Overview

The term BFSI stands for Banking, Financial Services and Insurance (BFSI). This term is widely used to address those companies which provide an array of financial products or services.

Financial services may include Mutual Funds, Insurance products, stock trading etc. while Banking services cover core banking, retail, private, corporate, investment etc.

Considering the increased use of technology by banks, the RBI constituted the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, which produced its report in January 2011. The Working Group was headed by Mr. G. Gopalakrishna and the report is popularly known as the Gopalakrishna Committee Report.

The committee’s objective was to issue a set of directives to Banks on IT security policies to mitigate security breaches and frauds and ensure a safe business network environment for crucial banking transactions.

An important part of the directive was that Banks are required to appoint a Chief Information Security Officer (CISO) who overlooks implementation of the said guidelines formulated by Gopalkrishna Committee.

This document covers the guidelines and regulations of Gopalkrishna report and educates the readers about Cyberoam solution to meet those guidelines and regulations.
1. **Regulation:** IT Performance should be monitored

**IT Impact: On-Appliance Reporting**

**Cyberoam Solution:**

Cyberoam appliances come with in-built monitoring and reporting features. Below is the list and description of various monitoring and reporting features available in Cyberoam:

- **Device Health Monitoring** – Cyberoam appliances display utilization summary of various system resources like CPU and Memory right at the appliance dashboard while the information of traffic passing through individual network interface is available in System Graphs.

- **Network Traffic Monitoring** – Cyberoam provides detailed On-Appliance reporting of egress and ingress traffic. In addition it gives visibility of user’s Internet behavior with the help of various user based reports. These reports include list of Websites and Applications used by the user. It also gives information of destination hosts and destination countries for the user. Cyberoam appliances can also be integrated with Cyberoam iView - a dedicated reporting solution which provides centralized consolidated reports for multiple Cyberoam appliances and other networking devices as well.
2. Regulation: Procedures for Problem, Change & Configuration Management is needed.

**IT Impact: IT Assets Management Solution**

**Cyberoam Solution:**
Cyberoam offers role based administration of Cyberoam security appliances; which means an administrator with certain privileges can perform certain configuration changes on Cyberoam appliance and others can have read-only privileges. These privileges are associated with the profile assigned to the administrator. Cyberoam offers 5 (five) default profiles; Administrator, Audit Admin, Crypto Admin, HAProfile, Security Admin.

You can even create custom profiles to provide selective access of Cyberoam menu items. This ensures customized access to security and management configurations.

Cyberoam keeps track of every change made by the administrator for meeting various compliance regulations. These logs contain detailed information of affected component, list of changes, time of changes and IP address of administrator user.
Cyberoam Central Console – a central management solution allows the administrator to view list of revisions for managed Cyberoam appliances. Revisions are the configuration changes stored in CCC repository. CCC also allows the administrator to view list of affected configuration settings, compare different versions of configurations and roll back to previous configurations.

3. **Regulation:** Banks to maintain enterprise information system to enable decision making

**IT Impact: Centralized Reporting Solution**

Cyberoam Solution:
Cyberoam offers extensive logs and comprehensive reports of user’s Internet behavior. It also provides visibility of network traffic trends, surfing patterns, application and Web category based traffic and Country based traffic analysis. This readily available information helps management in decision making for empowerment and protection of IT infrastructure.

For example, given below is the report showing list of top applications used for attacks. With the help of this report, the administrator can proactively block access to these applications and secure the organization’s network from approaching attacks.
4. **Regulation:** Suspicious activity reporting, Proactive risk & vulnerability assessment to be in place

**IT Impact:** Centralized Reporting Solution, Vulnerability & Risk Assessment Solution

**Cyberoam Solution:**
Cyberoam’s On-Appliance threat reports give visibility of attack attempts along with details like attacker, victim, platforms and applications used for attacks and source countries of attacks.

**Top Attacker Countries**

<table>
<thead>
<tr>
<th>Country</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>47935</td>
</tr>
<tr>
<td>Singapore</td>
<td>4741</td>
</tr>
<tr>
<td>India</td>
<td>17</td>
</tr>
<tr>
<td>Canada</td>
<td>14</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>12</td>
</tr>
<tr>
<td>British Virgin Islands</td>
<td>5</td>
</tr>
<tr>
<td>Ireland</td>
<td>4</td>
</tr>
<tr>
<td>Philippines</td>
<td>4</td>
</tr>
<tr>
<td>Germany</td>
<td>1</td>
</tr>
</tbody>
</table>

It also provides details of network vulnerability tried to be exploited by the attacker with details like impact, affected systems, attack scenarios etc.
Moreover Cyberoam Risk meter assesses total risk associated with the network and presents it in the form of number, a higher number shows higher level of risk.

5. Regulation: Privilege policy to access application and change authorization must be maintained

IT Impact: Application Management and Control

Cyberoam Solution:
Please first refer to Regulation 2.

While implementing security policies, Cyberoam puts Human Layer i.e. User identity at the top of network stack. It enables organizations to control access to network resources based on the user identity, work profile and application access requirement. It also offers user identity-based security in dynamic Wi-Fi, DHCP and shared endpoint environments.
Cyberoam’s Application Filtering module categorizes applications on the basis of Risk Level, Category, Characteristics and Technology and allows User, Role and Schedule based access control for the applications.
6. Regulation: Operational risk should include IT Risk

**IT Impact:** IT Risk Reporting Solution

**Cyberoam Solution:**
Please refer to Regulation 2 and Regulation 4

Cyberoam’s comprehensive reports offer actionable intelligence to the administrators. The administrator can take corrective decisions based on network traffic patterns and users’ behavior. Given below are some examples of Cyberoam’s detailed reports.

<table>
<thead>
<tr>
<th>User Group</th>
<th>Data Transfer</th>
<th>Uploaded</th>
<th>Downloaded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales Group</td>
<td>811.89 MB</td>
<td>272.86 MB</td>
<td>539.03 MB</td>
</tr>
<tr>
<td>Marketing Group</td>
<td>560.80 MB</td>
<td>164.87 MB</td>
<td>396.93 MB</td>
</tr>
<tr>
<td>Training Group</td>
<td>222.01 MB</td>
<td>43.15 MB</td>
<td>178.86 MB</td>
</tr>
<tr>
<td>Team Leads</td>
<td>214.64 MB</td>
<td>23.9 MB</td>
<td>190.75 MB</td>
</tr>
<tr>
<td>Clientless Group</td>
<td>77.40 MB</td>
<td>13.4 MB</td>
<td>64.08 MB</td>
</tr>
</tbody>
</table>

7. Regulation: Comprehensive MIS to be in place

**IT Impact:** Centralized Reporting Solution

**Cyberoam Solution:**
Cyberoam iView – a dedicated reporting solution provides centralized and consolidated reports for multiple Cyberoam appliances deployed across the globe. Cyberoam iView’s rich set of reports are
categorized under multiple report groups like Web Usage, Blocked Web Usage, Application Usage, Blocked Application Usage, Virus, Spam, Attacks, Events, Search Engine, Compliance, VPN and SSL VPN. These reports can be filtered for various filter criteria to get leaf level visibility of any network event.

| 8. Regulation: Control Objectives for Information and Related Technology (COBIT) |
| Cyberoam Solution: |
| By deploying Cyberoam product range i.e. Cyberoam Network Security Appliance, Cyberoam iView and Cyberoam Central Console collectively, COBIT can be achieved. |

| 9. Regulation: Effective IT Reporting, Periodic testing to avoid break downs, Business continuity to be maintained |
| IT Impact: Reporting, High Availability and Multilink management |
| Cyberoam Solution: |
| Cyberoam supports Multiple Link Management (MLM) and High Availability to ensure uninterrupted business connectivity. The salient features of Cyberoam MLM includes an automated WAN load balancing, automatic WAN link failover and policy based routing based on user, source, IP and protocol. |
| In addition Cyberoam offers Active-Active and Active-Passive High Availability which makes sure that you never go out of Cyberoam’s security shield. In High Availability deployments when one Cyberoam appliance goes down due to any reason, other Cyberoam appliance takes over seamlessly. |
| Moreover Cyberoam supports load balancing and Fail-Over for VPN traffic which gives continuous business connectivity to remote and branch offices. |
| For reporting please refer to Regulation 1 |

| 10. Regulation: Digital evidence needed as legal proof, 2 factor authentication a must |
| IT Impact: Change Management Solution, SSO, Work Flow solutions |
| Cyberoam Solution: |
| Cyberoam uses Authentication, Authorization and Accounting for Identity-based total security approach. Under this approach, only an authenticated user is authorized to use the resources as per identity-based custom policies. All the usage is strictly accounted for through the audit trail. |
Cyberoam supports Single Sign On (SSO) and AAA for Local, Windows PDC, AD, LDAP, RSA SecurID and RADIUS authentication servers.

11. **Regulation:** Authorization based Access

**IT Impact:** Secure Access Management & SSO

**Cyberoam Solution:**
Please refer to [Regulation 10](#).

12. **Regulation:** Security audit to be done periodically. All critical IT information must be provided for audit

**IT Impact:** Audit and Compliance Reporting

**Cyberoam Solution:**
Cyberoam On-Appliance reports and dedicated reporting solution Cyberoam iView allows the administrator to reap benefits of ‘Actionable Intelligence ‘of Cyberoam’s security approach. With 1200+ reports, Cyberoam iView ensures complete visibility of 4Ws i.e. Who, What, When and Where in the network.

Having Cyberoam iView in place the administrator can ensure real-time and historical monitoring and reporting of organization’s network activities.

Cyberoam also helps organizations to comply with HIPAA, GLBA, FISMA, SOX and PCI DSS standards, by providing various compliance reports.
13. Regulation: Strict Data Security

**IT Impact:** Encryption tools, Privileged access, Identity Management, Risk Assessment Solution

**Cyberoam Solution:**
Cyberoam’s Threat Free Tunneling (TFT) ensures malware free, encrypted VPN traffic in the organization’s network.

Please refer [Regulation 10](#) and [Regulation 4](#).

14. Regulation: Data transfer must be automated and secure

**IT Impact:** Security, Authorization and Encryption tools

**Cyberoam Solution:**
Please refer [Regulation 13](#) and [Regulation 10](#).

15. Regulation: Effective malware threat detection needs to be in place

**IT Impact:** Proactive Security

**Cyberoam Solution:**
Cyberoam Network Security appliances secure organization’s network with the help of:
- Stateful Inspection Firewall – Patent pending Identity based Firewall
- VPN (SSL VPN & IPSec) – Threat free VPN tunnels
- Intrusion Prevention System – IPS system with 4500+signatures
- Anti-Virus & Anti-Spyware – 99.5% detections rate
- Anti-Spam – 99% spam detection rate and false positive rate 1 in 1.5 Million
- Outbound Spam Protection – On-Appliance outbound anti-spam
- Web Filtering – 89+ Web categories, 100+ million URLs
- Application Visibility & Control – Controls 2000+ applications
- Web Application Firewall – On-Appliance WAF
- Data Leakage Prevention – Blocks HTTP and FTP uploads, Email and IM attachments, supports Transparent Mail Activity Reporting
- On-Appliance Reporting – 1200+ reports
16. **Regulation:** Strong controls for remote employees and remote facilities

**IT Impact:** Security, Access Management Solution, Cloud Management solution

**Cyberoam Solution:**
Please refer to [Regulation 15](#), [Regulation 13](#) and [Regulation 10](#).
Cyberoam's range of entry level appliances (CR 15wiNG, CR 25wiNG, CR 35 wiNG) offer blend of excellent routing capabilities and security solutions for remote and branch offices.

Cyberoam extends its security shield to protect organization’s business critical cloud infrastructure by providing Identity based access control and security offerings for cloud.


**IT Impact:** Risk Management solution

**Cyberoam Solution:**
Please refer to [Regulation 4](#).

18. **Regulation:** Board needs awareness of IT Infrastructure and ability to meet business objectives

**IT Impact:** Asset Management solution, Reporting & Centralized Management tools

**Cyberoam Solution:**
Cyberoam Central Console offers centralized security management across distributed Cyberoam network security appliances, enabling high levels of security for MSSPs and large enterprises. With Layer 8 Identity-based policies and alerts, CCC provides granular security and visibility into remote and branch offices across the globe. The administrator can configure and manage thousands of Cyberoam appliances through CCC.

Please refer to [Regulation 7](#).

19. **Trend:** Increase usage of Mobile by customers

**IT Impact:** Secure Policy based Access, Encryption, Authentication, Application control

**Cyberoam Solution:**
Cyberoam’s Human Layer 8 Technology, allows network administrators to design identity-based policies, which extends throughout the network, irrespective of the device used by the employee to connect to the network. Along with Layer 8 Technology, Cyberoam UTM offers secure AAA (Authentication, Authorization, Audit) over a single device, allowing control and knowledge of who is connected to your network, using what device and what are they accessing. You can design security policies that allow you to decide, what each user /user group can access in terms of websites/applications over Internet and for how long, the amount of data transfer and bandwidth they can consume.
<table>
<thead>
<tr>
<th>Client Type</th>
<th>Data Transfer</th>
<th>Uploaded</th>
<th>Downloaded</th>
<th>Used Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Client</td>
<td>4.86 GB</td>
<td>594.43 MB</td>
<td>4.28 GB</td>
<td>69 days 21:26:33</td>
</tr>
<tr>
<td>Win Client</td>
<td>1.53 GB</td>
<td>100.85 MB</td>
<td>1.43 GB</td>
<td>138 days 22:38:41</td>
</tr>
<tr>
<td>SIB</td>
<td>204.29 MB</td>
<td>16.6 MB</td>
<td>214.80 MB</td>
<td>279 days 24:44:57</td>
</tr>
<tr>
<td>iOS Client</td>
<td>109.46 MB</td>
<td>10.51 MB</td>
<td>179.15 MB</td>
<td>118 days 23:32:40</td>
</tr>
<tr>
<td>Android Web Client</td>
<td>53.97 MB</td>
<td>2.10 MB</td>
<td>46.88 MB</td>
<td>12 days 23:38:09</td>
</tr>
<tr>
<td>Android Clients</td>
<td>24.12 MB</td>
<td>2.42 MB</td>
<td>26.69 MB</td>
<td>19 days 02:02:29</td>
</tr>
<tr>
<td>KS Web Client</td>
<td>3.17 MB</td>
<td>250.06 KB</td>
<td>2.92 MB</td>
<td>2 days 20:13:12</td>
</tr>
</tbody>
</table>

Toll Free Numbers


www.cyberoam.com | sales@cyberoam.com

Copyright 1999 - 2014 Cyberoam Technologies Private Ltd. All rights reserved. Cyberoam, Cyberoam logo are trademark of Cyberoam Technologies Pvt. Ltd.

Cyberoam assumes no responsibility for accuracy or completeness of information. Neither is this a legally binding representation. Cyberoam has the right to change, modify, transfer or otherwise revise the publication without notice.