

# 10 Tips to

## Maximize Cyber Insurance Recovery in the Hospitality Industry



**By: Joshua Gold**  
*Anderson Kill*

Virtually every U.S. industry has been touched by data breaches, and the hospitality business is no exception. Hotels and resorts process payment almost entirely by credit card, deal with customers from all over the world, and are often prone to high employee turnover -- all factors contributing to the likelihood of a breach. No matter how good your risk management procedures, the possibility of a data breach cannot be eliminated.

When a breach does occur, insurance is a key line of defense. The insurance marketplace for cyber risk is in flux and fragmented, however. Obtaining the right insurance and pursuing claims effectively are challenges unto themselves. The 10 tips below will help you maximize cyber insurance recovery.

**1. Make sure your insurance matches the way you conduct online business and process data.**  
For example, there are insurance coverage implications if you use cloud computing or other vendors for hosting and processing data. Many cyber-risk insurance policies available today can be tailored to reflect the fact that the policyholder may delegate to third-party data management and hosting.

**2. Do not rule out coverage for a claim under traditional business policies.**  
If a cyber loss occurs, consider D&O, E&O, crime and general liability insurance coverage depending on the claim against your company or the form of loss. We have had success in winning coverage for our clients for cyber-related losses under traditional coverage.

**3. Avoid cyber insurance policy terms that condition coverage on the policyholder having employed "reasonable" data security measures.**

These clauses are so vague and subjective that they are bound to lead to coverage fights. Further, given the lightning speed of technological innovation and amorphous nature of cyber risks, a cyber security practice that was reasonable just months ago may look reckless with the benefit of hindsight.

**4. If you possess or process consumer or business credit card information, make sure that you have coverage for fraudulent card charges and credit card brand assessments and fines — these can be large exposures when there is a significant data breach.**

**5. If you do business with individual consumers and obtain their personal identifying information, make sure you have coverage (including attorneys' fee coverage) for the inevitable expenses of responding to informal inquiries and formal proceedings that ensue from state attorneys general, the Federal Trade Commission and others when a breach occurs (often implicating residents of several states).**

**6. Make sure that your insurance covers breaches arising from mobile devices that may or may not be connected to the company's computer network.**

More and more employees can access systems through tablets, smartphones, and PCs. The ever-growing size of hard drives and the ubiquity of portable drives mean that some employees may create security risks, even when the device is not logged onto the company servers.

## 7. Complete insurance applications carefully, including D&O applications.

Underwriters will be focusing more and more on computer risk areas, and insurance application responses often are used against policyholders to contest insurance claims.

## 8. Avoid cyber insurance policies with contractual liability exclusions.

Contractual liability claims often are made in conjunction with statutory claims, negligence claims and other forms of relief, and policyholders are best off not enduring a huge allocation fight over what portion of the claim is covered.

## 9. If you are buying or renewing specialty cyber insurance policies, make sure you work with a very good and experienced broker.

There is not presently uniformity of product in the cyber insurance marketplace, and lots of terms are open for negotiation. A good broker can help get you the best coverage.

## 10. Provide notice to your insurance companies quickly after a breach.

The cost meter starts immediately. When you have a breach situation, every second counts, and you undoubtedly will incur costs quickly for computer forensics, attorneys and other consultants. Providing proper notices and advising of these costs promptly can increase the odds of recovering these costs from your insurance companies.

*Joshua Gold (jgold@andersonkill.com) is a shareholder in the New York office of Anderson Kill, a national law firm. Mr. Gold is a member of the firm's Hospitality Industry group and chair of the firm's Cyber Insurance Recovery group. He has extensive experience in insurance coverage analysis, consulting and litigation, with an emphasis on directors' and officers' insurance, errors and omissions insurance, online and high-tech liability and property insurance coverage issues and offshore market insurance products.*

# Don't forget to Like us on Facebook



New York State  
**HOSPITALITY  
& TOURISM**  
Association

## SIMPLE WEAR AND TEAR CAN SHORTEN THE LIFE OF YOUR FURNITURE.



Your Solution for Innovative Interior Design and FF&E -  
Purchasing, Warehousing and Installation

**DESIGN & SUPPLY**  
SERVING THE  
LODGING INDUSTRY

LEE STRANBURG, MHS  
600 HORIZON DRIVE • CHALFONT, PA 18914  
T. 215.997.8850 • LEESTRAN@DESIGNANDSUPPLY.COM

[WWW.DESIGNANDSUPPLY.COM](http://WWW.DESIGNANDSUPPLY.COM)