Run(a)way Success

King Khaled International Airport (KKIA) leads the way with its cyber risk strategy

Run(a)way success

Riyadh Aiports Company (RAC) in partnership with Deloitte Touche Tohmatsu Services, Inc.

The aviation industry faces a wide range of challenges in the coming decades, with the need for new infrastructure to manage the capacity and services required for the forecast double-digit growth, but also the need to manage the cybersecurity risk amid the ongoing digital transformation.

As part of the privatization program of the aviation sector in Saudi Arabia, which forms part of the Kingdom's Vision 2030, "Riyadh Airports Company (RAC)" was created and is now managing and operating King Khaled International Airport (KKIA) in the Saudi capital. In its role, RAC is embarking on upgrading KKIA's infrastructure and expanding facilities with new services, and is thus playing a major role in the modern transformation of the Kingdom.

While aligning with Vision 2030, RAC must meet the various challenges of protecting the airport from cyber risks arising from the ongoing digital transformation of the airports industry and by the emerging IT/ OT technologies that have been recently implemented by RAC's various business functions.

Thus, Mohammad Al-Qahtani, Director of Cybersecurity – RAC saw the need for a comprehensive and well-integrated cybersecurity strategy that aligns with the airport's business and enables the business functions to operate securely and safely, with a three-year plan to improve the security of the airport's digital services while positively contributing to the passenger experience. Mohammad Al- Qahtani also identified internal challenges faced by the Cybersecurity department, which increased the complexity of the overall risk situation within RAC, namely:

1. **Culture**, where Cybersecurity culture within the Airport is not well-considered or not seriously taken in the overall business as usual activities.
2. **Enforcement**, where the absence of

While aligning with Vision 2030, RAC must meet the various challenges of protecting the airport from cyber risks arising from the ongoing digital transformation of the airports industry and by the emerging IT/OT technologies that have been recently implemented by RAC's various business functions.

Mohammad Al-Qahtani, Director of Cybersecurity – RAC saw the need for a comprehensive and well-integrated cybersecurity strategy that aligns with the airport's business and enables the business functions to operate securely and safely

Cybersecurity policies, processes, and procedures is evident as there was no awareness made for the implemented Cybersecurity controls within the Airport.

3. **Effectiveness**, where Cybersecurity is portrayed as a complementary function within IT, and not a partner to the Airport business.

4. **Skillsets scarcity** in the market for Cybersecurity resources in general and within the airports industry specifically is another key challenge. The lack of Cybersecurity knowledge within the airports industry adds another complexity for RAC in terms of how to train and retain those resources once they are hired.

5. **Lengthy Business induction** cycles are required. As soon as the Cybersecurity resources are onboarded, they should undergo an extensive on job rotational training across the various airport functions to build the missing contextual knowledge that they should have if they were to come from the same industry.

6. **Cultural DNA** of RAC is not mature from a Cyber perspective. A significant amount of time and awareness is to be invested to include not only RAC direct employees but also the entire ecosystem of partners of the airport including the individual subcontractors who are all serving the business but coming from different Cybersecurity backgrounds.

7. **Business Silos** exists within the Airport, where some business functions have their own Cyber environment (in the form of Cloud setup) without the full control or visibility form the Cybersecurity function within the Airport.

Based on these challenges, RAC identified the need to build a new structure and control for Cybersecurity through a comprehensive and well-integrated Cybersecurity Strategy that aligns with the Airport's business and enables the business functions to operate securely and safely, with a three-year forward-looking plan to improve the security of the Airport digital services while positively contributing to the passenger experience throughout this major digital transformation.

RAC also affirmed the need to engage a capable consulting partner to support it in building a robust cybersecurity strategy program and protect the airport from imminent threats while assisting the RAC Cybersecurity team in implementing the advanced security controls that will secure and deliver new capabilities and services across the airport functions. Following a formal procurement process, Deloitte, a partner with a strong local and global presence, and with expertise in both airports and cybersecurity, was selected by RAC as its consulting partner to build a cybersecurity strategy with all its supporting elements.

Working hand in hand with Deloitte, RAC launched a cybersecurity transformation program that embraces a "Cyber Everywhere" philosophy. This seeks to create an internal capability that sufficiently mitigates risk but at the same time becomes an enabler of next-generation airport operations.

Embracing this practice through the strategy enabled RAC to develop a comprehensive cybersecurity knowledge and awareness program that will nurture the culture within RAC to step beyond the tactical and technical concerned teams and gain credibility and support from leaders across the organization. Inherent to this new operative is the imperative to move beyond the role of compliance monitors and enforcers to better integrate with the business, manage information risks more strategically and work toward a culture of shared cyber-risk ownership across the organization.

Through such a partnership, RAC and Deloitte have demonstrated the benefits of collaboration in managing current and potential cyber risks while strengthening the organization for the future on its digital transformation journey. In so doing, RAC has played a pioneering role in managing aviation cybersecurity risk in the Kingdom and provided a success story that can inspire others to follow.

Based on these challenges, RAC identified the need to build a new structure and control for Cybersecurity through a comprehensive and well-integrated Cybersecurity Strategy that aligns with the Airport's business and enables the business functions to operate securely and safely

Deloitte.