CIO

Working Group

RECAP

September 16 - 17 | Washington, DC

EXECUTIVE SUMMARY

The CIO Working Group gathered September 16-17, 2019 in Washington, D.C. to talk through strategic and operational aspects of agency operations from the technological perspective. The group started with a collaborative discussion on key challenges and individual questions posed to the group. The Working Group focused on succession planning, cultivating, retaining and acquiring talent, information security, budgeting and forecasting your IT budget, and open systems. The group then received a state of affairs update from Joel Wood, senior vice president of The Council's government affairs team.

MAIN TOPICS

Strategic Questions Asked by CIOS During Group Share

- What are the actual use cases for Blockchain in the insurance industry?
- How do you vet the hype from the noise in the technology evaluation process?
- What are your remote work/mobility strategies for employees?
- What are you doing to comply with CCPA or GDPR?
- What new technologies are you investigating?

Succession Planning, Cultivating, Retaining and Acquiring Talent

Technology leaders are dealing with huge change, and talented team members being recruited away from firms is a never-ending challenge.

Key Points:

- Having a strong organization design can be as important as having a succession plan. You need to know what capabilities are required to support the business.
- Executive leadership tends to see next highest-ranking IT leader/member as the heir-apparent, which may be "worse" than it is across other executive levels because the skillset/mindset can be so different.
- Talent is difficult to find, so management needs to develop leaders from within.
- Technology leaders are now dealing with a different generational challenge: the younger workforce doesn't presume they will be working for any company for 10 years.

Information Security

October is Cybersecurity Awareness Month. As we are seeing more and more breaches in the news, the group discussed multi-factor authentication, single sign-on, device management policies and end point security among other items.

Key Points:

- NIST is now recommending to not have a password change policy.
- Having a breach response plan is important to an incident response plan.
- Segmented networks are complex and require a lot of design and expertise. Segmentation is no longer about credentials and firewalls.
- Hardware like laptops are becoming a thing of the past with the popularity of virtual desktop infrastructures available today.

Open Systems

The group discussed the apparent lack of open systems to solve agency needs. Agencies are largely left to solve these deficiencies on their own and in their own way. It's "Stockholm Syndrome" with millions of dollars at play.

Key Points:

- Retail businesses ultimately have a choice between two AMS vendors. Neither vendor is modern enough to upset the other in differentiation or innovation.
- Today it can take five to six applications to deliver a solution for a service manager. These applications make up for the deficiencies of these closed AMS platforms.
- "Very available" is what is expected by customers and clients. For example, ordering from McDonald’s via its mobile app because the drive-thru experience is too slow. The upcoming generation will not have the tolerance for how cumbersome we deliver.

SEE YOU IN NOVEMBER!

The next CIO Working Group meeting is Feb 10-12, 2020. The group will meet at the Legislative & Working Group Summit in Washington, D.C. Registration will be open soon