TITANIA
Assured Accuracy

Case Study

Financial Services International Bank Case Study

Background

This bank was founded in 2004 and from its headquarters, manages seven full-service branches in its country's largest cities, handling 23% of all domestic customer deposits. Operating on a national and international scale, the multi-award-winning bank is the preferred partner of multilateral lenders, development agencies, charitable institutions and numerous government entities.

Continually looking at how it can improve its technology infrastructure to support its day-to-day operations, in 2017 the bank decided to undertake a review of its systems and processes. At this point, Mr Adefemi Onanuga, was brought on board by the bank as its joint CIO and CISO.

Challenge

When Mr Onanuga joined, he took on responsibility for running all aspects of the organisation's IT, from payments and compliance to legal, human resources and contracts. Business Continuity was another key focus, given the need to be able to keep operating in a region where natural disasters and civil disturbance are not uncommon. His remit also included cyber security, drawing on his experience at previous financial institutions.

Starting with a gap analysis of the IT systems and processes already in place, he was able to quickly identify the areas where improvement was necessary. Reviewing the banks' structure, service desk and business continuity, he also assessed its approach to cyber security.

To date, the bank had conducted vulnerability assessments from time to time, using outside consultants, but didn't have a dedicated SOC (Security Operations Center) in place to monitor, analyze and improve the bank's cyber security. Benchmarks had not been set and there wasn't a uniform process for how to react to an alert or cyber incident.

People on the ground from across the bank were committed to their work but lacked the skills and knowledge when it came to cyber security and the part everyone across the whole organization needed to play.

"Nipper is definitely the best...why waste your time using anything else!"

Financial Services International Bank Case Study

Solution

Infrastructure first

Before Mr Onanuga turned his attention to a solution for the bank's cyber security requirements, his priority was to ensure that the right infrastructure was in place to support any investment. "My first priority following the gap analysis of the bank's IT set up was to make sure the infrastructure and equipment was audited, updated or replaced where necessary. This was essential before investing in any new systems –applications are like cars, if the road on which they are running isn't smooth and strong it won't work, you can't run the bank," said Mr Onanuga.

Cybersecurity

The desire was to move away from intermittent Pentesting and to build a robust cyber security programme for the bank. As Mr Onanuga explained: "Pentesters only have a limited amount of knowledge of your organization, not the unique faults that could occur, they don't know the wider architecture like I do with more of a helicopter role. That said, banks are not SOC experts and it makes complete sense to me to work with an outside organization that is." With previous experience of Titania's Nipper Cybersecurity solution, it was Mr Onanuga's first choice when reviewing outside software providers to audit the bank's firewalls, switches and routers for its 50+ Cisco devices. "I've used various different cyber security software solutions in previous roles and Nipper is definitely the best. It's easy to use, reports are generated within seconds and the user reports are easily understandable for the teams who need to fix the problem. I am always recommending it to other organizations for network assessments – why waste your time using anything else!"

"The immediate impact of Nipper was the instant visibility across networks..."

Results

Technical

Before getting Titania onboard, cyber vulnerabilities on network devices were scoring as high as 90 (out of 100) on its existing scale of measurement but since installing Nipper, there are no high risks. Medium risks have been identified and a decision made on which are priority. In addition, the bank is using Nipper to ensure that SWIFT wire payments are up to date and configured, routing is correct and structured in accordance with guidelines. Visibility across all networks, domains and sub domains has hugely improved, instant assessments are now possible and the ease and accuracy of reporting means remediation for administrators is simple.

"The immediate impact of Nipper was the instant visibility across networks, the automated identification of risks and the ease by which we could categorise them to focus our resource on dealing with the biggest priorities. The reports generated on a monthly and quarterly basis are easy for my team to understand, making remedial action straightforward. I've rarely needed support when using the software but when I have contacted the Titania team, the advice is always straightforward and easy to understand", said Mr Onanuga.

Financial Services International Bank Case Study

Compliance

The bank is also using Nipper to monitor and maintain compliance, due to its built-in ability to automatically check networks against industry standards. Key for financial institutions dealing with multiple transactions, Mr Onanuga is able to use Nipper to ensure the bank is compliant with the PCI (Payment Card Industry) standards and be automatically notified of any key updates or changes to it. The bank is also benchmarking against NIS, CIS and the ISO9001, to ensure its new cyber security programme and wider approach to IT and quality systems is as robust as possible.

People

Mr Onanuga understood from day one that the success of the transformation of infrastructure and processes at the bank would only be fully realized if people across the organization bought into the changes. With this in mind, developing the skills of employees – those directly involved with IT and cyber security and the wider team – was a priority for Mr Onanuga. Enthusiasm was certainly present but a dedicated programme of education and awareness building was put in place to harness this and embed new behaviours, especially when it came to the reporting of cyber risk incidents and following the correct procedure for remediation. This was from the ground floor up including managers who were key to building a culture based on minimizing risk and leading by example when it came to modelling new behaviours.

The cyber security team were also helped to develop their skills so they could get the most out of the bank's investment in Nipper. They were supported in building their knowledge of risk assessments, risk ratings and remediation.

Future

With robust IT infrastructure and cyber security systems now in place, Mr Onanuga's vision is to keep improving on the standards, practices and new behaviours the bank has embraced. True to his promise, the organization is currently working towards becoming the first bank in the region to be ISO9001 level 5 compliant, measuring against 114 controls to achieve this. They have also enrolled in SWIFT's Customer Security Programme, in which members pledge to secure and protect their own environment, manage relationships with counterparts and to share information about potential threats with other members for mutual benefit.

"The future is promising, we've already managed to operate for many weeks without disruption during Covid-19, which is testament to the systems and behaviours we now have at the core of our business. We want to make continuous improvement a part of our culture and the more aware employees become of the importance of cyber security the more they understand why it's so important to us and our customers," said Mr Onanuga. Following his positive experience with Titania, Mr Onanuga is considering outsourcing other elements of the bank's IT requirements in the future. The move to the cloud will also have an impact on this and when it comes to cyber security, upskilling in cloud assessments will be a part of this. Making sure the cyber security team understand security requirements and how to identify problems in a cloud environment.

"Ultimately, all of the improvements we've made around IT infrastructure, cyber security and our knowledge and culture of them across the bank, are with the customer in mind. Customer confidence in what we do is extremely important, knowing that we operate to stringent industry standards and take information security seriously means that we will remain first choice for them, now and in the future," Mr Onanuga concluded.