Enterprise Security Architecture

Business-driven security

April 2012

ERNST & YOUNG
Quality In Everything We Do
Agenda

- Facilities and safety information
- Introduction
- Overview of the problem
- Introducing security architecture
- The SABSA approach
- A worked example
- Security architecture components
- Facilitated discussion
The Problem: Information Security
The business perspective
The problem: answering the difficult questions

- How do we ensure security supports the business?
- How do we demonstrate alignment with the business risks?
- Are we spending too much or on the right things?
- How do we embed security in the wider business?
- How do we keep business and security aligned?
- How do we minimise security gaps and remediation costs?
Introducing security architecture?
Traditional architecture vs. security architecture

- What type of structure do I want?
- Why do I want this structure?
- How will it be used?
- Who will be the users of the structure?
- Where should the structure be located?
- When will it be used?

What type of information system is being considered and what will it do?
- Why is it needed?
- How will it be used?
- Who will use it?
- Where will it be used?
- When will it be used?

Building a physical structure
Protecting business information

- Designing a secure business information system could take a number of directions, but there is considerable potential for the security and business requirements to clash and neither party is satisfied with the end result.
- The answers to these questions provide the architect with the business requirements which can then be fed into the design process.
How do I solve this problem
What is business security architecture?

The challenge in developing the architecture is to balance between risk, cost and usability.

Security architecture controls are composed of people, process and technology controls.

An organisation needs security controls that are:

► Driven by business requirements rather than technical considerations
► Directly traceable to business objectives
► Designed from the outset to be cost-effective, avoiding remediation effort
► Meet legal, regulatory and policy compliance requirements by design
► Are appropriate to both the business risks and organisation’s risk appetite
Why do this? Benefits of the security architecture approach

**Customised information security control framework**
- Driven by the organisation’s business requirements
- Meeting compliance
- Alignment with the business’ risk appetite

**Reduces information security, IT and security audit costs**
- Eliminates redundant controls
- Reduces ad hoc security implementation
- Provides detailed agreed security requirements

**Informs executive management about security risk**
- Articulates impact of information security risk in business terms
- Provides structured control framework to evaluate compliance
- Creates foundation for quantitative assessment of security ROI
The SABSA approach
Step by step

- Business driver
  - Identify the business drivers/objectives.
  - Prioritise drivers.

- Business attributes
  - Translate drivers into business security attributes.
  - Security attributes are provided by SABSA framework.

- Threat analysis
  - Perform threat analysis.
  - Identify actual threats to business attributes/business drivers.

- Impact analysis
  - Use qualitative or quantitative methods to define impact of the realisation of the threat on the identified business objectives.

- Control objectives
  - Define control objectives to mitigate the identified threats to acceptable levels.

- Security services
  - Identify security services to provide the required controls objectives.
The SABSA approach
An architect’s perspective – Here comes the science!

<table>
<thead>
<tr>
<th>Business</th>
<th>Motivation</th>
<th>Process</th>
<th>People</th>
<th>Location</th>
<th>Time</th>
</tr>
</thead>
</table>
Contextual & conceptual security
Understanding the business and its risks

Gather, assess and analyse business requirements

- Business strategy
- Business processes and functions
- Organisational structure – personnel, geographical, partnerships
- Budgets, technical constraints, time dependencies

Describe the business requirements

- Use the business attributes database to describe the business in terms of strategy, related assets, business goals and objectives → business attribute profile

Analyse the business risks

- Perform a threat analysis on the business assets, goals and objectives
- Define the business impact of the realisation of the threats
- Identify technical and procedural vulnerabilities
An overview of SABSA attributes database
A logical security architecture
What does it look like?

Business Attributes Profile
- Select business attributes (mapped to business drivers).
- Define enterprise-specific business attributes, a measurement approach, metrics and targets.

Control objectives
- Derive control objectives from the Business Attributes Profile and the Business Risk Model developed at the Conceptual layer.

Security strategies
- Define appropriate security strategies based on the business process model, the Business Attributes profile, the control objectives and the assessment of the current state of security

Security services
- Layered model of security services, including:
  - Prevention
  - Containment
  - Detection and notification
  - Event collection and tracking
  - Recovery
  - Assurance
A worked example
Business drivers

**Business driver**

- Protect customer information
- Prioritised

**Business attributes**

- Compliant
- Access-controlled
- Protected

**Threats**

- Customer data is disclosed to internal users through inappropriate access controls
- Staff leak customer information to unauthorised third parties
- Customer information is disclosed in transit to third-party processor.
- Sensitive* customer data is disclosed to unauthorised parties
# A worked example

## Control objectives

**Control Objectives: Protect customer information**

*Business attributes – Compliant, access-controlled and protected*

### Operations, process and procedures

- User access management
- Monitoring user access levels and user activity, particularly third parties
- Incident response for data breach

### Technology

- Identity management
- Authentication and authorisation
- Database and network encryption to protect personal data in storage and in transit
- Auditing and logging of access to sensitive* personal data

### People

- Training and awareness for all staff on data protection
- Focussed training for high-risk areas, e.g., call centres

### Governance

- Nominated Data Protection Officer
- Data protection policies, standards and procedures
- Third party risk management framework
- Data protection assurance

*Compliant, Access-controlled, Protected*
A worked example
Security services

### Technical security services
- Identity management tools
- Authentication
- Access control
- Authorisation
- Auditing
- Storage encryption
- Link encryption
- Breach

### Technical security services
- Security management
- Incident management
- Policies, standards, procedures, guidelines
- Training and awareness
- Proactive reviews
- Third party management frameworks
Security architecture deliverables
What do you get?

Contextual Architecture
- Business Drivers
- Prioritised drivers
- Impact Assessment

Conceptual Architecture
- Business Attribute Profile
- Business Risk Model
- Security Domain Model

Logical Security Architecture
- Security Domains and associations
- Logical security services framework

Physical and Component Architecture
- Detailed infrastructure and component solution design
- Documented controls against control objectives

Operational security control framework
Portrait of a successful security architect

An architect’s skill-set is different from a tradesman
Understands the business strategy and objectives
► There are more than just ‘security’ requirements
Thinks in business terms at all times
► Why are we doing this?
► What are we trying to do?
Has good communication skills
► Bridges the gaps between business and technology
Maintains strength of character
► Defends the security architecture
► Meets the constant challenge
Optimising your investment in security architecture – measuring success

- Characteristics of a good business security architecture
- Strategic alignment: aligned to the current business strategy
- Agility: designing a security architecture to deal with the changing legal, regulatory and client requirements
- Extensibility: expanding the architecture on a phased basis throughout an organisation
- Robustness: demonstrates a thorough development with appropriate input, review and approval and will withstand critical evaluation from detractors
- Pragmatism: reflects the operating environment of the organisation and imposes appropriate security controls for the people and culture.

Good security controls

- Driven by business requirements rather than technical considerations
- Directly traceable to business objectives
- Appropriate to both the business risks and organisation’s risk appetite
- Meets regulatory, audit and compliance requirements by design
- Designed from the project outset to be cost-effective thereby avoiding remediation effort
Security Architecture
Summary

Evaluate compliance and inform management

Understand the business requirements

Assess the risk to business objectives

Balance risk, cost and usability

Implement agreed security controls
EY Contacts
Security architecture experience

Hugh Callaghan
Director
Direct Tel: +353 (0)1 221 2411
Direct Fax: +353 (0)1 475 0557
Mobile: +353 (0)87 983 8511
E-mail: hugh.callaghan@ie.ey.com

Patricia O’Gara
Senior Manager
Direct Tel: +353 (0)1 221 2008
Direct Fax: +353 (0)1 475 0557
Mobile: +353 (0)87 235 6023
E-mail: patricia.ogara@ie.ey.com

Eoin O’Reilly
Senior Manager
Direct Tel: +353 (0)1 221 2698
Direct Fax: +353 (0)1 475 0557
Mobile: +353 (0)86 770 9820
E-mail: eoin.oreilly@ie.ey.com

Vasilijs Mihailovs
Assistant
Direct Tel: +353 (0)1 221 2653
Direct Fax: +353 (0)1 475 0557
Mobile: +353 (0)86 176 6444
E-mail: vasilij.mihailovs@ie.ey.com
Thank you