Hospitality & Gaming Risk Management and Insurance Against Cyber Risk

By Joshua Gold and Marshall Gilinsky

Securing data against unauthorized and unintentional disclosure continues to be elusive. For those businesses that need to capture and process third-party customer information through their networks, 2015 proved to be a challenging year from a variety of standpoints, including a legal standpoint. The Hospitality industry was not spared.

One federal court of appeals reinstated class action litigation against a large retailer that had been hacked. Another federal appeals court affirmed the Federal Trade Commission's power to police business' cyber security for consumer information. Reading the tea leaves, 2016 does not promise to be any better.

As such, companies will need to pursue a strategy that includes careful contracting, quality insurance coverage, and cyber security due diligence.

Risk Management

Hospitality firms have seen first-hand that data breaches attract the attention of state attorneys general, the Federal Trade Commission (FTC), and other regulators. For public companies, the Securities and Exchange Commission undertakes additional regulatory measures concerning cyber security and disclosures.

Among other requirements, the FTC has made it plain that businesses of all kinds must assess (and address with adequate resources) data security risks in detail. What's more, the FTC will scrutinize all statements aimed at consumers addressing data protection.

While certainly not exhaustive, below are key steps to take to secure your organization's data and computer systems:

1. In most instances, data needs to be encrypted — especially when dealing with guest account and personal information as well as certain categories of employee information.
2. Data security protocols must be established for password protection, encryption, employee mobile devices (so-called "BYOD" policies), and placement of data on mobile devices such as laptop hard drives and thumb drives. Employee training needs to be continuous and updated to match new threats.
3. Data mapping is essential to know what data you have and on what systems that data resides.
4. Due diligence must be performed on any computer vendors you are considering using (for example, cloud computing firms) and any "outsiders" authorized to access your systems.
5. Regular reminders to employees are important to help ensure company-wide compliance with security protocols.

Insurance Coverage

Hospitality businesses will also want to make sure that they have insurance coverage for any mishaps that occur in the course of their computing activities. There are now over 50 different insurance companies that promise to protect policyholders against cyber-losses via dedicated specialty insurance. None of this coverage is uniform at present. Furthermore, many of the insurance products are downright confusing concerning the scope of protection they promise.

Given that some cyber insurance companies have already contested the scope of insurance coverage under their cyber insurance policies (in court and elsewhere), it also is important to examine what coverage your business has under its traditional policies and identify potential coverage gaps. Make sure as well that coverage will be available (whether under cyber policies, business package policies, E&O policies or crime bonds/policies) when cloud computing services are used. Most insurance coverage can readily be adapted to expressly cover data theft, even when the unauthorized access takes place on someone else's network, devices or servers.

As always, mind the fine print. Insurance companies often revel in contesting claims on the basis of hard-to-digest exclusionary language — which confusingly may not always be located in the section of the policy entitled, "Exclusions." It's important to use diligence and to be prepared to push back if coverage is denied.

Joshua Gold (jgold@andersonkill.com) is a shareholder in the New York office of Anderson Kill and chairs the firm's Cyber Insurance Recovery Group. Marshall Gilinsky (mgilinsky@andersonkill.com) is a shareholder in the firm's Burlington, VT office.