Executive summary | September 26, 2023

Wipfli Tribal Government CFO Exchange

Host: Lisa Desotelle | Wipfli
Host: Tom Wojcinski | Wipfli
Facilitator: Austin Evans | Profitable Ideas Exchange

Introduction

Fourteen chief financial officers (CFOs) from tribal governments 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, Lisa Desotelle, partner, hosted the exchange and Austin Evans 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:

- Trends in cybersecurity
- Enhancing cybersecurity

Trends in cybersecurity

Tom Wojcinski of Wipfli shared insights on the recent MGM cyberattack and the social engineering behind it.

- The attack was similar to the social engineering Wipfli uses for a penetration testing regimen wherein a target firm's help desk employees are strategically chosen as subjects.

- In one example, this test began with a "password spray" of educated guesses on passwords, leading to the illicit access of an employee's personal email account. Subsequently, the compromised email account was exploited to facilitate a legitimate request for a new laptop on which the attack could be continued.

Trends in cybersecurity

Wojcinski presented an additional scenario wherein their team evaluated the effectiveness of a tribal government's physical security protocols.

- Through social engineering, they were able to gain access to all targeted sites, and in four out of five attempts, they succeeded in implanting a rogue device on the network.
- During the testing process, it came to light that the organization exhibited subpar password security practices, characterized by IT professionals and network administrators employing identical passwords across diverse domains.

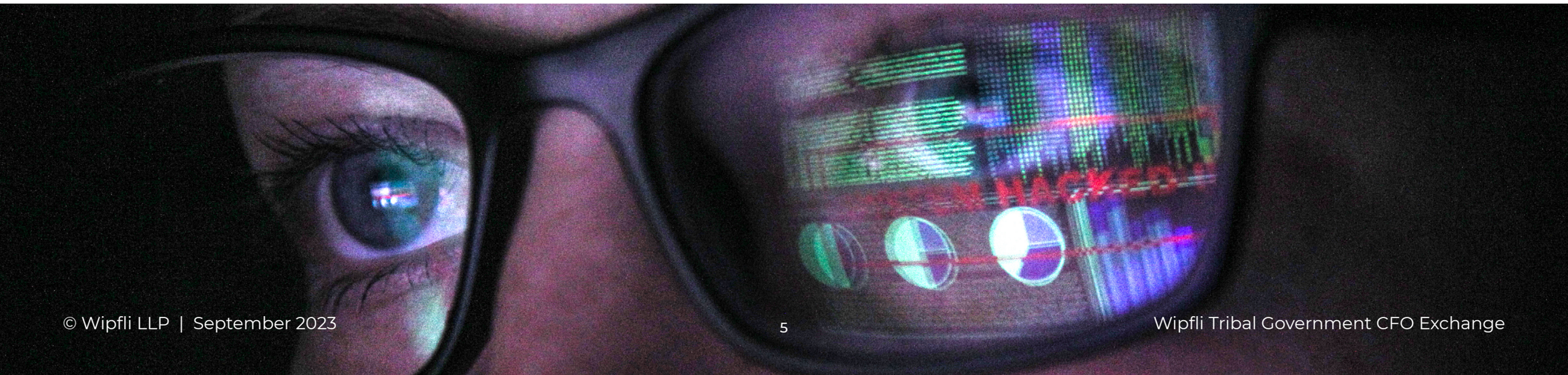
More tribal governments are adopting cloud-based systems, a trend attributed to the cloud's elevated security attributes.

- Many leaders remain hesitant about cloud adoption due to concerns with data sovereignty. Thankfully, the integration of diverse encryption techniques and confidential computing mechanisms has empowered tribal governments to exert substantial control over their data assets.
- Wojcinski explained the benefits of cloud migration as a security strategy and counseled tribal entities to consider migration, particularly when compared to the alternative, cost-intensive investment in new data centers.
- Whether tribes move to the cloud or continue with on-prem solutions, they still have a responsibility to enact robust cybersecurity processes and procedures.

Trends in cybersecurity

Cybersecurity insurance costs have experienced a notable escalation while, simultaneously, their accessibility has become difficult.

- This trend can be attributed to heightened awareness among insurance underwriters regarding the inherent risks associated with insuring clients for cybersecurity.
- The application process for cybersecurity insurance has become more complex, demanding comprehensive data and information submissions from prospective policyholders, aimed at mitigating insurable risks.
- In light of these developments, Wojcinski emphasized the importance of judiciously scrutinizing insurance agreements. He recommended completing a meticulous technical review to increase the likelihood of insurance claims being approved.



Enhancing cybersecurity

Security awareness training, coupled with the utilization of firewalls and nontechnical internal safeguards, constitute effective measures for reducing the susceptibility to business email-related cyberattacks.

- It's imperative for tribal governments to invest in comprehensive employee training programs aimed at enhancing email vigilance.
- These initiatives are particularly vital in countering typo squatting. With typo squatting, malicious actors craft deceptive emails that closely resemble their legitimate counterparts to perpetrate fraudulent activities.

The proliferation of servers within an infrastructure amplifies the vulnerability to cyberattacks.

- An effective response is server reduction wherever deemed appropriate.
- An executive mentioned an ongoing collaborative effort with their IT department, focusing on server consolidation as a proactive measure to mitigate their potential exposure to future cyberthreats.

Enhancing cybersecurity

Proprietary internal technological solutions have emerged as an effective strategy in cyberthreat mitigation.

- A member of the group detailed the development of an in-house email scanning system designed to scrutinize every incoming email prior to employee access. This bespoke email scanning system has assumed a pivotal role within their operational framework, especially given their high-volume email interaction.

Revisiting payment protocols and guidelines is instrumental in curbing fraudulent cyberattacks.

- In the case of one participant, successive cyberattacks prompted them to take proactive measures to better protect payments. They instituted revised payment guidelines, mandating additional verification steps for certain payment methods, including mandatory follow-up phone calls for authentication.

Other members shared efforts to enhance security measures in their governments.

- These include policy shifts requiring employees to physically complete direct deposit forms, thereby eliminating the convenience of email-based changes for direct deposits.

- One executive underscored the reduction of Automated Clearing House payments, favoring a structured protocol for wire transfers to bolster safeguards against fraudulent activities.

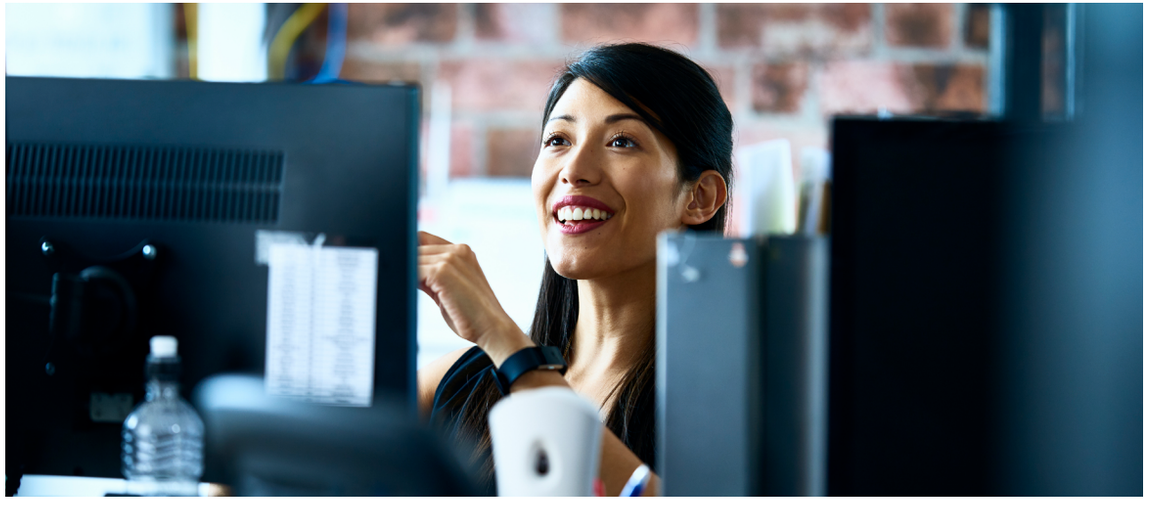
Enhancing cybersecurity

Systematic assessment of employee preparedness is crucial in gauging susceptibility to prospective cyberthreats.

- An executive described their previous employment within a tribal government wherein employees were subjected to succinct yet insightful 15-minute cybersecurity assessments on an annual basis.
- Another executive detailed an innovative monthly training initiative introduced by their tribal government. This ongoing program, orchestrated by their IT department, entails the distribution of simulated phishing emails to employees, which are to be identified and reported. Subsequently, employees displaying lower proficiency scores are assigned additional training resources, thereby enhancing their resilience.

Consistent security training and frequent testing have emerged as pivotal factors in reducing an organization's susceptibility to phishing emails.

- Wojcinski shared that companies lacking such routine security training and testing protocols face a 22% likelihood of falling prey to phishing email attacks. With sustained training, that rate can come down to 2%-3%.




WIPFLI
wipfli.com/tribal