CONVERGING RISKS IN A DIGITAL ECONOMY:

HOSPITALITY INDUSTRY

This is one installment in a series of "White Papers" prepared by ThinkRisk Underwriting Agency discussing the converging risks faced by various industry segments as a result of the digital economy. The white papers provide real-world claims examples, and explore the insurance ramifications of these emerging exposures. This installment of the series discusses risks faced by the hospitality industry including hotels/motels, restaurants, event planners, cruise lines and similar businesses.

Introduction to the convergence phenomenon: Digital technology is a powerful tool that has changed the way virtually all businesses and other organizations operate. Digital technology has unleashed corporate creativity and efficiency, leading to new ways to manage and store data, new products, and new ways to interact and communicate with constituencies. At the same time, digitization and the way it permits businesses to gather, create, distribute and store information and media content has altered the risks of doing business in a fundamental way, and exposes inadequacies in the current insurance response to these new risks. Here's how this phenomenon affects businesses in the hospitality industry.

Network security and data privacy

Digital technology makes transacting business far easier and allows businesses such as hotels and restaurants to gather and store data more efficiently, creating opportunities for the hospitality industry to collect and store vast amounts of data, including employee information but also data concerning visitors, customers, suppliers and others. This data may include names, addresses, social security numbers, personal email addresses, medical information, and of course financial data. Over 50% of all travel reservations are now made online. Travel and hospitality is the world's largest industry, with the World Travel and Tourism Council predicting revenues in excess of US$15 trillion by 2017. Many segments of the hospitality industry have rewards programs that encourage customers to frequent a particular establishment or chain. These programs necessarily store personal and financial information in order to facilitate reservations, billing and payment and benefit awards. In addition, online reservations and payments as well as transactions processed on-site involve collecting credit card or other personal financial information from customers.

The consequences of a security breach can be significant. In the event of a potential breach of security, state laws in most jurisdictions require the business to notify all potentially impacted persons of the breach, the cost of which can be astronomical. If the information is used in a way that is damaging, the business could face liability claims as well, for failing to protect the data by maintaining reasonable safeguards. Finally, the business may face additional costs such as purchasing credit monitoring services, hiring a forensic team to determine the cause of the breach and take corrective measures, and in some cases hiring a public relations firm to help manage communications with customers and other impacted persons.

Remarkably, hotels became the single most breached sector for credit card data theft in 2009, representing just over a third of all major breaches. There have been many examples of data breaches involving hotels and other businesses in the hospitality industry, including those listed below. The nonprofit organization Privacy Rights Clearinghouse maintains a chronological listing of data breaches, which can be found at www.privacyrights.org.

- In June 2010, hackers broke into the payment processing system of Destination Hotels & Resorts, a high-end chain best known for its resort hotels in destinations such as Vail, Lake Tahoe and Maui. Destination uncovered a malicious software program inserted into its credit card processing system from a remote source. The attackers appear to have hit point-of-sale processing systems, where credit cards are swiped for purchases.
- In May 2010, three servers from the Cheesecake Factory in Washington, D.C. were charged with using skimming devices to make over $117,000 in fraudulent charges to customer credit card accounts. This demonstrates the importance of structuring insurance coverage so that it extends to breaches of security by employees – so-called “rogue employee” coverage.
- Also in May 2010, at the Vine Tavern and Eatery in Tempe, Arizona, personal documents including applicant names, Social Security Numbers, and dates of birth were found in a dumpster. Customer checks with banking information and credit card receipts were also found. Because of instances such as this, data security insurance coverage should extend to physical data as well as electronic records.
- Westin Bonaventure Hotel & Suites’ four restaurants – Lake View Bistro, Lobby Court Bar, Bonavista Lounge and L.A. Prime – along with its valet parking operation, may have been hacked at some time between April and December, 2009, disclosing names, credit card numbers and expiration dates printed on customers' debit and credit cards.
- In January 2010, Payless Travel and Cruises discovered that one of its employees had stolen an unknown number of customers’ credit card details. Losses associated with this incident have not been disclosed.

Content: Hotels, restaurants, cruise lines, travel agencies and the like live and die by the power of their brand recognition and reputation. As a result, trademarks and copyrights are among these business’s most valuable assets, and the hospitality industry can be quite aggressive in protecting those assets against actual or perceived infringement, which could tarnish the business’s goodwill and reputation.

Indeed, the terms of use on the websites of many hotel and restaurant chains contain prominent notices warning against infringement of the business's intellectual property.

In addition, hospitality businesses communicate frequently with their reward club members and other customers via email. Most such companies have newsletters and websites which are likely to contain photographs, chat rooms, and other such content. Many hospitality businesses have Facebook pages, Twitter accounts and utilize other social networking tools to reach out to existing and prospective customers. And, of course, these businesses frequently engage in local and national advertising. All of these activities give rise to content liability exposures, similar to those faced by media companies and ad agencies, such as copyright, trademark and commercial misappropriation.

As a result , there are many examples of media and intellectual property claims involving the hospitality industry, including the following:

- The Hilton hotel group was sued in March 2009 for trademark infringement by rival hotel chain Prestige Resorts & Destinations, which owns trademark registrations for PRESTIGE and PRESTIGE RESORTS & DESTINATIONS. Hilton registered the mark HILTON PRESTIGE PORTFOLIO. In its lawsuit, Prestige alleges that Hilton's registration amounts to trademark infringement and unfair competition.
- In a Minnesota case, Tolkien Enterprises sued a Minnesota travel agency called "Hobbit Travel" for trademark infringement of Tolkien's "hobbit" mark. Tolkien Enterprises controls the worldwide distribution rights to J.R.R. Tolkien's *Lord of the Rings* franchise and related intellectual property.
- Tomdan Enterprises, Inc., which does business under the more recognizable "Tommy's Original World Famous Hamburgers" name and trademark, filed a trademark and trade dress infringement, Lanham Act unfair competition, and trade secret misappropriation lawsuit against Tommy's Original Chili Factory, Inc.
- The heirs of rock legend Jerry Garcia are suing a burrito franchise based in Atlanta for improper use of the singer's image in its restaurants and advertising. Not only does Moe's Southwest Grill offer the "Alfredo Garcia" fajita, but nearly all 130 restaurants prominently display a portrait of the renowned singer, according to the filed by Jerry Garcia Estate LLC.

Coverages in the standard insurance marketplace

Although most hospitality industry businesses purchase Commercial General Liability ("CGL") coverage, typical CGL policies provide limited coverage for media and network security claims. Data breaches, and the attendant costs and claims associated with such breaches, are generally outside the scope of the GCL, as well as a standard property policy, which requires physical loss or damage. With respect to media claims, libel and invasion of privacy in publications may be covered by the CGL, but that leaves much media activity unprotected. For instance, intellectual property is excluded under most newer versions of the CGL, except for limited coverage for copyright in "advertisements," which is strictly defined. This means that the litany of trademark and related intellectual property claims discussed above would likely not be covered. Website content is generally not covered, unless the content is considered "advertising," which is construed narrowly. Similarly, many D&O policies have intellectual property and other similar exclusions that would defeat coverage in many of the high-exposure areas

discussed in this paper. Even when such coverage is provided, it is generally not robust, and the carrier may not have the necessary legal expertise to deal with highly specialized or technical claims.

ThinkRisk's Converging Risk Liability Policy: The Converging Risk Liability Policy from ThinkRisk addresses these unique and emerging exposures, and fills the gaps left by traditional policies. The policy is "modular" and can therefore be customized to meet the needs of the particular business. Coverage Part A of the Policy provides coverage for claims arising out of the distribution of content, whether by print, electronic or any other means. To the extent that the business provides any type of professional service, Coverage Part B can provide coverage for claims alleging errors and omissions in the course of providing such services. Coverage Parts C and D provide network security coverage, both for liability claims brought against the business (Part C), as well as for certain costs incurred by the institution in responding to a breach (Part D), such as the cost of notifying impacted persons and retaining a public relations consultant.

To obtain a quote, please contact your insurance agent. For more information, contact us at info@thinkriskins.com or (816) 994-6400.

Coverage features described in this paper are summarized. Refer to the actual policy for a full description of applicable terms, conditions, limits and exclusions.
©2010 ThinkRisk Underwriting Agency LLC. 310 w.20th Street, Suite 200, Kansas City, MO 64112, www.thinkriskins.com