Multinational investment bank

Implementing cyber recovery for operational resilience

A British multinational investment bank and financial services company headquartered in London wanted to avoid the fate of many prominent financial organizations that had fallen prey to cybercriminals in recent years. The bank decided to augment its operational resilience by co-creating a novel cyber recovery solution with Kyndryl and Amazon Web Services (AWS).

Business challenge

To improve its operational resilience, the bank needed to strengthen its ability to rapidly respond to and recover from cyber incidents and minimize disruptions. Though the bank hadn't experienced a major attack yet, the prevalence and frequency of attacks on its peers over the last few years made senior executives at the bank reassess the way they approached resiliency and recovery.

Transformation

The bank, Kyndryl, and AWS co-created a solution to enable automated cyber recovery capabilities that allowed the bank to isolate and protect critical data, automate compliance reporting, and rapidly recover from breaches or attacks.

Results

- Provides the ability to recover from a cyberattack in hours instead of days
- Delivers 24X7 forensics checking, alerting, and quarantine
- Minimizes human intervention and enables automated regulatory compliance reporting
- Significantly minimizes attack vectors and defines recovery timelines

"Kyndryl's openness to flexible delivery and commercials and to doing what was needed to deal with issues and new demands as they came up, was hugely important to us. It was a huge part of the success of the initial operating capability and deployment."

– Global CSO Strategic Programmes Director, Multinational British bank

Dramatically increasing operational resilience

Financial services organizations are 300 times more likely to experience an attack or a breach than other kinds of organizations. These breaches and attacks are a significant financial burden on the organizations.

The average cost of a mega breach in 2021 was as high as $401 million for breaches involving 50-65 million records. In fact, financial services companies have more difficulty retaining customers following a data breach than many other types of companies. The global average customer turnover rate following a security breach is 3.9%; the financial services industry average is 5.9%[1].

The British multinational bank was acutely aware of this reality. With a focus in the UK and the North American markets, the bank offers a variety of core financial services, including personal, corporate and investment banking, credit cards, and wealth management to more than 48 million customers worldwide. It understood the critical importance of protecting itself against sophisticated and destructive security threats that are increasingly common in the digital era.

Its reputation, customer base and even profitability were at stake. “With the bank processing around one-third of all payments in the UK, it also had to consider the impact any attack and the consequent service disruption would have on the broader economy,” says the Global CSO Strategic Programmes Director at the bank.

There was a growing realization among the decision makers that the threats were not going away and that they would become more challenging and difficult to prevent over time. The key, they realized, was to pivot from prevention and to focus on resilience, so that even if the worst happened the bank would to be able to recover quickly.

Solution

To dramatically improve its operational resilience, the bank first needed to integrate across many layers of the organization, including crisis management, communications management, regulatory reporting, disaster recovery, and security. Second, it needed a powerful resiliency and recovery solution that met its needs. The responsibility of transforming the bank’s cyber recovery approach and designing a solution to further improve its operational resilience fell mainly on the Chief Security Officer director.

A novel take on augmenting operational resilience

The CSO director's goal was to prepare the bank to respond to and recover from even the most devastating cyber and data corruption events. To that end, a cyber vault and resiliency orchestration solution was co-created with Kyndryl and AWS.

The solution, which combines AWS-based data vaults and Kyndryl Resiliency Orchestration capabilities, enables the bank to automate cyber recovery, secure storage and re-establish the IT infrastructure, applications and data sources that underpin the bank's key business services. This means that the solution puts critical data completely beyond the reach of threat actors active today. The solution also needed to provide data access as necessary, in an organized way, at pace, and with confidence.

Kyndryl, leveraging Resiliency Orchestration, delivered an enterprise-wide management capability for platform, configuration, and application data protection. This allows the bank to track the current status of its cyber recovery capability and provide alerts as necessary. Additionally, Kyndryl enabled the bank's operational resilience team to have a real-time view of readiness to recover key business services from known, clean, securely vaulted copies of data objects.

Kyndryl also provided a third site for cyber recovery, cyber incident recovery for data to help recover files and databases, and air-gapped, immutable copies of data to support data restore. Partnering with AWS, Kyndryl also helped accelerate the bank's drive to leverage cloud—multicloud in particular. Kyndryl's ability and willingness to work with the bank's preferred storage provider and build a hybrid resiliency orchestration solution was key in realizing the bank's strategy.

From days to hours: Improved operational resilience in action

By deploying this co-created solution, the bank has significantly increased its operational resilience. The solution allows the bank to simulate cyberattacks and initiate recovery. The results from many simulations show that the bank now has the ability to recover in hours instead of days.

A large part of that success can be credited to the recovery automation enabled by Kyndryl Resiliency Orchestration Management Suite, which ensures that predictable recovery outcomes are delivered within clearly defined recovery time objectives. The suite also helps minimize human intervention and disaster recovery testing overhead, while enabling automated regulatory compliance reporting.

Another benefit the bank has gained is the ability to significantly minimize attack vectors. This is achieved through the adoption of strict architectural principles, including ensuring there is no direct connectivity to the vaults and using immutable storage and deployment of hundreds of vaults with separate encryption to reduce the blast radius of any potential breach.

In addition, the bank has seen its existing comprehensive recovery procedures enhanced to better accommodate more cyber and data corruption scenarios. This is enabled by the detailed recovery testing driven by Kyndryl Resiliency Orchestration across all of its key business services.

Take the next step

To learn more about the Kyndryl solutions featured in this story, please contact your Kyndryl representative or Kyndryl Business Partner, or visit Kyndryl Cyber Recovery as a Service, or Kyndryl Cloud Resiliency Orchestration. Or visit Kyndryl.com

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.

The performance data and client examples cited are presented for illustrative purposes only.
Actual performance results may vary depending on specific configurations and operating conditions.

[1] IBM Security, Cost of a Data Breach Report, *2019 https://www.ibm.com/downloads/cas/RDEQK07R*