CASE STUDY:

GULF INTERNATIONAL BANK

Gulf International Bank B.S.C. (GIB) was established in 1975 and commenced operations in 1976.

GIB aims to be the preferred financial services partner, delivering banking solutions to a wide customer base in the region and beyond. This includes corporate banking, digital retail banking, and investment banking through its fully owned subsidiary GIB Capital.

In addition to its main subsidiaries, London-based GIB (UK) Ltd., and Riyadh-based GIB Capital, GIB has branches in London, New York, Abu Dhabi, Dhahran, Riyadh and Jeddah with a representative office in Dubai.

CHALLENGES

GIB was researching multifactor authentication solutions to meet compliance requirements for two factor authentication. The guidelines were put in place by New York State Department of Financial Services Cybersecurity Law: Section 500.12 Multi-Factor Authentication Compliance Effective Date: March 1, 2018.

"This regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers."

HOW PRODUCT HELPED

BIO-key introduced the organization's banks located in New York, and in need of a two-factor compliance solution, to ID Director for Windows. ID Director adds a layer of secure, yet convenient biometric authentication, to the organizations Active Directory environment. Paired with PIV-PRO ,a FIPS-C compliant fingerprint scanner, users enroll their fingerprints, which are associated with their credentials in Active Directory. Once enrolled users have the option of biometric sign-in or the ability to sign-in using the incumbent solution.

In this particular use case, the banks employees withll use BIO-key's ID Director as a second form of authentication for accessing records and conducting transactions.

RESULTS, RETURN ON INVESTMENT AND FUTURE PLANS

The implementation at the New York location was deemed a success by branch management. The next step is to create a roadmap for further deployment throughout the organization. The long-term objective is to enhance security, protect access to shared work stations, and improve workflow through one-touch biometric authentication.