbitrator, and is a Member of the AAA National Roster of Arbitrators.

Peter has been recognized annually by Super Lawyers as a New York Metro Rising Star for Insurance Coverage since 2013.

Disclaimer: This profile constitutes attorney advertising and is for informational purposes only. The content is not legal advice and does not create an attorney-client relationship. Do not act upon information without seeking your own legal counsel. Unless specifically stated, an indication of a special area of practice, expertise, skill or endorsement does not imply certification by a state bar or other certifying organization.



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.



Aarti Soni
McGriff, Seibels & Williams – Cyber Director & Product Innovation Counsel
Contact:
W: (470) 332-8367
E: aarti.soni@mcgriff.com
URL: https://www.mcgriff.com/

McGRIFF, SEIBELS & WILLIAMS

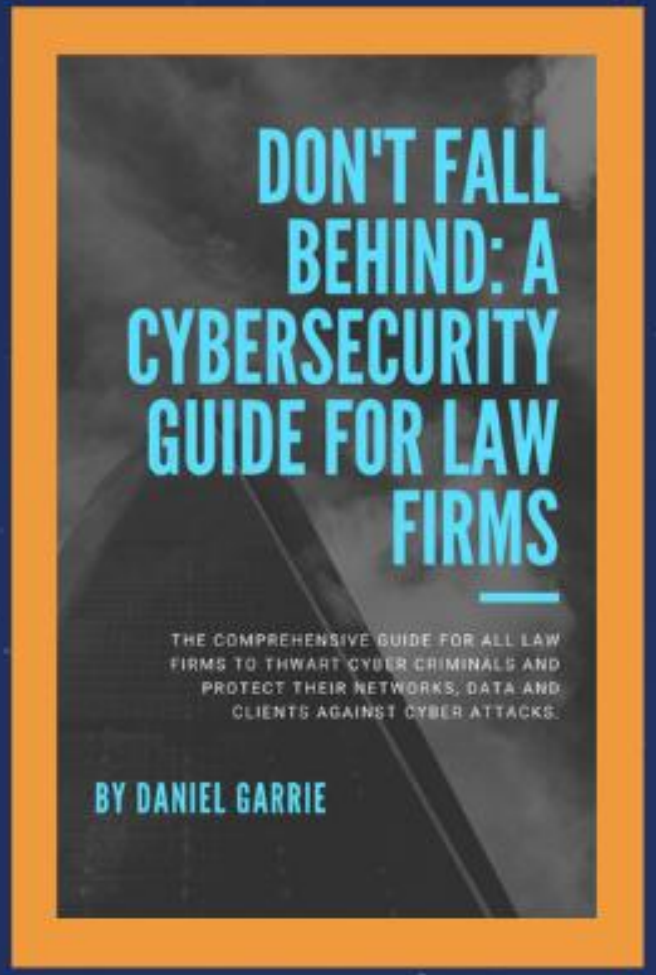
McGriff, Seibels & Williams Inc. named Atlanta-based Aarti Soni cyber director and product innovation counsel in its financial services division. Previously, Ms. Soni was senior vice president and cyber coverage leader for Marsh LLC.

She focuses her work on large, complex accounts in the cyber, technology, media and professional coverage arenas.

Aarti's current responsibilities include supporting clients by reviewing and negotiating policy wordings and serving as a resource on cybersecurity offerings and services, both pre- and post-event. Aarti also assists clients throughout the claim life cycle.

Aarti joined Marsh in July 2016. Prior to that time, she was a Claims Analyst at American International Group (AIG). She also worked an associate at two national law firms, where she handled complex insurance coverage litigation. Aarti most recently served as Assistant General Counsel, Professional Liability & Cyber Counsel at Chubb, where she was a member of the Cyber Product Board. There, she provided client support to Errors and Omissions (E&O) and cyber risk underwriters.

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) 2021 Lexeprint Inc. All Rights Reserved.