CASE STUDY

CYBER SECURITY CASE STUDY OF A LARGE BANK IN MONGOLIA
Introduction

One of the leading banks of Mongolia comprising 500+ branches and approximately 2 million customers, treats its employees, customers, and shareholders with utmost dedication and sincerity. A mutually beneficial collaboration is one of its core values. A highly ethical organization committed to excellent customer service; it is known for its integrity and professionalism.

Considering the fact that banking operations are largely computerised with data and sensitive information of the customers being stored on the cyber network, it is paramount to tighten the security of its infrastructure and network to secure data & maintain confidentiality of customers.
The Problem

The bank had a security network infrastructure in place that acted as a first tier security set up but they were on the lookout for more sturdy and robust security solutions that would encompass the entire network and leave no scope for loopholes.

With the constantly evolving nature of technology both in terms of hacking data (malware) and development of cyber ware, it was imperative to keep pace and ameliorate the level of security to avoid cyber-attacks. Although the bank was conducting internal testing at regular intervals, taking a proactive approach they decided to get an external testing done to validate its current state of security affairs. The bank was on the lookout for a cyber-security solutions provider who would provide a number of vital service options. They were looking for practical testing and especially wanted somebody with sufficient experience in the banking sector.

They floated a proposal to companies across the globe in the lookout for the ideal cyber security solutions provider. Some of the other factors the bank was keen on were certifications, experiences, customization, approach, technology, solutions, scalability, reputation, and customer satisfaction.

Infopercept engaged - as an experienced MSSP

Infopercept fitted the bill perfectly and was selected among many top globally reputed contenders including some of the ‘Big 4’ companies too. Infopercept in its presentation had showcased its strength in the banking sector with advanced capabilities of managing and securing extremely sensitive information.

One of the members of the selection committee later commented “We had received many applications for this, however, we were impressed with the focus of Infopercept in the domain of Cybersecurity and their detailed presentation with multiple references to their experiences in the banking sector.”

Once the partnership was formalized, Infopercept swung into action without further ado.

A team of top officials of Infopercept, comprising the Director of the Red Team, a senior level Specialist of Application Security, and the Director of Compliance were sent from India. They carried out a detailed risk assessment. It involved identifying relevant threats, internal as well as external vulnerabilities, impact of those vulnerabilities and possibilities of its exploitation.

In order to ascertain the current security posture of the bank, Infopercept decided to do the risk assessment in two phases.
Phase 1

Testing: As part of the Phase 1 of the risk assessment, Penetration Testing (PT) and Man In The Middle Attack (MITM) methods were employed to carry out internal testing. Simulated cyber-attacks such as these helped expose the vulnerabilities in the system. The authorized hacking attempts using wireless technologies revealed the weak access points and security protocols.

Simultaneously, external Penetration Testing by the Red Team from Infopercept was also conducted. This was a critical area as the perimeter systems connected to the internet are usually exposed and hence more susceptible to malicious attacks. A clear Open Source Intelligence (OSINT) strategy helped mitigate the risks and aided by critical thinking, boosted the cyber security defense. A quantitative assessment methodology of phishing was carried out rather than a qualitative one. This provided correct insight and a more accurate assessment to the risk assessors.

Outcome:

Once a thorough investigation was carried out, Infopercept reported more than 1500 vulnerabilities of which 100+ were very critical ones. More than 70 vulnerabilities were reportedly in the high risk category and the rest were in the medium to low risk categories. An important point to note here would be that even a low risk vulnerability can lead to a potential hack by a persistent hacker.

On account of the successful simulated phishing and MITM attacks by Infopercept, they were able to ascertain passwords, break into the Wi-Fi systems and access the bank’s customer database. IT risk mapping of the bank was complete. The entire phase 1 was completed in 90 days.

Phase 2

Phase 2 began after 60 days of completion of phase 1. A detailed report which enlisted the susceptible areas were highlighted and remedial measures were suggested at the end of Phase 1. The time period between the two phases gave ample time for the bank’s security team to work on security lapses. In this corrective period, the bank’s internal security team worked to resolve issues. Once the corrective period was over, retesting was done by Infopercept. Although some issues were resolved, all security lapses highlighted by Infopercept were not patched up. These were again reported back to the bank with another set of suggestions containing remedial measures and ways to plug these loopholes.
Benefits of these comprehensive and professional activities:

The Infopercept team studied the landscape of the network and infrastructure of the bank in its entirety. This provided it with the necessary vantage point that enabled it to detect security lapses at various levels.

In order to understand the vulnerabilities posed by a bank from the hacker’s point of view, it is imperative to understand the structure of the bank. Primarily the banking sector can be categorised into its customers, front desk employees and the internal staff. The hackers usually attempt to break into the system via the external user (customer) or the internal user (employee). These hacks can occur without much effort especially if multi-factor authentication is not in place. To attempt to break into the system through the internal staff, although harder, is more dangerous as more authorizations are given to them.

Infopercept was able to study the loopholes from all these angles and provide an exhaustive summary of possible vulnerabilities or hits the bank could take. After intense scrutiny of the external hardware systems and other software based applications, databases etc., weak links were identified.

Since Infopercept has an experienced team of experts who help in various compliances including the *PCI DSS certification*, their help was sought to identify various gaps in compliance related issues as well and this helped the bank with its compliance needs. This way the bank was able to protect and safeguard all sensitive data and information of the customers thereby building a long lasting trusting relationship with its customers.

Solutions:

Infopercept, through its *Offensive Security Practices*, was able to design solutions to patch the software anomalies and fix the vulnerabilities detected. Although some issues were fixed, there were areas that needed more work. Apart from suggesting methods for fixing the recently discovered loopholes in the systems, Infopercept further advised the use of *Offensive Security*, a proactive and adversarial approach that would help the banking systems and network from future attacks. This will enable the bank’s internal security team to seek out the perpetrators in the future even before they attempt to disable or disrupt their operations.
About INFOPERCEPT

Infopercept’s vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions 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 & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions for your specific business needs, exactly the way you want it to be.