#### HP World 2002 - Session 7084

## Managing Risk: Architecting The Secure Enterprise

Stuart Gavurin
Managing Principal

Sunil Misra Managing Principal

Unisys



## **Agenda**

- Security Mindset
- Security Framework
- Planning Effort Approach
- Solution Definitions
- Key Results
- Case Studies



## Session Objectives

- Gaining a basic insight into security issues and terminology
- Defining how to align business priorities with security architecture
- Identifying flexible security alternatives and solutions that provide the appropriate level of protection



## Why Security? Many Focus on Fear, Uncertainty, and Doubt...

- Enterprises engaged in Web commerce are three times as likely to experience security breach (PricewaterhouseCoopers)
- Financial losses from computer crime \$80B by 2003 (FBI)
- 62% of organizations responding to CSI survey reported security breaches within last 12 months



## ... but the Truth is that CXO's:

- Are concerned about their organization's ability to proactively manage risk in their environment
- Find themselves never quite getting a handle on the issues that most impact the business - everything seems tactical
- Never quite feel that security technology investments maximize the efficiency and effectiveness of investments in security technology
- Are seeking to build a framework and develop a strategy for addressing security from an enterprise perspective

Conference & Expo

Business executives require a practical framework and architecture access to make <u>informed decisions</u> regarding the security posture of their environment

### Motivations for Security Planning



**eBusiness** 

**Customer Self Service** 

Globalization

Expectation Of 24x7 Operation

Increased Dependence on 3<sup>rd</sup> Parties

More Real-Time Transactions

Increased Dependence On Complex Technology

#### **Changing Environment**

New Government Regulations Emerging Insurance Requirements

New Competition for Customers

Loss of Key Personnel to RIFs, Retirement

#### **Changing Threats**

Technology Failure

Current Events

Risks of Global Connectivity



## What has to change in the security model and mindset?

- Focus on the business not on technology eBusiness is still a core strategy
- It's okay not to be perfect just balance exposure and risk against investment - "proper level of investment"
  - Vulnerabilities will always exist understand them to guide a strategic path
  - Don't feel guilty
- Encourage, enable access; Don't confuse the concepts of access and trust!!!
- A quickly done plan eases angst and establishes the basic roadmap - the 80/20 rule!!
- Security model must adapt to the world beyond our control that's the point

## **Effective Security**

What has
to be
considered
for an
effective
security
plan?



#### Risk

Vulnerability, threats and impact



#### Access

Asset privacy and utilization



#### **Trust**

Confidence and information integrity

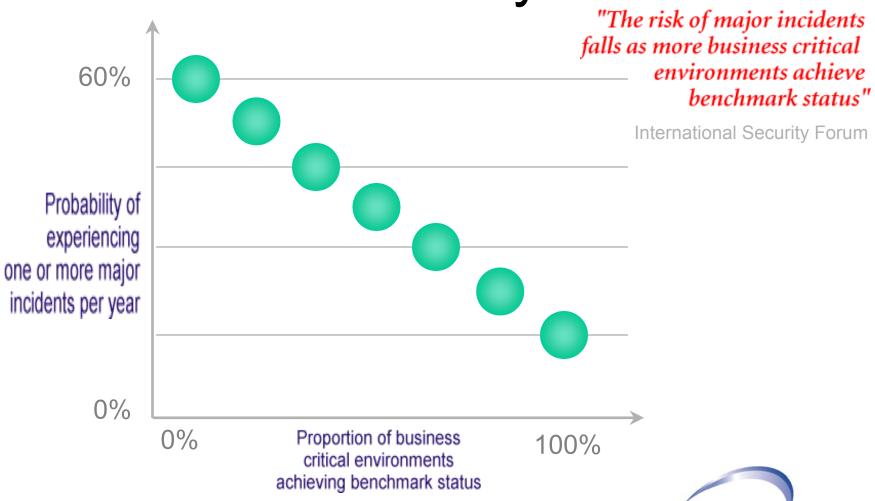


#### **Compliance**

Policy, best practices and legislation



## Does Security Work?



Conference & Expo

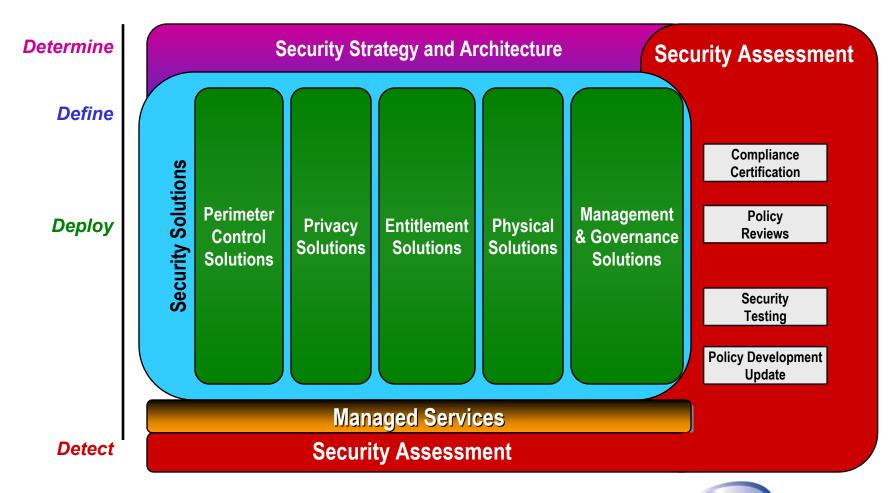
### The 4-D Model

#### **Security Assessment** Monitor/Maintain Risk and Threat Policy Security Audit Determine Organization Intrusion & Virus Mgt. Technology **Incident Response** Risk Profile Fraud Detection **Security Training** Risk Access **Detect Define** Trust Compliance **Security Infrastructure Security Policy** Standards/Procedures **Implementation** Security Architecture **Perimeter Solutions Technology Specifications Entitlement Solutions Technology Selection Deliver Physical Solutions** Organizational Specifications Management & Governance **Privacy Solutions**

HP WORLD

Conference & Expo

### Context for 4-D





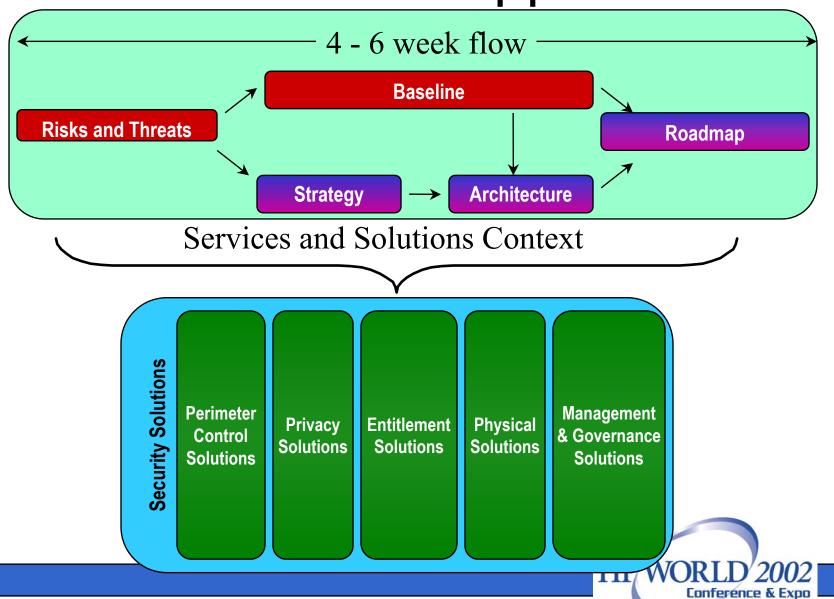
## Defining an Adaptive Roadmap

**Determine Security Strategy and Architecture Security Assessment Define** Compliance Combine the planning work with a real understanding of the Certification current environment **Policy** •Accelerate the effort - keep it under 6 weeks. Let the result Reviews define when the details should be completed. Focus on services and bundled solutions; not specific Security technologies or policies **Testing** •Set a 2-3 year direction that will guide you as needs arise, **Policy Development** don't focus on designing it all Update Detect

**Security Assessment** 



## Accelerated Approach



## Strategy and Architecture

#### **Risks & Threats**

Discover - Gathering information on business policy and regulatory environment; Identifying the enterprise business model, constituents, and necessary business assets. Analyze - Identify the relevant threats from the Discovery stage; Examine how other enterprises have coped with similar threats: Determine strengths and weaknesses of current security policies and measures. Perform vulnerability analysis for identified threats; Perform risk analysis for those vulnerabilities.

Model - Identify information security requirements for enterprise; Perform gap analysis; Determine high level end state for enterprise security. Describe the desired end state for information security organization and infrastructure.

- Information Security Context
- Information Risk Assessment

#### **Baseline**



#### Strategy

**Outputs** 

Prioritize Risk and Threat Assessments towards specified company goals

Identify and analyze measures to close the gap between information security requirements and current capabilities

#### **Architecture**

#### **Security Requirements**

Create detailed technical specifications and test plans for all of the technology components of the target security environment.

Define and document the processes by which the technical security mechanisms will be managed, monitored and audited.

Draft the information security policies that were identified as needed within the security policy and process framework.

#### Roadmap

Our three year architecture blueprint will be mapped out here and a timeline for implementation recommended.

#### **Outputs**

- Enterprise security gap analysis
  - Detailed Risk and Threat assessment

#### **Outputs**

- Security Specification Document

#### **Outputs**

A detailed plan of action for achieving the targeted security environment



### Perimeter Control Solutions

Protecting the organization from risks of downtime, loss of data, cash or other critical assets from threats that are external to the enterprise (e.g., Internet, business partner networks)

Service	Definition / Key Characteristics
Network Partitioning Services	Connectivity and security technologies needed to isolate networks from other networks     Technology to create DMZs     Predictive blocking
Virus & Content Control Services	Technologies for improving data and system integrity by preventing or controlling the transmission of hostile applications



## **Entitlement Solutions**

Entitlement is establishing the rules and infrastructure around trust and the consequential permissions.

Service	Definition / Key Characteristics
Authentication Services	<ul> <li>Verification of the identity of communicating endpoints</li> <li>Each party presents "proof of identity" to the other party</li> <li>Each party then associates the communication "session" with the identity of the other party until the session ends</li> </ul>
Authorization Services	<ul> <li>Associates an identity with the permissions assigned to it</li> <li>Permissions are often recorded in a structured data store</li> <li>Permissions can be User-based or Group profile-based (role-based)</li> <li>Typically depends on a Directory Service to hold information</li> </ul>



## **Privacy Solutions**

Privacy is ensuring that information is only shared between parties with the appropriate rights. Participants must feel safe in balancing trust and need.

Service	Definition / Key Characteristics
Encryption Services	Technologies for storing or transmitting information in a such a way that it can only be read by a designated party or parties
Privacy Governance Services	<ul> <li>Formal risk management approach for privacy</li> <li>Privacy training</li> <li>Third-party verification services</li> </ul>



## Management and Governance Solutions

Policies, Standards, and Guidelines to oversee the execution and response of security solutions. Areas addressed include:

- Governance Organization
- Incident Management
- Training
- Measurements and Metrics
- Vulnerability and Security Assessment Cycles
- Standards Maintenance and Stewardship
  - Technology
  - Physical

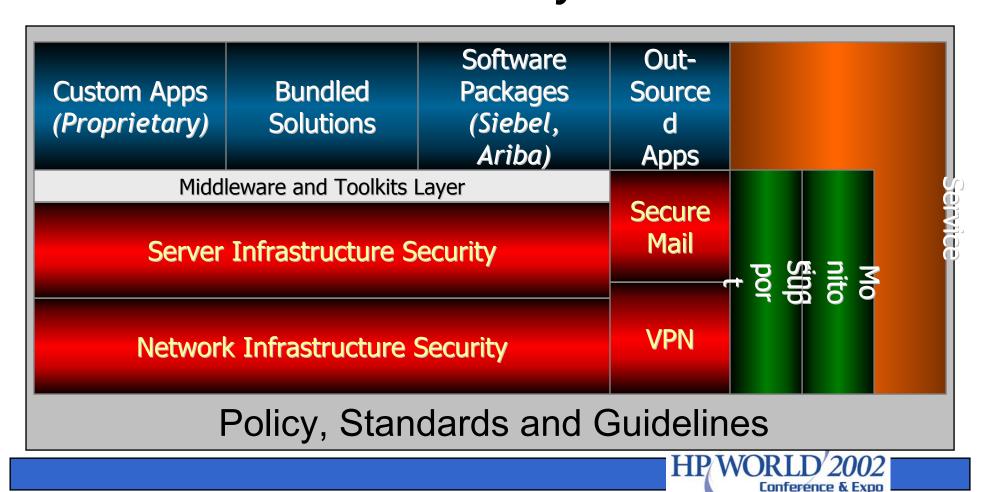


## Result of Process Must Include...

- Security Technology Architecture
  - Aligned to business
  - Mirrors budget and resource realities
- Management and Governance Architecture
- Roadmap
  - Reflects priorities
  - Contains communications plan
  - Includes budget estimates



# Technology Security Architecture - ... employs a unified approach to security



### Partners Matter

Focusing On Reality Means Staying Away from Theory





















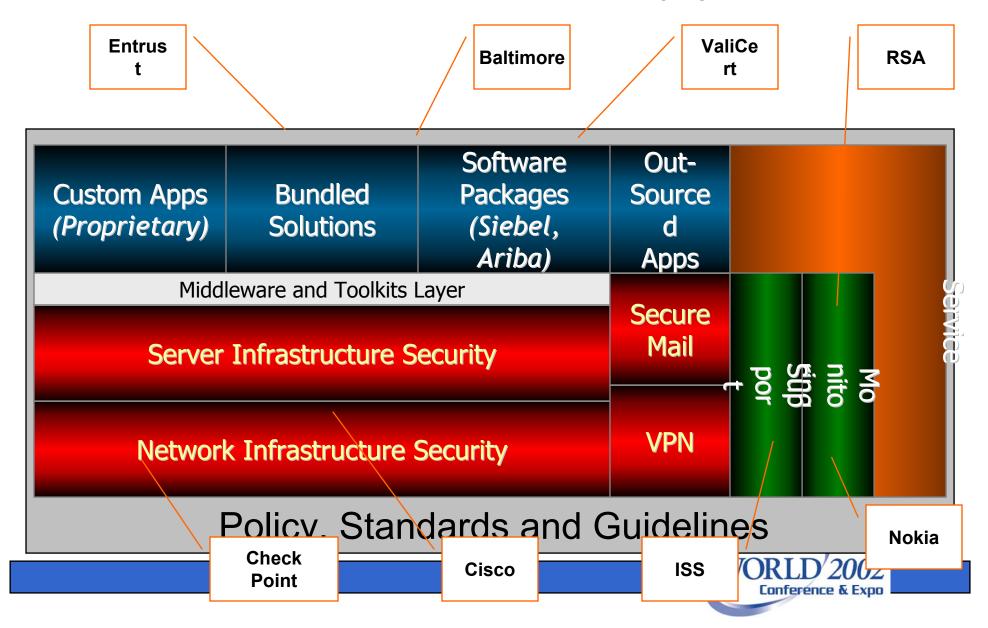








## Partners Matter (2)



## **Case Studies**



## Final Thoughts & Questions

- Solutions and services over technologies
- Fast track the planning process
  - Reduce your need for perfection and get moving
- It's about the business not about cyber warfare

#### Contact Information:

- Stu Gavurin stuart.gavurin@unisys.com
- Sunil Misra sunil.misra@unisys.com