CASE STUDY

CYBER SECURITY & RISK ASSESSMENT

TOPMOST BANK IN CENTRAL ASIA

Infopercept

SECURE • OPTIMIZE • STRENGTHEN

Overview

We have worked to minimize the vulnerabilities of a leading bank in Central Asia serving a large customer base. The Bank already had expensive solutions and security network infrastructure in place. The bank had an intermediate security framework already in place to ward of potential cyber-attacks. But needed a to spin up a more proactive & robust Security Network.

Problem

The bank had invested exponentially in the Cyber Security infrastructure & were regularly running SOC & had established Security Plans in place. They also had an INFOSEC team to assess & monitor the overall security framework health. The bank's security was already vetted by top industry names for years. But were still not able to achieve the outcome in terms of the security with regards to the overall investment incurred.

We were selected from among the various third-party Security Assessment & Service vendors by the Bank. As we conformed to all of the Vendor criteria as mentioned by the bank. Like

The bank had invested exponentially in the Cyber Security infrastructure & were regularly running SOC & had established Security Plans in place. They also had an INFOSEC team to assess & monitor the overall security framework health. The bank's security was already vetted by top industry names for years. But were still not able to achieve the outcome in terms of the security with regards to the overall investment incurred.

We were selected from among the various third-party Security Assessment & Service vendors by the Bank. As we conformed to all of the Vendor criteria as mentioned by the bank. Like

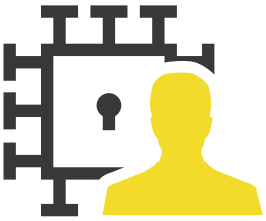
- A partner & someone already trusted and proven in the industry.
- Solid tech knowledge coupled with great service as this was going to be a marathon & not a sprint
- Using innovative technology, that is reliable & constantly evolving so as to not slow down the process if chasing false positives.
- A one stop shop for vulnerability management, penetration testing in identifying risks.
- Value based service & an advisory partnership, so they can have the guidance while constructing the security network.

Solution

The bank had invested exponentially in the Cyber Security infrastructure & were regularly running SOC & had established Security Plans in place. They also had an INFOSEC team to assess & monitor the overall security framework health. The bank's security was already vetted by top industry names for years. But were still not able to achieve the outcome in terms of the security with regards to the overall investment incurred.

We were selected from among the various third-party Security Assessment & Service vendors by the Bank. As we conformed to all of the Vendor criteria as mentioned by the bank. Like

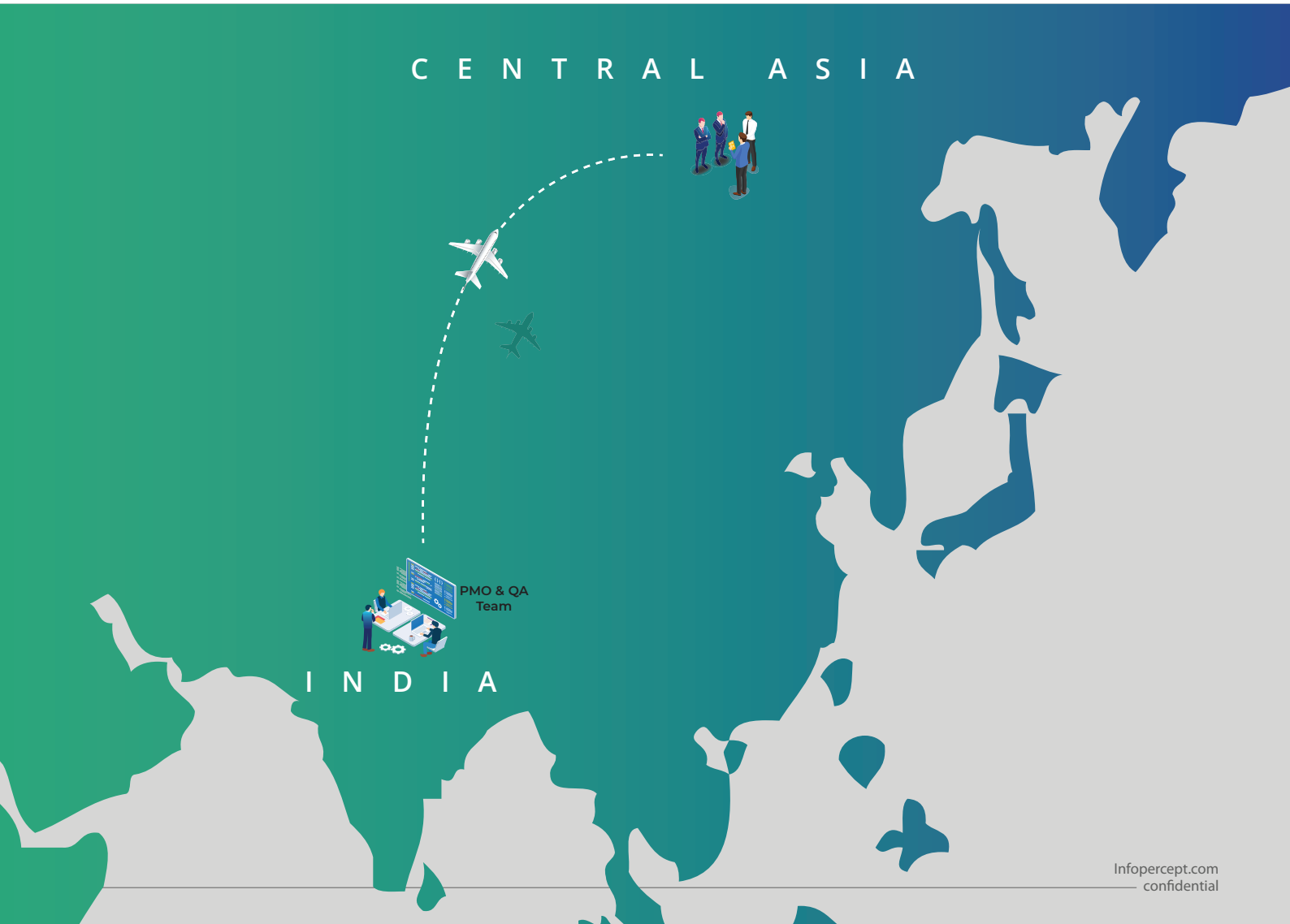
Tester & Researcher



Application Security Expert

Risk Assessment Expert

This team was subjected to Remote Governance & quality Review from our main office.



Once reaching the Bank's location in Central Asia, our team initiated our patented 7 step process for security assessment & optimization along with our core philosophy of Understanding, Experience & Expertise. These 7 steps include:

Goals & Scope

Information Gathering

Information Analysis & Planning

Vulnerability Detection

Attack & Penetration/ Privilege Escalation

Result Analysis & Reporting

Clean Up

After a thorough assessment of the Bank's security Network we were able to ascertain that although the core banking was protected by a strong security framework. It was internally integrated with other banking applications and networks. Which were less safe and more prone to be compromised.

To prove the criticality of this security lapse we were able to show the Bank's management how a hacker or cybercriminal may use the undefended zones to breach and infiltrate the core banking and can inflict massive damage in terms of Money, Reputation and Classified Information loss/ theft.

After recognizing the weak zones of the existing network, we subsequently patched them up by Hardening, Optimizing & performing the right integration using the Existing Security Solution available to the bank.

Following our security optimization procedure and patching the vulnerabilities. Bank was able to more safely utilize its Core banking, including Net Banking, mobile banking as well as its internal transaction payment apps.

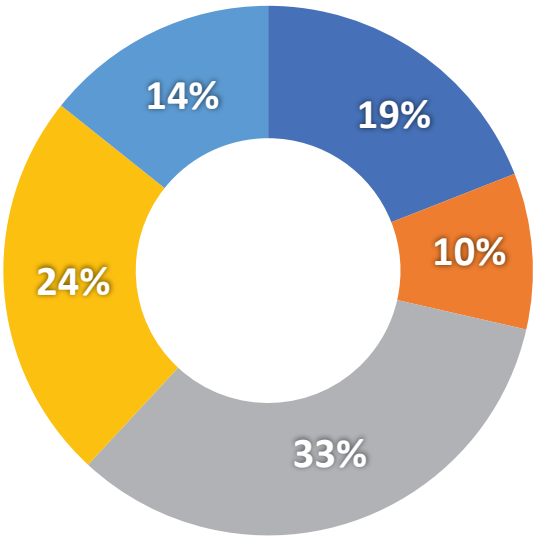
Helped the Bank to realize that safeguarding a particular Business-Critical zone without proper Network segmentation and the suitable integration won't be able to guarantee overall Network Security & Integrity.

We also shared and imparted our unique approach of SOS (Security Optimization Strengthen) for Cyber Security SOS.

As we believe in the adage of Prevention is better than cure. We want the organizations to be self-motivated & take proactive steps to better strengthen and optimize their Security framework periodically so as to mitigate the occurrence of cyberattack & threats in the business-critical zones.

For Businesses to continue their Operations uninhibited we recommend implementing Cybersecurity SOS for an Emergency SOS situation.

Statistics of Assessment



- Mobile Banking app Security Issues
- External Web Application Vulnerabilities
- Internal Network and ATM Machine
- Risk Assessment
- Social Engineering Attack

Major Critical Observations

- Credit card data dumped by exploiting mobile application
- Clear text bank transaction captured using main in the middle attack
- Server Exploitation with Zero day exploitation
- Confidential Information gathered using Phishing attack

About **Infopercept**

Infopercept's Vision and core values revolve around making organization more aware and secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decision about their Security Practices & goals. With our synergistic vision to combine, technical expertise and professional experience we aim to further establish our place as a one stop shop for our clients and partners' Cybersecurity and accreditation needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & continuous knowledge in the Cybersecurity domain, latest trends and Security innovations, ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

Infopercept

SECURE • OPTIMIZE • STRENGTHEN

Corporate Office:
Infopercept Consulting Pvt. Ltd.
H-1209, Titanium City Center, Satellite, Ahmedabad-380015.
India.

www.infopercept.com | Follow us on -