New Nevada Gaming Commission Cybersecurity Regulation

By Glenn Light, Patrick Emerson McCormick, and Karl Rutledge

In an ever increasingly digital world, the significance of cybersecurity has reached unparalleled heights, and, in turn, has become an essential safeguard for individuals, businesses, and governments alike. Accordingly, on December 22, 2022, the Nevada Gaming Commission ("NGC") amended its regulations to create NGC Regulation 5.260, Cybersecurity. This Regulation took effect on January 1, 2023.

Regulation 5.260 requires that "gaming operators take all appropriate steps to secure and protect their information systems from the ongoing threat of cyberattacks." This Regulation applies to any entity with: a nonrestricted license as defined in NRS § 463.0177; a gaming license allowing for the operation of a race book; a gaming license that allows for the operation of a sports pool; and/or a gaming license that permits the operation of interactive gaming. These are defined as "covered entities."

Most of the requirements found in Regulation 5.260 are reasonable best practices for any entity that has substantial capital and consumer data. These new requirements can be summarized in five categories.

First, a covered entity must perform an initial risk assessment and develop best practices, then monitor and regularly update them as needed. Regulation 5.260(3) provides a list of best practices for guidance in developing the covered entity's own best practices (including, without limit, CIS Version 8, COBIT 5, ISO/IEC 27001, and NIST SP 800-53, or later versions thereof). Importantly, covered entities have until December 31, 2023, to comply with this requirement.

Undertaking an initial risk assessment will be the first critical step in ensuring compliance with Regulation 5.260. Covered entities should identify all assets (including hardware, software, data, and networks), assess potential vulnerabilities, and determine the potential impact of cyber threats on each of these assets. A covered entity may use a third-party cybersecurity professional to provide a comprehensive and technically detailed risk assessment, as well as to provide ongoing monitoring and evaluation.

While not explicitly required by Regulation 5.260, any covered entity would do well to formulate a robust data breach response plan after performing its risk assessment. Such a plan should include well-defined procedures for identifying, containing, and eradicating a potential cyber threat, and address the recovery process as well as post-incident review and analysis. All the requirements in Regulation 5.260 should be preemptively addressed in this plan.

Second, Regulation 5.260(4) creates a notification requirement in the event of a cyberattack, requiring providing notice to the Nevada Gaming Control Board ("NGCB") within 72 hours after becoming aware of the cyberattack. This is in addition to an entity's requirement to comply with NRS § 603A.220, which governs data breaches in the State of Nevada generally, and any other relevant state or Federal statutes.

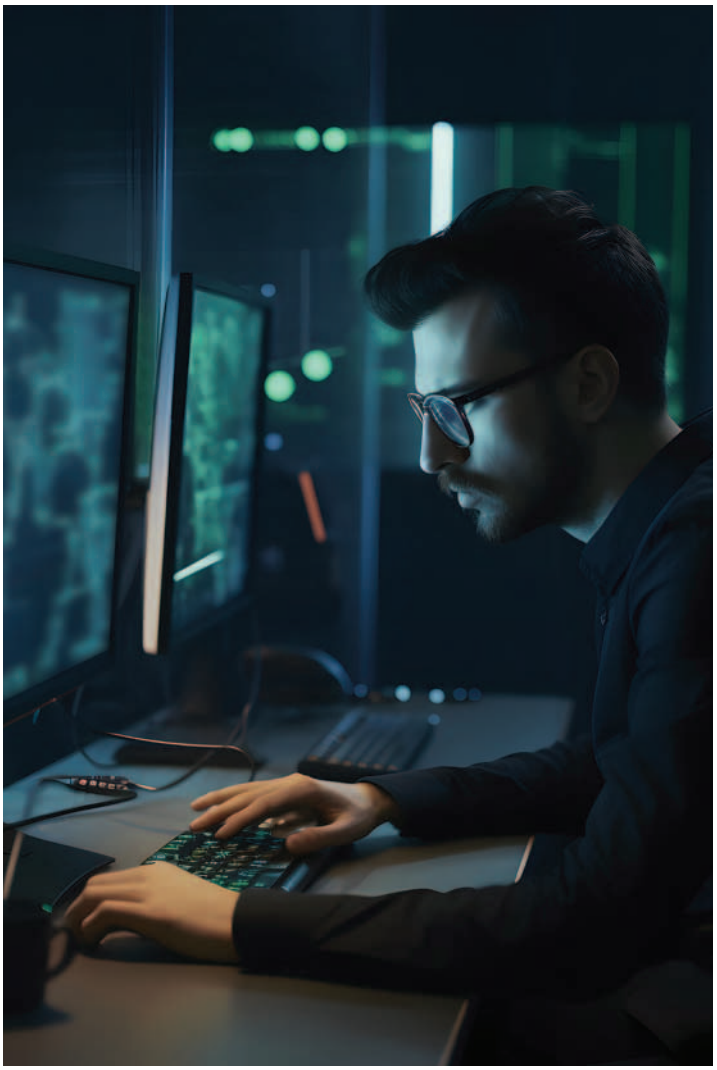
The data breach response plan should also include a clear communication strategy for managing external and internal communications after an incident. This includes a framework for informing all affected parties, from customers to employees. It is important to understand the legal obligations for notification, which may vary state-by-state and also depend on federal guidelines. All these requirements, timelines, and contact information can and should be explicitly included in a comprehensive data breach response plan.

Third, covered entities must also perform an investigation into any cyberattack, including documenting the results of the investigation and making a report available to the NGCB with specific findings, including the cause and extent of the attack. This requirement goes above and beyond most existing notification requirements, which do not typically require the breached entity to disclose its post-attack report.

Responding entities should take care in their written communications related to the post-attack forensic investigation, even with their attorneys. Some courts have held that such investigations are performed for business purposes rather than for legal reasons, and as such no attorney-client privilege protects the entity's communications with its attorneys. Nevada courts have not yet opined on this matter, but Regulation 5.260's requirement for the creation and disclosure of a post-attack report increases the likelihood that a court will view communications related to the investigation as a business operation, not a legal one.

Fourth, Regulation 5.260(5) requires Group I licensees (per Reg 6.010(8)) to have a designated, qualified individual responsible for the covered entity's cybersecurity best practices and procedures. Group I licensees must also perform annual audits and reviews of their best practices, procedures, and security. While Regulation 5.260(5) does not address all covered entities, any covered entity should also review its best practices and procedures at least annually to ensure compliance with Reg 5.260(3), which requires any covered entity to "continue to monitor and evaluate cybersecurity risks to its business operation on an ongoing basis."

While not required, a Group I licensee (and any other covered entity) should consider an annual tabletop exercise in addition to its annual audit and review. Conducting regular tabletop exercises help identify potential gaps in a security system and refine the data breach response plan. They also train the members of the covered entity in the flow of responding to a breach, much like a practiced fire drill.



Finally, all steps taken to comply with Regulation 5.260 must be memorialized in writing and retained for five years, per Regulation 5.260(6). Failure to exercise due diligence in compliance with any section of Regulation 5.260 "shall constitute an unsuitable method of operation and may result in disciplinary action." While not entirely clear from the language of Regulation 5.260(6), it is likely a covered entity need only retain the documents necessary to memorialize its compliance that must be retained and produced upon request (and not all writings created to comply with Regulation 5.260). This subsection is also silent on attorney-client communication privilege. Until there is further guidance on this issue, a covered entity and its counsel should proceed as though all written communications relating to a data breach response covered by Regulation 5.260 may not be protected by attorney-client communication privilege.

In conclusion, the requirements set forth in Regulation 5.260 are fairly reasonable, advisable precautions that will make covered entities better prepared and protected from a data breach, which will in turn provide a return on investment beyond compliance if done with intentionality. The vague and potentially onerous notification requirements will increase costs in the event of a breach, but not significantly beyond other existing Nevada and Federal notification requirements. Due to the strict nature of the new Regulation 5.260 requirements, every covered entity would do well to have a data breach response plan that it reviews and updates at least annually. ■

Glenn J. Light is a Partner and Chair of Lewis Roca's Commercial Gaming Industry Group. He provides counsel on nearly every aspect of commercial gaming transactions, including licensing, corporate structure, financing and due diligence.

Karl F. Rutledge is managing partner of Lewis Roca's Nevada offices, which include Las Vegas and Reno, and a member of the firm's Commercial Gaming Industry Group providing counsel on gaming, eSports, fantasy sports, sports betting, and promotional marketing.

Patrick Emerson McCormick, CIPP/US is an associate in Lewis Roca's Data Privacy and Cybersecurity Group. He assists clients on how to comply with the growing number of data and cyber regulations, how to best protect themselves from data breaches, and how to respond if one occurs.

[1] For example, each state has its own set of requirements in the event of a data breach, including who must be notified, timelines for the notification, and what information must be included. The Federal Trade Commission provides additional guidelines for businesses on what to do in the event of a data breach.

[2] Current revenue thresholds for Reg 6.010(8) can be found here: https://gaming.nv.gov/modules/showdocument.aspx?documentid=8372