



**Cognizant**  
Passion for building stronger businesses

# Reducing Application Vulnerabilities by Security Engineering



- **Subash Newton**  
Manager – Projects (Non Functional Testing, PT CoE Group)

# Agenda



**Background**



**Application Security**



**Myths and Reality**



**Application Security – Conventional Approach**



**Vulnerabilities**



**Security Engineering**



**Trends**



**Q & A**

# Background

## *Hacking incidents*

- » *Greek Ministry website hit by Hackers intrusion – Feb 2008*
- » *Indiatimes.com visitors risk high exposure to malware – Feb 2008*
- » *Hacker steals Davidson Cos customer data – Feb 2008*

*- Web Application Security Consortium*

- *Over 75% of internet attacks occur through ports 80 and 443 which must be left open to conduct business*

*- Gartner Group*

- *Network Security Management is getting mature*
- *Web Applications are becoming #1 target for hackers*

# Background

## *Reasons*

- *Very Less awareness in Application Security Testing*
- *Today Security Testing is being seen as optional Testing*

## *What is the Solution?*

- *Should we need to have dedicated Security Testing Team?*
- *Can Security Testing be outsourced?*
- *Can we incorporate Application Security in our development lifecycle?*

# Application Security

## *Vulnerability*

*A weakness in the application which can be a design flaw or an implementation bug, that allows hacker to cause harm to the stakeholders of an application*

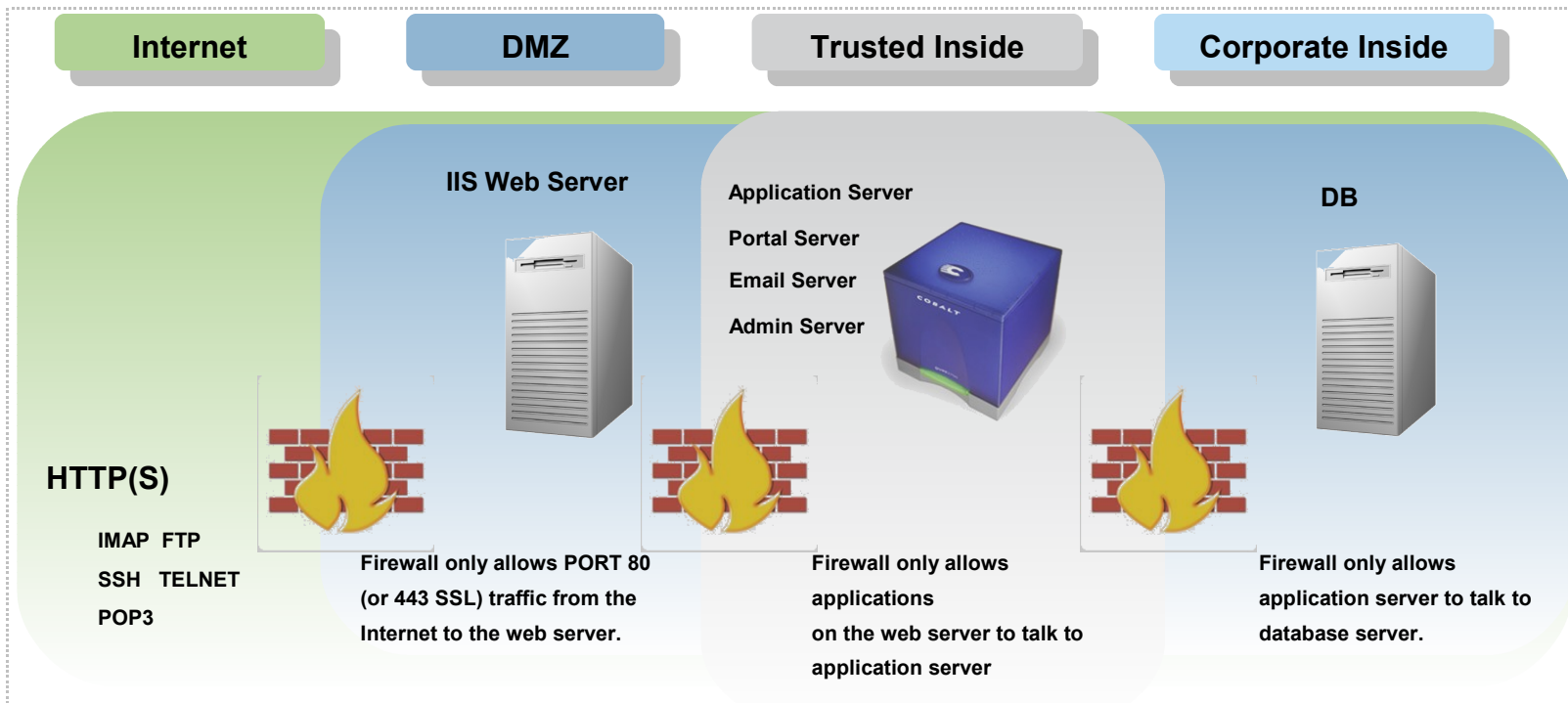
## *What is Application Security?*

*Use of software, hardware and procedural methods to protect applications, data and their control from external threats throughout its lifecycle*

## *Need for Application Security*

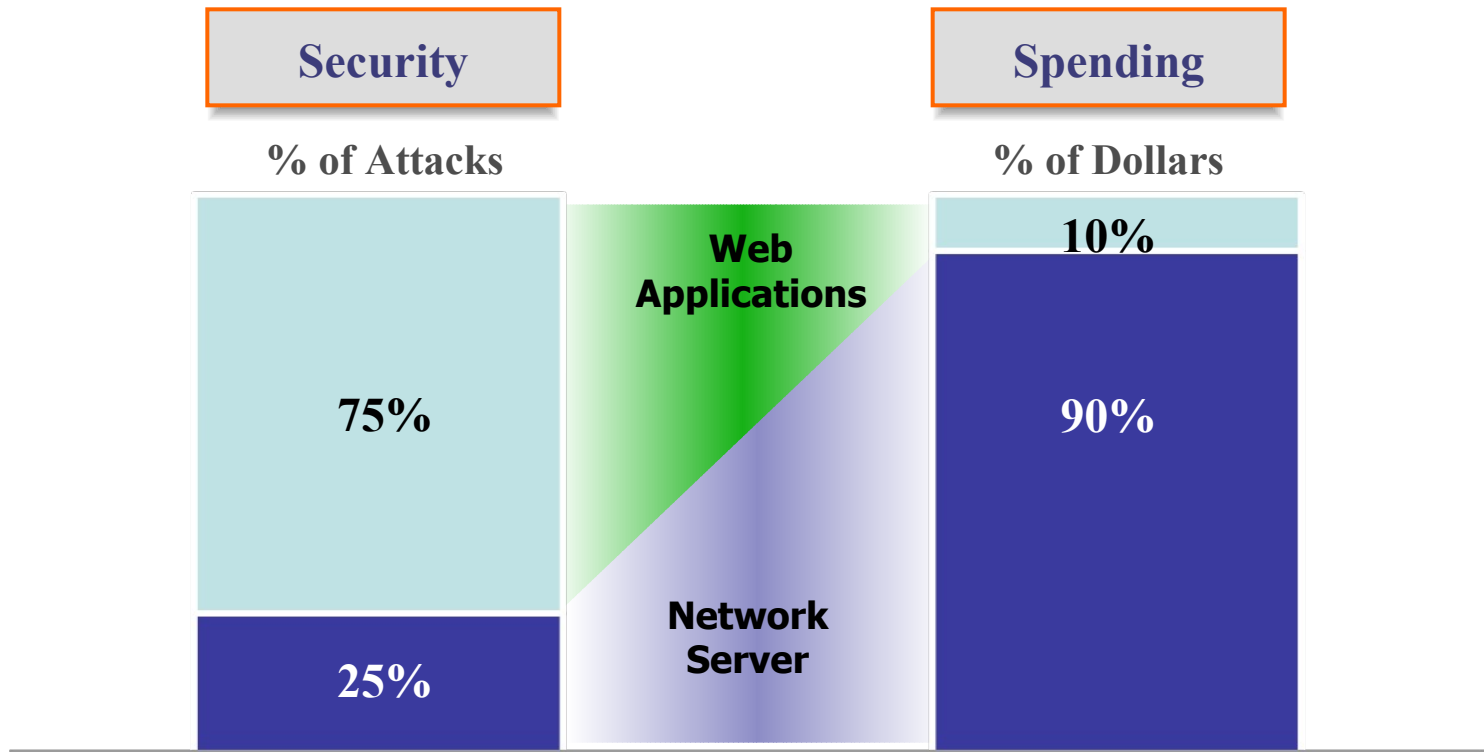
- *Patching or rebuilding application is expensive*
- *Interaction between 3<sup>rd</sup> party code and custom business logic creates vulnerabilities*
- *More investments are focused on infrastructure*

# Common Myths



- **Firewall Protects the website**
- **Security Assessments are performed on the website every year**
- **Vulnerability Scanner reported no security issues**
- **Website uses SSL**
- **Web Application Security is a Developer problem**
- **There is no ROI in Security Testing**

# The Reality

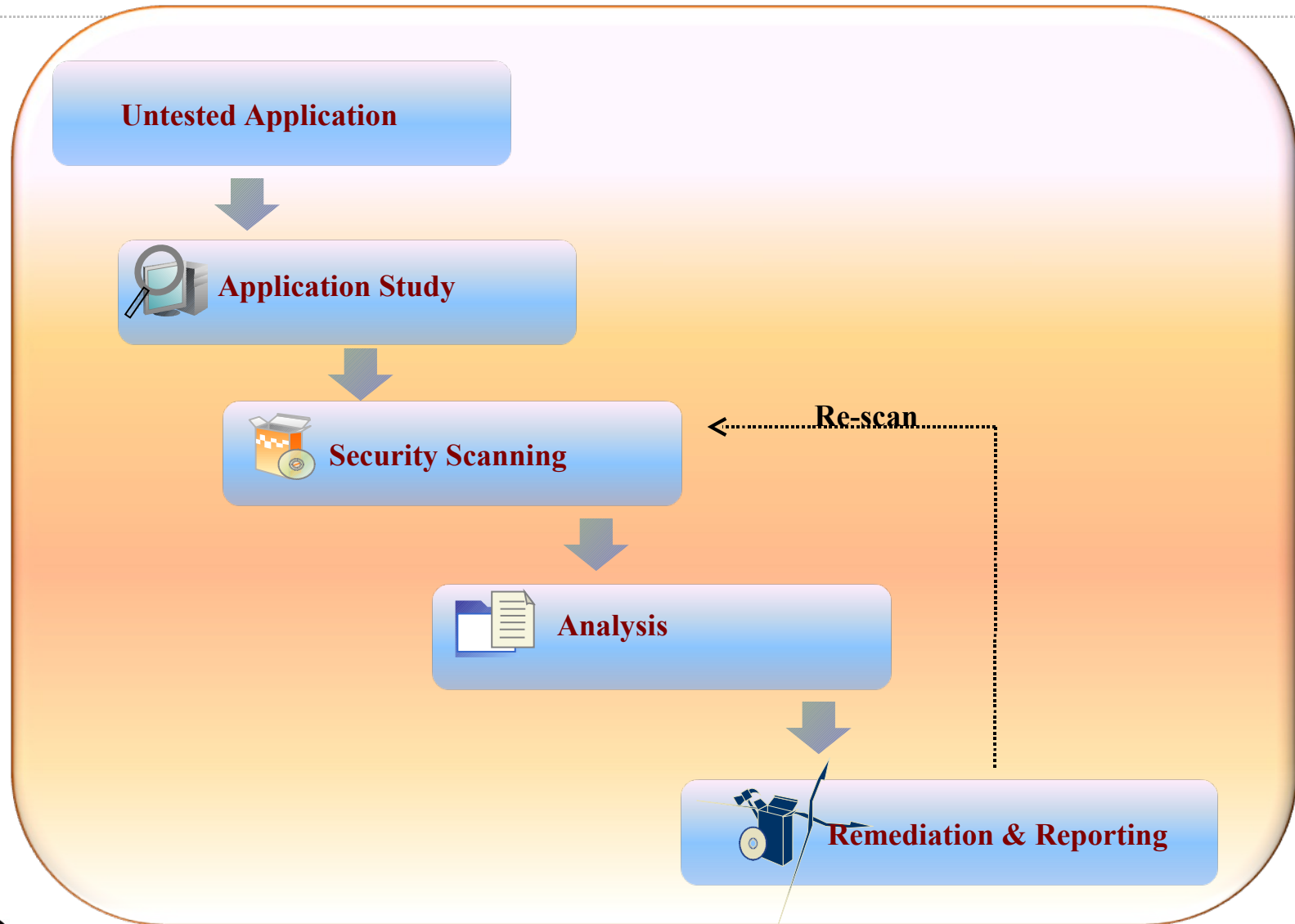


**75%** of All Attacks on Information Security Are Directed to the Web Application Layer

**2/3** of All Web Applications Are Vulnerable

**Gartner**

# Application Security – Conventional Approach



# What it Leads to?

- Failure to capture vulnerabilities in all layer of the application
- High cost for Fixing issues identified at later stage
- Loss of Revenue
- Loss to Client



**Cognizant**  
Passion for building stronger businesses

## Vulnerabilities



# Top 10 Vulnerabilities - 2007

Top 10 are key vulnerabilities that should be eliminated from any application as defined by OWASP (Open Web Application Security Project)

Vulnerability	Vulnerability Type
Cross Site Scripting (XSS)	Application
Injection Flaws	Application
Malicious File Execution	Application
Insecure Direct Object Reference	Application / Platform
Cross Site Request Forgery (CSRF)	Application
Information Leakage and Improper Error Handling	Application
Broken Authentication and Session Management	Application / Administrative
Insecure Cryptographic Storage	Application
Insecure Communications	Application / Administrative
Failure to Restrict URL Access	Application

# Vulnerabilities – Few Causes

- **Less Server side validation**
- **Port 80, 443 are always open for e-business**
- **Improper User Authentication**
- **Assuming Guest level user might not have technical competencies to exploit applications**
- **Rely on https implementation**
- **Stores clear text DSN connection strings in the configuration files**
- **Assuming cross site scripting is not a big issue**
- **Development Team typically under deadlines**
- **Not following Secure coding guidelines**
- **Networks handling traffic on internet are programmed to trust each other for the best routes for data**

# Possible Attack Areas

## Application Based

- Parameter Tampering
- SQL injection
- Cross site scripting
- Buffer overflows

## Network Based

- Denial of Service
- Session Hijacking
- Password Brute Force Attack
- Directly exploiting the Database remotely (in case of intranet)

## User Based

- Attempt to upload malicious scripts as an un-privileged user
- Perform activities that are only permissible to admin users
- Modify, delete or add data as an un-privileged user



**Cognizant**  
Passion for building stronger businesses

## Security Engineering



# Overview

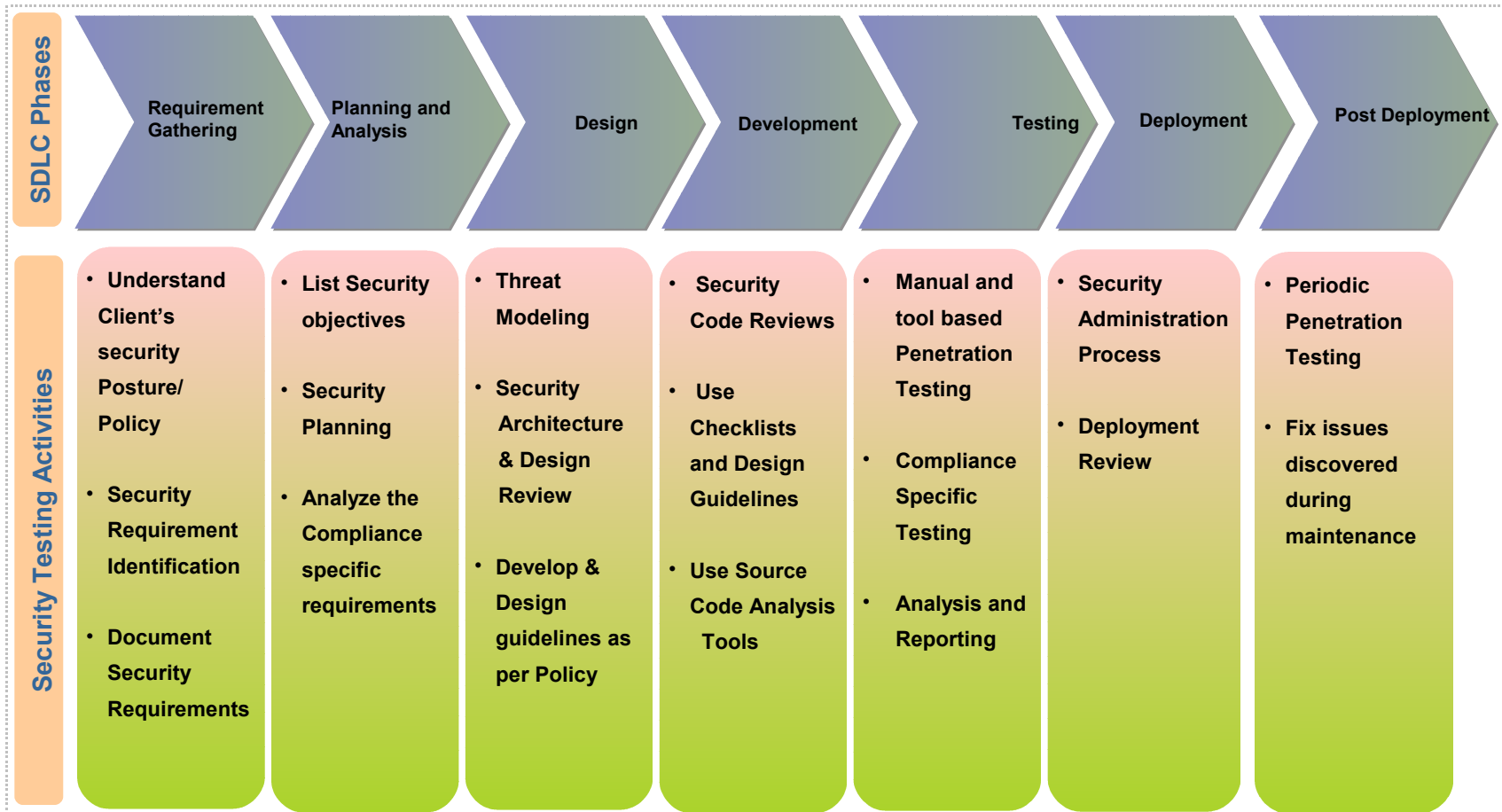
## Conventional View

- **Software Engineering is about “Ensuring that certain things happen” whereas Security Engineering is about ensuring that they don’t.**

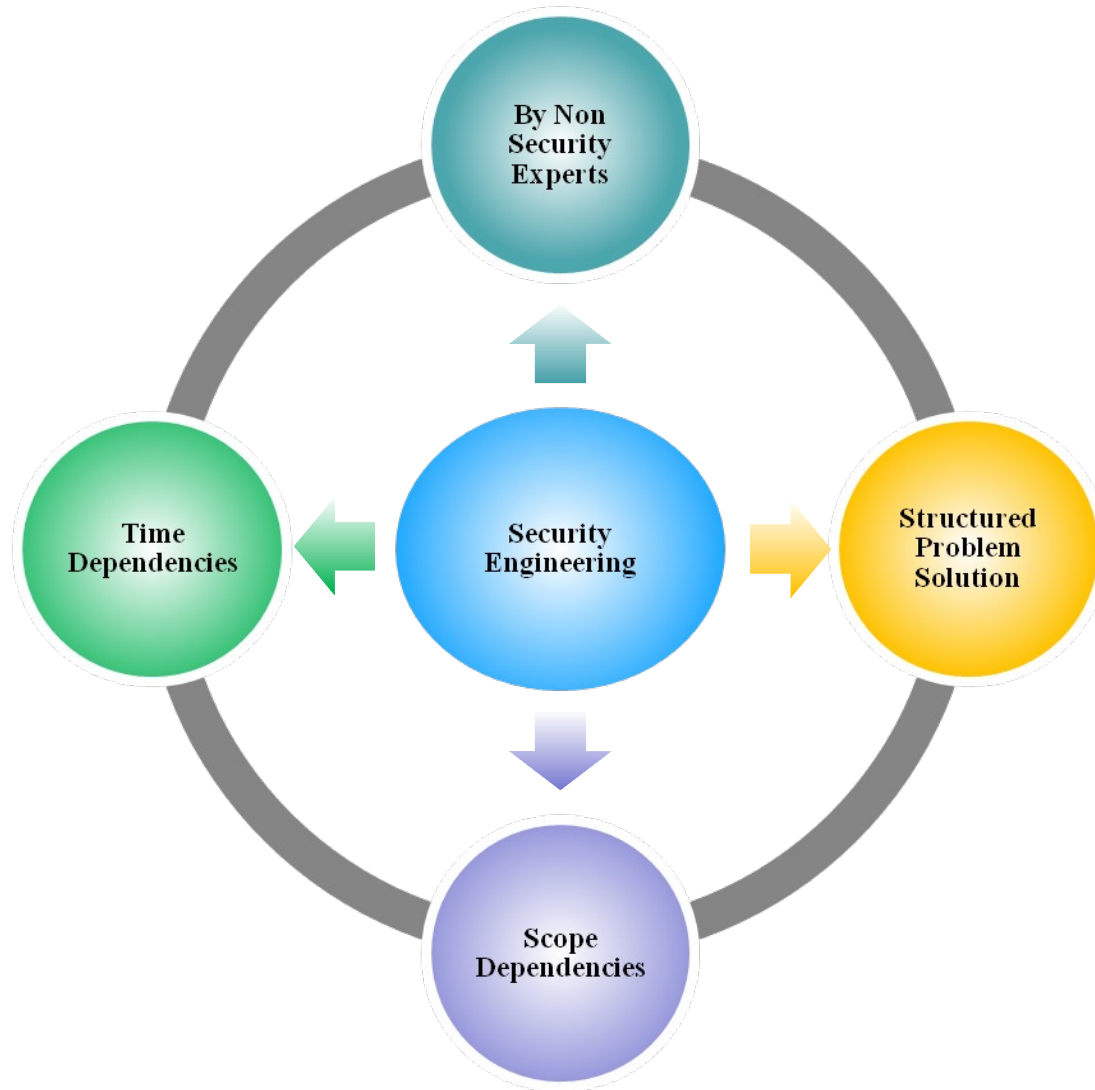
## Reality

- Security Systems differ greatly from one system to other.
- One typically needs some combination of user authentication, transaction integrity and accountability, fault tolerance and message secrecy.
- Many systems fails because their designers protect the wrong things or protect the right things in the wrong way

# Process



# Patterns



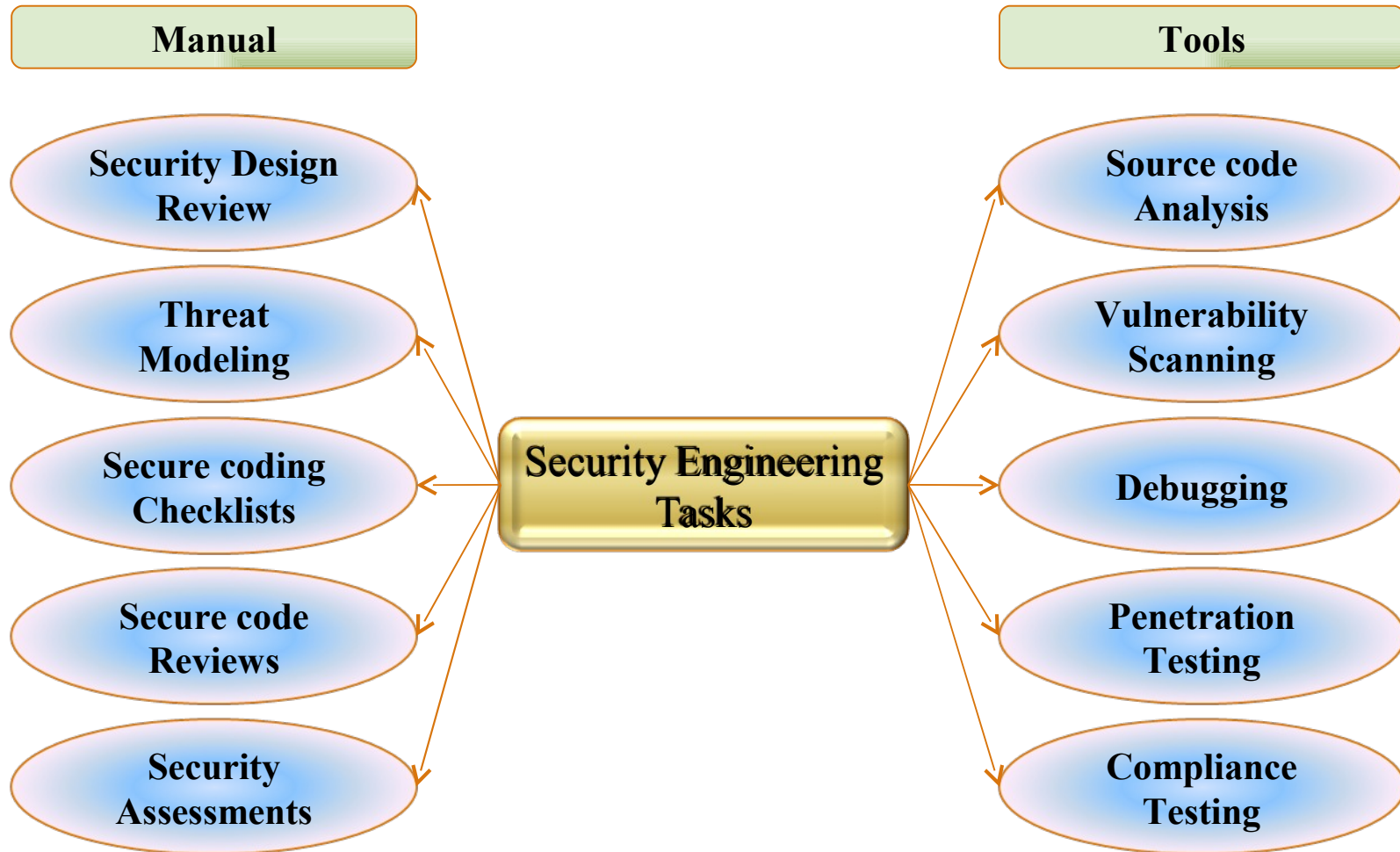
# Advantages

- Provides confidence in Project Teams that the project is “On Track”
- Earlier detection of Security related issues
- Faster resolution of identified issues
- Reduces cost associated in finding fixes in OAT Phase
- Iterative tests allows proper tuning of the application
- Development team gets more time for Security bug fixing related activities

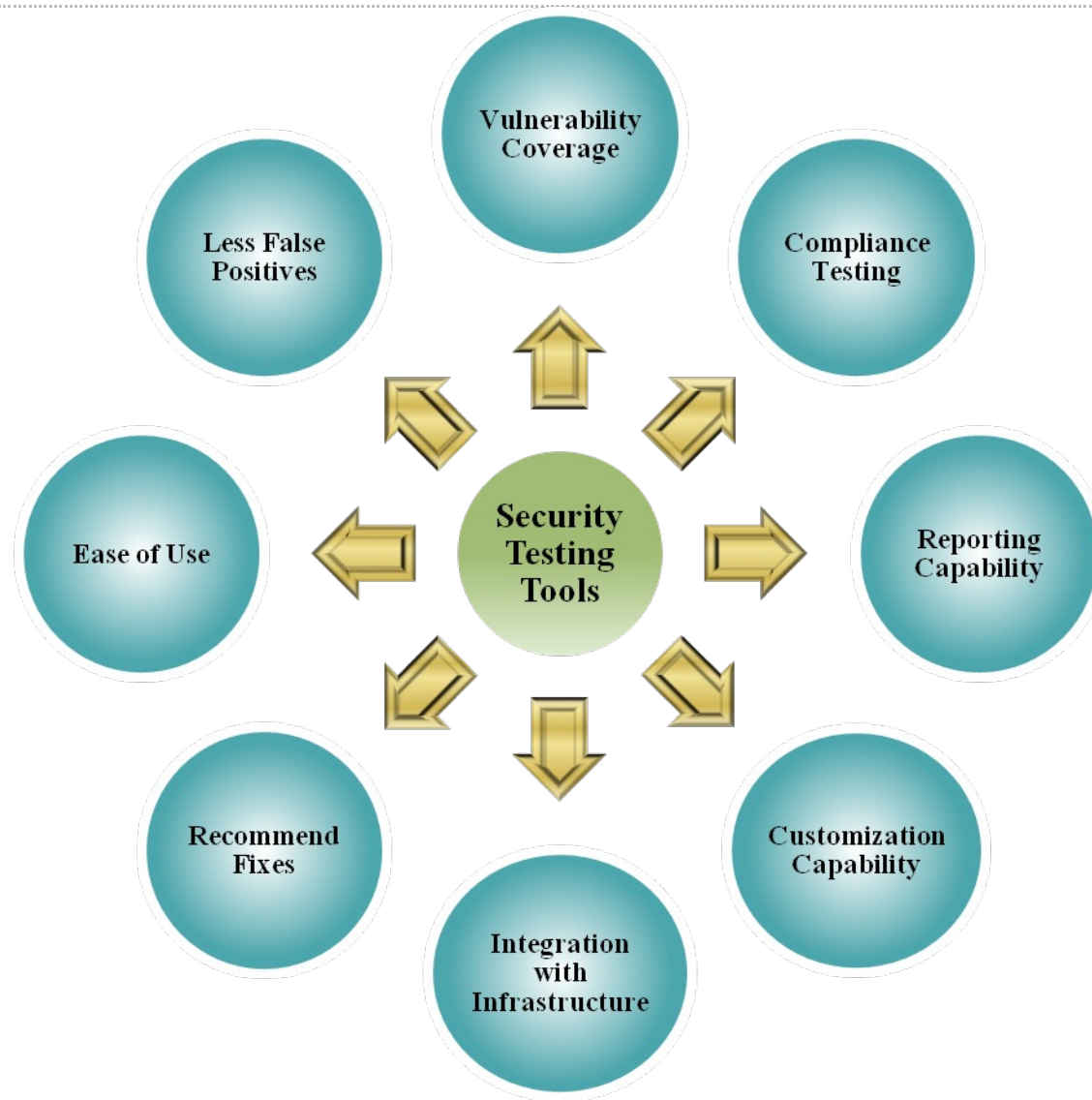
# Risks

- Major change in the application needs rework
- Non Availability of interfaces
- Non availability of Inter dependent modules
- Need to get Developers involved – May require change in existing process

# Tasks



# Tool Selection Criteria



# Best Practices

- **Engage Security Testing Team in early stages of Application Development**
- **Ensure Security is part of the iterative Development Process**
- **Follow the security coding principle**
- **Application Development Team should accept that application security is their responsibility**
- **Knowledge Transfer to clients on Development techniques for secure applications**

# Data Security

## Data Sanitization

- Process of disguising sensitive information in test and development databases by overwriting it with realistic looking but false data of a similar type

## Data Sanitization Techniques

- Encryption/Decryption
- Substitution
- Masking Data
- Shuffling records
- Number variance
- Null'ing out

# Future Security Trends

- Cell phone worms will infect more phones, jumping from phone to phone over wireless data network
- Voice over IP (VoIP) systems will be the target of cyber attacks
- Spyware will continue to be a huge and growing issue
- Security Testing will grow from conventional testing methodology to deeper analysis phase on identifying the traces of malicious code
- Laptop encryption will be made mandatory
- By 2009 , 60 percent of IT organizations will make security vulnerability detection an integral part of their SDLC processes - Gartner

# Questions?





**Cognizant** | *උනේන් හි කැමැත්ත*  
Passion for building stronger businesses



# Thank you

**Subash Newton**

Subash.Newton@Cognizant.com