Developing the Corporate Security Architecture

www.avient.ca

Alex Woda
July 22, 2009
Avient Solutions Group is based in Markham and is a professional services firm specializing in infrastructure, architecture, applications security and project management.
Key Points

- Why do we need a Corporate security architecture?
- Enterprise Architecture Frameworks
- Examples of security architecture
- Designing and Implementing a Security Architecture
- How to assess the security architecture
Information Security Challenge

Change in Infrastructure

Change in Info-structure

Value Based Management
Privacy & Security

Trust and Truth

Change in the Nature of Work

Changes the Nature of Risk

Key Performance Indicators:
Revenue, Profitability, Cash flow, Value creation
Business Drivers

- **Government Regulations and Audits**
  - Sarbanes Oxley
  - Bill C-198
  - PIPEDA Bill C-6

- **Industry Security Regulations**
  - Payment Card Industry Data Security Standards
  - Open Web Application Security Project (OWASP)
  - ISO 17799, ISO 27002

- **Business Relationships**
  - Outsourced services
  - Supply chain integration
  - Remote access to internal systems
Technology Drivers

- New Technologies and Infrastructure
  - Purchased applications
  - Integration of systems

- New information collection and storage
  - Sensitive data and encryption
  - Data leakage

- Cloud Computing
  - Web based access to applications
  - Third party control

- Malicious code
  - Trojans, viruses
  - Vulnerabilities in software

- External attack methods
  - Cross site scripting
  - Buffer overflows
  - Memory parsers
Information Security Stakeholders

- Shareholders
  - Risk Management
  - Trust and Safety
  - Investment Protection

- Customers
  - Privacy Protection
  - Trust and Safety
  - Safeguards

- Employees
  - Health and Safety
  - Privacy protection
  - Trust

- Management
  - Information Integrity
  - Confidentiality
  - Intellectual Property protection
  - Cost management

- Information Security Management
  - Network connections
  - Service Agreements
  - Continuity Planning

- Suppliers
  - Laws and Statutes
  - Security and Privacy
  - Compliance management

- Regulators
Enterprise Architecture Frameworks

- **TOGAF Enterprise Architecture Framework**
  - Integration of security into different domains
  - Architecture development method available

- **Zachman Enterprise Architecture Framework**
  - Set of models to represent WHAT, HOW and WHERE
    - Complete the design with WHO, WHEN and WHY
  - Systematic description of business models, processes, data requirements
  - Set of standard artifacts to foster communication and collaboration
  - Security Architecture called SABSA

- **Vendor Defined Architecture**
  - IBM Architecture Methods
Security Architecture Frameworks

- TOGAF Version 9
- SABSA - Sherwood
- ISO 17799 security framework
- Agile Security Strategies
- ISO 13335 - security practices
- ISO 7498-2
- NSA standards - Gold for Win2K
- Cisco SAFE
TOGAF and Security

- Security domain is pervasive across the other domains
- Areas of focus:
  - Authentication
  - Authorization
  - Audit
  - Assurance
  - Availability
  - Asset Protection
  - Administration
  - Risk Management
Security as part of Enterprise Architecture

Integrated with Enterprise Architecture
- Business architecture
- Information architecture
- Application architecture
- Technology architecture
- Security architecture

Security participation in project teams

Creation of security analysis and design plans for each significant project
Conceptual Security Framework

Example of a Security Architecture Model

IBM has a model for Security Architecture. This is illustrated in the following diagram. The Security Services correspond to the logical Components within the IT Architecture. As such there is a natural linkage between the two Architectures.
## Enterprise Architecture - A Framework

<table>
<thead>
<tr>
<th>Scope (Contextual)</th>
<th>Planner</th>
<th>Function (How)</th>
<th>Network (Where)</th>
<th>People (Who)</th>
<th>Time (When)</th>
<th>Motivation (Why)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enterpise Model (Conceptual)</strong></td>
<td><strong>Owner</strong></td>
<td><strong>System Model (Logical)</strong></td>
<td><strong>Designer</strong></td>
<td><strong>Technology Model (Physical)</strong></td>
<td><strong>Builder</strong></td>
<td><strong>Detailed Representations (Out-of-Context)</strong></td>
</tr>
<tr>
<td>Data (What)</td>
<td>Data Type</td>
<td>Functionality</td>
<td>Location</td>
<td>Organization</td>
<td>Event</td>
<td>Objective</td>
</tr>
<tr>
<td><strong>Enterpise Designer</strong></td>
<td>Data = Field</td>
<td>Function = Process</td>
<td>Location = Node</td>
<td>People = Organization</td>
<td>Time = Event</td>
<td>End/Mean = Goal/CSF</td>
</tr>
<tr>
<td><strong>System Model (Logical)</strong></td>
<td>Data Type</td>
<td>Functionality</td>
<td>Location</td>
<td>Organization</td>
<td>Event</td>
<td>Objective</td>
</tr>
<tr>
<td><strong>Technology Model (Physical)</strong></td>
<td>Data Type</td>
<td>Functionality</td>
<td>Location</td>
<td>Organization</td>
<td>Event</td>
<td>Objective</td>
</tr>
<tr>
<td><strong>Detailed Representations (Out-of-Context)</strong></td>
<td>Data Type</td>
<td>Functionality</td>
<td>Location</td>
<td>Organization</td>
<td>Event</td>
<td>Objective</td>
</tr>
<tr>
<td><strong>Functioning Enterprise</strong></td>
<td>Data Type</td>
<td>Functionality</td>
<td>Location</td>
<td>Organization</td>
<td>Event</td>
<td>Objective</td>
</tr>
</tbody>
</table>

### Planner
- **Entity** = Class of Business Thing
- **Function** = Class of Business Process
- **Node** = Major Business Location
- **People** = Major Organizations
- **Time** = Major Business Event
- **End/Mean** = Major Bus. Goal/Critical Success Factor

### Owner
- **Ent** = Business Entity
- **Proc.** = Business Process
- **Node** = Business Location
- **People** = Organization Unit
- **Time** = Business Event
- **End** = Business Objective

### Designer
- **Ent** = Data Entity
- **Proc.** = Application Function
- **Node** = IS Function
- **People** = Role
- **Time** = System Event
- **End** = Structural Assertion

### Builder
- **Ent** = Segment/Table/etc.
- **Proc.** = Computer Function
- **Node** = Hardware/System Software
- **People** = User
- **Time** = Execute
- **End** = Condition

### Sub-Contractor
- **Ent** = Field
- **Proc.** = Language Strut
- **Node** = Addresses
- **People** = Identity
- **Time** = Interrupt
- **End** = Sub-condition

### Functioning Enterprise
- **Data**
- **Function**
- **Network**
- **Organization**
- **Schedule**
- **Strategy**

---

**John A. Zachman, Zachman International (810) 231-0531**
### Zachman Based Security Architecture (SABSA)

<table>
<thead>
<tr>
<th>Level</th>
<th>Data (What)</th>
<th>Function (How)</th>
<th>Network (Where)</th>
<th>People (Who)</th>
<th>Time (when)</th>
<th>Motivation (why)</th>
<th>Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contextual</td>
<td>Identify general nature of data (personal, confidential, financial, critical) Collection Methods</td>
<td>Business driven information security management program</td>
<td>Business field operations management Interfaces to trading partners – Data collection and usage (Sensitivity)</td>
<td>Stakeholders, users, external parties (Privacy, Sensitivity)</td>
<td>Stakeholders, users, external parties (Privacy, Sensitivity)</td>
<td>Stakeholders, users, external parties (Privacy, Sensitivity)</td>
<td>Charts 1, 2 and 3 of TRA High level PIA</td>
</tr>
<tr>
<td>Conceptual</td>
<td>Business Continuity Management Identify data of sensitive or personal nature (Privacy, Integrity)</td>
<td>Identify sensitive and critical Processes and resources Risk identification</td>
<td>Location and network protection requirements (firewalls, encryption)</td>
<td>User authentication and authorization requirements Privacy impact</td>
<td>Availability and recovery requirements Service Levels</td>
<td>Availability and recovery requirements Service Levels</td>
<td>Identify specific assets and functions at risk Vulnerability analysis Identification of security mechanisms and components (PKI, encryption)</td>
</tr>
<tr>
<td>Logical</td>
<td>Security requirements for Personal and Critical data fields (Isolation, edits, encryption)</td>
<td>Security requirements for sensitive processes (logging, access control)</td>
<td>Middleware security and data transfer security requirements</td>
<td>Access to functions and transactions Security Administration requirements</td>
<td>Business and system impact analysis When is security enforced?</td>
<td>Business and system impact analysis When is security enforced?</td>
<td>Determine level of protection required for assets, functions and data (accepted risk) Chart 4 &amp; 5 of TRA Complete PIA Select security products</td>
</tr>
<tr>
<td>Physical</td>
<td>Database security mechanisms File security Audit trails and log security</td>
<td>Security components, objects and mechanisms</td>
<td>Network communication security mechanisms</td>
<td>Security interface for users and administrators Authentication mechanism</td>
<td>Security logging, access control, security reports Backup plans</td>
<td>Security logging, access control, security reports Backup plans</td>
<td>Integration of security components and mechanisms Security test strategy and test plans</td>
</tr>
</tbody>
</table>

**Avient Solutions Group Inc.**
### Security Building Blocks

**Security Policy**
- A security policy outlines an organization's position on security issues. It must be endorsed and supported by Management.
- A good security policy can be simply stated, easily understood and in a form that can be widely communicated.

**Security Standards**
- Security standards make specific mention of technologies, methodologies, implementation procedures and other details.
- It is used by the enterprise to implement the security policy.

**Security Processes**
- Processes are created and implemented with respect to policies and standards.
- Part of the process is an assessment of existing process to ensure business needs are still met.

---

**THE SECURITY LIFECYCLE**

- **Policy**
- **Standards**
- **Processes**
  - Risk Assessment
  - Implementation
  - Audit
  - Administration
Security Architecture Foundation Deliverables

- Risk Management Templates and Guidelines
  - Threat risk assessment process
- Privacy Management guide and forms
- Enterprise security architecture vision
- Security Architecture Design Document templates
- Technical security standards - Baseline
- Project team training program
- Enterprise security architecture migration plan
Risk Assessment Methods

- Spans across all domains and is applied in context
- Formal methods and deliverables must be used
- Should be facilitated or reviewed by security experts
- Industry Standards (samples)
  - Operationally critical threat asset vulnerability evaluation (OCTAVE)
  - NIST SP 800 Threat risk assessment guide
  - New Zealand / Australia AZ/NZS 4360 method
  - IRM, ALARM
Threat Risk Assessment Process

Planning
- Scope
- Boundary
- Responsibility
- System and data Asset inventory
- Acceptable risks
- General Threats

Preparation
- Identify Assets
  - Tangible
  - Intangible
- Statement of Sensitivity

Analysis
- Threat Analysis
  - Identify Threats
  - Probability of Occurrence
  - Consequence
- Risk Analysis
  - Vulnerabilities
  - Controls
  - Assessment

Action Plans
- Accept Risk
- Improve Controls
- New Controls
- Manage Risk
  - (Avoid)
  - (Transfer)
Threat Risk Assessment Deliverables

- Security Plan for the system
  - Description of the risks and environment
  - Component placement, server functions, diagrams
  - Data classification
- Description of risks and key controls to be used
- List of baseline security components
- Identify new security methods or components
- Security testing methods
- Logging and Monitoring requirements
Privacy Risks

- Unauthorized disclosure of data to external parties
- Construction of data profiles
  - Data matching and user monitoring
- Unauthorized use of private data
- Inadequate protection and safeguards
- Incorrect data used for decision purposes
Privacy Impact Assessment

- Assessment of privacy risks during systems under development
- Privacy risk assessment document to be completed
- Identify and classify personal private data
  - Where and how is it collected?
  - Where is it processed?
  - Where is it stored and with what other data?
  - Is the data disclosed to other users or systems?
- Document data flow and user actions
- Select controls and establish processes
Security Architecture Benefits

- **Business Alignment**
  - Risk driven selection and management of controls
  - Participation during system development
  - Business support and business enablement

- **Cost Management**
  - Reusability of components and processes
  - Efficient administration and maintenance

- **Ease of Integration**
  - Scalability of solutions
  - Trusted solutions
Life Cycle Risk Management

Money/Risk

The objective is to lower the risk

Design reviews
Audit
Tests and certification
Technology insertion

Information Protection Center and Information Security Operations

Practices and technology

Information Security Operation

Governance

Time
Security at the Systems Layer

Logical Security Architecture

- Compliance to Policies and Standards
- Identity management
- Authorization services
- Messaging security
- Data encryption
- Audit and logging facilities
- Malicious code protection
- Application Integration

Deliverables:
- Logical Threat Risk assessment
- Privacy impact assessment
Security at the Technology Layer

Infrastructure Protection

- Network Perimeter security protection
- Network Segmentation
- Network identity management
- Authorization
- Intrusion detection
- Remote System Access
- VPN and Encryption
- Logging and monitoring

Deliverables:

- Physical Threat Risk assessment
- Testing Methods
- Logging and monitoring tests
Security Strategy

Technology
- Network protection methods
- Intrusion detection
- Logging and monitoring
- Channel level encryption
- Security Standards
- Security Administration
- Code protection

Security Analysis and Management
- Enterprise Architecture Methods
- Risk Management Methods
- Privacy assessment methods
- Identity, authentication and authorization
- Multi-layered Security architecture
- Incident management
- Governance, Risk and Compliance processes
Security Management Maturity model

Process II
Security Abstraction

Technology centric

Process III
Security Formalization

Process I
Security Diffusion

Fragmented

Integrated

Human centric

Security Policies
Operations centric security testing

Governance and Risk Management
Enterprise security models and tools
Integrated Security Management system

Isolated Groups
Fragmented Security
Lack of standards

Individuals
artisans
professionals
managers

Avient Solutions
Group Inc.
Developing the Corporate Security Architecture

- Define Security Principles and Standards
  - Security Policies, Principles and Standards
  - Security Vision
  - Baseline security methods and controls
  - Define Security Artefacts and templates
  - Integrate with Technology and application domains

- Define and document Core security tools and services
  - Identity management
  - Logging and Monitoring
  - Network protection (firewalls and IDS)
  - Malicious code protection

- Define IT Security Governance processes
  - Participation in Systems development and technology procurement projects
  - Integration with Project management methods
  - Phased approach for development of security artefacts (Risk Management Plan and security diagrams)
  - Define Security testing requirements
  - Assess if the security methods / tools will be sustainable
  - Define a refresh process for the security architecture
Security Architecture Development

- What architecture development methods are right for you?
- Can the security architecture be developed as a standalone domain?

**Formal ADM (Strategic)**
- Formal templates and processes
- Architecture Vision and Definition
- Architecture Core Teams and Review Boards
- Architecture Foundation and reference library

**Guidelines (Tactical)**
- Just in time architecture
- Architecture LITE
- Security Vision and templates
Security Architecture Development Methodology

Conceptual Risk Assessment

- Identify Security business requirements
  - Description of current environment and processes
  - High level Risk Assessment of business practices, data and technology
  - Assess applicability of government or industry regulations
  - Refine risk assessment and include future plans
  - Create conceptual risk report
    - Business risks
    - Technology risks
    - Operational / financial risks
  - Decide level of project involvement
Security Architecture Development Methodology

Logical Risk Assessment

Logical Security Model Development

- Review with project team and create logical security architecture using core components
- Identify new security components or methods
- Create logical threat risk assessment document
  - Risk assessment of each component in system
  - Security methods and controls to be implemented
- Assess data protection methods and privacy impact
- Review with Enterprise Architecture
Security Architecture Development Methodology

Physical Security Assessment

Information Security Deployment and Testing

- Review physical deployment diagrams
  - Validate that security requirements are implemented
- Review security methods and activities
  - System logging and monitoring
  - User management
  - Source Code validation
- Define / Execute Security test strategy and plan
  - Security Scans
  - Vulnerability assessments
  - Penetration tests
  - Disaster Recovery Test
- Update Enterprise Architecture documents
- Update governance risk and compliance processes
Assessing the Security Architecture

- Control Objectives for IT (COBIT)
  - Developed by ISACA as a governance framework
    - Plan and Organize
    - Acquire and Implement
    - Deliver and Support
    - Monitor and Evaluate
  - Includes a guide for measuring maturity

- Capability Maturity Model
  - Must be tailored for the organization
  - Applied to security functions and services
Corporate Security Architecture Assessment

Step 1 - Preliminary Review of Security Architecture

- Review the scope of the security architecture
- Review target security architecture
- Review security policies and standards
- Review security principles and vision
- Assess security organization and staffing
- Identify Regulatory Compliance requirements
- Evaluate the Risk Assessment methods in use for projects and systems
- Identify and map out the Architecture governance process for security
- Review Risk issue management process
- Assess Security Design Plan templates and completed forms
- Review security management procedures
- Assess Business Continuity Plan and maintenance
Corporate Security Architecture Assessment

Step 2 - Evaluate Security foundation and components

- Validate security plans to actual implementation
- Assessment of security methods, technology
- Security awareness and risk management training
- Assess how security is integrated with other architecture domains
- Assess Security Components
  - Identity management
  - Logging and Monitoring systems
  - Network protection
  - Encryption key management processes
  - Malicious code protection
Corporate Security Architecture Assessment

Step 3 - Assess the Technical Security Architecture

- Security implemented for the Technology and Application layers
- Vulnerability Assessment methods in use
- Security Scan test methods
- Security Reviews completed by third parties
- Source code reviews and testing
- Physical security
- Technical support access
- Backup and Recovery processes
- Network security
Summary and Conclusions

- New risks created by new technologies and business processes
- Regulatory compliance, including privacy is driving enhanced security requirements
- Increase risk of attacks from external sources
- Enterprise Architecture is growing in popularity
- Challenge to implement and maintain
- Security architecture is pervasive across the other domains of architecture - Business, data, technology and applications
- Security architecture is completed in layers
  - Conceptual, Logical, Technical
- Requires a framework of risk management methods, baseline standards and governance process
- Comprehensive risk management plan for security, privacy and business continuity