Payatu

National Bank Infrastructure Security Assessment

A Case Study

Being one of the biggest banks in the Middle East, what matters for our customer is the best quality service.

TABLE OF CONTENTS

THE CLIENT

This National Bank is among the top ten largest banks in the Middle East. It is a major bank listed on the National Exchange and has received an 'A' rank from Standard and Poor's. Operating from 1950, this bank has more than 5000 employees and international presence in the UK.

GOALS

Our Client maintains high-quality security standards across all its premises which includes the Headquarters, the branches, and the remote locations. And these high-quality standards are backed and maintained by regular assessments and audits rom the world-class security professionals.When the team of Payatu was entrusted for this task, we had the following four goals to deliver:

1. **Assess Huge and Complex Infrastructure -**
   The bank's infrastructure assessment was not only huge in terms of number systems but also very wide in variety and number of technologies used in their processing and communication infrastructure. We had to cover:

   - **All the computing devices, servers and endpoints**
   - **Network, communication and calling Infrastructure**
   - **Physical and Infrastructural Security**
   - **Applications, Business logic**
   - **Social Media Usage Risk Management**
   - **User & Business data Security**
   - **Security Infrastructure**

   In addition to the above, we Designed and launched various Security Awareness campaigns within the organisation.

2. **Comply with Industrial & Federal Regulatory Standards -**
   Our client emphasized on rigorous security assessments not only to meet the Federal and Industrial regulatory standards but also, to honour its commitment to maintaining high standards of security. For this purpose, we had to assess the infrastructureto comply with:

   - **FIPS Standards**
   - **PCI-DSS 3 Standards**
   - **National Monetary Agency Standards**
   - **Proprietary Standards adopted by the Bank**

3. 0 Tolerance for disruption and losses -
   Since it was a National Banking each element of its infrastructure was operationally critical. We had to ensure that our assessments are

   - **Non-Disruptive**
   - **Lossless**
   - **Complying with the non-disclosure agreement**
   - **Accurate yet deep enough to uncover the hidden security threats and vulnerabilities**

4. Reporting the critical findings and help with Remediation -
   After finding numerous vulnerabilities, operational gaps, and critical flaws, our responsibility was to take the client in confidence and help them fix and address those issues.

5. Assessment and Education of Human Resources for Security -
   In addition to the Infrastructural components, humans are the crucial part of the Organization. To assess the human aspects, we designed and carried out various Campaigns like:

   - **War Dialling**
   - **Wardriving**
   - **Phishing Campaign**

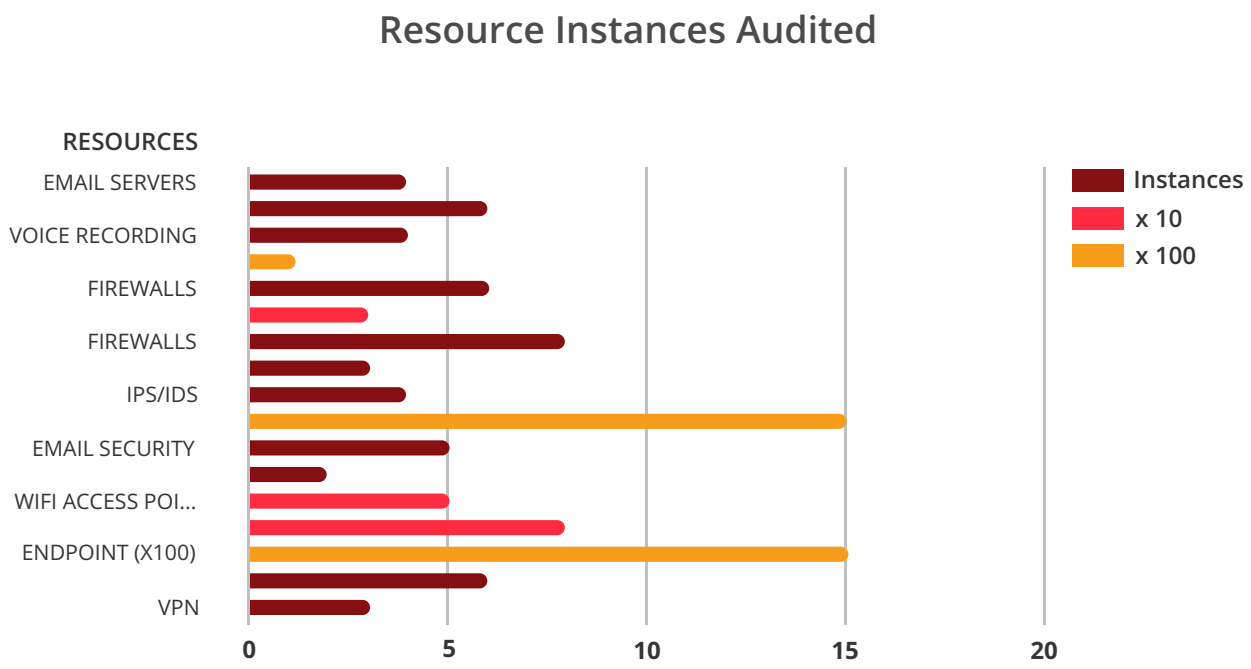
   All these followed by specifically designed awareness sessions to bridge the gaps.

THE TEAM

Payatu had deployed the professionals who possess a variety of skills and expertise in widespread disciplines of Information security. In total 12 professionals for the time of 3 months, were assigning every communication line, every computing system, and interacting with each and every one of the owners of these systems.

THE INFRASTRUCTURE

The Bank's infrastructure was spread across multiple locations, in all 6 buildings with an average of 7 floors each. Each floor was of 500K sq. feet in area. We had to assess the wireless connectivity outside each of the premises, and every computing devices, connections, communication lines in those premises.



Few major infrastructure systems are broadly categorized as follows -

- All the computing devices, servers and
- Network, communication and calling Infrastructure
- Physical and Infrastructural security
- Applications, Business logic

THE PROCESS

1. Scoping of the work and Resource allocation -

We divided the entire work into smaller segments. For each distinctive segment, we worked out the right mix of skills, experience, and the optimum number of team members

2. Understanding the System -

To begin the assessment, we need a thorough understanding of the existing system. For this, we try to understand:

- System deployments & configurations
- Process for change-management
- Approval chains or communication history maintained
- Any operational manuals, documents
- Access controls, accounting measures deployed etc.

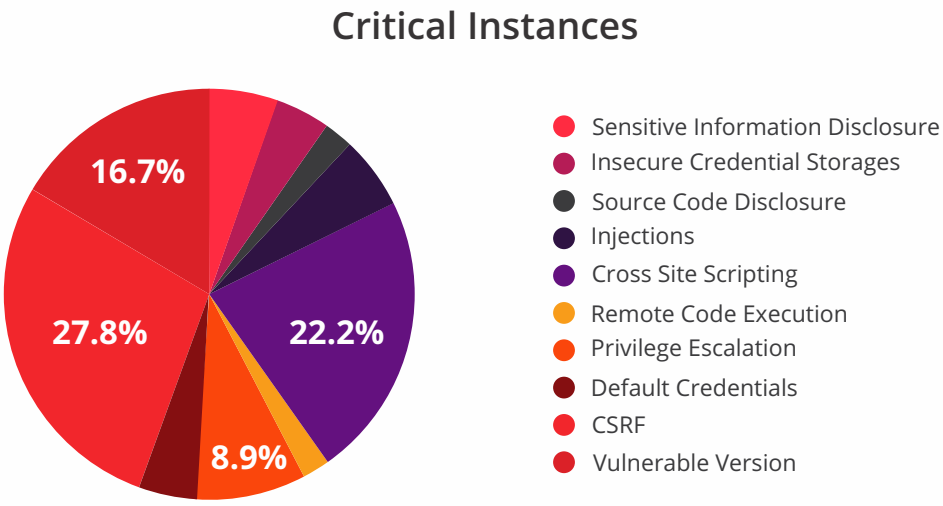
Once we have a good understanding of the functioning of the system, we try to gain a finer and deep understanding of the
system using various sources. These could be:

- Interviewing the system owners
- Reading the procedural documents
- Learning about the proprietary security standards and best practices.

3. The Assessments -

After acquiring a thorough understanding of the systems our team carries out various assessments. These, apart from standard checklists, include lots of customised testing and research. Few of the steps we follow are:

- Tool-based vulnerability assessments
- Manual client-side testing
- Developing client emulators, custom scripts to uncover specific vulnerabilities
- Validating the existing systems configurations and process with industry standards
- Gap analysis, variance/deviation from the targeted compliance standards



4. Reporting the findings -

The team documents their findings throughout the assessment process. Reports on specific and sensitive findings are deliveredat the end of every assessment phase. We take following care during the reporting of the findings.

- **Report the findings along with proper severity & criticality score.**
- **Give technical details of the findings along with step by step procedure to reproduce the same.**
- **Provide any custom POCs and scripts employed for the findings.**
- **Non-disclosure of personal or business-sensitive information.**

At the end of the assessment phase, we provide an executive summary with top critical findings classified in 10 categories.

5. Remedial Recommendations and Closing -

Along with reporting the findings we also give the corrective course of action for each of the reported issues. With specific requests from the client, we help their team in Remediation and fixing the security issues found by us. We also help our client with Remedial actions and fixing security issues disclosed and reported by others.

VALUE TO YOU

It's a given that many companies are competing in the space of security assessments and audit. Payatu has some unique value propositions. Due to its wide community reach and rich connections in the industry, talent acquisitions for specific missions is an easy task. Our collective Industrial experience and researches give us an unmatched advantage over all other competitors.

Highly Skilled Professionals -

Certified professionals with a proven track record in the information security industry.

Broad Coverage -

Our team is skilled in various disciplines of information security. This helps us ensure maximum coverage of widespread technologies of Banking domain with an optimum number of professional resources.

Research Focus -

Our proprietary process is focused on understanding the underlying and researching on possible known and unknown security lapses rather than iterating over standard checklists. The professionals who present their researchers at global security and hacking summits bring their richer security experience and research work to benefit our clients.