



Changing Landscape of Application Security



Maninder Bharadwaj

Director, Deloitte Touché Tohmatsu India Private Limited

Recent Media Headlines

Japan's defense industry hit by its first cyber attack

- The Reuters September 19 2011

Lockheed Martin , a major defense contractor to the US government, hit by Security Breach

- Wall Street Journal May 28 2011

Twitter, Facebook Sites Disrupted by Web Attack

- Wall Street Journal Aug 07 2009

Digital Fears Emerge After Data Siege in Estonia

- The New York Times May 29 2007

Pentagon reveals 24,000 files stolen:
- Toronto Star July 15 2011

Sony PlayStation Network Down After Attack

- The New York Times April 25 2011

Google uncovers hacking of personal e-mail accounts of top-notch American officials, military personnel and journalists.

- Daily Telegraph June 06 2011

Iran Fights Malware Attacking Computers

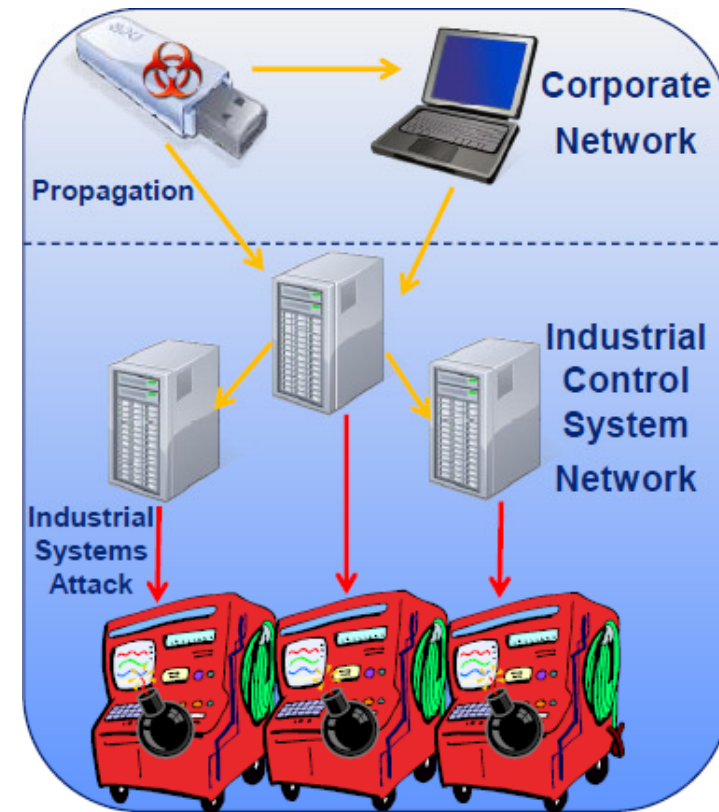
- The New York Times September 26 2010

Stuxnet Virus

In 2010, a security firm based discovered a highly sophisticated computer worm that was specifically conceived to target Industrial Control Systems (ICS), also known as 'SCADA'. The worm has been confirmed to exist at least one year prior.

What went wrong

- Took advantage of four zero-day vulnerabilities not solved by software vendors and utilized a Zero-day USB key autorun
- Exhibited rootkit components to hide from Antivirus software or malware detectors
- Leverages stolen digital certificates
- Exploited in-depth knowledge of SCADA fundamentals that resulted in being able to forge PLC control messages
- Affected primarily two nuclear facilities in Iran; however, a recent report from Symantec stated that there were about 62,000 infected machines world wide.

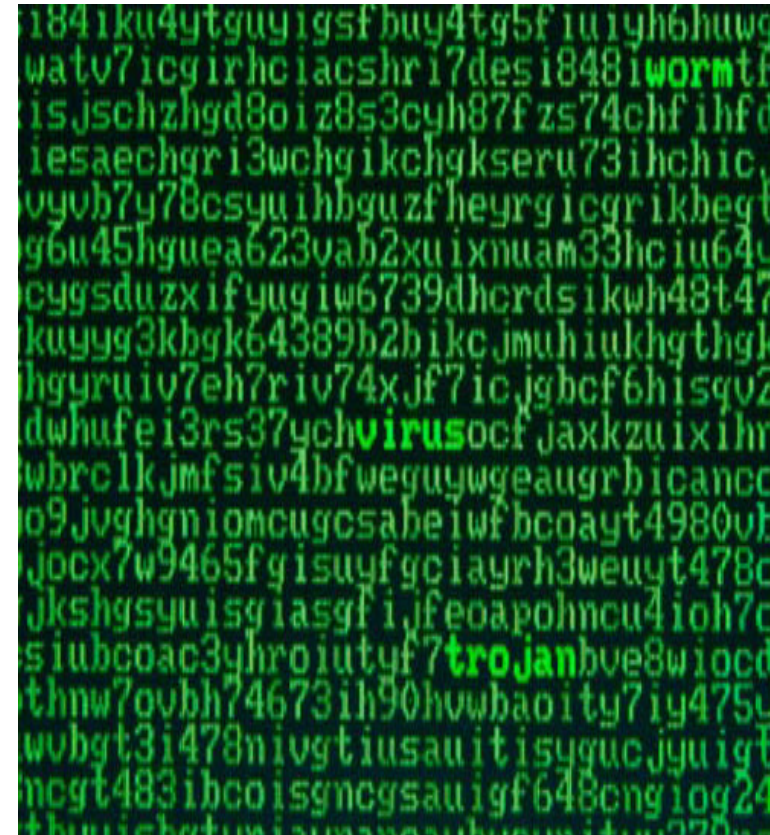


Sony Network: 77 million records hacked

In April 2011, hackers targeted Sony PlayStation Network bringing down the entire network for over a week and compromising 77 million records

What went wrong

- Disguised as a purchase, to prevent being flagged by network security systems.
- Exploited a known vulnerability in the application server to plant software that was used to access the database servers behind the firewalls
- Compromised 77 million users of the network and over 10 million credit card records
- Sony later confirmed that credit card records were partially encrypted, however, all other personal information fields were left unprotected.



Mitsubishi Heavy

On September 20th, Mitsubishi Heavy Industries Ltd., Japan's biggest defense contractor announced that hackers had gained access to its computers.

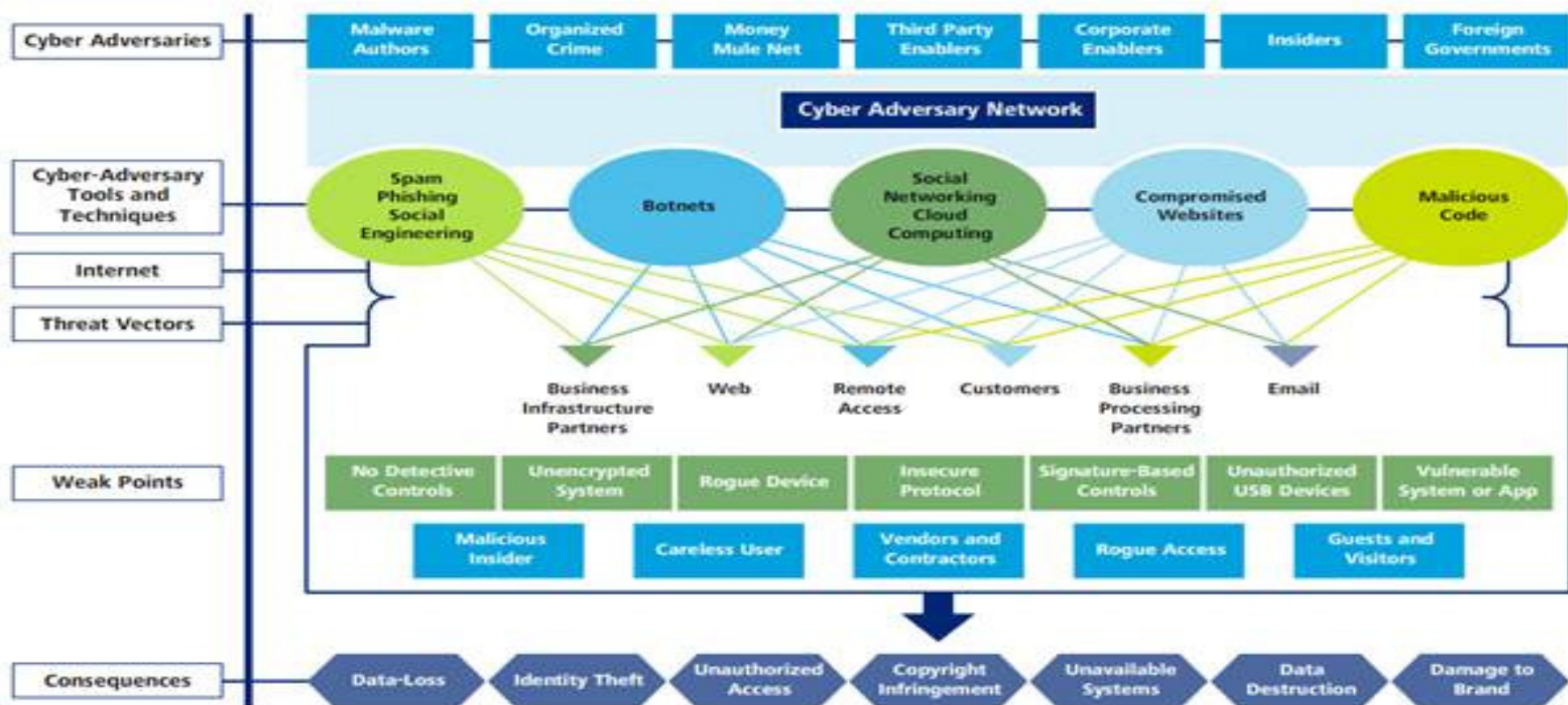
What went wrong

- Used at least 8 different kinds of computer viruses
- Affected 83 computers and servers at 11 locations, including its head office, factories, and R&D centers, were accessed
- Attacked the records in August 2011, Mitsubishi realized the extent of impact just a couple of days back
- Made connections to 14 overseas sites, including at least 20 servers in China, Hong Kong, the United States and India
- This cyber attack took place within a month after Japan's defense ministry urged greater protection against cyber crimes.

The Changing Threat Landscape

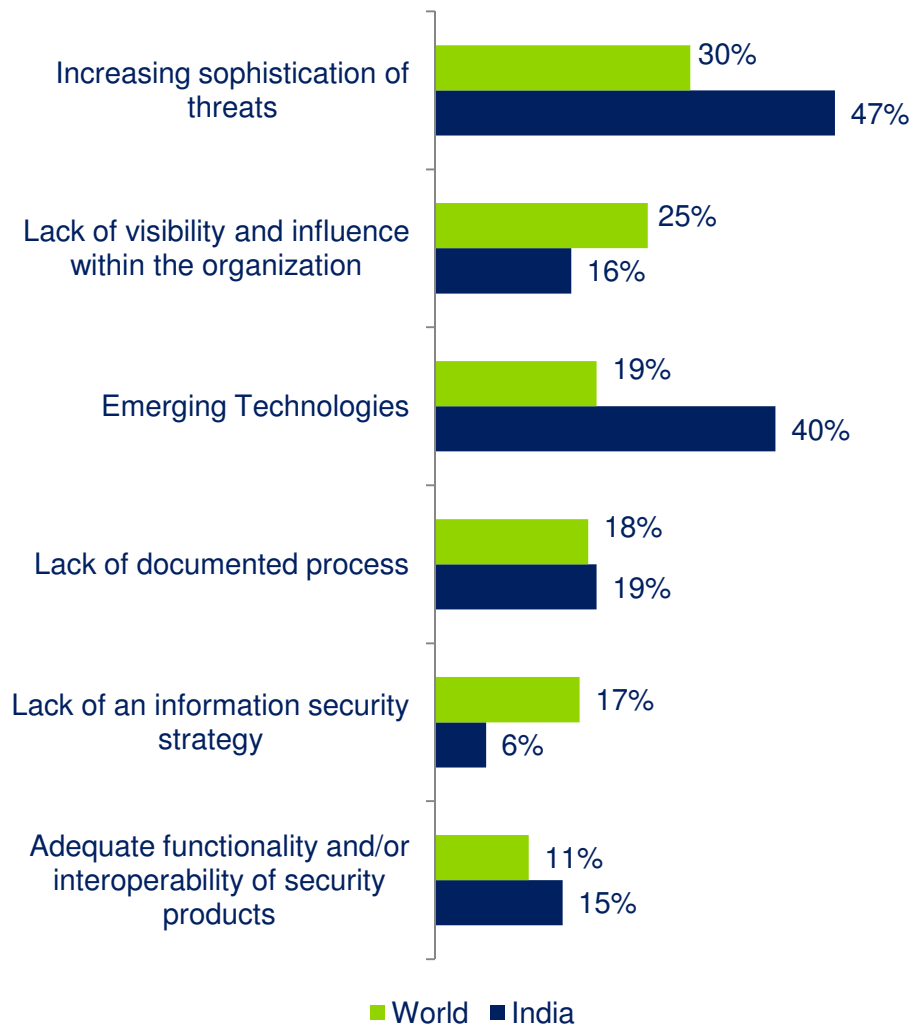
The cybercrime landscape has evolved into a set of highly specialized criminal products and services that are able to target specific organisations using a sophisticated set of malware exploits and anonymisation systems which routinely evade present-day security controls.

The Changing Threat Landscape



Deloitte's Global Security Survey

Major Barriers for an Organization



Top Security Initiatives



Changing Landscape in Application Security

Increasing business reliance on applications...

Increasing number of applications managing confidential information. These applications are the front door to valuable data, data that can be monetized quickly.

Highly distributed and component based...

IT Infrastructure are increasingly distributed, coupled and complex. Emerging technologies and methodologies for organization and description are posing new security threats from the assimilation of information.

Perimeter of the organisation is ever expanding....

Emerging definition of 'trusted users' not only includes users, but also includes external sources such as partners, data providers, third party development/service providers, and support organizations.

Increasing agile, highly integrated functional-specific applications ...

Organisations are employing holistic integration strategies to provide seamless experience to the users as well as reduce the TCO for managing the environment. An integrated application security approach is essential to avoid high cost of source cause analysis and remediation

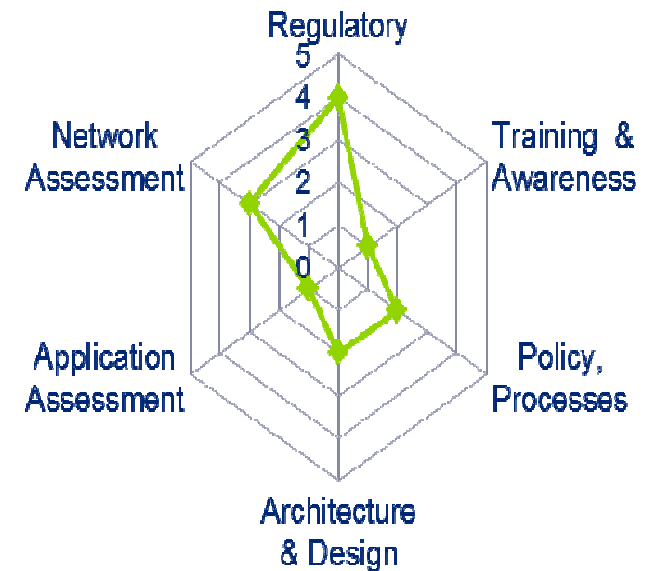
All this and the old issues and challenges still apply...

Applications continue to roll into production with vulnerabilities, many organizations have a backlog of identified vulnerabilities, technology change over time and new vulnerabilities are introduced, newer attacks can bypass traditional security defenses, etc.

Customer Requirements, Compliance Requirements

Customers and other regulatory bodies requires the compliance to their requirements to be demonstrated. Any violation would lead to penalties, reputation damage, penalties and fines.

Where do organizations typically stand? *

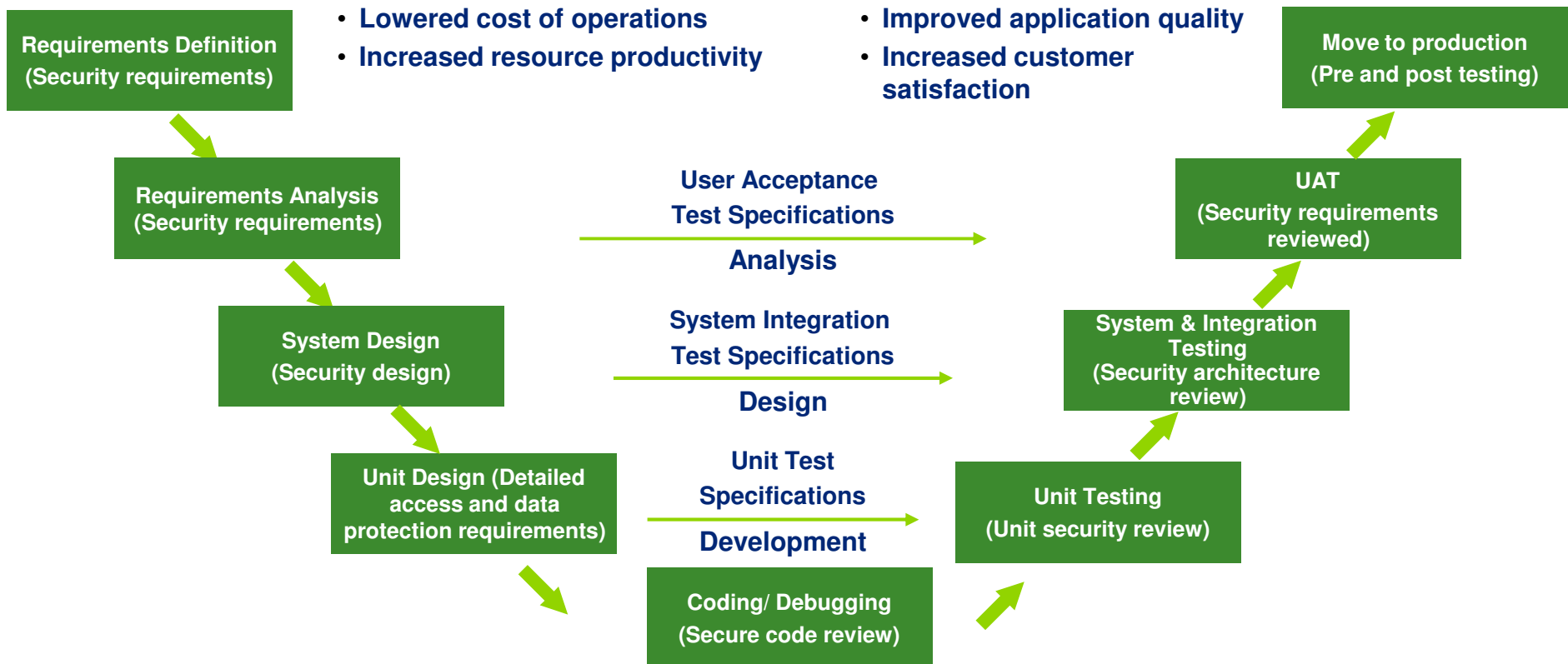


* Based on the study carried out by Deloitte across Organisations and Industries

Core Principles

Integration of security activities throughout the standard systems / application development process enables *timely, risk-based identification and remediation of security vulnerabilities throughout the lifecycle.*

When security is built into the SDLC, results will be...



Key Security Components

Key System Development Lifecycle (SDL) components integrated into an organization's standard SDLC processes enable the organization to understand application risk posture while also identifying and mitigating risks.

Governance

Provides business drivers, project alignment, project demand, prioritization, review, approval, communication plan, stakeholder involvement and KPI.

Secure coding & Security guidelines

Provides technology specific guidelines to assist the application development team

Security architecture review

Security architecture review focuses on indentifying weakness in the design, implementation and security controls

Secure code review

Secure code review focuses on identifying insecure coding techniques and vulnerabilities

Vulnerability testing

Consists of a controlled security test of the IT system & application environment to identify potential external exposures (including web services, etc.)

Risk assessments and remediation

Assessment of risks and implementing remediation solutions is an integral part of an SDL

Metrics and reporting

Essential reporting requirements include developing metrics and reporting capabilities for key risk/performance indicators and measuring program effectiveness and maturity

Solution for Secure Enterprises

Focus on Governance, People, Process & Technology for Securing Enterprises

Methodology					
	Planning	Design	Development	Testing	Sustain
Current state analysis	Criticality assessment	Threat modeling	Potential threat scenarios	Penetration testing	Security development process assessment
	Software development process analysis	Access control analysis	Source code assessment	Functional security testing	
	Risk assessment process analysis	Cost benefit evaluation criteria	Impact assessment	Impact assessment	
Definition	Security standards definition	Potential threat scenarios	Security risk mitigation plan	Security risk mitigation plan	Risk assessment integration strategy
	Security goals definition	Potential impact definition	Integrated testing guidelines		Periodic security assessment activities
	Data classification guidelines	Mitigation guidelines	Training & Awareness		Functional constraints definition
	Security staffing plan	Security test plan definition			Ongoing Training & Awareness
Conformance evaluation	Approvals conformation	Mitigation security controls evaluation	Mitigated system / source Code security evaluation	Mitigated security component evaluation	Functional constraints validation
					Periodic security assessments & Validation
Report	Security requirements traceability matrix	Security risk assessment matrix	Security risk assessment matrix	Security risk assessment matrix	Residual risk report
		Security test plan	Security issues tracking matrix	Security issues tracking matrix	Security Dashboard
Governance	Quality Assurance Change Management & Training				

Secure Enterprise Implementation Approaches

Understanding the pros and cons of for the various implementation options is critical when devising your Secure Enterprise implementation strategy.

	Replace	Overlay	Modular
Definition	Replaces the existing security processes completely	Adds processes, people, and technology on top of the existing security processes	Targeted modifications to an organization's security processes that are rolled out over time
Advantages	<ul style="list-style-type: none"> • Can be done quickly • Includes all aspects to secure the organisation • Clean break from previous security processes 	<ul style="list-style-type: none"> • Can be done quickly • Includes various aspects of secure enterprise approach • Can be rolled out over time 	<ul style="list-style-type: none"> • Tailored to organization's existing requirements for safeguarding organisations • Prioritizes changes • Can be rolled out over time • Minimal disruption
Disadvantages	<ul style="list-style-type: none"> • Can be very disruptive • Can be expensive • May require extensive help from third party • May not align with organization's culture 	<ul style="list-style-type: none"> • Can be disruptive • May not address root causes • Can be expensive 	<ul style="list-style-type: none"> • Can take a long time to fully implement • Can be expensive

Key Success Factors

Governance

- Assign responsibilities and identify players
- Streamline conflicting and overlapping regulations and standards
- Leverage required regulations to improve business process
- Requires identifying and mapping operational, financial, and regulatory risks

People

- Appropriate application security awareness training across the organization
- Independent self assessment procedures at various system development and maintenance check points
- Effective mechanism for communication and escalation of security issues
- Periodic physical space review procedures enabling discovery of potential information leakage
- Procedures to avoid single point of failures (talent and program management)

Process

- Integrates suitably to the organization's risk management program
- Provides impact analysis and risk measuring procedures for software security vulnerabilities
- Provides procedural enhancements for organizations to react adequately to the emerging internal and external threats
- Lifecycle driven approach for consolidating and tracking of vulnerabilities in new, proposed, and implemented technology and software solutions
- Requires and enables development of a mitigation plans

Technology

- Leverage appropriate toolkits, technologies and methodologies for security assessments on design, source code, and software components
- Vulnerability assessments customizable to organization's changing technology landscape
- Capable of both automated and manual security assessments in executing black-box, gray-box, and white-box approaches
- Includes threat & vulnerability information gathering mechanism pertaining to software developing technologies
- Vulnerability tracking and mitigation strategies reporting follow a well defined, consistent, and broad approach

People- Training and Awareness

People progress through the levels of learning curve must be continuously supported through the following:

Change Management

- People Risk & Impact Management
- Stakeholder and Leadership Engagement
- Communication
- Learning
- Tools and Training
- Capability Transfer

Communication plan

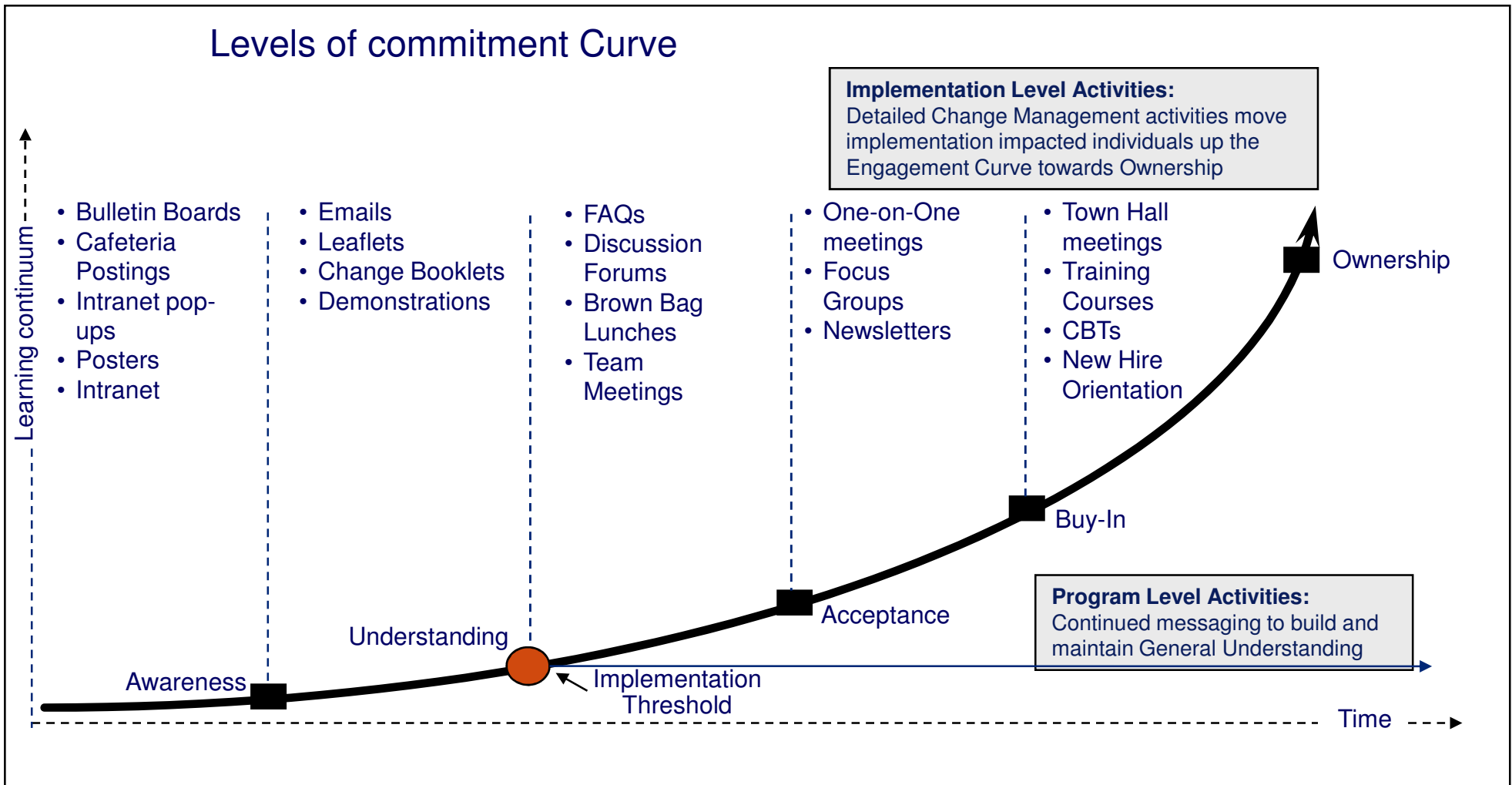
- Communication Plan for the employees, division, and enterprise
- Provide focused messages on specific objectives, such as creating awareness,
- Deliver messages through various media channels

Role-specific training

- Tailored made training program to meet the needs of specific roles
- Identify objectives
- Propose delivery models
- Develop content
- Seek feedback and enhance delivery model
- Provide support

People- Learning Continuum

The communication around Security Awareness is designed to support employees with appropriate messages and move key stakeholders through the “Stages of Commitment”.



People- Training and Awareness

Develop Training Content

Develop customized training content for the target audience identified by the client.

Deloitte.

Fundamentals of Application Security

Slide 1

Slide X

Slide Y

Security Principles

Principles are important in defining security requirements, making architecture and implementation decisions and identifying possible weaknesses in systems

Principles	Practices
Reduce Attack Surface	<ul style="list-style-type: none"> Identify and remove unnecessary services in the application Minimize external dependencies on the host and the network Do not expose unnecessary interfaces from the application Reduce the number of entry points of the application
Defense in depth	<ul style="list-style-type: none"> Use multiple layers of defense to control access to the application Do not rely on one-size-fits-all solutions Identify and monitor application operations Identify the privileges of users who will use the application Verify the actual privileges required by the application to carry out application operations Determine user roles based on the above information
Separation of privilege	<ul style="list-style-type: none"> Granularity of user rights should be high enough for the software to be secure How are administrator actions logged? Can the administrator read/edit his own logs?
Least privilege	<ul style="list-style-type: none"> Grant privileges at the point where it is necessary Verify credentials of users and components at each step Do not take for granted that caller has access to the accessed resource
Resistant to Trust	

Managing Application Security

Five core components required to manage application security as depicted below:

Management is concerned with risk, compliance, and financial bottom line

Develop Demos

Practical demo based on common attack scenarios caused due to insecure coding.

```
#include "stdafx.h"
#include "Form1.h"
#include "MainPage.h"
#include "Common.h"
#include <windows.h>

using namespace System;
using namespace System::Net::Sockets;
using namespace System;
using namespace System::Windows::Forms;
using namespace Demo;

//Form1 *pForm1 = NULL;

int APIENTRY _twinMain(HINSTANCE hInstance,
                    HINSTANCE hPrevInstance,
                    LPSTR lpCmdLine,
                    int nCmdShow)
{
    System::Threading::Thread::Start( new Thread( new ApartmentSTA
    Common::InitializeSocketLib(VC);

    //SetCurrentDirectory((System::IO::Path::Combine(System::IO::Path::DirectoryName(Application::ExecutablePath)),
    TCHAR strModuleName[256] = _T("Demo.exe");
    DWORD dwFileLength = 0;
    TCHAR strPathSep[256] = _T("\\");
    TCHAR strFileName[256] = _T("Common.h");
    if (NULL != strFileName)
    {
        (*strFile) = _T("\\");
        //Now, strModuleN contains the directory components
        //SetCurrentDirectory(strModuleN);
    }
    Form1 *pForm1 = new Form1();
    Application app;
    Application.Run(pForm1);
    return 0;
}
```

Develop Quizzes

Develop quiz to assess the understanding of target audience.

Deloitte.

Secure Coding Workshop
Post - Survey Form

Drive value through secure application development
How was the session? Your suggestions and comments are most appreciated and will be taken into careful consideration as we plan future sessions.

Name (Optional): _____
Group Name: _____

Please circle the appropriate number using the following scale:
1 = Poor; 2 = Fair; 3 = Good; 4 = Very good; 5 = Excellent

Content	1	2	3	4	5
Presenter -	1	2	3	4	5
Overall session evaluation	1	2	3	4	5

Years of Development Experience

1-3 Years 3-5 Years 5-10 Years Over 10 Years

Which of the following programming languages do you currently program in?

Java C/C++ C# Perl/PHP

1) what of the following integer operations cannot result in an integer overflow?
A. Multiplication
B. Division
C. Unary operation
D. Right shift

2) vulnerabilities resulting from race conditions can be mitigated by making concurrent race windows:
A. as small as possible
B. critical sections snatched
C. snatched
D. mutually exclusive

3) which statement declares p as a constant pointer to type T?
A. p * const T;
B. T * const p;
C. T const * p;
D. p const * T;

Process- Develop policies and processes

Developing policies and processes will help enable an overall secure enterprise by providing structured approach and clearer objectives to all the stakeholders

Methodology					
	Planning	Design	Development	Testing	Sustain
Current state analysis	Criticality assessment	Threat modeling	Potential threat scenarios	Penetration testing	Security development process assessment
	Software development process analysis	Access control analysis	Source code assessment	Functional security testing	
	Risk assessment process analysis	Cost benefit evaluation criteria	Impact assessment	Impact assessment	
Definition	Security standards definition	Potential threat scenarios	Security risk mitigation plan	Security risk mitigation plan	Risk assessment integration strategy
	Security goals definition	Potential impact definition	Integrated testing guidelines		Periodic security assessment activities
	Data classification guidelines	Mitigation guidelines	Training & Awareness		Functional constraints definition
	Security staffing plan	Security test plan definition			Ongoing Training & Awareness
Conformance evaluation	Approvals conformation	Mitigation security controls evaluation	Mitigated system / source Code security evaluation	Mitigated security component evaluation	Functional constraints validation
					Periodic security assessments & Validation
Report	Security requirements traceability matrix	Security risk assessment matrix	Security risk assessment matrix	Security risk assessment matrix	Residual risk report
		Security test plan	Security issues tracking matrix	Security issues tracking matrix	Security Dashboard
Governance	Quality Assurance Change Management & Training				



- Formulate organization policies
- Define business processes
- Design process flows
- Establish roles and responsibilities
- Identify applicable regulatory standards and industry benchmarks
- Establish guidelines
- Provide a checklist

Process- Develop policies and processes

Identify Areas to Focus Upon

Identify different application security areas to focus upon to deal with common programming errors of the programming lang.

- #1: Input/output Validation
- #2: Authentication
- #3: Logging (Error and Exception Management)
- #4: Cryptography
- #5: File Handling
- #6: Multithreading
- #7: Memory Management
- #8: System/Process Integration
- #9: Network and Inter Process Communication
- #10: Interrupt and Signals
- #11: Secure Development Processes
 - a. Security Requirements Sample
 - b. Security Design consideration
 - c. Security Test Cases (Misuse Cases)
 - d. Security Testing (tools/techniques)

Develop Table of Contents

Develop customized table of contents as per the requirement and confirm with the client.

Table of Contents

1.	INTRODUCTION	3
1.1.	Intent	3
1.2.	Audience	3
1.3.	Scope	3
1.4.	Implementation Strategy	3
2.	DESCRIPTIONS OF THE SECURE CODING GUIDELINES	4
#1:	General Coding Guidelines	4
#1:	Cryptography	4
#2:	File Handling	4
#3:	Multithreading	4
#4:	Memory Management	5
#5:	System/Process Integration	5
#6:	Network and Inter Process Communication	5
3.	CHECKLISTS FOR THE SECURE CODING GUIDELINES.....	6
#1:	Common C++ Coding Guidelines Checklist	6

Technology- Tools

Multiple tools that are customizable to organization's changing technology landscape and are Capable of both automated and manual security assessments in executing black-box, gray-box, and white-box approaches. The list of such tools* is as below:

- Axivion Bauhaus Suite .
- Black Duck Suite .
- BugScout
- CAST Application Intelligence Platform
- Checkmarx
- Coverity
- DevPartner
- DMS Software Reengineering Toolkit
- Compuware
- GrammaTech
- Imagix 4D

- HP Fortify Source Code Analyzer
- Lattix, Inc.
- LDRA Testbed
- Logiscope
- MALPAS
- Micro Focus
- Ounce Labs
- Optimyth checkKing
- Parasoft
- Klocwork Insight
- Intel
- JustCode

- Polyspace
- ProjectCodeMeter
- Rational Software
- ResourceMiner
- SofCheck Inspector
- Software Diagnostics
- Sotoarc/Sotograph
- Syhunt Sandcat
- Understand
- Veracode
- JSP, ColdFusion, PHP and Objective-C
- Visual Studio Team System

*Deloitte does not recommend any specific tool from the list above

Questions?



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

This material and the information contained herein prepared by Deloitte Touche Tohmatsu India Private Limited (DTTIPL) is intended to provide general information on a particular subject or subjects and is not an exhaustive treatment of such subject(s). None of DTTIPL, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering professional advice or services. The information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this material.

©2011 Deloitte Touche Tohmatsu India Private Limited