# Accenture Technology Vision 2012: What does it mean for security?


IBM Pulse 2012

Tor Jomar Nordhagen
Director, Security ANZ

Paul O'Rourke
Managing Director, Security, APAC

accenture

consulting | technology | outsourcing

# What is the Accenture Technology Vision?

- Accenture's position on emerging technology and major technological changes
- A platform for our clients to guide investments in technology
- Strategic guidance for Accenture's investments in new and existing business areas

# The 6 key trends for enterprises

- Context-based services
- Social-driven IT
- Converging data architectures
- Industrialized data services
- PaaS-enabled agility
- Orchestrated analytical security

Security underpins all of these!

# Context-based services

# Context will drive the next wave of digital services


Context-based services:

- Are more than simple location-based services
- Require rapid aggregation and analysis of data from multiple sources
- Must be relevant and add value to the individual

Insight → *actionable* insight → insight at the *point of action*

# Implications of context-based services to security


- Need for greater federation with external sources
- Identities need to be portable
- User-driven privacy controls
- Opportunity for great context-based security

Accenture Technology Vision 2012

# Social-driven IT

# Social platforms will have business-wide impact


- Social media has changed how we communicate
- It will continue to disrupt the way companies do business
- Need to socially enable each business operation
- Establish metrics so that social can be monetised beyond the “like”.

# Implications of social-driven IT to security


- Identity needs to evolve from channel-specific to cross-channel and integrated with social identity
- Social authentication – using social for greater identity proofing and security
- New threats arising from social integration
- Dealing with privacy in a socially integrated world

Accenture Technology Vision 2012

# Converging data architectures

# Big Data - data architectures must bridge the old and the new


- Unstructured data: new solutions to old problems, and new problems as well
- Big Data: Data as a platform
- Three fundamental architectural changes required:

**Rebalancing** | **Coexistence** | **Cross-pollination**

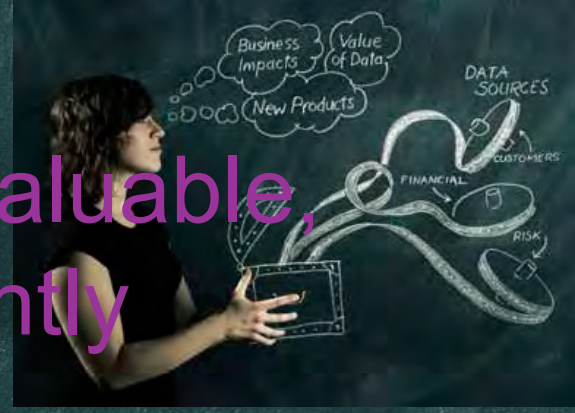
# Implications of converging data architectures to security


- Security must move from applications to the data

- Data governance: IT shifts from data owners to data stewards

# Industrialized data services

# Sharing will make data more valuable, but only if it's managed differently




- Data should be managed as an asset
- New, industrialised approaches are required for data management
- Evolution towards centralised data management
- Attaching a value to data

# Implications of industrialised data services to security


- "Data as an asset" helps to assess information risk
- How to classify and protect shared data?
- Responsibilities across the "data supply chain"
- Data privacy becomes more complex in a distributed data platform environment

# PaaS-enabled agility

# PaaS will shift the emphasis from cost-cutting to business innovation


- Platform-as-a-Service (Paas) offerings are maturing
- PaaS is not just a tool for squeezing cost out of IT
- Business processes are like a string of pearls
- Emergence of the hybrid cloud
  - **Wave 1 (now) – point-to-point integration**
  - **Wave 2 – workflow spanning on-premise and off-premise**
  - **Wave 3 – seamless mixing of on-premise and cloud**

# Implications of PaaS-enabled agility to security


- Move services to the cloud based on risk
- Integrate security across on-premise and PaaS
- Use hybrid cloud models to reduce risk
- PaaS-based security services

# Orchestrated analytical security

# Security breaches are inevitable. Data platforms will be how you deal with them


- Increasingly connected means increasingly exposed
- Breaches are inevitable – detect and respond rapidly
- Leverage new data platforms to better detect incidents
- Shift from a compliance mindset to a risk mitigation one
- Orchestrate security resources and responses

www.accenture.com/technologyvision

www.accenture.com/security


accenture

consulting | technology | outsourcing

# What are the security implications?


## Context-based services

- Need for greater federation with external sources
- Identities need to be portable
- User-driven privacy controls
- Opportunity for great context-based security


## Social-driven IT

- Identity needs to evolve from channel-specific to cross-channel and integrated with social identity
- Social authentication – using social for greater identity proofing and security
- New threats arising from social integration
- Dealing with privacy in a socially integrated world

# What are the security implications?

## Converging data architectures

- Security must move from applications to the data
- Data governance: IT shifts from data owners to data stewards


## Industrialized data services

- "Data as an asset" helps to assess information risk
- How to classify and protect shared data?
- Responsibilities across the "data supply chain"
- Data privacy becomes more complex in a distributed data platform environment

# What are the security implications?


## PaaS-enabled agility

- Move services to the cloud based on risk
- Integrate security across on-premise and PaaS
- Use hybrid cloud models to reduce risk
- PaaS-based security services

## Orchestrated analytical security

- Increasingly connected means increasingly exposed
- Breaches are inevitable – detect and respond rapidly
- Leverage new data platforms to better detect incidents
- Shift from a compliance mindset to a risk mitigation one
- Orchestrate security resources and responses