Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How Tribes Can Avoid Gambling With Casino Patrons' Data

Law360, New York (September 21, 2016, 5:26 PM EDT) --


Erica J. Dominitz


Venus McGhee Prince

Not a day seems to go by without at least one attention-grabbing and fear-inducing headline about a data breach. While data breaches are prevalent and have come to be expected, the types of breaches that different organizations experience vary quite a bit. Sometimes the victims of the breach are large corporations; other times they are relatively small businesses. Sometimes the hackers or perpetrators are foreign enemies; other times, they are an organizations' own employees. Sometimes a breach is the result of intentional misconduct; other times it is a result of negligence. At the end of the day, regardless of what type of data breach an organization experiences, all breaches have at least one thing in common: they are disruptive and expensive. Although tribes, tribal casinos and tribal businesses ("tribal organizations") might have sovereign immunity against third parties' claims against them that arise out of such data breaches, they are not immune to direct costs and expenses to their organizations or legal expenses associated with these breaches and third-party claims.

To protect against, or at least minimize, the likelihood and extent of a breach, all tribal organizations should implement and enforce robust risk management protocols. One important tool in any organization's risk management toolbox is cyberinsurance, which can help pay for the various, and often steep, costs associated with responding to a breach. Although cybercoverage sometimes can be found in traditional insurance policies, such as general liability policies and property insurance policies, this article focuses specifically on cyberinsurance policies, which provide coverage for losses stemming from data breaches, cyberattacks, privacy violations and other, similar types of events.

Data Breaches Happen

Cyberlosses are Prevalent and Costly

While all organizations, regardless of size, are vulnerable to data breaches and other events,[1] casinos seem to be particularly attractive targets for cybercriminals for obvious reasons. Below are a few examples of casinos that recently have fallen victim to a cyberattack:

- *Hard Rock Hotel & Casino Las Vegas data breaches*: On June 27, 2016, the Hard Rock Hotel & Casino Las Vegas issued a statement notifying its customers of a data breach that may have compromised payment card data of customers who visited the resort between Oct. 27, 2015,

and March 21, 2016.[2] This announcement came about a year after the resort had announced a previous data breach that spanned from September 2014 through April 2015.[3]

- *Landry's/Golden Nugget data breaches*: Earlier this year Landry's Inc. Golden Nugget Hotels and Casinos reported that hundreds of restaurant, hotel and casino locations owned by them were affected at various times between May 2014 and December 2015 by a massive data breach exposing cardholder payment card data.[4]

- *River Cree Resort and Casino*: In March 2016, the River Cree Resort and Casino announced that it was the victim of a series of cyberattacks that resulted in the theft of customer and employee data.[5]

- *Sands Casino*: On Feb. 10, 2014, Sands Casino properties, which owns the Venetian and Palazzo in Las Vegas, among many other global properties, was the subject of a massive cyberattack perpetrated by Iranian hacktivists.[6]

Of course, this list of casinos or other gaming industry businesses that have reported a data breach or a cyberattack that compromised customer information is not exhaustive — and keep in mind that not all data breaches are even reported.

Moreover, the cost of responding to a cyberattack typically is substantial. According to the 2016 Ponemon Report, the average cost of a data breach is $4 million.[7] While tribal organizations should implement strong cyber-related risk management measures, even when they do, not all risks and losses can be avoided. In 2012, FBI Director Robert Mueller stated, "There are only two types of companies: those that have been hacked, and those that will be."[8] Technology insiders have since modified that statement, and now say that there are two types of companies — those that have been hacked, and those that do not yet know that they've been hacked.[9] Like nontribal companies, tribal organizations accordingly should purchase cyberinsurance that aligns with their respective risk portfolios.

Debunking the Myth: Not Only Large Organizations Need Cybercoverage

Individuals at smaller companies or organizations, like tribal organizations, often believe that only extremely large companies need cyberinsurance, but not only large organizations get hacked. Smaller ones do, too, but often are subject to less media coverage. Additionally, not all data breaches are publicly disclosed and reported. And, of course, not all cyberevents and losses are the result of intentional hacking. Sometimes they result from unintentional errors by well-intentioned individuals, the proverbial "oops!" events. In any event, as noted above, the cost of responding to a breach can be just as staggering for small companies or tribal organizations with a lot of confidential data as it can be for large companies with a lot of confidential data, so even tribal organizations should consider buying cyberinsurance.

What Type of Cyberinsurance Do You Need?

Cybercoverage is not One-size-fits-all

One important consideration to keep in mind is that, for a few reasons, cyberinsurance policies are not one-size-fits-all. For one thing, different organizations have different cyberrisk portfolios and cyber-related exposures depending on, among other things, the nature of their organizations, the nature and amount of sensitive data that they handle or maintain, and the form of and locations in which such data

is maintained. For example, some businesses or other organizations collect credit card information and social security numbers, whereas others do not.

Additionally, cyberpolicies vary quite a bit from form to form, both in terms of the types of cybercoverages that are provided and in terms of the scope of the different coverages. Review these policies not only for the types of coverages afforded, but also the policy language, including coverage grants, definitions of defined terms, and exclusions, to understand just how broad, or conversely how narrow, any given policy's coverage grants are. In short, carefully assess the risks that your organization faces and buy coverage that protects against those risks.

You Can and Should Combine Different Options for Cybercoverage

In general, cyberpolicies contain a combination of first-party coverages — i.e., coverage for losses directly suffered by the policyholder as a result of the breach, such as loss of data and network damage — and third-party coverages — i.e., liability coverage for claims that others assert against the policyholder as a result of the breach. Here is a brief description of various types of first-party and third-party coverages that are often found in cyberinsurance policies.

First-Party Coverages

- · Breach response expense coverage — There are a number of types of coverages that fall within this category, including:
    - Forensic investigation expense coverage — covers expenses to investigate a system intrusion into an insured computer system.
    - Legal expense coverage — covers expenses to review and determine responsibilities under privacy laws.
    - Notification expense — covers expenses to comply with privacy law notification requirements.
    - Credit and ID monitoring coverage — covers expenses to provide up to (typically) 12 months of credit monitoring.
    - Crisis management / public relations expense coverage — covers expenses to hire a public relations firm.
- Data recovery expense coverage — covers expenses to recover data damaged on an insured computer system as a result of a failure of security.
- Cyberextortion coverage — covers reasonable and necessary (and typically must be consented to by carrier in advance!) costs of responding to demands for ransom or e-extortion threats to prevent a threatened cyberattack.
- Property damage coverage — covers damage to computer hardware and software.
- Business interruption and extra expense coverage — covers lost revenues and extra costs incurred as a result of an interruption to an insured computer system as a result of a security failure.

Third-Party Cybercoverages

- Privacy liability coverage — provides defense and indemnity coverage for allegations that an insured failed to protect electronic or nonelectronic information in its care, custody or control.
- Network security liability coverage — provides defense and indemnity coverage for allegations that an insured's computer system failed to prevent a security breach or a privacy violation.

- Regulatory liability coverage — provides liability coverage for lawsuits or investigations by federal, state or foreign regulators relating to privacy laws.
- PCI assessments coverage — covers contractual assessments, fines and penalties owed under the terms of a service agreement with a merchant due to noncompliance with the Payment Card Industry Data Security Standards and as a result of the data breach.
- Media liability coverage — covers the insured for claims alleging various torts, including infringement of copyright and other intellectual property rights and misappropriation of ideas or media content. Note that claims alleging patent infringement and theft of trade secrets typically are excluded.
- Technology errors and omissions coverage — provides defense and indemnity coverage for professional negligence / wrongful acts allegedly committed by a provider of technology services or products.

Complete the Application Carefully, and Look Out for Exclusions and Other Traps

Tribal organizations purchasing cybercoverage should carefully review their policies to make sure they understand the scope and amount of coverage provided, as well as policy deadlines, other conditions and other traps hidden in the fine print. While different tribal organizations have different needs, here are some of the issues and provisions worthy of extra attention (although, of course, all policy provisions should be carefully reviewed).

The Importance of, and Perils Associated With, the Application

As a general rule, pay careful attention to the questions set forth in any insurance application, and give complete and accurate responses to them, as misrepresentations — even accidental ones — can jeopardize your coverage for a particular claim and, even worse, can provide a basis for voiding the policy. This principle deserves even greater emphasis in the context of cyberinsurance applications for a few reasons. First, cyberinsurance applications tend to ask technical questions about information technology systems and practices that might be unfamiliar to individuals who ordinarily handle and organization's risk management functions and tasks and will require close coordination with others in the organization. This situation can be ripe for misunderstanding and, thus, inadvertent misrepresentations. Additionally, some cyberinsurance policies exclude coverage for "failure to follow minimum required practices" identified in the insured's application for insurance. The following case illustrates this risk.

In Columbia Casualty Co. v. Cottage Health System,[10] the policyholder sought coverage for a putative class action alleging that confidential medical records of more than 30,000 patients at affiliated hospitals were negligently disclosed and released to the public on the internet. The underlying plaintiffs alleged that the policyholder had negligently — not intentionally — disclosed this confidential patient information. The insurance company denied coverage for the underlying lawsuit and filed a lawsuit against the policyholder seeking a declaration that it had no obligation to provide coverage for the claim. The carrier invoked the policy's exclusion for failing to follow minimum required practices by failing to continuously implement the procedures and risk controls outlined in the policyholder's application for the policy. The carrier also asserted a material misrepresentation defense, relying on a policy condition stating that the policy will be null and void if the application contains a material misrepresentation or omission. Although the case ultimately was dismissed without prejudice because the policy contained a provision requiring the policyholder and the carrier to try to resolve their dispute in mediation before initiating a lawsuit,[11] this case underscores the importance of taking a team

approach to the application process.

On a related note, cyberpolicy applications sometimes contain questions that are ambiguous or otherwise virtually impossible to answer with precision. For example, cyberapplications often ask questions about the policyholder's compliance with certain laws. Along these lines, some applications ask the following question: "Have you confirmed your compliance with the following ... PCI-DSS, HIPAA, Graham-Leach-Bliley, *other*?" (emphasis added). It is hard to imagine a word broader than "other," and, for most organizations, it would be difficult to answer this question affirmatively, as the question could be interpreted to require the policyholder to confirm that it is in compliance with every conceivable tribal, local, state, federal and international law on virtually any and every topic under the sun. While one certainly could argue that, in the context of this question, "other" should be narrowly interpreted to refer only to laws of a similar nature as the other specified laws, try to avoid this ambiguity and ask the carrier or broker for clarity. Additionally or alternatively, you could respond to a question like this by specifying the particular laws with which the policyholder has confirmed compliance. Failure to do so creates a risk that the carrier might later assert a material misrepresentation defense or seek rescission on the basis of the answer to this question. The main point is that you should have a very clear understanding of what each question means and, if you do not, ask for clarification.

Exclusions Often Asserted in Support of Coverage Denials

War Exclusion

Most cyberpolicies have some version of a war exclusion, which arguably would apply to state-sponsored hacking incidents, but some are broader than others. For example, some war exclusions encompass, among other things, "acts of foreign enemies" and "warlike operations," terms which typically are undefined in the policies and the interpretation of which is subject to debate, whereas other variations of the war exclusion are narrower in scope. Concerns about this exclusion were written about extensively in the aftermath of the 2014 cyberattack on Sony Corporation, particularly after United States officials reported that North Korea played a central role in the attack (although this conclusion has been subject to much debate). Because of tribal sovereignty, war exclusions might apply somewhat differently to tribal cyberclaims than to nontribal cyberclaims, tribal organizations nevertheless likewise have an interest in making sure their policies war exclusions are narrowly tailored.

Exclusions for Human Error and System Glitches, and for Acts by Employees

Businesses typically buy insurance, at least in part, because they recognize that, despite the best of intentions, people sometimes are negligent, and negligence often leads to liability claims and other losses. In fact, according to the 2016 Cost of Data Breach Study: Global Analysis issued by the Ponemon Institute, 52 percent of data breaches were caused by human error or a system glitch (25 percent were caused by human error; 27 percent were caused by a system glitch). Despite this, and although there usually is no dispute that traditional insurance policies typically cover claims arising from negligence, many cyberpolicies purport to exclude coverage for losses arising from at least some forms of human error or negligence. For example, some cyberpolicies exclude coverage for "any loss caused by an employee." Others exclude coverage for "any malfunction or error in programming or error or omission in processing," or for "mechanical failure," or for "error in design." While there may be arguments around these exclusions, avoid these disputes altogether, if possible, by buying cybercoverage that does not have these types of exclusions.

Bodily Injury and Property Damage Exclusion

Many cyberpolicies contain an exclusion for losses arising from bodily injury or property damage. This exclusion can be particularly problematic if the control systems in your facilities are connected to / operated through your computer network or the internet such that a cyberattack can result in property damage or bodily injury. Moreover, general liability policies, which typically provide coverage for liability arising from property damage or bodily injury suffered by others, often contain cyberexclusions. Hence, if you face these types of risks, make sure at least one of your policies provides coverage for these types of losses.

Other Hidden Traps in Cyberpolicies

Data Breaches Involving Vendor Networks

In today's world, many organizations store or rely on data in a number of locations, including on their vendors' networks. If you fall within this category, then make sure that your cyberpolicy extends coverage to such networks. Some policies provide that broad coverage, expressly extending coverage for third-party losses arising from, among other things, "a cloud computing provider's system failure or impairment." Other policies, by contrast, do not limit coverage to computer systems that are defined as computers, devices and networks that are "rented by, owned by, leased by, licensed to, or under the direct operational control of" the insured.

Cyberlosses Resulting From Social Engineering Crimes

Many organizations consider social engineering crimes — i.e., crimes in which an employee is tricked, through an email that appears to be from a legitimate source, into transferring funds to a fraudster — to be a type of cyberrisk. By contrast, a number of carriers do not, and have denied coverage for these types of losses, asserting that the loss was not the result of a hacking event but rather resulted from an employee's voluntary transfer of funds. While there are arguments as to why these should be deemed cyberlosses, many carriers now exclude them and may offer separate social engineering coverage, typically for additional premiums.

Policy Sublimits

Another consideration is that a cyberpolicy's overall policy limit may not be available for or applicable to all types of losses. Rather, some coverages can be, and often are. subject to sublimits, or limits lower than the overall policy limit. At times they can be quite low. Organizations should assess their major areas of exposure, and to endeavor to obtain adequate coverage for those types of losses. That being said, sometimes carriers erroneously assert that a particular sublimit applies to a given loss when in fact it should not. Under these circumstances, state your disagreement and argue for application of the higher limit.[12]

Retroactive Dates

Many cyberpolicies exclude coverage for breaches or other cyberlosses that took place prior to the policy's retroactive date, which can be particularly problematic because many data breaches go undetected for a period of time. For example, the Hard Rock Hotel & Casino Las Vegas data breaches described above lasted several months before they were detected. The same is true for many other data breaches. Therefore, negotiate as early a retroactive date as possible.

Conclusion

The unfortunate reality is that data breaches and other cyberlosses have become part of the new normal, and even tribal organizations with robust risk management programs can experience a breach and incur staggering costs responding to it. Cyberinsurance can help pay for these costs — but only if your cyberpolicy covers the types of risks facing your tribal organization and your coverage limits are adequate.

—By Erica J. Dominitz and Venus McGhee Prince, Kilpatrick Townsend & Stockton LLP

Erica Dominitz is a partner in Kilpatrick Townsend's Washington, D.C. office and a member of the firm's insurance recovery team. Venus Prince is counsel in Kilpatrick Townsend's Washington, D.C. office and a member of the firm's Native American affairs practice. Prince is a member of the Poarch Band of Creek Indians.

[1] See, e.g., Constance Gutke, No Business Too Small to be Hacked, N.Y. Times, Jan. 13, 2016,http://www.nytimes.com/2016/01/14/business/smallbusiness/no-business-too-small-to-be-hacked.html?_r=0 (reporting that 60 percent of all online attacks in 2014, targeted small and midsize businesses).

[2] Steve Ragan, Hard Rock Las Vegas Suffers a Second Data Breach, CSO Online, June 28, 2016,http://www.csoonline.com/article/3089449/security/hard-rock-las-vegas-suffers-a-second-data-breach.html.

[3] Id.

[4] Mitch Strohm, 300 Restaurants Part of Huge Data Breach, Bankrate.com, Feb. 5, 2016, http://www.bankrate.com/financing/identity-protection/300-restaurants-part-of-huge-data-breach/.

[5] Alex Boyd, River Cree Casino Hacked, Metro News, Mar. 18, 2016, http://www.metronews.ca/news/edmonton/2016/03/18/river-cree-casino-subject-of-cyberattack-.html.

[6] Mark Seward, Head in the Sands: One Year After the Sands Casino Data Breach, exabeam, Feb. 26, 2015, http://blog.exabeam.com/head-in-the-sands-one-year-after-the-sands-casino-breach.

[7] Ponemon Institute, 2016 Cost of Data Breach Study: Global Analysis (2016).

[8] FBI Director: Hacking Will Replace Terrorism as the Nation's Top Worry, Business Insider, Mar. 1, 2012, http://www.businessinsider.com/robert-mueller-fbi-hacking-terrorism-2012-3.

[9] Nicole Perlroth, Hacked v. Hackers: Game On, N.Y. Times, dated Dec. 2, 2014, http://bits.blogs.nytimes.com/2014/12/02/hacked-vs-hackers-game-on/.

[10] No. 2:15-cv-03432, 2015 WL 4497730 (C.D. Cal. Jul. 17, 2015) (dismissed without prejudice per ADR clause).

[11] Id.

[12] See, e.g., New Hotel Monteleone LLC v. Certain Underwriters at Lloyd's of London, No. 2:16-CV-00061 (E.D. La. 2016) (filed in Civil District Court for Orleans Parish, Dec. 10, 2015, removed to federal court on Jan. 1, 2016).
