Data#3 Customer Story

Reserve Bank of Fiji

Reserve Bank of Fiji invests in security solution for the future

Data#3

Benefits

- Heightened security skill level and awareness
- Reduced risk
- Enhanced reputation as a leader in the region
- The assurance of 24/7/365 monitoring
- Enable IT security staff to focus on other key security priorities
- Single platform using world-leading cyber managed security service provider
- Contextually based alerts without the noise
- Increased visibility of threats
- 24/7/365 incident response capability
- IT team is mentored by experts

Objective

The Reserve Bank of Fiji wanted to improve its security posture for better protection against increasingly sophisticated cyber security threats.

Approach

The bank issued a selective tender, inviting a shortlist of IT partners with high-level security capabilities, to submit a proposal. Data#3 and SecurityHQ were selected thanks to a high-quality proposal that was globally backed, along with Fiji-based expertise and support.

Solutions & Services

☑ Managed SOC

☑ Professional Services

Highlight

“We now have assurance that someone who is equipped with the right technical skills looking at things we may miss, enabling our bank to achieve increased visibility, global threat intelligence, and an improved cyber security posture.”

Ariff Ali,
Governor for Reserve Bank of Fiji.

Data#3 Customer Story

Reserve Bank of Fiji

> **“We knew there were SOC services available, and it made sense to change our approach to something managed for the extra support.”**
>
> **Rajnesh Chand,**
> **Manager Cybersecurity & Innovation,**
> **Reserve Bank of Fiji.**

The Background

As the central bank of the Republic of Fiji, the Reserve Bank of Fiji’s (RBF) functions include issuing currency and promoting monetary and financial stability in the economy, while providing policy advice and financial services to the government.

While the growing threat to the landscape has become increasingly challenging worldwide, several high-profile security incidents has highlighted the increased focus by cyber criminals within the Pacific region. For the RBF, limited visibility and a lack of specialised resources has made implanting effective security measures a challenge.

The Challenge

The RBF relies on a small, busy IT team to provide the tools that it needs to function. As the critical area of security has become more complex, specialist skills not available in-house were needed 24/7. For Manager Cybersecurity & Innovation, Rajnesh Chand, introducing a security operations centre (SOC) was a logical step.

“We knew we wanted to have a SOC solution in place, we knew how important it was. We had a vision, and initially we took it on in-house and put a solution together, and tried to get a sense of what having a SOC means. From this experience, we realised that it takes much more than a few security personnel to manage a SOC, given other priority security areas.”

External factors necessitated the need to raise the bar of expectations. The onset of the global pandemic increased the number of employees working remotely, which saw an increase in cyber security incidents in the region.

“There were other things that COVID-19 brought, especially security concerns, and we started to see breaches closer to home. These factors made us look outward for help, and we wanted to make it a less painful, more enriching experience,” recounted Chand.

“We knew there were SOC services available, and it made sense to change our approach to consider something managed for the extra support. With service organisations, they have the set-up, and the experience of implementing security solutions for longer than we had, so we knew we could reap the benefits of that experience.”

With the global skilled labour shortage, especially in experienced security specialists, implementing the right SOC choice would create opportunity for RBF’s IT team to develop its knowledge through a transfer of skills.

The current solution in place did not give the RBF the visibility and confidence about focusing attention where it was most needed, and with their analysis process still largely manual, more was needed if the RBF was to narrow down to the right datasets.

The Solution

Data#3 proposed a solution in partnership with global managed security service provider, SecurityHQ, that featured 24/7 SOC support and availability, with built in incident response. Service and management of the solution were included, which featured a Data#3 Customer Experience Manager, in conjunction with the Fiji-based Data#3 team. Chand said that this combination of local service and global expertise gave him assurance that the RBF was in safe hands.

> **“Data#3 really made us understand what the solution entails, how we could consume that service, and what we could expect.”**
>
> **Rajnesh Chand,**
> **Manager Cybersecurity & Innovation,**
> **Reserve Bank of Fiji.**

“First, we knew they had the capability. We knew the partnerships that Data#3 has, because we had already been long-term customers for our Microsoft licensing. We had been to some of their JuiceIT events, so we had exposure to their experts, and they have a local presence in Fiji as well, so there is knowledgeable support we can reach out to locally” explained Chand.

During the tender phase, Data#3 and SecurityHQ presented their proposal in detail, taking time to gather information at every stage, and this attention to detail helped to prepare for the SOC implementation.

“They really made us understand what the solution entails, how we could consume that service, and what we could expect. They showed us how they would set up the SOC, and what it would look like in reality, and that really stood out to us,” described Chand.

The combination of advance information gathering, and the work that the RBF had already done in their initial venture into trialling a SOC, helped ensure an easy onboarding process. Detailed instructions were provided on how to onboard, along with a knowledge log of how everything works.

“I think the first ten days we went through a learning phase, trying to understand what we should classify as a major alert. It was a good experience and gave us instant transparency in terms of things we may not have otherwise viewed as a threat. We introduced more rules to reduce false positives, and now we have a SOC that gives us visibility across all layers of security,” stated Chand.

During this period, the RBF team was able to experience first-hand what it was like to have a global team of security specialists monitoring their environment round the clock.

“Any analyst working on our system knows what to do with alerts and how to classify it according to our own business. Personally, it feels like having a light switch from zero to hero overnight,” said Chand.

As a part of the solution, the RBF conducts weekly meetings with Data#3 and SecurityHQ. These are attended by RBF’s IT team as well as the bank’s executive risk management team, and other business leaders where needed. This reflects the commitment by the leadership of the RBF to better understand and manage cyber risk.

Aside from the meetings, weekly and monthly reports that show incidents are generated and submitted to the team. The risk team also receives notifications of incidents. The managed SOC solution frees up time for the team to focus on other operational priorities, knowing that someone is constantly monitoring security.

“Having the managed SOC in place allowed the IT team to prioritise its focus on other areas, necessitated by the level of our security posture. Without the SOC in place, our IT team would need to work outside of business hours, always ensuring the phone is close by to make sure no warnings or suspicious activity were missed. Now, getting a call means it is a big issue, while anything else can wait for office hours. That has made it easier to sleep at night.”

"The people there make a real difference – they have experience and expertise in technology across a wide client base, and are familiar with most of our challenges."

Rajnesh Chand,
Manager Cybersecurity & Innovation,
Reserve Bank of Fiji.

Conclusion

The RBF has a mandate to supervise licensed financial institutions, and provide guidance on key issues including cyber security.

Governor for RBF, Ariff Ali, commended the team on achieving the compliance expected and reiterated the assurance afforded to the RBF team, now that they have the extra support from Data#3 and SecurityHQ.

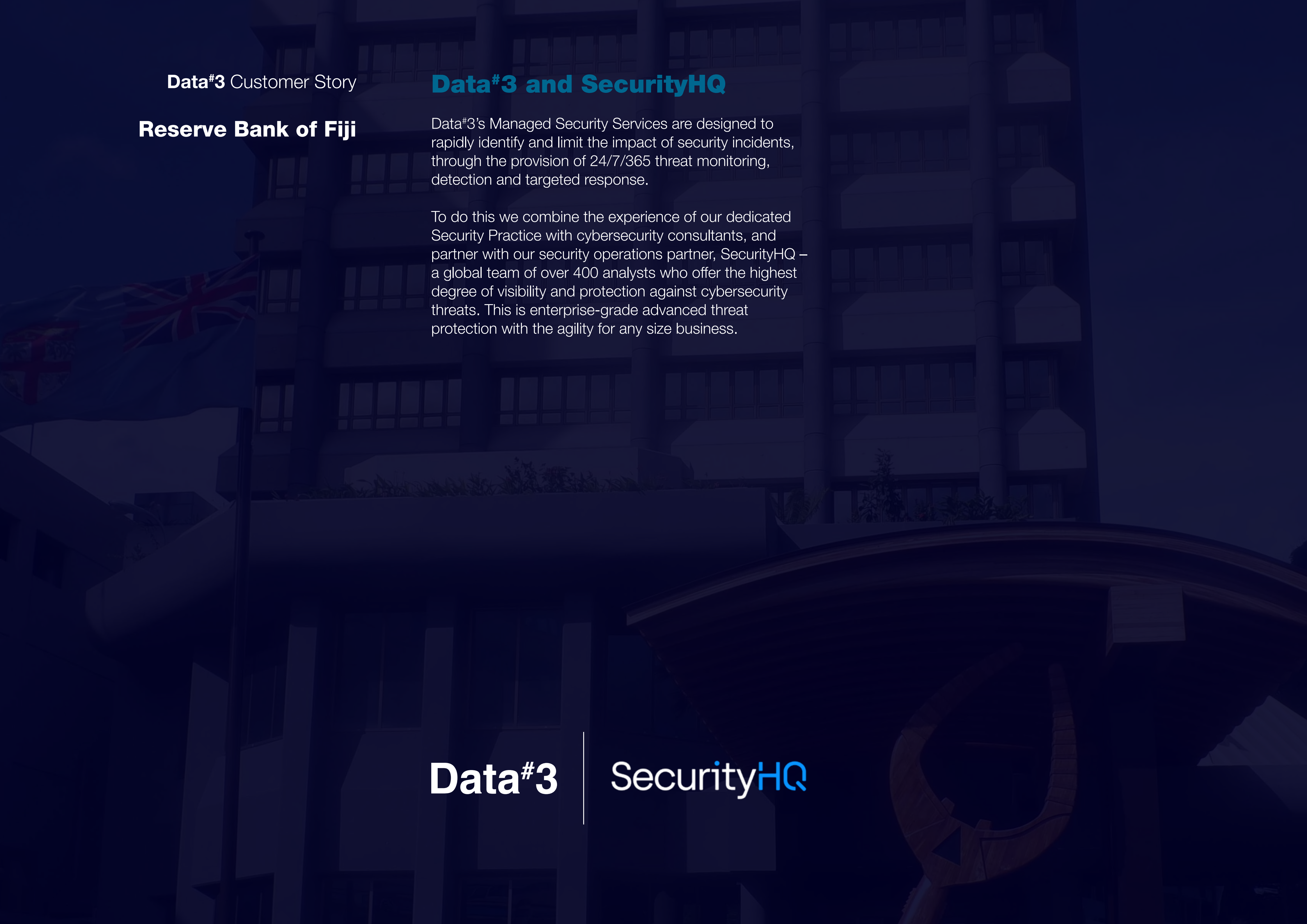
"The security measures and controls the Reserve Bank has put in place have improved our posture and given us visibility and insight into any security concerns in real-time. This comfort allows the IT team to provide that advice previously absent with in-house support," highlighted Susan Kumar, Chief Manager Currency and Corporate Services, Reserve Bank of Fiji.

"Because Data#3 has a local presence, we are able to have easy access to their services, while SecurityHQ offers us expertise in security. In addition, having a local relationship with Data#3 has provided great comfort to the RBF given its usual conservative stance with outsourcing," said Kumar.

"The people there make a real difference – they have experience and expertise in technology across a wide client base, and are familiar with most of our challenges," added Chand.

"When looking back at the progress already achieved, seeking specialist external skills through the managed SOC was a "no brainer", as the reach of the service went far beyond anything that could have been reasonably achieved with the small internal team."

In his reflection, Chand says, *"coming across another Data#3 customer case study a few years back, I wondered whether we would ever have such a use case that we could publish and feel proud of as an institution. Now, we are in a good place, and we are proud of what we have achieved it."*



Data#3 Customer Story

Reserve Bank of Fiji

Data#3 and SecurityHQ

Data#3's Managed Security Services are designed to rapidly identify and limit the impact of security incidents, through the provision of 24/7/365 threat monitoring, detection and targeted response.

To do this we combine the experience of our dedicated Security Practice with cybersecurity consultants, and partner with our security operations partner, SecurityHQ – a global team of over 400 analysts who offer the highest degree of visibility and protection against cybersecurity threats. This is enterprise-grade advanced threat protection with the agility for any size business.