Cybersecurity risk management, due diligence crucial

BY JOSHUA GOLD AND MARSHALL GILINSKY
HM COLUMNISTS

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. 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' cybersecurity for consumer information. 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 cybersecurity due diligence.

RISK MANAGEMENT

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

Below are a few 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.
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 and any "outsiders" authorized to access your systems.
5. Regular reminders to employees are important to help ensure companywide compliance with security protocols. **HM**

Joshua Gold (jgold@andersonkill.com) is a shareholder in the New York office of Anderson Kill and is chair of the firm's Cyber Insurance Recovery Group. His practice involves matters ranging from data security, international arbitration, directors' and officers' insurance, business income/property insurance, commercial crime insurance, and insurance captives. Marshall Gilinsky (mgilinsky@andersonkill.com) is a shareholder in the firm's New York office. His practice is focused on property insurance, data security, commercial general liability insurance, directors' and officers' insurance, captive insurance and reinsurance issues.