NIGC Tech Alert

CYBER HYGIENE: WHY SECURITY-CONSCIOUS ORGANIZATIONS ADHERE TO IT!

The increase in ransomware attacks on casinos, particularly tribal properties, continues to keep IT departments and leadership on high alert. In 2023 attacks against tribal properties were above 60 percent (cdcgaming.com). Anticipating 2025 to continue that trend, tribes need to develop and maintain more stringent cyber security practices. Cyber hygiene, or more accurately stated as cybersecurity hygiene, is a standard of information technology practices organizations and personnel use regularly to maintain the cyber health and security of users, devices, networks and system data. The key goal of employing a cyber hygiene strategy is to ensure sensitive data is secure and in the event of a security breach, an organization's capability to effectively recover is enhanced.

The concept of cyber hygiene works similarly to that of personal hygiene. Individuals maintain their health by taking regular recommended actions, such as flossing to minimize cavities or gum disease and handwashing to avoid viral infections (techtarget.com). Organizations can maintain high-quality cyber health by preventing data breaches and other security incidents through employment of precautionary cyber hygiene measures. The National Indian Gaming Commission (NIGC) minimum internal control standards are designed to provide tribes with bare minimum IT compliance requirements with 25 CFR 543.20. NIGC encourages each Gaming Operation to develop and maintain tribal internal controls as well as system internal controls as it applies to their unique organization to ensure a strong cyber hygiene strategy is being employed.

Regardless of gaming operation, establishing critical cyber hygiene practices can significantly reduce IT vulnerabilities, threats and risk. Almost all successful cyberattacks take advantage of conditions that could be reasonably described as "poor hygiene" including, failure to patch known vulnerabilities, poor configuration management and inefficient management of administrative privileges (cisecurity.org). To establish and maintain an effective cyber hygiene consider the following:

- **Protection:** Deploy layered security solutions, including encryption, firewalls and regular backups to protect critical assets and data
- **Detection:** Uncover weaknesses and risks through regular vulnerability scans, threat intelligence, and continuous real-time monitoring
- **Maintenance:** Strengthen your defenses by consistently applying software updates, patching known vulnerabilities and retiring legacy systems as soon as possible
- **Monitoring:** Continuously observe systems activity to detect anomalies and unauthorized access in real time
- **Awareness:** Empower employees with tailored cybersecurity training to identify and avoid phishing, malware and social engineering attacks

For more information on casinos dealing with an increase in cyberattacks, please find it at
https://cdcgaming.com/tribal-casinos-deal-with-an-increase-in-cyberattacks/

For minimum internal control standards, please find the NIGC IT Audit 25 CFR 543.20 Toolkit at
https://www.nigc.gov/images/uploads/training/Toolkit_ITAudit_Rev12_4.pdf

If you have questions concerning any remote access attack, social engineering compromise or any other technical matter, please email ocio@nigc.gov.

DIVISION OF TECHNOLOGY

February 2025