Network Security Review Approach
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>3</td>
</tr>
<tr>
<td>2. The need to Network Security</td>
<td>7</td>
</tr>
<tr>
<td>3. What is Network Security</td>
<td>9</td>
</tr>
<tr>
<td>4. Methodology</td>
<td>11</td>
</tr>
</tbody>
</table>
1. INTRODUCTION
It is a Unsafe Cyber world..
Threats Continue to Rise...

Figure 4
Ransomware Attacks During the Previous 12 Months

Source: Osterman Research, Inc.

New Ransomware

Source: McAfee Labs, 2015.
Recent data from IBM Security Services shows 55% of all attacks were found to be carried out by malicious insiders or inadvertent actors.

**Who are the “bad guys”?**

45% Outsiders
31.5% Malicious insiders
23.5% Inadvertent Actor

---

**The Spectrum of Insider Threats**

- Traditional Insiders
- Privileged Users
- Hackers Actively Targeting Insider Accounts
  - Criminal Hackers
  - Nation States
  - Porous Perimeters
  - Cloud/SAAS
  - Big Data

*Source: Internet*
2. NEED FOR NETWORK SECURITY
Need for Network Security Review

- To improve network security awareness
- To assess risk
- To mitigate risk immediately
- To reinforce the network security process
- To assist in decision making processes
- To Validate that current security mechanisms are working
- Compliance to various security standards and regulations such as ISO 27001, IT ACT 2000, SOX, HIPAA, PCI, etc.
3. WHAT IS NETWORK SECURITY?
What is Network Security

Our Network Architecture Reviews will help you identify configuration and topology issues through analysis of the design and configuration of the network.

Regardless of recent improvements in network performance and capacity, it is essential for network administrators to periodically assess the reliability of network technology and its ability to meet business needs. Consequently, network performance assessments can help organizations determine whether the programs, hosts, and applications that are installed on the corporate network function properly.
4. METHODOLOGY
Methodology for Network Security

1. Scope / Goal Definition
2. Segregation of Networks
3. Reviewing Information Flow
4. Network Threat Assessment
5. Network Architecture Review
6. Network Device Configuration Audit
7. Network Process Audit
1 Scope / Goal Definition

- Understanding the companies Network Infrastructure / Network Topology
- Number of Branches and its location
- Locations of Datacentre
- Inclusion / Exclusion
Segregation of Networks

- Ensuring that the network has been designed as per RFC 1918 addressing.
3 Reviewing Information Flow

- Understand critical business applications and their flow
- Understanding the flow of information for critical business applications such as E-Mail, Internet to analyse the various risks the data and corresponding systems are exposed too.
Network Threat Assessment

Threats facing the network

- Evaluating the network and the systems against current network threats.

- Some of the threats that today’s network are subjected too include buffer overflow, IP Spoofing, Identity spoofing.

- The current network’s implementation shall be audited so as to analyse if it can effectively mitigate the network threats.
Component Placement Review

- Checking the presence/absence of key access control devices for a secure network architecture posture.
- Firewalls are the most common form of access control devices and need to be suitably placed to protect all external and internal connections to the network.
Network Device Configuration Audit

Network Device Audit

- Auditing the network devices against industry best practices
Network Process Audit

- Auditing the network process against industry best practices. The network process audit shall cover areas such as incident management, change management, backup, network monitoring, network documentation, security reviews.
Deliverables

Organize Data/related results for Management Reporting

- Consolidation of Information gathered.
- Analysis and Extraction of General conclusions.
- Recommendations.
Challenges & Why Infopercept?

- Quality & Experience of Auditors
- Ensuring all the findings are reported to the Management
- Conduct Periodic Auditing
www.infopercept.com