Best Practices for Engaging with Law Enforcement and Understanding Cyber Insurance

Speakers:

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

Andrew Dawson, Assistant United States Attorney, U.S. Department of Justice

Benjamin Kingsley, Chief, Oakland Branch, United States Attorney's Office, Northern District of California

Donovan McKendrick, Special Assistant, Department of Justice, Federal Bureau of Investigations

Bridget Quinn Choi, Cyber Insurance Executive

Peter Halprin, Partner, Pasich LLP

(c) 2023 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, as spoken and do not reflect those of their employers or clients.



This presentation is offered for educational and informational uses only.



Soliciting speakers is strictly prohibited.

(c) 2023 Lexeprint Inc. All Rights Reserved.

Speakers



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



Andrew Dawson
Assistant United States Attorney
U.S. Department of Justice

Benjamin Kinsley
Chief, Oakland Branch
United States Attorney's Office, Northern District of California



Donovan McKendrick
Special Assistant
Department of Justice, Federal Bureau of Investigations

(c) 2023 Lexeprint Inc. All Rights Reserved.

Agenda

- Part 1
  - Best Practices For Engaging with Law Enforcement Before and During Cyber Incidents
- Part 2
  - Overview of Cyber Insurance
  - What are the Different Types of Cyber Insurance?
  - Issues with Cyber Insurance Today
  - Best Practices

(c) 2023 Lexeprint Inc. All Rights Reserved.

Best Practices For Engaging with Law Enforcement Before and During Cyber Incidents

(c) 2023 Lexeprint Inc. All Rights Reserved

What is the role of the FBI and AUSAs in cyber incidents?

(c) 2023 Lexeprint Inc. All Rights Reserved


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

Understanding the Role of the FBI and AUSAs

- FBI
  - Investigations
  - Threat analysis
  - Attribution
  - Coordination
  - Prosecution
  - Victim Assistance
- AUSAs
  - Prosecution
  - Advice and guidance
  - Negotiations and pleas
  - Victim advocacy

(c) 2023 Lexeprint Inc. All Rights Reserved.

Why should boards and corporations engage with the FBI and AUSAs before or during cyber incidents?

(c) 2023 Lexeprint Inc. All Rights Reserved


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

Why Boards Should Engage

- Some of the reasons include:
  - Demonstrating active oversight and commitment to compliance.
  - Accessing expertise and resources.
  - Obtaining threat intelligence to help prevent future attacks.
  - Receiving support in coordinating with other agencies.
  - Detering would-be attackers.
  - Protect reputation.

(c) 2023 Lexeprint Inc. All Rights Reserved.

How should boards and corporations engage with the FBI and AUSA before or during cyber incidents?

(c) 2023 Lexeprint Inc. All Rights Reserved


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

How Boards Should Engage

- Establish a response team and incident response plan.
- Contact counsel.
- Report the incident.
- Cooperate and share information.
- Understand the investigative process.
- Preserve evidence.
- Coordinate with other agencies.
- Maintain regular communication channels.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Cybersecurity Information Sharing Act (CISA)

- The Cybersecurity Information Sharing Act (CISA) establishes a voluntary system for sharing cyber threat indicators and defensive measures between federal and nonfederal entities.
- The CISA has two Main Components:
  - (1) Authorizes companies to monitor and implement defensive measures on their own information systems to counter cyber threats.
  - (2) Provides protections to encourage companies to share information about cyber threat "indicators and defensive measure" with federal and state governments.

(c) 2023 Lexeprint Inc. All Rights Reserved.

Ransomware Hypothetical:

Facts: A ransomware attack is crippling your organization's critical infrastructure. Steps have been taken to isolate the affected systems and assess the impact.

Question: When and how should you involve law enforcement?

(c) 2023 Lexeprint Inc. All Rights Reserved


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

Best Practices Checklist

- Law enforcement agencies often have the specialized skills to assist in the technical, legal, and procedural elements of the response.
- Best practices include:
  - Activating the incident response plan and connecting with law enforcement contacts.
  - Preserving evidence for law enforcement.
  - Consulting inside and predetermined outside counsel to understand obligations and liabilities.

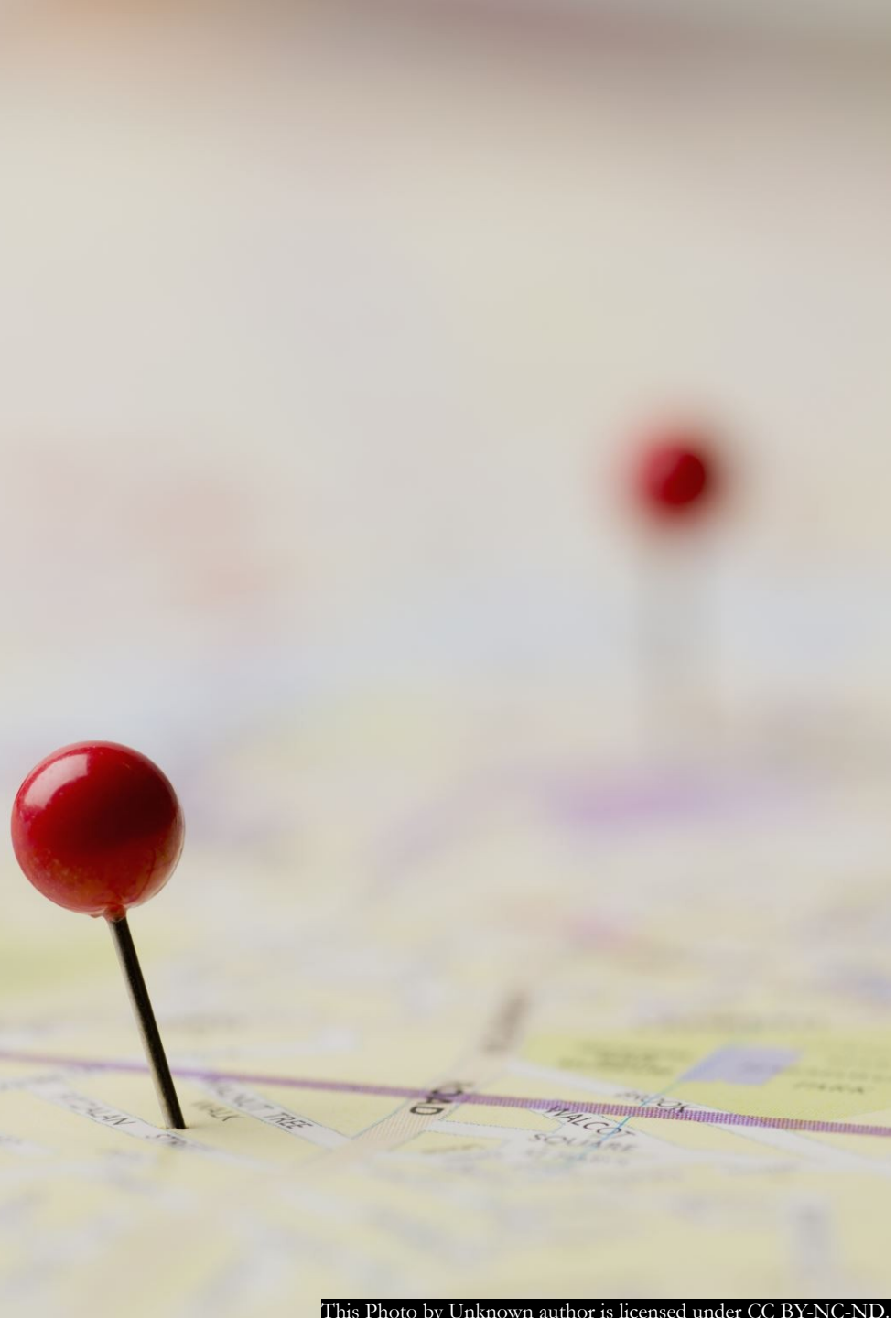
(c) 2023 Lexeprint Inc. All Rights Reserved.


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

Building a Pre-Incident Relationship

- Establishing a relationship with law enforcement is critical for effective action during an incident and in the aftermath.
- These relationships can help streamline and accelerate response times and result in more effective actions.
- Regular briefings with law enforcement can additionally keep the board updated on emerging threats.

(c) 2023 Lexeprint Inc. All Rights Reserved.


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

Incident Response Plan

- Organizations' incident response plan should include specific protocols for engaging with law enforcement.
  - This may include who to contact and how.
- Incident response plans should be dynamic, through regular updates and testing.
- It should be a living document that evolves with the threat landscape and organizational changes.

(c) 2023 Lexeprint Inc. All Rights Reserved.


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

Outside Counsel

- Retain legal counsel specializing in cybersecurity laws and regulations.
- Legal counsel can guide when and how to engage with law enforcement.
- Counsel can also help navigate legal obligations and potential liabilities.

(c) 2023 Lexeprint Inc. All Rights Reserved.

Speakers



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



Peter Halprin
Partner
Pasich LLP



Bridget Quinn Choi
Cyber Insurance
Executive

(c) 2023 Lexeprint Inc. All Rights Reserved.



Daniel will serve as the moderator.

Overview of Cyber Insurance

(c) 2023 Lexeprint Inc. All Rights Reserved

What is the value of cyber insurance?

What role does cyber insurance play in cyber risk management?

(c) 2023 Lexeprint Inc. All Rights Reserved


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

What is Cyber Insurance?

- Cyber insurance is an insurance policy that provides businesses with a combination of coverage options to help protect the company from data breaches and other cyber security issues.
- Information subject to breaches can include the following:
  - Social Security numbers;
  - Credit card numbers;
  - Account numbers;
  - Driver's license numbers; and
  - Health records.

(c) 2023 Lexeprint Inc. All Rights Reserved.


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

What Does Cyber Insurance Cover?

- Cyber insurance covers a business' liability for a data breach in which the personal information of the firm's customers and clients is exposed or stolen by a hacker.
- Policies **may** also cover liability arising from:
  - Business interruption
  - Data loss/destruction
  - Computer fraud
  - Fund transfer loss

(c) 2023 Lexeprint Inc. All Rights Reserved.

What are the Different Types of Cyber Insurance?

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

(c) 2023 Lexeprint Inc. All Rights Reserved.



Two Types of Cyber Insurance

- Cyber insurance can include both First Party Insurance and Third-Party insurance.
- First Party Coverage covers the cost to respond to a hack or data breach on your computers.
- Third-Party Coverage covers the people and businesses responsible for the systems that allowed a data breach to occur.

(c) 2023 Lexeprint Inc. All Rights Reserved.


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

Third-Party Cyber Coverage

- Third Party Cyber insurance (also called Cyber Liability insurance) pays claims to Third-parties who were affected by a cyber event, such as customers, clients, regulators, partners, employees and other organizations.
- Questions to ask:
  - 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) 2023 Lexeprint Inc. All Rights Reserved.

First v. Third Party Coverage Agreements

First-Party Insurance coverage: direct loss and out of pocket expense incurred by insured

Coverage	Description
Business Income/ Extra Expense	Reimbursement for loss of income and/or extra expense resulting from an interruption or suspension of computer systems due to a failure of technology. Includes coverage for dependent business interruption and forensic expenses.
Data Asset Protection	Recovery of costs and expenses you incur to restore, recreate, or recollect your data and other intangible assets (i.e., databases, software, applications) that are corrupted or destroyed by a computer attack.
Event Management	The following costs resulting from a privacy breach: Forensic services; Breach notification services (including legal fees, call center, etc.); Identity/fraud monitoring expenses; and public relations.
Cyber Extortion	Costs of consultants and extortion monies for threats related to interrupting systems and releasing private information.

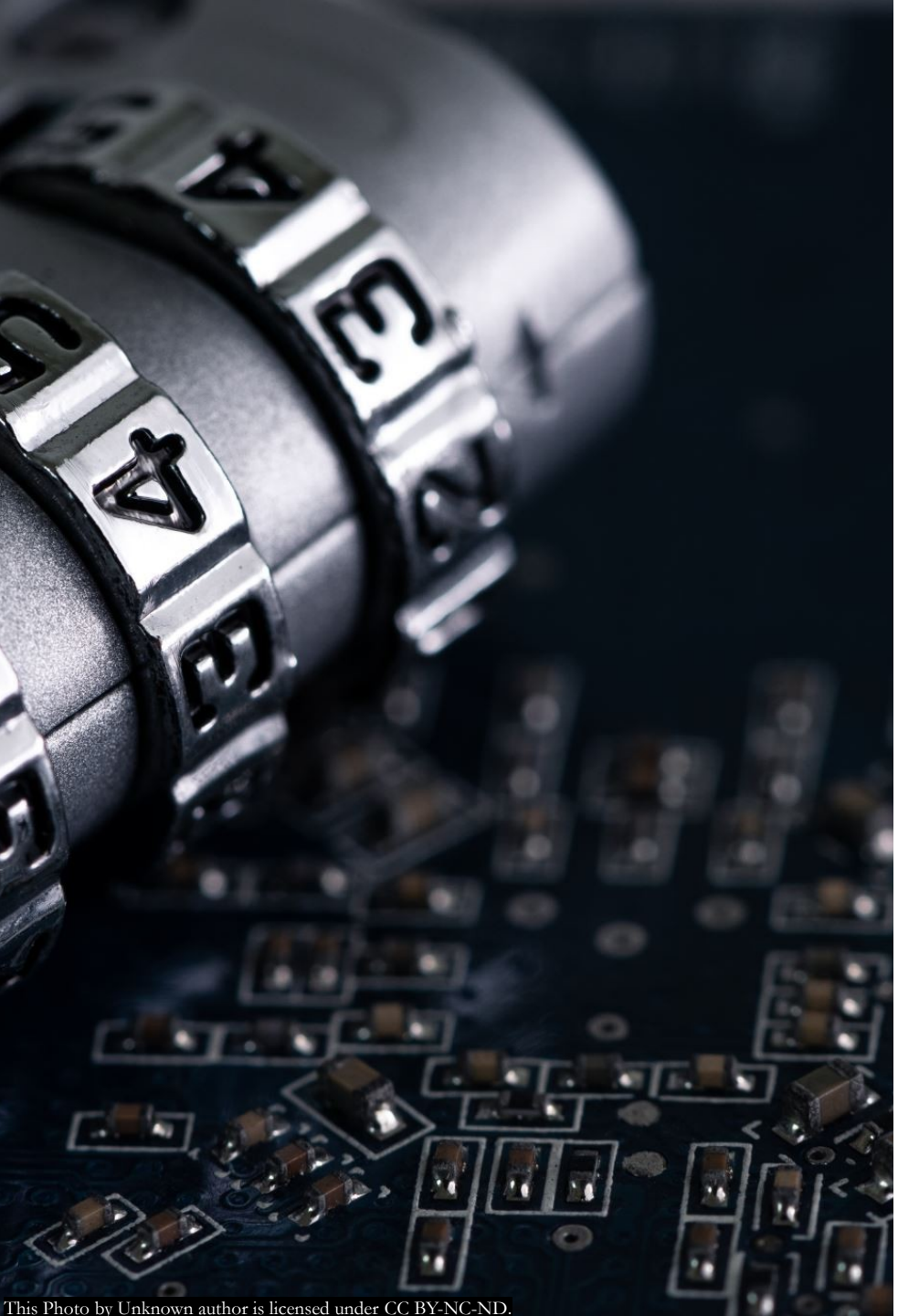
(c) 2023 Lexeprint Inc. All Rights Reserved.

First v. Third Party Coverage Agreements

Third-Party insurance coverage: liability incurred from harm caused by the insured, including defense of claims

Coverage	Description
Privacy Liability	Defense and liability for failure to prevent unauthorized access, disclosure or collection of confidential information, or for failure of others to whom you have entrusted such information (e.g., pension actuary, data storage facility, credit card processor). Also includes liability for not properly notifying of a privacy breach. Coverage includes corporate information such as third-party trade secrets. Likely Claimants: customers, employees, trading partners.
Network Security Liability	Defense and liability for failure of system security to prevent or mitigate a computer attack including but not limited to spread of virus or a denial of service. Failure of system security includes failure of written policies and procedures addressing technology use. Likely Claimants: Third-Party Loss, customers, employees.
Privacy Regulatory Defense Costs	Costs to defend an action or investigation by regulator due to a privacy breach, including indemnification for any fines or penalties assessed. Likely Claimants: Attorney General, FTC.
Media Liability	Defense and liability for online libel, slander, disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, negligence in content to those that relied on content. Likely Claimants: authors, producers, publishers, competitors, license holders.

(c) 2023 Lexeprint Inc. All Rights Reserved.


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

Stand-Alone vs. Endorsement Policy

- **Stand-Alone** insurance product
  - Refers to policy 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.
- **Cyber Risk "Endorsements"**
  - Refers to 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) 2023 Lexeprint Inc. All Rights Reserved.

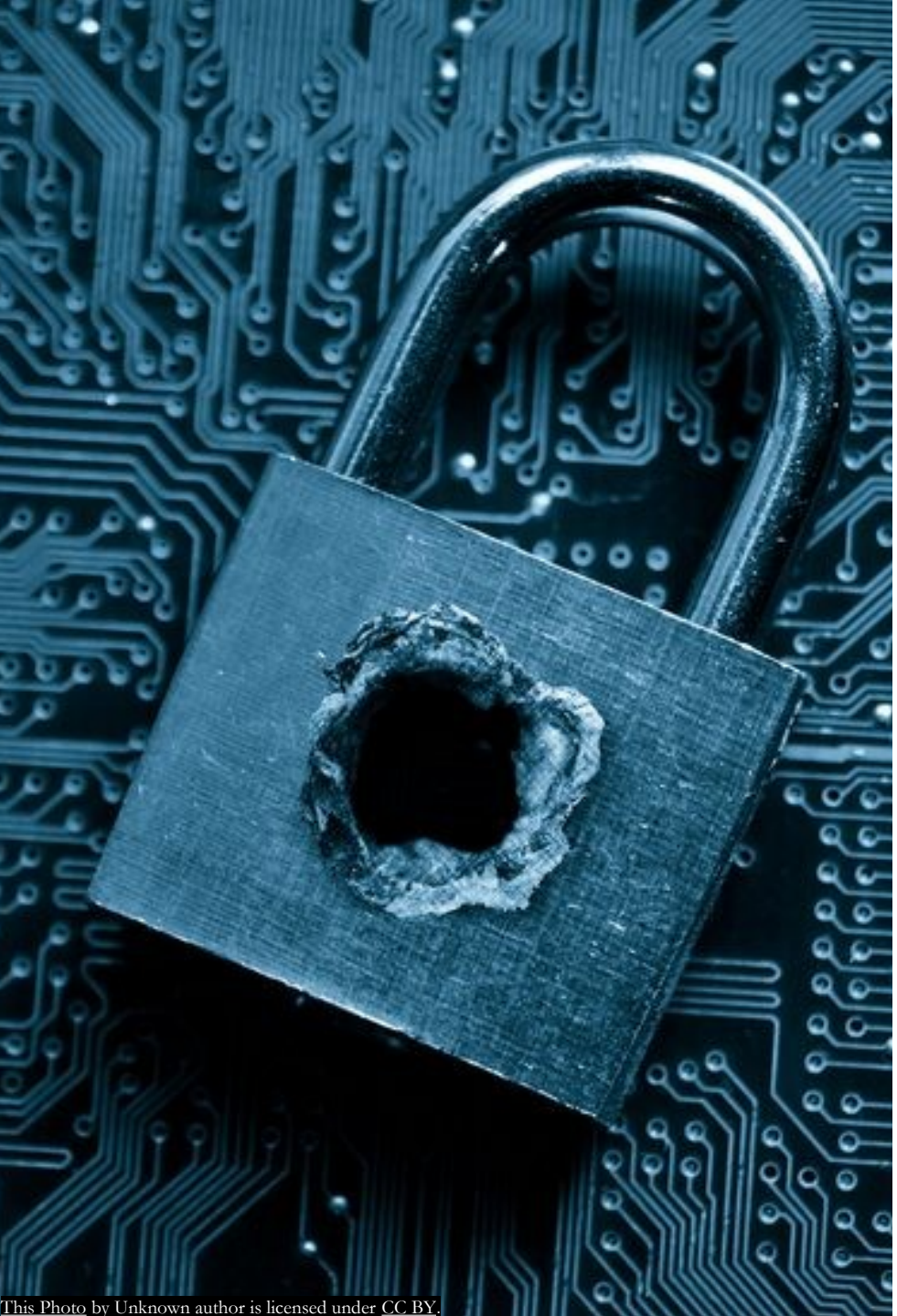


This Photo by Unknown author is licensed under CC BY-SA.

Threats Cyber Insurance Can Protect Against

- Internal Threats
  - Social engineering
  - Lost mobile devices
  - Improper handling of PII
  - Unintentional disclosure
  - Rogue employees
  - Coding inaccuracies
- External Threats
  - Hackers
  - DDOS attacks
  - Vendors
  - Ransomware

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY.

Factors Examined by Underwriters

- Type of business/industry;
- Size of business;
- Type of data handled (e.g., financial information, health information, credit information);
- Existing data protection and controls;
- Disaster recovery and business continuity plans;
- Risk of suppliers, vendors, and business partners; and
- Breach/loss history.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Issues with Cyber Insurance Today

(c) 2023 Lexeprint Inc. All Rights Reserved.

What are some issues or challenges of cyber insurance?

(c) 2023 Lexeprint Inc. All Rights Reserved



This Photo by Unknown author is licensed under CC BY.

The Importance of Cyber Insurance Policy Application

- Understanding the application of cyber insurance is foundational for the coverage.
- Oftentimes, cyber applications ask extraordinarily broad and complex questions and expect a risk manager to check a box with a simple "yes" or "no" response.
- However, when yes-or-no responses are not adequate, it is easy for material information to be omitted or misstated in the application — constituting application fraud or resulting in a denial of coverage for a claim.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Coverage Sub-limits

- Cyber policies often come with numerous coverage grants, each with a "sublimit" of coverage. This can be confusing, especially if there are endorsements that modify either the grants or the sub-limits of coverage.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Duty to Defend

- Duty to Defend: Insurer obligation to provide legal defense and coverage for claims against the insured party.
- Most cyber liability policies are written on a "duty to defend" basis —implying that decisions such as which law firm to use, how to defend a claim, and terms of the settlement are determined by the insurance carrier and not the insured.
- Insurers, Brokers, and Risk Managers should discuss defense arrangements during the procurement process.
- It is imperative for risk managers to carefully review the defense arrangements with the board, general counsel's office, and the IT department in advance of a claim.

(c) 2023 Lexeprint Inc. All Rights Reserved.


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

Limitations in Cyber Liability Policies and Coverage

- Despite the great work being done by insurance carriers to improve policies that can meet the needs of businesses, there can still be several limitations that vary amongst policies.
- Areas of coverage issues:
  - Limitation or no coverage for cyber incidents that arise from computer hardware that is not owned by the insured (for example: an employee's personal laptop, tablets , and other smart devices); and
  - Limitation or no coverage for social engineering claims, such as funds transfer fraud incidents.

(c) 2023 Lexeprint Inc. All Rights Reserved.


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

Lack of Uniformity

- Unlike traditional insurance industries, the Cyber Insurance field suffers from a severe lack of uniformity and industry standards.
- An important example is that there is frequently a coverage gap that may exist under some policies for insider cyber-attacks. An insider attack is committed by employees, vendors, suppliers, and others who may have authorized access to critical or sensitive data.
- Many cyber insurance policies may only cover cyber-attacks and data breaches committed by external hackers.

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY.

War Exclusions

- 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.
- For purpose of this exclusion, "Cyber Terrorism" means any actual, alleged, or threatened attack against the Insured's Critical System with the intention to cause harm or further social, ideological, religious, or political objectives or to intimidate any person or entity in furtherance of such objectives.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Best Practices

(c) 2023 Lexeprint Inc. All Rights Reserved.

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


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

Best Practices

- Cyber Policy Considerations
  - It is important for organizations to understand its unique exposures and associated risk;
- Incident Response
  - If a cyber-event occurs, corporations should:
    - Contact their insurance provider immediately and prepare for a potentially lengthy investigation;
    - Communicate with their broker;
    - Provide data to forensic analysts; and
    - Create and implement an incident response plan.

(c) 2023 Lexeprint Inc. All Rights Reserved.



(c) 2023 Lexeprint Inc. All Rights Reserved.

Contact Us



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



Andrew Dawson
Email: andrew.dawson@usdoj.gov
URL: https://www.justice.gov/



Peter Halprin
Email: PHalprin@PasichLLP.com
URL: https://pasichllp.com



Benjamin Kingsley
Email: benjamin.kingsley@usdoj.gov
URL: https://www.justice.gov/



Bridget Quinn Choi
Email: bridgetquinn@gmail.com



Donovan McKendrick
Email: donovan.mckendrick@usdoj.gov
URL: https://www.justice.gov/

(c) 2023 Lexeprint Inc. All Rights Reserved.



Daniel B. Garrie, Esq.
Law & Forensics LLC – Founder
JAMS – Neutral
Harvard – Adjunct
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: https://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, Esq. is the Co-Founder of Law & Forensics LLC, where he heads the Computer Forensics and digital discovery Cybersecurity teams. Daniel has been a dominant voice in the computer forensic and cybersecurity space for the past 20 years, as an attorney and technologist. He is an adjunct professor at Harvard for Computer Forensics and prior to Law & Forensics, 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. He is a mediator, arbitrator, and e-discovery special master for JAMS and is a partner and head of the Cybersecurity at Zeichner, Ellman & Krause LLP. Daniel has both a Bachelor's and a Master's degree in computer science from Brandeis University, as well as a J.D. from Rutgers Law School.

Daniel has led cyber and forensic teams in some of the most visible and sensitive cyber incidents in the United States. He and his team have worked for two of the top five banks in the globe, and dozens of the largest private and public companies in the world. In addition, Daniel has been awarded several patents for advanced cybersecurity and forensic platform he built with his team that is currently used in the industry, TableTop.AI, CustodyTrack.IO, and Forensic Scan.

Daniel is also well-published in the cybersecurity space and has authored more than 200 articles and books. His work is cited by Black's Law Dictionary 10th Ed. In defining the terms "software", "internet", and "algorithm." Lastly, he has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Andrew Dawson
U.S. Department of Justice – Assistant United States Attorney
Contact:
E: andrew.dawson@usdoj.gov
URL: https://www.justice.gov/

Andrew Dawson is an Assistant United States Attorney at the U.S. Department of Justice, Northern District of California.

(c) 2032 Lexeprint Inc. All Rights Reserved.



Benjamin Kingsley
United States Attorney's Office, Northern District of California – Chief, Oakland Branch
Contact:
E: benjamin.kingsley@usdoj.gov
URL: https://www.justice.gov/

Benjamin Kingsley is the Chief of the Oakland Branch of the U.S. Attorney's Office.

(c) 2032 Lexeprint Inc. All Rights Reserved.



Donovan McKendrick
Department of Justice, Federal Bureau of Investigations – Special Assistant
Contact:
E: donovan.mckendrick@usdoj.gov
URL: https://www.justice.gov/

Donavan McKendrick is a Special Assistant U.S. Attorney in the Northern District of California and a sworn Special Agent with the Department of Justice, FBI, working Cyber Crime and Cyber Counter Intelligence, Cryptocurrency Investigations and Seizures, Asset Forfeiture, White Collar Crime, and Regulatory Compliance violations (e.g. AML requirements).

(c) 2032 Lexeprint Inc. All Rights Reserved.



Bridget Quinn Choi
Cyber Insurance Executive
Contact:
E: bridgetquinn@gmail.com

Bridget Choi is a cyber insurance executive and consultant. Choi has a broad perspective of cyber risk from her various roles within the industry Most recently she has served as the head of cyber underwriting for North America at a major cyber insurance carrier, as well as the director of Incident Response for Booz Allen Hamilton. Choi is an attorney, cyber insurance subject matter expert, and consultant with extensive experience in guiding clients through cyber incidents.

Before joining Booz Allen, Choi worked as General Counsel and Managing Director of Strategy for an incident response company and money service business, where she managed legal, risk and compliance, including the team that negotiated with attackers and assisted clients in the facilitation of ransom payments. Additionally, Choi served as Assistant Vice President and cyber claims counsel at various insurance companies and practiced as an attorney in New York. Choi earned a Juris Doctor from New York Law School before being admitted to the New York State Bar in 2006 and to the U.S. District Court, Southern and Eastern Districts of New York in 2007.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Peter Halprin
Pasich LLP – Partner
Contact:
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 cyber breaches and cyber crime, COVID-19 and natural disasters, professional services, regulatory investigations, and technology disputes. 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 helped clients pursue insurance coverage for business e-mail compromise schemes, cyber crimes, data breaches, fraudulent e-mails, invoice manipulation schemes, phishing and whaling attacks, ransomware attacks, privacy and statutory liability, and technology E&O disputes. He is also a prolific author and speaker on insurance coverage for cyber risks.

In addition to being a Faculty Member at the Global Cyber Institute, he is an Adjunct Professor of Law at the Benjamin N. Cardozo School of Law, and a Fellow with the Chartered Institute of Arbitrators. He also recently completed a Harvard VPAL course entitled "Cybersecurity: Managing Risk in the Information Age."

(c) 2032 Lexeprint Inc. All Rights Reserved.