Introduction to Ransomware

Speaker:

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

David A. Cass, Senior Partner, Law & Forensics

Lynda Jensen, Mullen Coughlin LLC – Partner

Richard Rushing, Motorola Mobility – CISO

(c) 2022 Lexeprint Inc. All Rights Reserved.

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

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.

Speakers



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



David A. Cass
Senior Partner, Law & Forensics
Adjunct Faculty Harvard & Rutgers Law



Lynda Jensen
Mullen Coughlin LLC – Partner



Richard Rushing
Motorola Mobility – CISO

(c) 2022 Lexeprint Inc. All Rights Reserved.

Agenda

- Overview of Ransomware
- OFAC Ransomware Advisory 2021
- Ransomware Concerns During COVID-19
- Recent Ransomware Developments
- Best Practices to Limit an Organization's Ransomware Risk

(c) 2022 Lexeprint Inc. All Rights Reserved.



Overview of Ransomware

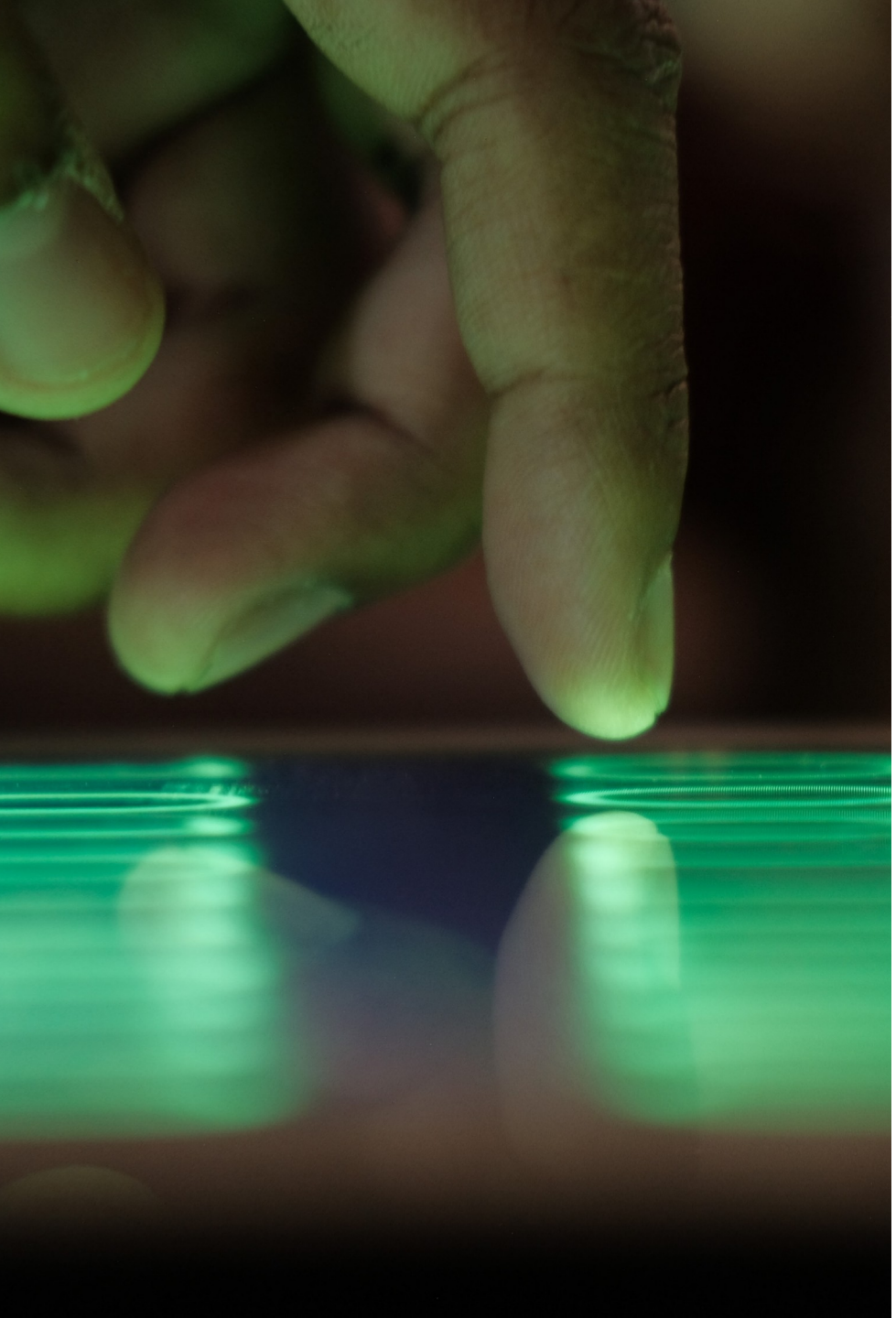
(c) 2022 Lexeprint Inc. All Rights Reserved.



What is Ransomware?

- Ransomware is computer malware that installs covertly on a victim's computer, executes a cryptovirology attack that adversely affects it, and demands a ransom payment to restore it.
- More advanced malware encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. The ransomware may also encrypt the entire hard drive.
- **Fake ransomware** is false encryption and destruction that is oftentimes irreversible (e.g., Not Petya).

(c) 2022 Lexeprint Inc. All Rights Reserved.



What are Ransomware Attacks?

- Ransomware attacks are cyber-attacks where a malicious actor will either:
  - (1) Demand a ransom for not encrypting data, destroying or not blocking access to a computer system or data, or
  - (2) Demand a ransom in exchange for restoring access to a computer system or to encrypt data that has already been encrypted.

(c) 2022 Lexeprint Inc. All Rights Reserved.


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

How does Ransomware Work?

- Ransomware uses asymmetric encryption which is a cryptography that uses a pair of keys to encrypt and decrypt a file.
- The most common way that ransomware can take access to a computer or system is by a ‘phishing’ spam.
- A ‘phishing’ spam is where victims receive an email that contains an attachment masqueraded as a file that they should trust.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY

How Does a Ransomware Attack Occur?

The IMB Security X-Force Report (2022) developed a five-stage model to detail the standard attack flow for ransomware attacks.*

- **Stage 1: Initial Access**
  - The most common access vectors for ransomware attacks continue to be phishing, vulnerability exploitation, and remote services such as remote desktop protocol.*

**IMB Security X-Force Threat Intelligence Index 2022 Report*

(c) 2022 Lexeprint Inc. All Rights Reserved.



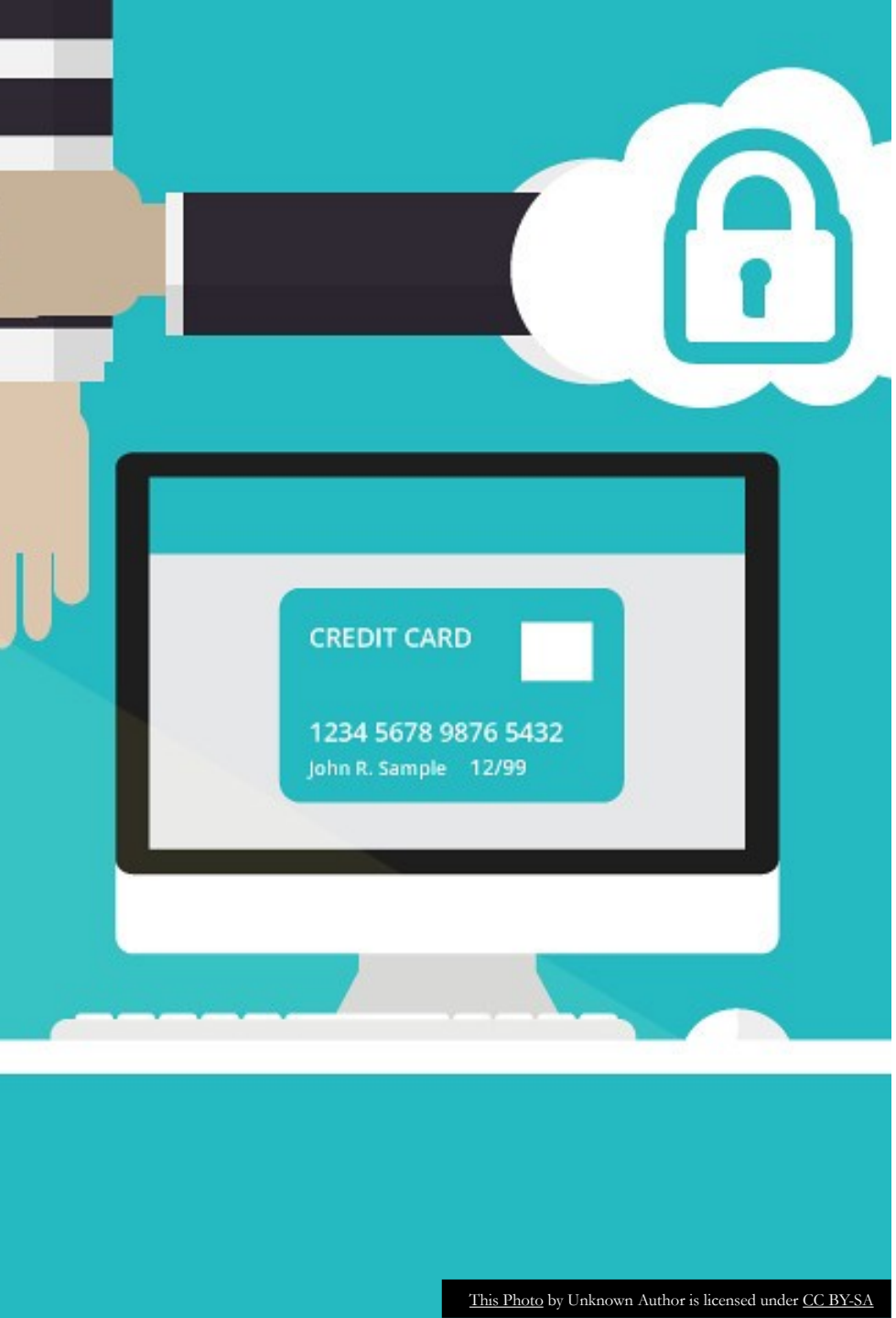
This Photo by Unknown Author is licensed under CC BY-SA-NC

How Does a Ransomware Attack Occur?

- **Stage 2: Post Exploitation**
  - Depending on the initial access vector, the second stage may involve an intermediary remote access tool (RAT) or malware prior to establishing interactive access with an offensive security tool.*
- **Stage 3: Understand and Expand**
  - During the third stage of the attack, attackers will focus on understanding the local system and domain and acquiring additional credentials to enable lateral movement.*
  - This includes gathering local reconnaissance, lists of hostnames, subnets to target, data sources, etc...

**IMB Security X-Force Threat Intelligence Index 2022 Report*

(c) 2022 Lexeprint Inc. All Rights Reserved.



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

How Does a Ransomware Attack Occur?

- **Stage 4: Data Collection and Exfiltration**
  - Almost every ransomware incident has involved the "double extortion" tactic of data theft and ransomware.
  - During this stage of the attack, the focus of the ransomware operators will switch primarily to identifying valuable data and exfiltrating it.
- **Stage 5: Understand and Expand**
  - Finally, the ransomware operators will target a domain controller as the distribution point for the ransomware payload.
  - This involves deploying ransomware using the domain administrator credentials via PsExec/SMB/group policy.*

**IMB Security X-Force Threat Intelligence Index 2022 Report*

(c) 2022 Lexeprint Inc. All Rights Reserved.



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

The U.S. Threat Environment

- The IBM X-Force Report details Ransomware remained the top attack type in 2021; sharing 21% of all cyber-attacks.
  - For over three years, ransomware has been the top attack type observed by X-Force.
- REvil, a ransomware type, was the most common ransomware strain observed for two consecutive years, making up 37% of all ransomware attacks, followed by Ryuk at 13%.*

**IMB Security X-Force Threat Intelligence Index 2022 Report*

(c) 2022 Lexeprint Inc. All Rights Reserved.


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

The U.S. Threat Environment (cont.)

- The Report details that ransomware attacks accounted for:
  - 38% of attacks on healthcare organizations;
  - 32% of attacks on professional and business services;
  - 25% of attacks on energy organizations;
  - 23% of attacks on manufacturing organizations;
  - 22% of attacks on education organizations; and
  - 10% of attacks on finance and insurance organizations.

**IMB Security X-Force Threat Intelligence Index 2022 Report*

(c) 2022 Lexeprint Inc. All Rights Reserved.


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

The Global Threat Environment

- Around the world, ransomware attacks remains prevalent.
  - In Asia, ransomware consists of 11% of cyber-attacks, taking second place after server access attacks.
  - In Europe, ransomware was the top attack, making up 26% of all attacks.
  - In North America, ransomware led as the top attack, making up 30% of all attacks.
  - In the Middle East and Africa, ransomware and server attacks were the top incident types, tying for first place with 18% of attacks each.
  - In Latin America, ransomware was the top attack, making up 29% of all attacks.*

**IMB Security X-Force Threat Intelligence Index 2022 Report*

(c) 2022 Lexeprint Inc. All Rights Reserved.


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

Ransomware and Law Enforcement

- The Report also details that 17 months is the average time before a ransomware group either rebrands or shuts down.
- Ransomware groups often spring up and rebrand once there is a threat of arrest or action by law enforcement.
  - Examples of groups who have renamed include GandCrab to REvil, Maze to Egregor, and DoppelPaymer to Grief.
- Law enforcement activity is the primary factor driving down the percentage of ransomware attacks; however, it is likely that the groups who have seemingly "disappeared" will rebrand and reemerge in 2022.

**IMB Security X-Force Threat Intelligence Index 2022 Report*

(c) 2022 Lexeprint Inc. All Rights Reserved.



OFAC Ransomware Advisory 2021

(c) 2022 Lexeprint Inc. All Rights Reserved.

This Photo by Unknown Author is licensed under CC BY



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

What is the OFAC Ransomware Advisory 2021?

- In September 2021, the U.S Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an updated advisory reinforcing that payments made to cyber actors are a violation of law.
- The payer is subject to civil penalties; specifically stating that it applies to cyber insurance companies, digital forensic, incident response companies, and financial services companies.
- This updated advisory was largely issued due to the increased demand of ransomware payments during the COVID-19 pandemic --- outlining the potential sanctions risks associated with making and facilitating ransomware payments.

(c) 2022 Lexeprint Inc. All Rights Reserved.



OFAC Language

- The Office of Foreign Assets Control (OFAC) issued the advisory to "highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities."
- 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 the cyber actor demanding ransomware payment.

(c) 2022 Lexeprint Inc. All Rights Reserved.


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

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) 2022 Lexeprint Inc. All Rights Reserved.



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

OFAC Advisory: History of Ransomware Attacks

- Ransomware attacks have now become more focused, sophisticated, costly and numerous.
- The IMB Security X-Force Report (2022) indicates that ransomware remained the top attack type in 2021; sharing 21% of all cyber-attacks.
- For over three years, ransomware has been the top attack type observed by X-Force.

(c) 2022 Lexeprint Inc. All Rights Reserved.


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

OFAC Advisory: Designations of Malicious Cyber Actors

- OFAC has designated numerous malicious cyber actors under its cyber-related sanctions program and other sanctions programs, including perpetrators of ransomware attacks and those who facilitate ransomware transactions.
- OFAC will continue to impose sanctions on these malicious attackers and others who materially assist, sponsor, or provide financial, material or technological support for these activities.
    - In September 2021, OFAC designated SUEX OTC, S.R.O. (SUEX), a virtual currency exchange, for its part in facilitating financial transactions for ransomware actors, involving illicit proceeds from at least eight ransomware variants.
    - In November 2021, OFAC designated Chatex, a virtual currency exchange, and its associated support network for facilitating transactions for multiple ransomware variants. *

** OFAC Ransomware Advisory 2021*

(c) 2022 Lexeprint Inc. All Rights Reserved.



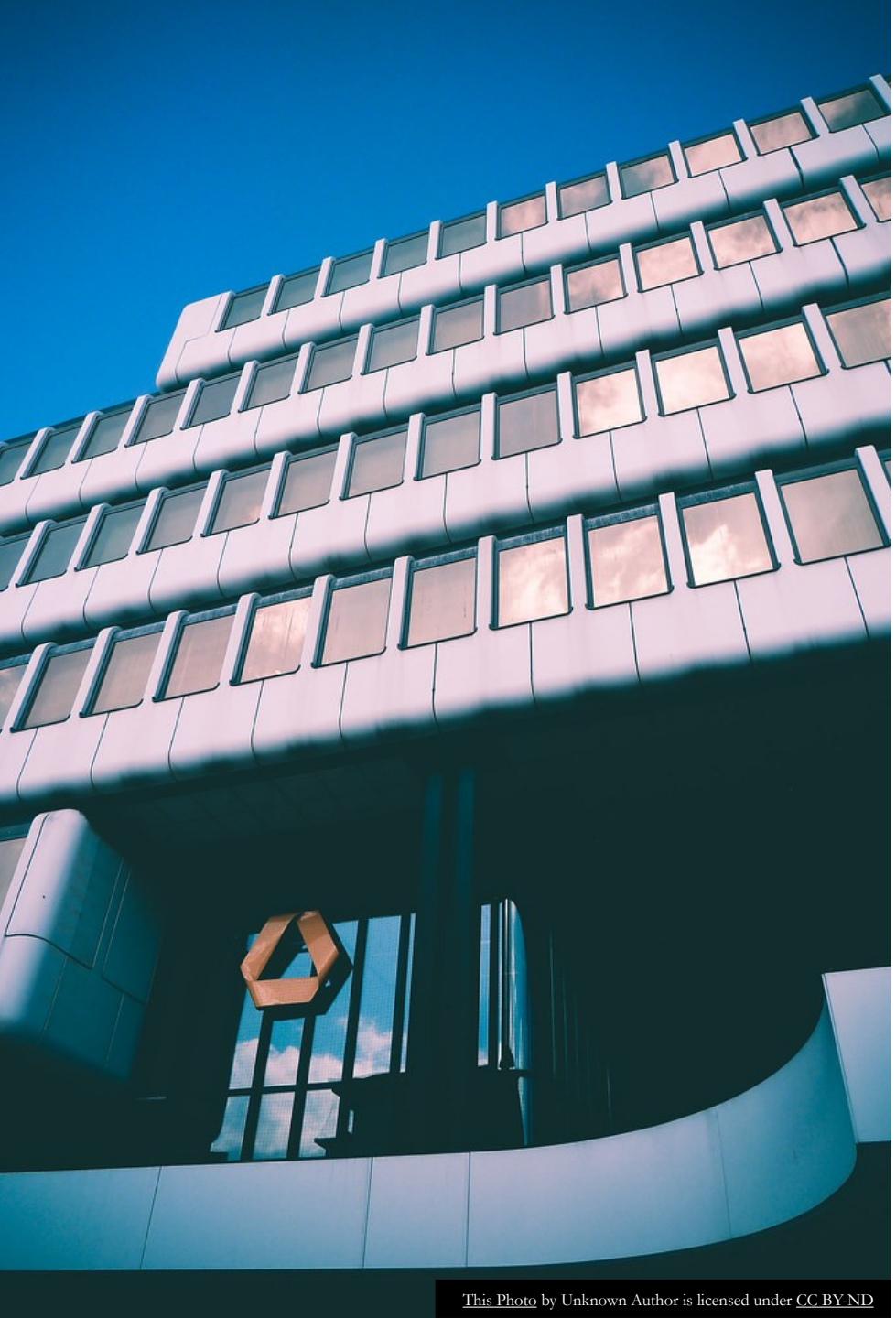
This Photo by Unknown Author is licensed under CC BY-SA-NC

OFAC Advisory: U.S. National Security Interests Threatened

- The advisory explains that paying the ransom to criminals may enable them to further advance their illicit aims --- encouraging future attacks.
- For example, ransomware payments made to sanctioned persons may be used to fund activities adverse to the national security and foreign policy objectives of the U.S.
- It is also important to note that paying a ransom to a cyber attacker will not always guarantee that the victim will regain access to its stolen data or any at all. *

** OFAC Ransomware Advisory 2021*

(c) 2022 Lexeprint Inc. All Rights Reserved.


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

OFAC Advisory: Paying Ransomware May Violate OFAC Regulations

- U.S. individuals are generally 'prohibited from engaging in transactions, directly or indirectly, with individuals or entities on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons and those covered by comprehensive country or region embargoes,' under the IEEPA or the TWEA.
- It was suggested that financial institutions and other companies implement a risk-based compliance program to mitigate exposure to sanctions-related violations.*

** OFAC Ransomware Advisory 2021*

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY

OFAC Advisory: Paying Ransomware May Violate OFAC Regulations (cont.)

- OFAC suggests that financial institutions implement a risk-based compliance program to mitigate exposure to sanctions-related violations.
- A company's self-initiated report of a ransomware attack to law enforcement will be a significant mitigating factor in determining enforcement outcomes if the case is concluded to have sanctions nexus.
- A company's full and timely cooperation with law enforcement during and after a malicious attack will also be considered as a significant mitigating factor when assessing any possible enforcement outcome.*

** OFAC Ransomware Advisory 2021*

(c) 2022 Lexeprint Inc. All Rights Reserved.


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

OFAC Advisory: Licensing Policy

- As Ransomware payments are a threat to U.S National security and foreign policy objects of the U.S., licensing applications for ransomware payments demanded as a consequence of cyber-enabled attacks will be reviewed by OFAC on a case-by-case basis with a presumption of denial.*

** OFAC Ransomware Advisory 2021*

(c) 2022 Lexeprint Inc. All Rights Reserved.



Ransomware Concerns During COVID-19

(c) 2022 Lexeprint Inc. All Rights Reserved.



Challenges Facing Organizations

- During the COVID-19 pandemic, organizations are facing simultaneous challenges:
  - The threat landscape is evolving to use COVID-19 as an allure to more successfully deposit ransomware in your network.
  - Preventative and detective controls may have had to be adapted to permit more flexible working practices.
  - The security team is having to manage incidents in unfamiliar conditions, including lockdown, with playbooks that don't cater to these operating modes.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Ransomware Activity Targeting the Healthcare and Public Health Sector

- In October 2020, Alert (AA20-302A) was released by the Cybersecurity and Infrastructure Security Agency CISA, FBI and HHS.
- Key Findings:
  - Malicious cyber actors are targeting the HPH Sector with TrickBot and BazarLoader malware, often leading to ransomware attacks, data theft, and the disruption of healthcare services.
  - These issues require administrators to balance this risk when determining their cybersecurity investments.

(c) 2022 Lexeprint Inc. All Rights Reserved.



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

Ransomware and Healthcare (cont.)

- In 2021, there were over 43 million records of healthcare data breaches in the United States – the highest in American history. *
- This resulted from a 94% increase in ransomware attacks on the organizations within the healthcare sector in 2021. *
- The Florida Healthy Kids Corporation data breach was the largest of 2021, with 3.5 million data records being breached.
- It is believed that this increased hacking can be attributed to the health care industry's rapid move to digital due to the Covid-19 pandemic; an increase in remote work has allowed for more avenues for cyber-attacks.*

- ** Infoblox, The 2022 Healthcare Cyber Trend Research Report*

(c) 2022 Lexeprint Inc. All Rights Reserved.


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

The Department of Health and Human Services (HHS) Cybersecurity Program: Hive Alert

- The Department of Health and Human Services (HHS) Cybersecurity Program was created in 2003 to protect HHS from information technology threats and vulnerabilities
- In April 2022, The HHS Cybersecurity Program issued an alert to healthcare providers warning them to guard against the "exceptionally aggressive" Hive ransomware group.
- Hive has been operational since June 2021 and hit 355 companies in its first 100 days of operation.*

**The Department of Health and Human Services Cybersecurity Program HC3 Analyst Note*

(c) 2022 Lexeprint Inc. All Rights Reserved.



Recent Ransomware Developments

(c) 2022 Lexeprint Inc. All Rights Reserved.

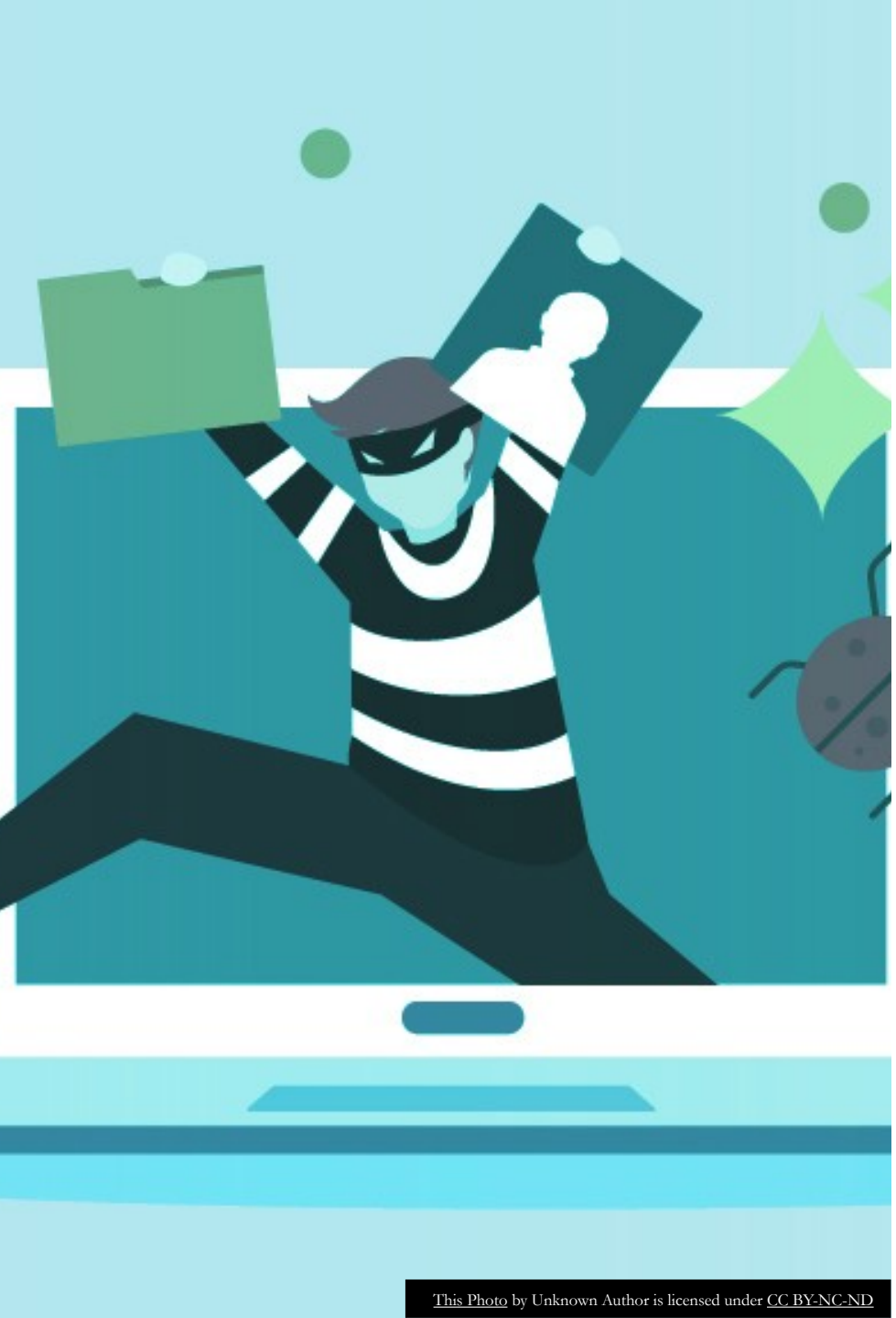


This Photo by Unknown Author is licensed under CC BY-ND

G&G Oil Co. of Indiana v. Continental Western Insurance Co (2020)

- **Facts:** 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. After three more bitcoin payments, the hijacker gave the company passwords to enable the decryption of their computers.
- **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.

(c) 2022 Lexeprint Inc. All Rights Reserved.



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

G&G Oil Co. of Indiana v. Continental Western Insurance Co (2020) (cont.)

- **Decision:** 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) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY

Indiana Supreme Court Reverses G&G (2021)

- 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) 2022 Lexeprint Inc. All Rights Reserved.


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

National Ink and Stitch, LLC v. State Auto Property and Casualty Ins. Co. (2020)

- **Facts:** The policyholder was the victim of a ransomware attack and despite paying the original ransom, the criminal demanded further payment. The policyholder paid a security company to install protective software on its server; however, there was a significant loss of efficiency, and the policyholder still could not access certain files.
- **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?

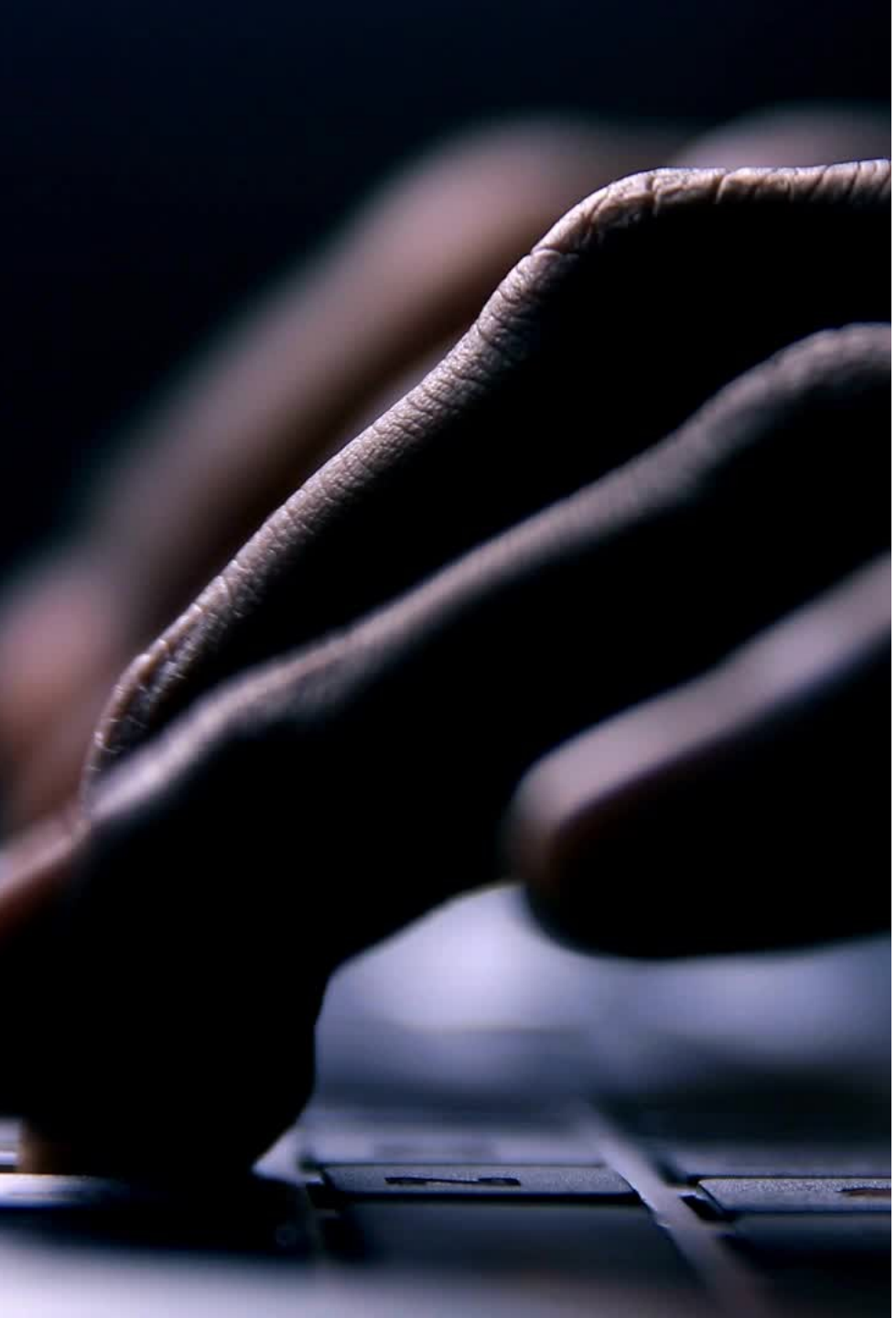
(c) 2022 Lexeprint Inc. All Rights Reserved.


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

National Ink and Stitch, LLC v. State Auto Property and Casualty Ins. Co. (2020) (cont.)

- **Decision:** The court held among other things, that the "loss of use, loss of reliability, or impaired functionality" were types of damage to covered property sufficient to trigger coverage.
- **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) 2022 Lexeprint Inc. All Rights Reserved.



EMOI Services, LLC v. Owners Ins. Co. (2021)

- **Facts:** All files on EMOI's computer system were encrypted by hackers. The files were made inaccessible to EMOI employees. The hackers demanded 3 bitcoins (roughly $35,000 at the time) for the files to be decrypted. The ransom was paid by EMOI, and the hackers provided EMOI with a key to decrypt their files. However, EMOI was not able to decrypt all files. As a result, EMOI changed their domain to a new one with better security. However, this change created problems. So, EMOI sued to enforce property insurance coverage after Owners Insurance denied their claim.
- **Issue:** Was EMOI entitled to coverage under the Electronic Equipment endorsement of Owners Insurance property policy?

(c) 2022 Lexeprint Inc. All Rights Reserved.



EMOI Services, LLC v. Owners Ins. Co. (2021) (cont.)

- **Decision:** The court ruled that a cyber-attack resulted in coverage under the commercial property insurance policy.
- **Observations:** The court found that "incursion" into the computer system did cause physical loss or damage. This ruling provides hope for policyholders who suffer from a cyberattack.
  - In addition, policyholders can put forward evidence showing precisely how their computer systems were damaged. There is a higher chance of physical loss or damage if hackers changed the computer system to prevent the policyholder from accessing it.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Best Practices to Limit an Organization's Ransomware Risk

(c) 2022 Lexeprint Inc. All Rights Reserved.

Ransomware Prevention: Planning Challenges to Consider

Understand the Environment	Know the Threat Landscape	Understand What you are Protecting
• Thousands of vulnerabilities; • Rapidly changing paradigms; and • Dozens of operating systems.	• Easy to evade signature detection; • New scams pop up daily; • Knowledge sharing is poor; and • Hard to know who might attack you.	• Confidentiality of critical data; • Availability of resources (DDoS); • Organization/data integrity; • Reporting requirements; and • Value to an attacker and to your organization.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Technical Considerations

- Access Controls – Least Privilege
- Sufficient Logging
- Breadth and Retention Length
- Capacity Planning
- Factor in DDoS attacks
- Network Visibility
- Logs, Metadata, Full Packet
- Detect and Block – Intelligence driven

(c) 2022 Lexeprint Inc. All Rights Reserved.



Non-Technical Considerations

- Business Impact Assessment
- Legal and Reporting Obligations
- Corporate Policies
- Internal and External Communication
- Cyber Insurance
- Law Enforcement
- External Investigators

(c) 2022 Lexeprint Inc. All Rights Reserved.



Back up Data Regularly and in a Secure Manner

- Legal, risk, and compliance teams need to work with IT to understand the architecture of the system and what data will be available under differing attack scenarios.
- Testing of both the system and the backup is critical.

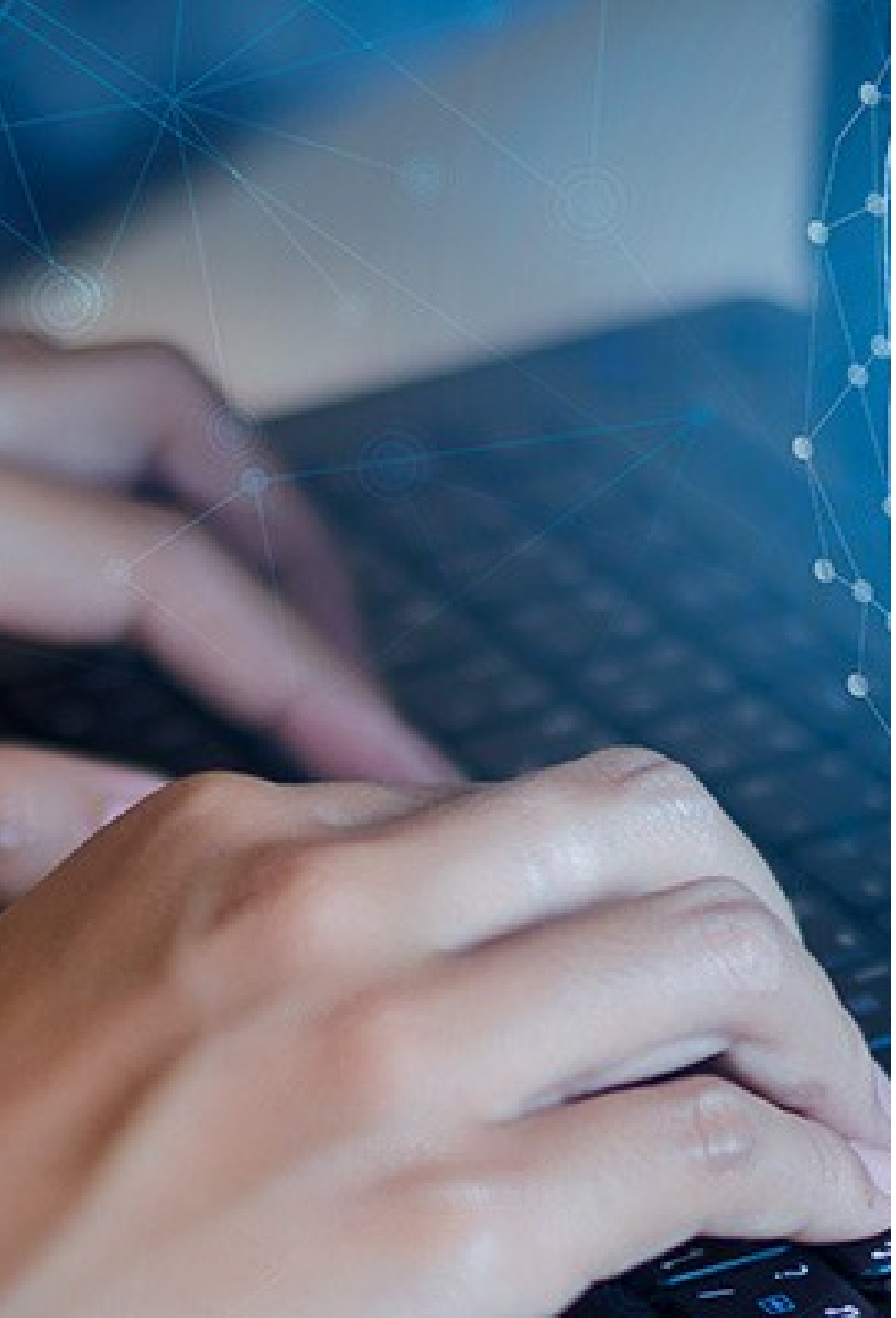
(c) 2022 Lexeprint Inc. All Rights Reserved.



Establish **Security Awareness** Campaigns that Stress the Avoidance of Clicking on Links/Attachments in Email.

- Don't click on links or download attachments in unknown/unexpected emails.
- When receiving an email message with a link or an attached file ask yourself:
  - 1) Do I know the sender?
  - 2) Do I need to open that file or go to that link?
  - 3) Did I order something from *FedEx*?

(c) 2022 Lexeprint Inc. All Rights Reserved.



Protect Company Data

- Use unique and strong login credentials; and
- Use a security software that gives multilayered protection.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Keep Your Computer's Operating System Up-to-Date

- **Patching** commonly exploited third party software such as Java, Flash, and Adobe will undoubtedly prevent many of these types of attacks from even being successful in the first place.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Restrict Administrative Rights

- Limit the ability of employees who do not need the authority to install software and limit the access of employees to data to only that data to which they need access.

(c) 2022 Lexeprint Inc. All Rights Reserved.



(c) 2022 Lexeprint Inc. All Rights Reserved.

Contact



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



David Cass
Email: davidcassciso@gmail.com
URL: www.lawandforensics.com



Lynda Jensen
E: ljensen@mullen.law
URL: https://www.mullen.law



Richard Rushing
E: rrushing@motorola.com
URL: https://www.motorola.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. 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, cryptocurrency, 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) 2022 Lexeprint Inc. All Rights Reserved.



David Cass
Law and Forensics Senior Partner
Contact:
E: david@lawandforensics.com
URL: www.lawandforensics.com

LAW & FORENSICS
A Global Legal Engineering Firm

Mr. Cass recently joined Law and Forensics as a Senior Partner. He leads the Crypto & Digital Banking Practice and is a key member of the Cybersecurity & Privacy practice. Prior to joining, David served as a regulator. He was the Vice President for Cyber & IT Risk for the Federal Reserve Bank of New York. David specialized in large institution supervision, Fin-Tech, AI/ML, and cryptocurrencies. Prior to this role, David served as the Chief Information Security Officer for IBM. He had global responsibility for all aspects of security practices, processes, and policies across the IBM Cloud SaaS business unit.

Previously David served as the SVP & Chief Information Security Officer for Elsevier, where he led an organization of experienced legal, risk and security professionals that provided data protection, privacy, security, and risk management guidance on a global basis for Elsevier.

David has extensive experience in IT security, risk assessment, risk management, business continuity and disaster recovery, developing security policies and procedures. He has played a key role in leading and building corporate risk & governance and information security organizations in the financial sector. As the Senior Director of Information Security Risk and Governance for Freddie Mac, David rebuilt the risk and governance function and developed a team to provide risk assessments, methodologies, tools, services, and training to improve the organization's capabilities and maturity. Prior to that he was Vice President of Risk Management for JPMorgan Chase and was responsible for providing an accurate assessment of the current risk management state, contributing to the future direction of risk management, continuity and disaster recovery capabilities for the organization.

David has a MSE from the University of Pennsylvania, and a MBA from MIT. He is adjunct faculty for Rutgers Law School and Harvard. He is also a frequent speaker at high profile industry conferences and served on several boards.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Lynda Jensen
Mullen Coughlin LLC – Partner
Contact:
E: ljensen@mullen.law
W: (267) 930-2303
URL: https://www.mullen.law

MULLEN COUGHLIN

Lynda Jensen is a Partner at Mullen Coughlin and an experienced privacy, cybersecurity and incident response attorney. Ms. Jensen focuses her practice on guiding organizations of all shapes and size through the incident response process when a privacy or security event has occurred, including from initial triage and investigation through performance of legal obligations the organizations may have. Ms. Jensen also advises organizations of their privacy and cybersecurity obligations under applicable laws and assists them with compliance efforts.

Prior to joining Mullen Coughlin, Ms. Jensen developed extensive experience as a civil litigator and a deep knowledge of computer-related events and crimes both as a practicing lawyer and as a Managing Director and Counsel of a team of as professionals handling crime, cyber and kidnap and ransom claims. This experience informs strategies that she recommends to clients before, during and after a data or privacy incident has occurred.

PUBLICATIONS

- "Fidelity Casenotes," Surety Claims Institute Newsletter
- "Discovery of Loss: The Contractual Predicate to the Claim," Chapter in *Financial Institution Bonds*, Fourth Edition, 2016
- "EMV – The New Frontier of Fraud," Co-Author, Community Bank Alert, 2015



Richard Rushing
Motorola Mobility – CISO
Contact:
E: rrushing@motorola.com
URL: https://www.motorola.com

Richard is the Chief Information Security Officer for Motorola Mobility. Richard participates in several corporate, community, private, and government Security Council's and working groups setting standards, policies, and solutions to current and emerging security issues. As Chief Information Security Officer for Motorola Mobility, he has led the security effort by developing an international team to tackle the emerging threats of mobile devices, targeted attacks, and cyber-crime.

He organized developed and deployed practices, tools and techniques to protect the intellectual property across the worldwide enterprise. A much-in-demand international speaker on information security Richard has presented at many leading security conferences and seminars around the world.