Setting up and Operationalising Cyber Security Operation Centre (C-SOC)

Introduction

1 - Banking Industry in India has evolved technologically over the years and currently delivering innovative services to its customers. These services are delivered nonstop, round the clock and the customers access these services using Internet and Mobile Connectivity. Security of the financial transactions is of paramount importance and therefore the RBI has come out with guidelines from time to time addressing the security and operational aspects for specific applications and services.

2 - It is important and pertinent to look at specifically the Internet facing applications and services that are currently delivered and proposed to be delivered in the immediate future in the Banking Industry and come out with Cyber Security guidelines across the applications and services.

3 - Constant and Continuous monitoring of the environment using appropriate and cost effective technology tools, clearly defined policies and procedures based on best practices and monitored by technically competent and capable manpower is the urgent need for the Industry. Compliance to the Government guidelines that are put out periodically covering the cyber security policy, protecting critical information infrastructure and the Information Technology Act are of paramount importance. It is important to address the governance, technology, operational, outsourcing and legal issues while setting up the Cyber Security Operations Centre.

4 – Issues that need to be kept in mind while setting up the CSOC is given below. These are indicative but not exhaustive.

Governance Aspects:

- Top Management/Board Briefing on Threat Intelligence
- Dashboards and oversight
- Policy, measurement and enforcement (key metrics, reporting structure, define what is to be reported)
- Informing stakeholders , stakeholder participation

Cyber SoC: Points to be considered

1 - Conventional or Traditional Security systems have always focussed on preventive approaches over the years and are reactive in nature. They are in a position to address the concerns regarding known attacks. It is to be noted that the threat landscape has changed significantly in the recent past and therefore the approach and methodology required to be put in place has to necessarily take into account proactive approaches rather than reactive approaches and have to also address possible unknown attacks. For example, zero day attacks and attacks for which signatures are not available have to be kept in mind.

2 - The Cyber SoC has to take into account proactive monitoring and management capabilities with sophisticated tools for detection, quick response and backed by data and tools for sound analytics.

3 - The systems that are implemented currently to monitor the security operation takes into account collection of the logs from each one of the point products deployed, storing and processing of the logs, correlation through appropriate SIEM tools, continuous monitoring of SIEM screens and finding the anomalies, if any and raising the alarms.

4 - The systems that NEED to be put in place as a part of the Cyber SoC requires the following aspects to be addressed.

- Methods to identify root cause of attacks, classify them into identified categories and come out with solutions to contain further attacks of similar types.
- Incident investigation, forensics and deep packet analysis need to be in place to achieve the above.
- Dynamic Behaviour Analysis. – preliminary static & dynamic analysis and collecting Indicators of Compromise (IOC)
- Analytics with good dash board, showing the Geo-location of the IP’s
- Counter response and Honeypot services

Expectations from SOC:

- Ability to Protect critical business and customer data/information, demonstrate compliance with internal guidelines, country regulations and laws
- Ability to Provide real-time/near-real time information on and insight into the security posture of the bank
- Ability to Effectively and Efficiently manage security operations by preparing for and responding to cyber risks/threats, facilitate continuity and recovery
- Ability to assess threat intelligence and the proactively identify/visualize impact of threats on the bank
- Ability to know who did what, when , how and preservation of evidence
- Integration of various log types and logging options into SIEM, ticketing/workflow/case management, unstructured data/big data, reporting/dashboard, use cases/rule design (customized based on risk and compliance requirements/drivers, etc.), etc.

Key Responsibilities of SOC could include:

- Monitor, analyze and escalate security incidents
- Develop Response - protect, detect, respond, recover
- Conduct Incident Management and Forensic Analysis
- Co-ordination with contact groups within the bank/external agencies

5 - Building blocks for the Cyber SoC:

TECHNOLOGY ISSUES:

First step is to arrive at a suitable and cost effective technology framework designed and implemented to ensure proactive monitoring capabilities aligned with the banking technology risk profile and business and regulatory

requirements. Clear understanding of the service delivery architecture deployed by the Bank to deliver innovative customer services will enable identification of the location for the sensors to collect the logs that are required to carry out the analysis and investigation. SIEM is able to meet this requirement to some extent but a holistic approach to problem identification and solution is required.

Second step is to have security analytics engine which can process the logs within reasonable time frame and come out with possible recommendations with options for further deep dive investigations

Third step is to look at deep packet inspection approaches which are currently implemented using the UTM solutions that deliver wire speed performance with on the fly deep packet inspection.

Fourth step is to have tools and technologies for malware detection and analysis as well as imaging solutions for data to address the forensics requirements

It is to be noted that the solution architecture deployed for the above has to address performance and scalability requirements in addition to high availability.

Need to think through by appropriately designing the

- SIEM architecture & use cases
- Log types and logging options (data sources, integration into SIEM)
- Integration of various log types and logging options into the SIEM, ticketing/workflow/case management, unstructured data/big data, reporting/dashboard, use cases/rule design (customized based on risk and compliance requirements/drivers, etc.), etc.
- Technology for improving effectiveness and efficiency (tracking of metrics, analytics, scorecards, dashboards, etc.)

PROCESS RELATED ASPECTS:

One of the key aspects that require attention while designing the CSC is to understand the process to be followed to identify the root cause of a security breach and further steps to mitigate such attacks in future.

Incident Management

Problem management processes with reference to security operations Vulnerability and Patch Management Security risk management Availability management Computer forensics and response management are the key metrics that need to be well understood and architectured while configuring the solution.

PEOPLE RELATED ISSUES:

CSC is managed and monitored by competent and capable staff round the clock and therefore it is important to look at a suitable structure for this requirement.

The Level 1 monitoring by adequately trained staff working round the clock is the first step. They need to have training and product/ vendor certification to handle the tasks efficiently.

Level 2 deals with highly trained staff in specific areas of network, data security, end point security etc. to address the requirements especially while carrying out the root cause analysis as well as suitable corrective steps.

Level 3 staff are called the SoC analysts. They have profound knowledge of security, perform deep packet analysis, collection of IOC, forensic knowledge for collection of evidence, malware reverse engineering and write custom scripts whenever required.

It is to be noted that all the staff involved in the above exercise need to have a good knowledge of the products and services deployed by the respective Bank.

- Banks need to seriously consider practical ways of tackling the following issues when it comes to hiring and managing staff/people for SOC. It is not any other function in the bank. There has to be a different approach

because such personnel with required skill sets that are hard to find and retain.

- Staffing of SOC – is it required to be 24x7x365, in shifts, business hours only….etc.
- Model used - Finding staff with required skills /managed service provider with required skill set
- Training own staff/training of staff by service provider
- Appropriate compensation/incentives to retain trained staff /staff with required skill set
- Metrics to measure performance of SOC
- Ensuring scalability and continuity of staff through appropriate capacity planning initiatives

EXTERNAL INTEGRATION:

While delivering services to the customers of the Bank, several stake holders are involved directly or otherwise. They do have experience which could be very useful. For example the threat intelligence feeds from various sources may be provided by the product vendors and other major players in the technology landscape. Security information feeds from other Banks in particular and the financial ecosystem in general will be quite useful.

Cyber response cells, CERT-In and telecom service providers of the Bank may add value to the discussions based on the happenings in the Industry at large.

IDENTIFYING A SUITABLE MODEL FOR IMPLEMENTATION:

Some of the decisions which have to be taken upfront is to look at BOO or the Outsourcing model. It is difficult to reverse this decision post implementation and therefore it is important.

- Should the SoC be in-house or outsourced?
- Should it address only the Internet facing environment or the complete IT infrastructure?

- Does each Bank need to set up independently or should we look at the consortium based approach?
- Do we need to keep in mind the Bank's risk posture?

Points to keep in mind while planning for SOC in view of

(a) Specialized skill set requirements of operating and managing a SOC,

(b) Difficulty in finding experienced staff,

(c) Time consuming and expensive trainings,

(d) Designing of suitable compensation strategies,

(e) difficulty of retaining staff due to continual need for updated training, lack of adequate career path options, and overstretching ,

(f) Resource requirements pertaining to other supporting functions such as (i) system administration of systems facilitating SOC operations such as SIEM/dashboard/reporting/workflow/case management systems, etc., (ii) receiving, integrating and using threat intelligence, (iii) implementing communication strategy, (iv) Supervision/ management of SOC staff/personnel, (v) meeting compliance requirements of regulators/laws/regulations