Security in knowledge

DATA AND APPLICATION SECURITY: A CONTEXT BASED APPROACH

Jonathan Hughes

Senior Vice President, Global Professional Services

Integralis

Agenda

► Why is context important?

► A context based approach to data and application security

► Lessons learned from good and bad examples of data security being implemented

► The Integralis recommended approach

Why is context important?

► Context is critical to prioritising in a world of limitless options

  ► Traditional network perimeter security is giving way to data/application centric security and as a result the information risk challenges grow exponentially

  ► Data is everywhere, largely unclassified and un managed

  ► Applications are excellent delivery mechanisms for data but are not generally managed in the context of the risks associated with the data they host.

  ► Without context the challenge of data/application security will swamp even the largest of organisations

INTEGRALIS
an NTT Communications Group Company

What is context?

► What are the business risks associated with data held within an organisation?

  ► Organisational threat landscape

  ► Classify data types within the organisation

  ► Quantify the possible outcomes from data loss by data type

► Are there regulatory requirements that must be adhered to in relation to specific data types?

  ► PCI DSS, HIPAA, SOX, Data Protection…..

► Who owns data within the organisation?

  ► It's not the IT department.

  ► Do business owners know they own the data and what their responsibilities are in relation to that data?

  ► Who needs access to data and why?

A context base approach

INTEGRALIS
an NTT Communications Group Company
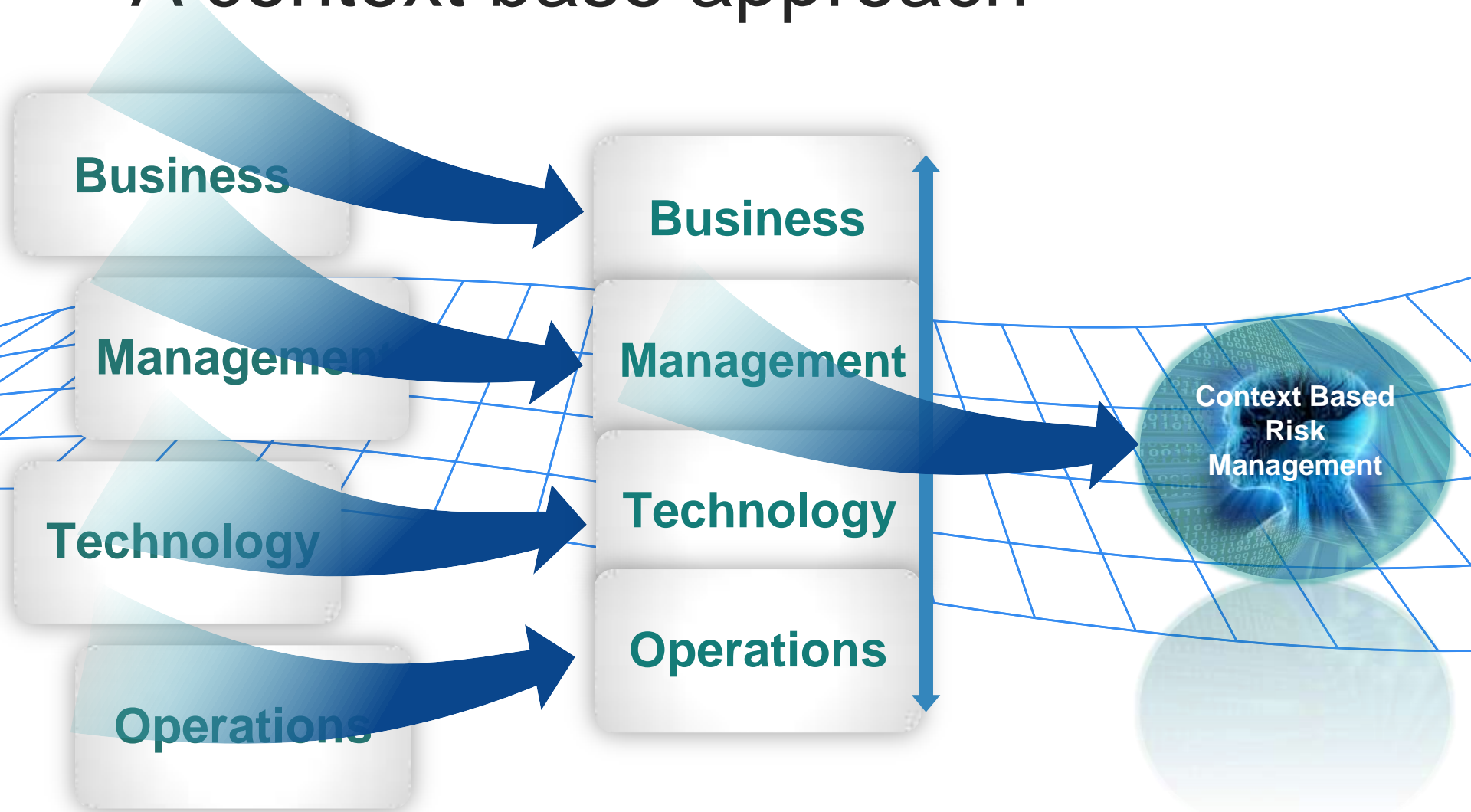
Lessons Learned

THE GOOD		THE BAD	
Global Retail Company	**Telecoms Company**	**Financial Services**	**Global Manufacturer**
• Threat landscape understood • Business data threat assessment understood • Systems and processes implemented to enforce data/application security rules	• PCI compliance needs • Structured data classification programme • Positive data/application controls and processed implemented • Poor legacy data management	• Time constrained policy vacuum • Technology solution implemented with no business rules • Little/no ROI in terms of business risk reduction	• No data/application classifications or controls • Flat global network • No data segregation • No data classification of critical IP

RSA CONFERENCE
ASIA PACIFIC 2013

Any questions?