
PHOTO CREDIT: SHUTTERSTOCK.COM

Not Your Dad's Eye in the Sky:

How Gaming Licensees and Regulators are Ensuring Cybersecurity Safety

Before casino floors were watched by security experts and smart computers in control rooms, there were real human eyes in the casino sky. These casino employees would be stationed in the rafters and ceilings of casino floors, closely watching table games and slot machines for cheaters and grifters, both to protect the casino from monetary losses, but also ensure the integrity of the games for all other casino patrons.

BY MICHAEL MORTON, ESQ.

Casinos clearly had a financial incentive to employ these skilled eyes – casino cheats were abundant back in the middle and late 20th century. However, gaming licensees also had a legal duty to ensure that these original black hats didn't succeed. In part, the statutory policy of the state, codified in Nevada Revised Statute (NRS) 463.0129, requires that gaming be competitive and conducted free of criminal elements. As a privileged licensee, each casino is obligated to ensure that the games provided on its floor are fairly played.

While that statutory duty has not changed, the ways in which a casino ensures that its floor is free from criminal elements and cheats surely has. Men in dark suits walking the casino rafters have been exchanged for vast networks of surveillance cameras, state-of-the-art control rooms, and facial recognition software. Unfortunately, as diligently as regulators work to ensure that only people with the highest levels of integrity are licensed to gain financially from the casino industry, there are bad actors around the world seeking to capitalize off of weaknesses in the market and the lack of situational awareness of those who operate within it. Hackers around the world are attacking casino operators every minute of every day, attempting to penetrate player reward program systems, casino floors, electrical systems, and cloud servers, not only to gain access to the personal identifying information from an expansive network of players, but also to exact ransom payments from operators who see an extended blackout of games as financially devastating and a risk to their licenses around the world.

Statutory Authority for Cybersecurity Oversight

A brief history on why cybersecurity risks are within the jurisdiction of gaming

CONTINUED ON PAGE 14

CONTINUED FROM PAGE 13

Not Your Dad's Eye in the Sky

regulators in Nevada is necessary to lay the foundation for why efforts to intensify cybersecurity infrastructure and safety must be a priority for Nevada's regulatory framework to remain successful in protecting the public.

Since 1955, when the state of Nevada chose to regulate gaming on a statewide basis, rather than at the city or county level, the policy of the state, set by the Nevada Legislature, has always been two-fold – that the gaming industry is vitally important to 1) the economy of the state; and 2) the general welfare of its inhabitants. It's clearly no secret that the gaming industry has been the prominent driver of Nevada's economy for close to 70 years now. But, more importantly, it's the "general welfare" portion of the state's policy that makes the industry so successful in Nevada.

The state's policy goes on to communicate that the continued growth and success of gaming is dependent upon public confidence and trust that licensed gaming and the manufacture, sale, and distribution of gaming devices and associated equipment are conducted honestly and competitively, that establishments holding licenses where gaming is conducted and where gambling devices are operated do not unduly impact the quality of life enjoyed by residents of this state, that the rights of the creditors of licensees are protected, and that gaming is free from criminal and corruptive elements.

To effectuate these goals, Nevada's policy has always required the strict regulation of all persons, locations, practices, associations, and activities related to the operation of licensed gaming establishments and the manufacture, sale, or distribution of gaming devices and associated equipment. While this requirement hasn't changed in decades, what constitutes an "activity related to the operation of licensed gaming establishments" certainly has. Placing a bet on a football game from a mobile application and cashless wagering were not gaming-related activities 30 years ago, but they definitely are now. Likewise, protecting a patron's personally identifiable information from a cyberattack was not an issue 50 years ago, but it certainly should be now.

What specifically from Nevada's legislatively approved gaming policy gives the Nevada Gaming Control Board and Nevada Gaming Commission the authority to regulate cybersecurity infrastructure in the gaming industry? NRS 463.0129 additionally states that all establishments where gaming is conducted and where gaming devices are operated, and manufacturers, sellers, and distributors of certain gaming devices and equipment must be, among other things, controlled and assisted to protect the public health, safety, morals, good order, and general welfare of the inhabitants of Nevada, to ensure the stability and success of gaming, and to preserve the competitiveness of the state's gaming economy and policies of free competition in Nevada. Nothing would hinder the safety, good order, and general welfare of the residents of Nevada more than a cybersecurity breach that stole personally identifiable information of residents or effect this state's competitive economy more than a ransom demand for the return of such information.

Even if it is without question that regulators in Nevada have the legislative authority to regulate cybersecurity issues in the gaming industry, should they? Is there a reason to create another layer of regulatory oversight, especially over an area of the industry where regulators might not have current and immediate expertise? While some readers may wish the answer was an emphatic "no," incidents over the past decade exemplify the need for oversight and accountability in the cyber security space, especially in the gaming industry. There have been reported hacks on a hotel's cloud server that housed personally identifiable information of hotel guests,[1] malware attacks on a casino's computer systems that held both patron and employee information,[2] and even an attack on a gaming licensee perpetrated by an adverse nation-state.[3] The risks are present, and the regulatory authority exists for increased protections of Nevada residents.

PHOTO CREDIT: SHUTTERSTOCK.COM

Nevada Regulators Seek to Combat Increased Cybersecurity Risks in Nevada

In September 2022, the Nevada Gaming Control Board conducted a regulatory workshop on proposed amendments to Regulation 5, which broadly establishes what is required to adequately operate a licensed gaming establishment in Nevada. The proposal creates two new requirements for licensees.[4] The first requires a licensee to perform an initial risk assessment of its business operation and develop best practices related to cybersecurity protection within the licensee's company. After performing the initial risk assessment, the licensee must continue to monitor and evaluate cybersecurity risks to its business operation on an ongoing basis and modify its established best practices and risk assessments as it

deems appropriate. According to the proposal, the risk assessment must be a process of identifying, estimating, and prioritizing risks to organizational operations and assets resulting from the operation of an information system. The proposal allows the initial risk assessment and ongoing monitoring and evaluation to be conducted by a third party with expertise in the field of cybersecurity.

The second portion of the regulatory proposal imposes reporting requirements on a licensee that experiences a cyberattack to one of its information systems resulting in a material loss of control, compromise, unauthorized disclosure of data or information, or any other comparable occurrence. If a licensee experiences a cyberattack, it must provide written notification of the cyberattack to the Nevada Gaming Control Board as soon as practicable but no later than 72 hours after realizing it was the victim of a cyberattack. Upon request by the board, the licensee must provide the board with specific information regarding the cyberattack. Additionally, the licensee must also perform an investigation into the cyberattack, prepare a report documenting the results of the investigation, notify the board of the completion of the report, and make the report available for review by the board. The report must include the root cause of the cyberattack, the extent of the attack, and any action taken or planned to be taken by the licensee to prevent a similar event in the future.

Since 1955, when the state of Nevada chose to regulate gaming on a statewide basis, rather than at the city or county level, the policy of the state, set by the Nevada Legislature, has always been two-fold – that the gaming industry is vitally important to 1) the economy of the state; and 2) the general welfare of its inhabitants.

Further, the regulatory proposal would require Group One licensees in Nevada – licensees that currently have a gross gaming revenue of more than $7,000,000 per year – to designate a qualified individual to be responsible for developing, implementing, overseeing, and enforcing the covered entity's cybersecurity best practices and procedures. The proposal also would require a Group One licensee to have its internal auditor or a qualified third party with expertise in the field of cybersecurity perform and document observations, examinations, and inquiries of employees to verify the licensee is following the cybersecurity best practices it established. The licensee must then retain all documents prepared by the internal auditor or third party and make them available to the board upon request.

The board recommended adoption of this proposed amendment to Regulation 5 to the Nevada Gaming Commission. The commission unanimously approved this regulatory proposal on December 22, 2022, and the amendments became effective on January 1, 2023.

CONTINUED ON PAGE 17

CONTINUED FROM PAGE 15

Not Your Dad's Eye in the Sky

Safety of Patrons Paramount

Casinos are a treasure trove of personally identifiable information about their patrons and stand to lose big – even a privileged license – if more is not done to prevent cyberattacks against licensed properties and entities. Not just in Nevada, but in countless regulated jurisdictions across the globe, licensed entities have a legal responsibility to protect their patrons from all types of bad actors, which now also include cyber actors.

ENDNOTES:

1. "MGM Resorts hack affected a reported 10.6 million former guests." *Las Vegas Review-Journal*. February 20, 2020, available at https://www.reviewjournal.com/business/casinos-gaming/mgm-resorts-hack-affected-a-reported-10-6m-former-guests-1961400/.
2. "Dotty's parent company announces data breach, says private info may have been released." KTNV. September 17, 2021, available at https://www.ktnv.com/news/dottys-parent-company-announces-data-breach-says-private-info-may-have-been-released.
3. "Iran's Cyber Attack on Billionaire Adelson Provides Lesson on Strategy." *Claims Journal*. January 6, 2020, available at https://www.claimsjournal.com/news/national/2020/01/06/294849.htm.
4. See generally https://gaming.nv.gov/modules/showdocument.aspx?documentid=19142.

MICHAEL KILPATRICK MORTON'S biography is available on page 6.