

The
HOSPITALITY LAW
CONFERENCE

Insurance and Casualty – How
Your Policies Will Respond to
Cyber Issues

Diana Shafter Gliedman and Dennis J. Nolan

May 9-10, 2023



Diana Shafter Gliedman

Shareholder, ANDERSON KILL

New York

- Shareholder with Anderson Kill's insurance recovery group.
- Represents policyholders in multi-party, multi-issue insurance coverage litigations, with an emphasis on Comprehensive General Liability Insurance, Directors & Officers Liability Insurance, Employment Practices Liability Insurance and Errors & Omissions/Professional Liability Insurance.
- Frequently works with members of the retail and hospitality industries, providing representation and counsel to major retail chains, restaurants, hotels, resorts, theme parks and casinos with regards to insurance, indemnity other risk transfer issues.

Thank you!



Dennis J. Nolan

Shareholder, ANDERSON KILL

New York

- Shareholder in Anderson Kill's New York office, concentrates his practice in commercial litigation with an emphasis on insurance recovery.
- Has extensive experience litigating complex chapter 11 reorganizations. He co-chairs the firm's Bankruptcy group, as well as the Marine Cargo Industry group and the Hospitality and Retail Industry group.
- Dennis advises policyholders with respect to a broad range of insurance policies, including Marine Cargo, Cyber, Directors and Officers, Errors and Omissions, Employment Practices Liability, Marine Cargo, and Commercial General Liability policies.

Thank you!

AGENDA

I. Introduction

II. Risks

III. Pre-Loss Risk Management

IV. Policies

V. Coverage Tips



Source: thebluediamondgallery.com

INTRODUCTION

- In 2017, every major hotel chain was hit with a cyber-attack.
 - Cyber threats continue to pervade the hospitality industry.
 - Cyber perils for the hospitality industry are not limited to hackers.
 - A new peril also exists – liability without any data breach.
- We will address some of the more common pitfalls that arise within the hospitality industry and appropriate risk management and insurance protections that both companies and individual owners in the hospitality space should consider when addressing cyber risks.

KEEPING UP WITH HOSPITALITY INDUSTRY RISKS

- The hospitality industry revolves around customers, which makes it particularly attractive to cyber-attackers.
- Ransomware/Hacking.
- Phishing/Social Engineering Attacks.
- Regulatory Liability.
- Litigation against the Board and corporate management.
- Biometric data violations.
- Supply Chain Attacks.
- Poor cyber hygiene.



Source: hospitalityrisksolutions.com

PRE-LOSS RISK MANAGEMENT

- You can't stop data breaches and violations, only contain them.
- Best practices pre-breach:
 1. Identify all data and whether special protection is needed;
 2. Follow published standards for cyber security;
 3. Create a written, clear internal policy that you regularly review and update;
 4. Implement and regularly maintain employee training programs;
 5. Conduct security auditing, pen testing and simulated attacks;



Source: crowdstrike.com

PRE-LOSS RISK MANAGEMENT (CONT'D)

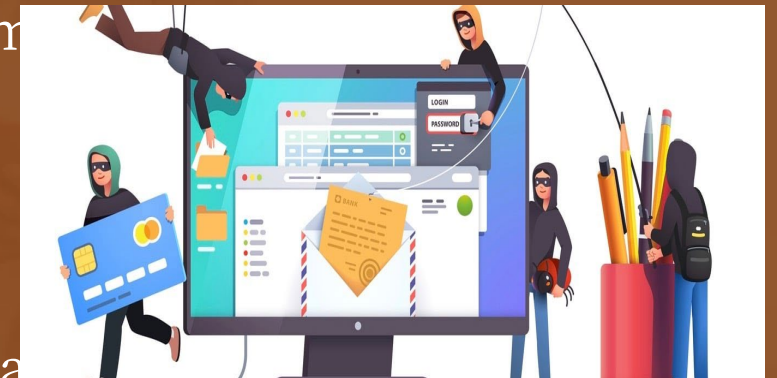
- Best practices a company should consider pre-breach:
(cont'd)
 6. Regularly update and patch computer systems;
 7. Proper disclosures;
 8. Develop robust pre-incident and incident response plans;
 9. If a corporation, mandate cyber-risk education for all employees, directors or recruit directors with a cybersecurity background;
 10. Don't skimp on money or personnel.



Source: anoopnair.com

INSURANCE COVERAGE FOR CYBER EVENTS

- Cyber breaches or misuse of data can lead to a number of different forms of loss, especially when customer financial data is involved.
 - compliance issues
 - notification requirements as to all affected customers
 - data integrity issues
 - ongoing data breach issues
 - litigation risks
 - losses from fraudulent use of the compromised data



Source: agilityprsolutions.com

WHAT INSURANCE POLICIES RESPOND?

- General liability policy
- Property & casualty policy
- D&O policy
- Stand-alone cyber policy
- Inland Marine insurance policy
- Crime policy



Source: bleuwire.com



Source: archerinsgroup.com



Source: insurancehub.com



Source: advisorsmith.com

NON-CYBER POLICIES MAY COVER CYBER-RELATED LOSSES

➤ Commercial General Liability Policies

- Third-party claims alleging actions/inactions caused or permitted the breach that compromised sensitive information.
- Liabilities from bodily injury and property damage or privacy violations for failing to safeguard personal data.
- Duty to defend; broad coverage of damages.
- “Publication” is a key issue.
 - “Sony I”
 - *Portal Healthcare; Landry’s Inc.*
 - *Target Corporation v. ACE American Ins. Co.*
 - BIPA Cases: *Krishna; Wynndalco*



Source: Investopedia.com

NON-CYBER POLICIES MAY COVER CYBER-RELATED LOSSES

- All Risk Property Policies.
 - Cover Property Damage.
 - Cover Business Interruption.
 - Have been held to cover data.
 - Have been repeatedly held to apply in ransomware cases.
 - *National Ink & Stitch, LLC v. State Auto Prop. & Cas. Ins. Co.*
 - *EMOI Services, LLC v. Owners Ins. Co.*
 - War Risk Exclusion
 - *Merck & Co. Inc. vs. Ace American Insurance Co.*



Source: crminsurace.com

NON-CYBER POLICIES MAY COVER CYBER-RELATED LOSSES

➤ Directors and Officers

- Proper corporate governance includes cyber insurance protection.
- At a minimum, coverage should be in place to protect the officers and directors, who could be left on their own to face the regulators, shareholders, and consumers who are pointing fingers at the Board.
- Significant risk for smaller companies that might not have the resources to provide adequate indemnification.
- One of the broadest liability policies around
- Terms to be on the look-out for:
 - Informal investigations coverage
 - Cyber exclusions
 - Conduct-based exclusions
 - Insured vs. Insured exclusions



Source: insuranceage.com

STAND-ALONE CYBER

- Bespoke policies
- First and Third-Party Coverage
- Breach of Contract Exclusion
- Known losses
- “Loss” carve-outs
- Securities and bodily injury claims



Source: [pinterest.com](https://www.pinterest.com)

COVERAGE TIPS

- Carefully fill out insurance applications.
- Limit retroactive and continuity dates.
- Avoid conditions on “reasonable” cyber measures.
- Endorsements for special coverage needs with respect to cloud providers and third-party vendors.
- Look Out for Possible Exclusions/Coverage Limitations:
 - May exclude certain types of property or property damage (e.g., costs to replace computer hardware may not be covered).
 - Temporal Limitations for coverage based on the “period of restoration.”
 - Typically excludes coverage for “improvements,” “upgrades” or “new functionality.”
 - Policy May Require Use of Pre-Approved Vendors/Cyber Consultants.



Source: avepoint.com

COVERAGE TIPS

NOTICE INSURANCE POLICIES PROMPTLY



CONCLUSION

- The hospitality industry has been hit with many high-profile data breaches over the last several years.
- The attack vectors are more varied, with ransomware becoming a popular way to infiltrate computer systems.
- No company is immune from a data incident, and no short-cut exists that will protect against cyber risks.
- Turning to cyber insurance policies and other liability policies is indispensable as it helps hospitality owners improve cybersecurity and risk management within their organization.
- Have insurance in place to provide for legal defense, cover each response costs, address public relations concerns, and respond to regulatory investigations and consumer or shareholder litigation.



Source: recruitability.com

QUESTIONS?



Source: hotelnewsresource.com



**WE APPRECIATE YOUR
TIME AND ATTENTION!**

Diana Shafter Gliedman, Esq.
Anderson Kill P.C.
1251 Avenue of the Americas
New York, New York 10020
(212) 278-1036
dgliedman@andersonkill.com

Dennis J. Nolan, Esq.
Anderson Kill P.C.
1251 Avenue of the Americas
New York, New York 10020
(212) 278-1659
dnolan@andersonkill.com

Thank you!