Executive summary | November 14, 2023

Wipfli Tribal Gaming CFO Exchange

Host: Grant Eve | Wipfli
Host: Barnaby Allen | Wipfli
Facilitator: Josh Iverson | Profitable Ideas Exchange

Introduction

Thirty-one chief financial and IT officers from tribal gaming facilities met virtually to share leading practices and discuss topics of mutual interest based on an agenda created through a series of pre-interviews. From Wipfli, Grant Eve, tribal industry leader, and Barnaby Allen, partner in the tribal gaming practice, hosted the exchange and Josh Iverson of Profitable Ideas Exchange facilitated.

Tom Wojcinski, principal in Wipfli's cybersecurity and technology management practice, joined to provide subject matter expertise. The focus of the discussion covered the following topics over the course of the hour:

- State of the industry
- Cybersecurity threats and responses
- Cybersecurity insurance

State of the industry

Wipfli's Grant Eve and Barnaby Allen opened the conversation by providing a short overview of the current state of the industry and the overall economy.

- CFOs can expect rates to stay relatively the same for the near term. Inflation is showing signs of abating, currently sitting around 3.7% and expected to decrease to around 2.5% by 2024. GDP is projected to end the year around 2.4%, with a dip to 1.4% in 2024.

- On the employment front, 26% of jobs offer work-from-home options, reflecting a decline from a high of 37% in the wake of the COVID-19 pandemic. Unemployment remains stagnant at about 3.8%, with a forecasted increase to 4.2%-4.3% in 2024.

State of the industry

- Commercial gaming indicated an overall year-over-year increase of 4.9%. Notably, commercial gaming saw a 1.0% rise in slot play and a 1.7% increase in table games, which is much slower growth than sports betting and iGaming. Commercial revenue was up 10.4% year to date. In August, an AGA report revealed that 17 out of 33 gaming jurisdictions reported increases.
- NIGC Chairman Sequoyah Simermeyer met with tribal leaders in September and emphasized the industry's shift, with a focus on technology and the need for tribes to adapt to new technologies and understand emerging threats around cyber and ransomware.

Cybersecurity threats and responses

Wipfli's Tom Wojcinski shared perspectives on cybersecurity in gaming.

- The recent attack on MGM and Caesars in September put a spotlight on ransomware as a continued top concern for gaming operations. In the case of MGM, the attack originated from the help desk, a vulnerability that Wojcinski has seen exploited in penetration testing with clients. Given that this type of attack involves an employee granting access to an attacker, it is crucial for gaming facilities to properly train help desk employees and have procedures in place to validate the identities of anyone making requests.
- Wojcinski identified certain ransomware threat trends, including instances of "double dipping" and soliciting payments under the pretext of preventing data disclosure after ransom payments.
- He also highlighted physical vulnerabilities that pose risks to casino operations. Specific to tribal entities, there are concerns about spillover from government vulnerabilities (i.e., governments are often much weaker in their security posture, so an attack on a tribal government could potentially cross over to the gaming side). A recent Wipfli penetration test illustrated weak security in tribal governments, revealing compromised credentials and lax practices around physical security. There is also an uptick in wipers (malware designed to delete data) recently as global conflicts lead to the spread of these weaponized cyber tactics.

Cybersecurity threats and responses

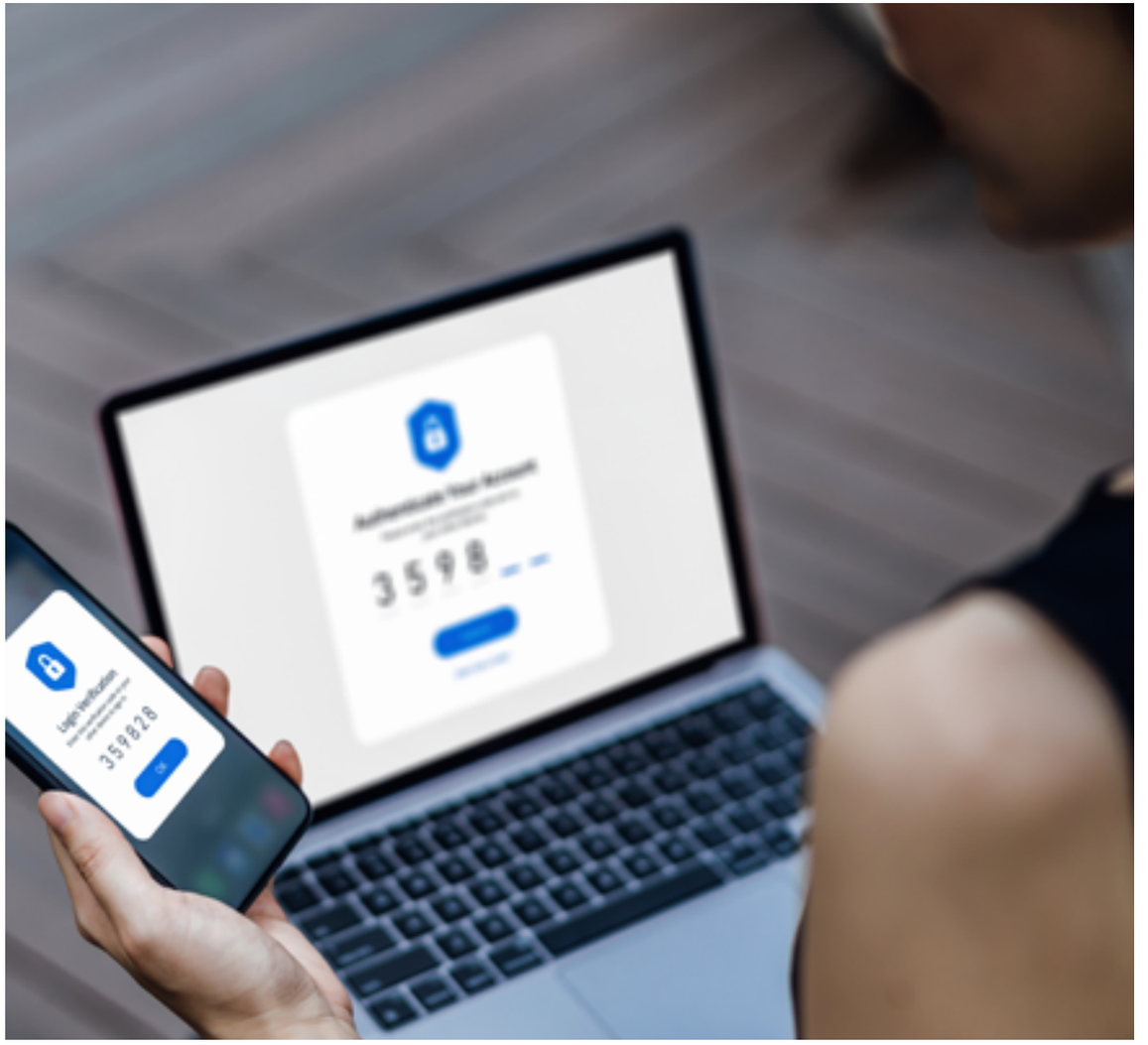
- Wojcinski noted the “tale of two responses” in the cases of MGM and Caesars — both were hit by ransomware, but Caesars paid and no one knew about it, while MGM refused to pay and was in the news. The decision of whether to pay a ransom is very specific to an organization. Asked how much data companies that pay are able to recover through the decryption keys they receive from hackers, Wojcinski estimated that decryption is successful in 80% of ransomware cases. One CFO shared a Gartner statistic that 39% of data is unrecoverable in a ransomware attack.

Cybersecurity insurance

Cyber insurance costs have surged by up to 300% in the past two years, accompanied by higher deductibles.

- The spike is attributed to insurers grappling with increased ransomware incidents, prompting them to raise premiums and increase coverage quality. To offset losses, almost all insurers are mandating security control upgrades for cyber coverage. However, some claims are being denied due to misrepresentation of cybersecurity safeguards during the application process.

- Despite dramatic increases in insurance coverage costs in 2022, recent trends suggest a plateau, attributed to organizations adopting multifactor authentication and other detection and response tools.



Cybersecurity insurance

Cyber insurance involves two major components: business interruption and ransomware payments.

- However, the two are not mutually exclusive — despite paying a ransom, there is still a likelihood of experiencing business interruption.

- A participant observed that addressing ransomware with cyber insurance may seem worthwhile for business interruption, but from an IT cybersecurity perspective, the success rate is viewed as 0%. Accurately identifying all entry and exit points is extremely difficult, especially since a compromise can occur weeks or months before an attack is initiated. As a result, the participant favors a zero trust approach that assumes everything is compromised and needs to be rebuilt from backups.

- Another CFO shared that in 2020, their baseline for cyber coverage premiums was around $40,000, but after an attack took place within the organization, the premium more than tripled to $150,000. Notably, deductibles saw significant changes: The business interruption deductible increased from $50,000 to $500,000 the following year. Ransom and extortion coverage decreased from $5 million to a quarter of a million.

- These shifts in deductibles and coverage are crucial considerations in discussions about the adequacy of cyber insurance, especially when addressing shareholder concerns following a major cyberattack. Another gaming operation saw their premiums increase due to a lack of specific security measures, such as multifactor authorization and server protection. Despite premiums staying the same, coverage decreased, and a coinsurance payment was required until the implementation of a multifactor system.

Cybersecurity insurance

While rising premiums are a point of frustration for CFOs, insurance companies provide a benefit in that, by imposing technical requirements, they are a driving force for organizations to advance technology and meet stringent cybersecurity standards.

- Without insurers, some CFOs worry there would be a lack of external pressure compelling organizations to prioritize cybersecurity. One member mentioned that some of this pressure is now coming earlier in the chain, with brokers employing third-party assessments urging organizations to remediate vulnerabilities before submitting to insurance carriers for optimal coverage.

Wojcinski observed that the federal government's regulatory stance on cybersecurity is hands-off, providing guidelines on desired outcomes but leaving the specifics to entity management.

- Recently, there is a shift toward seeking assurance mechanisms to verify the presence of cybersecurity controls. The AICPA's efforts in developing specialized audit reports on cybersecurity controls are an example, indicating a growing market adjustment. The lack of precise regulatory guidelines has led to assurance-based approaches driven by insurance requirements and initiatives within the CPA field.


WIPFLI
wipfli.com/tribal