

5 Threats

to Tribal Revenue Streams



One Attack Could Shut Down Your Entire Tribal Government

Your casino, government offices, health clinic, and social services all share the same internet connection. Hackers get into one system and spread to everything. Casino down. Clinic closed. Government services frozen. Social services stopped. Per capita payments delayed. Everything your tribe depends on—gone in one attack.

Do you know if your systems are connected in a way that makes this possible?



Someone Could Steal Millions Using the Chairman's Voice

New AI technology can clone your chairman's voice with just 3 seconds of audio from a public meeting. Attackers call your finance team using a perfect voice copy and authorize a \$500,000 wire transfer. By the time you realize it's fraud, the money is gone. This happened to 1 in 6 organizations last year—a 1,900% increase.

Can your team tell the difference between real and fake?



A Data Breach Could Disrupt Casino Revenue for Months

If hackers access guest payment or personal information, the impact goes far beyond IT. News travels quickly. Trust can erode. Guest visitation may decline while the tribe works to restore confidence. Operational disruption, forensic investigations, notification requirements, potential regulatory scrutiny, and payment card compliance issues can all follow. The financial effects are not limited to technical recovery costs — they can include lost revenue, increased security investments, higher insurance premiums, and reputational damage that takes time to rebuild.

Is protecting your guests' data & the continuity of your gaming operations a top priority?



Your Health Clinic Could Stop Serving Your People

If a cyberattack shuts down your clinic's computer systems, clinicians may lose access to patient records, billing systems can go offline, and care delivery can grind to a halt — often for weeks. Downtime from ransomware and data breaches in healthcare can last two to three weeks or more, disrupting appointments, billing, and essential services. The financial impact is significant — the average healthcare cyber incident costs between \$2 million and \$8 million, not including potential regulatory penalties under HIPAA if patient data is exposed.

Could your tribe afford to lose healthcare revenue for a month?



Your Vendors Could Be the Weak Link That Destroys You

You trust your slot machine company, your payment processor, your IT support team. But hackers attack them first, then use their access to get into your systems. 6 out of 10 cyberattacks start this way. Your security doesn't matter if your vendors have weak security. Average cost: \$4.5 million.

Do you know how secure your vendors really are?

How Maxxsure Helps

- Financial Exposure Analysis
- Simple, Executive-Level Cyber Risk Scoring
- Cyber Insurance Alignment
- Analytics That Drive Action
- Ongoing Risk Monitoring

Ready to Protect Your Tribal Enterprise with Maxxsure?

 Email nancy.viner@maxxsure.com to schedule a 20-min call