# NIGC Tech Alert

## CYBER RESILIENCE: AN EVER-EVOLVING CONSTRUCT

Historically, when organizations looked at cyber resilience, the focus was primarily on creating effective system disaster recovery plans, business continuity plans and incident response plans as key mechanisms to follow a cybersecurity attack. Of course, this also included a myriad of checklists and procedures for key IT personnel and critical senior leadership. Today, cyber resilience where an organization prepares for, respond to, and recover from cyberattacks or security breaches, requires more, including a crisis management plan, a cyber resilience plan and a physical security plan. Even as the newest cybersecurity tools are being implemented within the network infrastructure, malware attacks are evolving. For example, Extortion ware is malware used to extort victims, stealing their sensitive data for threats. Extortion ware is unlike ransomware, which forces a business to either pay up or lose access to the stolen data, extortionists threaten to publicly release the collected information. This often pressures the business to comply, which increases the likelihood the victim will adhere to the extortion demands (techtarget.com). In tribal gaming, cyber resilience is about minimizing the impact and recovering from disruptions to the core organization – the gaming operation! Cyber resilience combines cybersecurity and business continuity, but with it requires an active offensive approach.

An effective cyber resilient system is typically tailor-made for the organization. Basic cybersecurity controls including penetration testing, vulnerability management and monitoring are typical, but more can be done. Cyber threat intelligence and extended detection response (XDR) may be used to maintain continuous situational awareness and situational understanding. This provides an external as well as internal view that can be used to quickly prioritize known vulnerabilities. You can also use active threat hunting to patrol your IT Geofence. Assume you have been attacked and do not wait for your detection system to show you something is wrong. Being cyber resilient means actively looking for weaknesses and remediating known vulnerabilities whenever and wherever possible.

Building a cyber resilient organization relies on planning:

1. Identify – What can you not afford to lose? And what can you afford not to lose?
2. Protect – How do you backup your mission critical data?
3. Detect – Can you detect data loss and corruption?
4. Respond – Can you restore fast and accurately?
5. Recover – Are your disaster plans tested and current?

The National Indian Gaming Commission 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 resilient strategy is being employed based on 25 CFR 543.20. CISA offers a free cybersecurity tools to assist with building a cyber resilient system (CISA.gov).

For information on Free Cybersecurity Services and Tools from CISA, please find it at
https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools

For more information on building a cyber resilient organization, please find it at
https://www.indiangaming.com/pioneering-progress-staying-ahead-of-the-cybersecurity-curve/

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