Understanding Cyber Insurance: Part 2

Speakers:

Daniel B. Garrie, Co-founder, Law & Forensics, Mediator, Arbitrator, Special Master, Jams

Tom Srail, Executive Vice President/Global Cyber Risk Advisors, Willis Towers Watson

(c) 2022 Lexeprint Inc. All Rights Reserved

Speakers



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



Tom Srail
Executive Vice President/Global Cyber Risk Advisors
Willis Towers Watson

(c) 2022 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) 2022 Lexeprint Inc. All Rights Reserved

Agenda

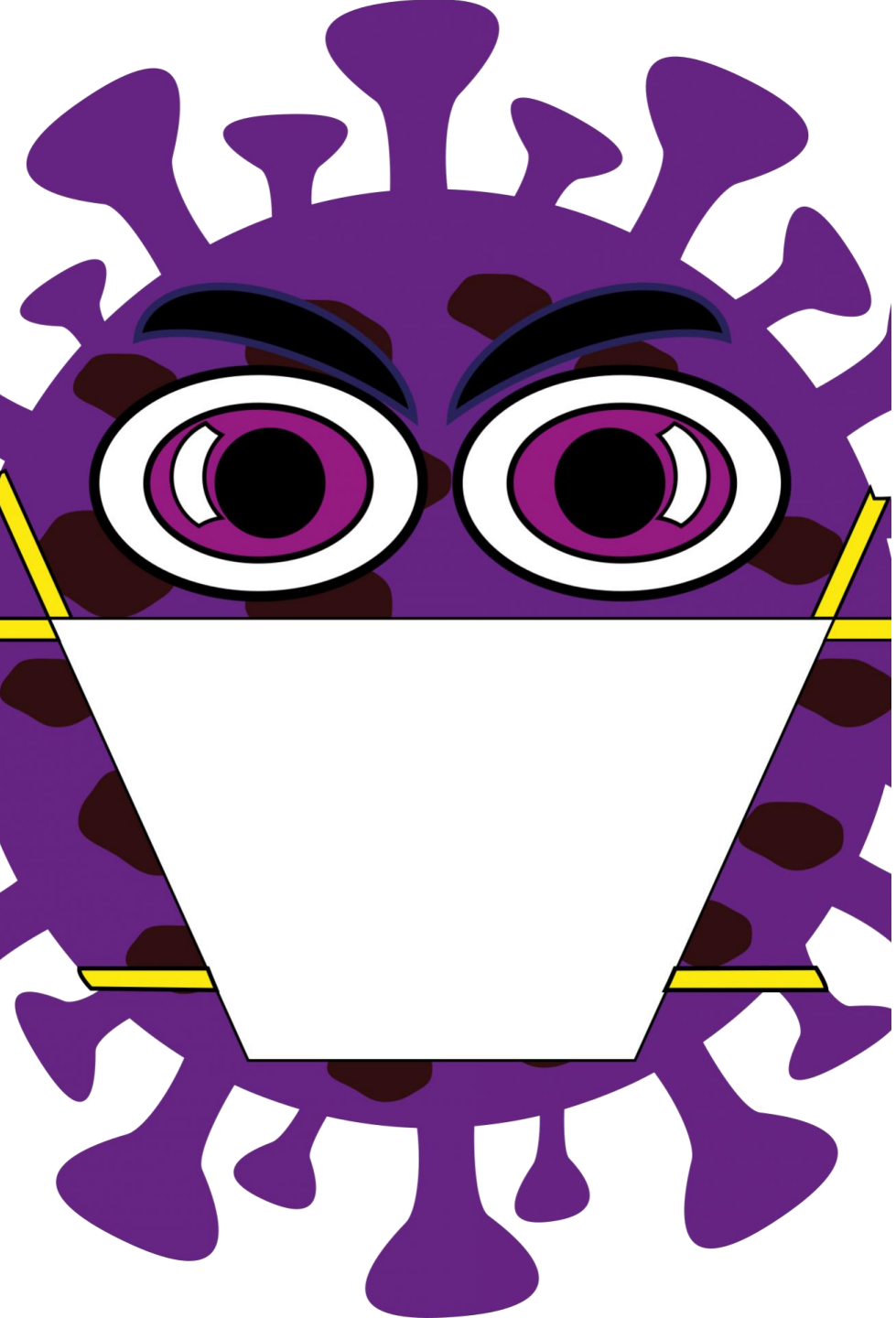
- The Growing Need for Cyber Insurance
- Cyber Insurance Overview
- Types of Insurance
- Current Cyber Insurance Issues
- Significance of these Cyber Insurance Concerns for Businesses
- Executive Orders Affecting Cyber Insurance
- Recent Cases
- Tips when Considering Cyber Insurance

(c) 2022 Lexeprint Inc. All Rights Reserved



The Growing Need for Cyber Insurance

(c) 2022 Lexeprint Inc. All Rights Reserved



COVID-19 Increased the Need for Cyber Insurance

- The ongoing COVID-19 pandemic has resulted in an increased interest and demand to secure cyber liability insurance coverage.
- As more people continue to work from home, there has been an increased volume of phishing, ransomware or other social engineering scams.
- Additionally, businesses have recognized that cyber-related losses are most likely excluded under the traditional general liability and property policies. As a result, they have started to focus on analyzing potential exposures and cyber risk management.

(c) 2022 Lexeprint Inc. All Rights Reserved



Increased Demand for Cyber Insurance

- As a result of this demand, the cyber insurance market is competitive as they work to offer coverages that meet businesses' needs.
- As insurance carriers gain experience from responding to voluminous cyber claims, they are able to offer guidance on preventing cyber incidents.
- E.g., Employing best technical security practices and internal back-up and recovery policies.
- **The United States continues to experience the highest data breach costs across the world, closely followed by the Middle East.**

(c) 2022 Lexeprint Inc. All Rights Reserved



Cyber Insurance Overview

(c) 2022 Lexeprint Inc. All Rights Reserved



What is Cyber Insurance?

- Cyber insurance generally covers your business' liability for a data breach involving sensitive customer information.
- Information subject to breaches can include the following:
  - Social Security numbers,
  - credit card numbers,
  - account numbers,
  - driver's license numbers, and
  - health records.

(c) 2022 Lexeprint Inc. All Rights Reserved



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) 2022 Lexeprint Inc. All Rights Reserved



Types of Insurance

(c) 2022 Lexeprint Inc. All Rights Reserved



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) 2022 Lexeprint Inc. All Rights Reserved



First Party Coverage

- First Party Cyber insurance covers direct financial losses that the insurance buyer suffers, such as lost business income, data restoration, expenses, theft and extortion losses.
- Questions to ask:
  - What security controls can you put in 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?

(c) 2022 Lexeprint Inc. All Rights Reserved



Third-Party Cyber Coverage

- Third Party Cyber insurance (also called Cyber Liability insurance) pays claims to 3rd 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) 2022 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

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

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.
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) 2022 Lexeprint Inc. All Rights Reserved



How Does an Insurance Company Assess Risk for a Cyber Underwriting?

Remember COPE:

- Construction
- Occupancy
- Protection
- Exposure

(c) 2022 Lexeprint Inc. All Rights Reserved



Construction

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

(c) 2022 Lexeprint Inc. All Rights Reserved



Occupancy

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

(c) 2022 Lexeprint Inc. All Rights Reserved



Protection

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

(c) 2022 Lexeprint Inc. All Rights Reserved



Exposure

- When an underwriter is assessing the exposure of a company's cyber network, they are looking at:
  - What is the potential for risk based on your industry and your location?
  - Areas include:
    - Processes and policies used by the organization to identify business and information security risks, and
    - System and network maintenance policies.

(c) 2022 Lexeprint Inc. All Rights Reserved

Potential Cyber Threats

Threats within an organization

- Social engineering
- Lost mobile devices
- Improper handling of PII
- Unintentional disclosure
- Rogue employees
- Coding inaccuracies

Threats from outside an organization

- Hackers
- DDOS attacks
- Criminals
- Vendors

(c) 2022 Lexeprint Inc. All Rights Reserved



If You Have a Cyber Policy

- Understand the unique exposures and associated risk.
- Be knowledgeable about the cyber insurance program so that program can be articulated to others.
- Prepare for responses to coverage inquires by leadership, including at the board level.

(c) 2022 Lexeprint Inc. All Rights Reserved



If A Cyber Event Occurs

- Contact your insurance provider immediately – prepare yourself for a potentially lengthy investigation.
- Communicate with your broker.
- Provide data to forensic analysts.
- Create and implement an incident response plan.

(c) 2022 Lexeprint Inc. All Rights Reserved



Current Cyber Insurance Issues

(c) 2022 Lexeprint Inc. All Rights Reserved



Limitations in Cyber Liability Policies and Coverage

- Despite the great work being done by insurance carriers to improve policies that can meet the needs to 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. E.g., An employee's personal laptop, tablets and other smart devices.
  - Limitation or no coverage for social engineering claims, such as funds transfer fraud incidents.

(c) 2022 Lexeprint Inc. All Rights Reserved



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) 2022 Lexeprint Inc. All Rights Reserved



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) 2022 Lexeprint Inc. All Rights Reserved



Significance of these Cyber Insurance Concerns for Businesses



Why are these Concerns Important to Businesses?

- Businesses should seriously consider the issues/concerns that can arise when considering cyber insurance as in a worst-case scenario of a cybercrime, a business can be lost altogether. Businesses may not be able to bounce back after a cyber incident without sufficient coverage.
- When considering a cyber liability insurance policy, employ an experienced cyber insurance coverage attorney that can identify and understand all available coverages and limitations. Also have the form policy as well as applicable endorsements reviewed. This should be done before the binding of the coverage.
- Once the policy is bound, have the experienced cyber insurance coverage attorney review the issued policy and other company insurance policies to understand how all insurance policies interact with one another and identify any potential coverage gaps.

(c) 2022 Lexeprint Inc. All Rights Reserved



Typical Costs for Cyber Insurance

- Cost of cyber insurance can vary enormously. It will depend on your business, the risks that it faces, and the amount of coverage needed.
- The average premium costs can range from a few hundred dollars per year to several thousand dollars per year.
- A recent study performed by AdvisorSmith Solution Inc. established that the average cost of cyber insurance for small businesses in 2021 was $1,589 per year for $1 million in cyber liability coverage.

(c) 2022 Lexeprint Inc. All Rights Reserved



Typical Costs for Cyber Insurance ctd.

- According to The Council's Commercial Property/Casualty Market Index for the third quarter of 2021, insurers continued to see a hard line on underwriting and pricing cyber covereage. Cyber premiums increased by 27.6%
- GRC World Forums reported that ransomware demands surged by 518% in the first half of 2021.
- Cybercrime was predicted to inflict damages nearing $6 trillion USD globally in 2021.

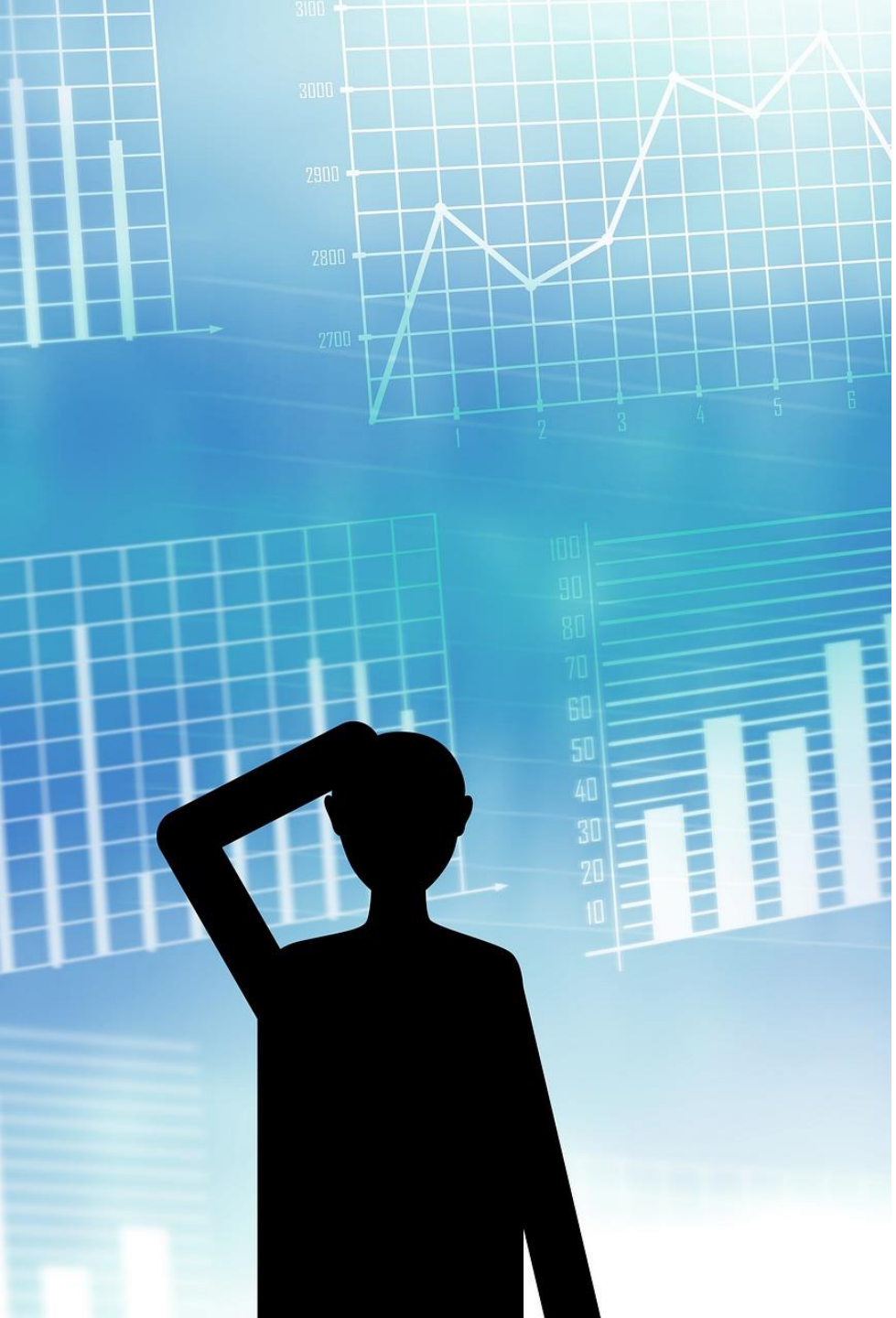
(c) 2022 Lexeprint Inc. All Rights Reserved



What Can Affect Cyber Insurance Costs?

- Size and Industry
- Amount and Sensitivity of Data
- Annual Revenue
- Strength of Security Measures
- Policy Terms

(c) 2022 Lexeprint Inc. All Rights Reserved



What to Consider When Assessing your Business' Risk Profile to Determine How Much Coverage is Needed

- Does your business store customers' personal data?
- Is your business in an industry that is susceptible to cyber-attacks or heavily regulated?

(c) 2022 Lexeprint Inc. All Rights Reserved



Executive Orders Affecting Cyber Insurance

(c) 2022 Lexeprint Inc. All Rights Reserved



Executive Order 13873

- On May 15, 2019, the then president issued Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," which prohibits high-risk information technology transactions with entities under the jurisdiction of a "foreign adversary," as determined by the Secretary of Commerce.
- While the executive order will affect buyers and sellers in a variety of industries, it's influence may even extend to cyber insurance litigation.

(c) 2022 Lexeprint Inc. All Rights Reserved



Executive Order 13873

- One area that may be affected is the interpretation of the standard war exclusion included in most cyber insurance policies as it applies to cyber hostilities.
- Specifically, the executive order may be interpreted as conflating private entities in foreign adversary jurisdictions with the foreign adversaries themselves, which could significantly broaden the range of entities that trigger the war exclusion under the terms of many cyber insurance policies.
- This could lead to a wave of coverage denials under the war exclusion and potentially a reconsideration of this standard policy language in the context of cyber.
- As evidenced by Mondelez International's recent lawsuit against Zurich American, the war exclusion is the latest battleground for cyber insurance litigation.

(c) 2022 Lexeprint Inc. All Rights Reserved



Recent Cases

(c) 2022 Lexeprint Inc. All Rights Reserved



EMOI Services, LLC v. Owners Ins. Co., No. 29128, 2021 WL 5144828 (Ohio Ct. App. Nov. 5, 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 edorsement of Owners Insurance property policy?
- Ruling: Yes. The court ruled that a cyber-attack resulted in coverage under the commercial property insurance policy.

(c) 2022 Lexeprint Inc. All Rights Reserved



EMOI Services, LLC v. Owners Ins. Co., No. 29128, 2021 WL 5144828 (Ohio Ct. App. Nov. 5, 2021)

- 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.
- 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



Landry's Inc. v. Insurance Co. of the State of Pa., 4 F.4th 366 (5th Cir. 2021)

- Facts: Landry's contracted with Paymentech to process credit card payments at its restaurants, hotels and casinos. A data breach was discovered by Paymentech across 14 Landry's locations that resulted in $20 million fraudulent credit card payments. It was found that the breach occurred because of an unauthorized installation of a program on payment-processing devices at several Landry's locations.
- Issue: Was the potential liability resulting from the data breach arise from "an oral or written publication?"
- Holding: The Fifth Circuit held that "an insurance company must provide a defense under Coverage B of a CGL policy for a claim arising out of a $20 million data-breach."
- Observations: The phrase "oral or written publication" was not defined in the policy and so the court adopted a broad definition of publication that was similar to the defamation context.
    - The court also held that the third party "published the [policyholder's] customers' credit-card information-that is, exposed it to view."

(c) 2022 Lexeprint Inc. All Rights Reserved

Tips When Considering Cyber Insurance

1

Implement an efficient training program that will help every employee to avoid phishing and other incidents that can lead to data breaches, ransomware attacks and other potential losses.

2

Do not wait until an incident occurs to figure out what to do! Ensure that you have a data response plan in place that is ready to be immediately triggered when needed.

3

Regularly review measures that may be needed to upgrade data protection, protect personal and proprietary data, and limit losses from data risks.

(c) 2022 Lexeprint Inc. All Rights Reserved



Questions?

(c) 2022 Lexeprint Inc. All Rights Reserved

Contact Us



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



Michael Phillips
Email: michael.phillips@gmail.com
URL: https://www.resilienceinsurance.com/



Tom Srail
Email: tom.srail@willistowerswatson.com
URL: https://www.willistowerswatson.com/en-US

(c) 2022 Lexeprint Inc. All Rights Reserved



Daniel B. Garrie, Esq.
Law & Forensics LLC – Co-Founder
JAMS – Special Master, Neutral, Arbitrator
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.



Tom Srail
Willis Towers Watson – Executive Vice President/Global Cyber Risk Advisors
Contact:
E: tom.srail@willistowerswatson.com
URL: https://www.willistowerswatson.com/en-US

Willis Towers Watson

Relevant Experience/Specialization

The Global Cyber Risk Advisory team for WTW is focused on innovative cyber risk management and brokerage services for our clients; Tom also leads our global Cyber Analytics solutions.

Tom previously led the Technology Media & Telecommunications (TMT) industry practice for North America, developing strategy and coordinating the efforts of our global industry specialists to build advanced solutions for clients that manage risk, optimize benefits, cultivate talent and expand the power of capital.

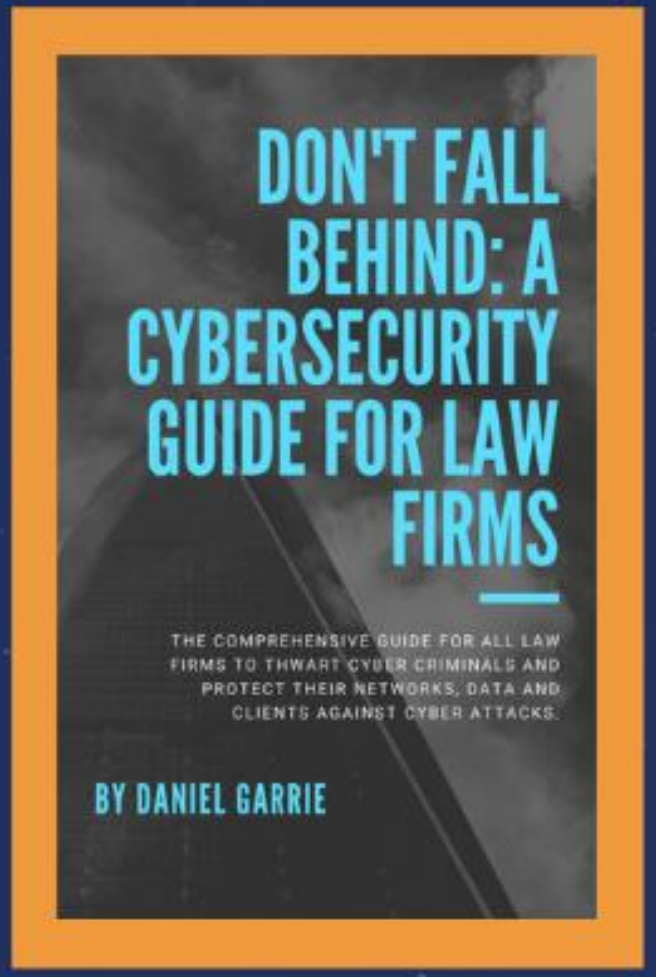
Tom joined WTW in 2004, and has over 25 years of experience in the risk management and technology industries. Tom has served as senior broker and risk advisor in WTW's Cyber and E&O Team, led the Information Risk Consulting Practice for another major broker, and held various positions in IT including Telecom manager, Network Operations Manager, Data Security, Network Engineering, and e-commerce marketing.

Named a 2013 *Power Broker* by Risk & Insurance Magazine for Technology, Tom is a frequent speaker and contributor to multiple publications and professional organizations.

Education and Credentials

Tom has a BS in Computer Science from Bowling Green State University.

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.