A Need for New Armor: Tribal Entities Under Cyberattack

By: Emma Kincade, Trent Shores, and Tom C. Vincent II
October 27, 2021

A number of tribal governments and their business enterprises are in the sights of cybercriminals. Cyberattacks threaten the security and critical infrastructure of tribal nations, many of which are integral to healthcare, education, justice, and other governmental services and operations. A number of tribes within Oklahoma's borders and beyond were targeted by ransomware attacks in 2021, leaving both their information technology systems and their citizens in peril. Government facilities, hospitals, justice systems, and gaming enterprises were forced to shut their doors and respond to what some tribal leaders have rightly identified as acts of terrorism against their sovereign nations.

The Federal Bureau of Investigation estimates that hackers launch nearly 4,000 ransomware attacks per day. More and more hackers have recently shown a focused interest in tribal enterprises, including gaming operations, because of their deep cash reserves. Cyberattacks in Indian Country are becoming more frequent and more destructive, prompting the National Indian Gaming Commission to announce that it will go "on the offense" and create a cybersecurity task force. Moreover, the need for action to protect tribal citizen's personal data and health information is pertinent and clear, especially as tribal governments transition to facilitate more online services during the COVID-19 pandemic.

Ransomware breaches are costly. Perpetrators have been known to demand thousands—or even millions—in cash for the return of data. The catastrophic nature of these attacks leave many leaders wondering if the tribe should pay a hacker's ransom. Some tribes have reported that after their data was returned for a high price, some files remained subject to encryption, leaving the files corrupt and sometimes unusable. Others have declined to pay ransom, resulting in days of shutdown at revenue-driving facilities because of prolonged damage to the tribes' IT systems. So, how do tribes defend their data? It depends. There is no one size fits all solution for Indian Country. Each tribe is unique in its history, people, culture, customs, language, and government. Tribes maintain different data for numerous purposes, and through various systems and access points. Because there is no uniform approach, guarding against sophisticated cyberattacks requires a firm understanding of a tribe's government structure, economic environment, and approach to self-governance.

The Transportation Security Administration, Securities and Exchange Commission, Department of Labor Office of Safety and Health Administration, and Department of Homeland Security have made cybersecurity regulation and enforcement a priority in 2021. Each shares a common message across the board: it is imperative that any individual, government, or business prepare its arsenal for responding to cyberattacks. Every good defense starts with a plan. Developing a comprehensive response plan that encompasses both the tribe's government and business operations will enable swift action by those best-suited to respond to attacks as soon as they come. Unlike the often top-secret plans used by America's armed forces to respond to enemy combatants, the best cybersecurity plan is one that is communicated to and understood by every person at every level of service. This includes a tribe's third-party vendors, because as more data is shared, more access points arise. Preventative measures, including employee training and system audits are necessary to prepare team members and vendors at every level of operation to avoid attacks and respond to crises as they occur. Even with a defense strategy in place, data is vulnerable to theft and corruption unless government and business IT systems are fortified. Guarding against sophisticated hackers will require more than

a few anti-virus updates; and everyone from tribal leaders to employees must understand their responsibilities to protect the tribe and the data it maintains.

Sadly, cybersecurity threats are no longer hypothetical and criminals are targeting every access point imaginable. Every link in the armor provides a stronger and more coordinated response to cybercriminals and others seeking to disrupt the self-governance of our tribal nations. It's evident that hackers are on the offense. It's time to secure the defense.

Emma Kincade
918-595-4856
ekincade@gablelaw.com

Trent Shores
918-595-4805
tshores@gablelaw.com

Tom C. Vincent II
918-595-4857
tvincent@gablelaw.com