Data Security: Is Your Company Protected?

The vast benefits of the ongoing technological revolution are undeniable. Businesses use troves of data to increase efficiency, enhance marketing, and uncover new opportunity. The same technologies that businesses employ in their operations, however, allow both inadvertent mistake and criminal conduct. Even technologically advanced companies, such as Las Vegas Sands Corp. and Target Corp., fall prey to myriad technology accidents and crimes. Because of the increasing risk to companies, data misuse can lead to significant corporate losses and may negatively harm one's brand. Consider Target's CEO, president and chairman, who was forced to resign after months of dealing with one data-breach event.

The data intrusions at Target and Sands are notorious examples of hackers, offshore data thieves and other external threats. The vast majority of data-loss events, however, are the result of inadvertent or intentional "inside job" activity. In other words, if your organization experiences data loss, it will most likely be an employee, not an external actor, who caused the loss. Armstrong Teasdale, for example, recently counseled clients with respect to data losses arising from a laptop stolen from an employee's car and a professional data thief who moved from company to company as a human resources employee for the purpose of stealing personal information.

Even if there is no evidence of misuse of the lost data, the cost quickly mounts to provide legally-required notice and mitigation, such as credit monitoring. If the seriousness of the breach is sufficient to interest regulators, then the cost of the investigation, defense, and, potentially, future mandatory compliance and fines further add to the data-loss burden.

A sound data security strategy should account for the threat of internal and external data-loss events. Focusing on several key elements of a company's data flow and storage can mitigate the threat. Start by asking questions regarding employee access, transmission and storage/disposal of company-held data. An organization should implement its data security strategy with appropriate policies, training, technology, and auditing. Data access policies should reflect authorized employees, allowable transmission, and appropriate retention and disposal. Likewise, hiring policies should include provisions for employees whose jobs allow access to sensitive information. Employee training should cover data security and retention policies, emphasizing the potential consequences of inappropriate data practices. The company's information technology personnel should carefully review its internal data security. Finally, companies should implement procedures to record access and transmission of data, and routinely check for data-policy compliance.

Cloud computing systems have their own data security implications. The primary impediments to adopting cloud computing include security, interoperability, vendor lock-in, regulatory compliance, reliability, complexity, privacy and pricing. These concerns raise contract drafting issues for cloud computing contracts. Because data security is the focus of this article, I will touch upon service level agreements (SLAs). SLAs should identify the infrastructure and security for the cloud service. When drafting a cloud service contract, one should define the required security parameters and monitoring in specific and measurable ways. Without these

specifics, it will be hard to evaluate security and contracts deliverables. Consider whether there should be penalties for noncompliance. Boilerplate provisions addressing breaches of the contract are often too general to provide a meaningful remedy.

For gaming companies, player tracking systems warrant additional attention. Player tracking data can be extensive, containing troves of personal data, including Social Security numbers, driver's license numbers, home addresses, and myriad other valuable information. This data is subject to unauthorized internal and external access. The system administrator should carefully limit access, and department heads should regularly review the list of authorized employees. Additionally, internal and external audits allow businesses to test their compliance, allowing weaknesses to be identified before data-loss events occur.

Finally, businesses should consider obtaining appropriate insurance coverage. While insuring against technology risks is a new, rapidly expanding field, such coverage could prove invaluable. This form of insurance can encompass numerous risk categories, including: 1) data breach coverage, which offers protection against expenses associated with responding to and mitigating a loss of third-party data; 2) regulatory action coverage, which protects against costs incurred in responding to and defending against regulatory claims; 3) outage coverage, which reimburses businesses for interruption losses related to system downtime; 4) data-loss coverage, which covers the cost of replacing the insured's lost data; and 5) liability coverage, which may include content coverage for claims relating to information posted on a business's website.

Given that data security is rapidly changing, it's wise to get advice from legal counsel familiar with the relevant law.

Bret Meich is a member of Armstrong Teasdale LLP. He can be reached at bmeich@armstrongteasdale.com or (775) 784-3206.