

Deloitte.

Security Transformation

19th May 2009

Warren Trakman

wtrakman@deloitte.co.uk

Audit . Tax . Consulting . Corporate Finance .



Security Transformation Overview

What's Going On in the Market?

What is Security Transformation?

Case Study: Large Global Retail Bank

- Challenges Faced
- Approach to the Problem
- Benefits Realised
- Example Projects

Types of Firms Transforming their Security Function

Why Deloitte?

Security Transformation

Headline News

Hackers steal AT&T customer data

Hackers have obtained the credit card details of almost 19,000 online shoppers from telecoms giant AT&T.



- HOME
 - NEWS
 - ENVIRONMENT
 - SPORT
 - COMMENT
 - STUDENT
- UK ↓ Europe World ↓ Business ↓ Health Science & Tech Media Education ↓ R

Home > News > UK > **UK Politics**

Drivers' details lost in new

By Colin Brown, Deputy Political Editor
Published: 18 December 2007

The personal details of more than 100,000 drivers are missing in another data blunder.

The names, addresses and telephone numbers of every candidate for the 2005 general election – for every candidate between September 2004 and April 2005 – which was lost in May at a supplier's data centre, told MPs.



World

FT Home > World > UK

- Home
- World
 - US & Canada
 - Europe
 - UK**
 - Asia-Pacific
 - Middle East
 - Africa
 - Americas

NHS trusts lose patients' records

By Jimmy Burns in London
Published: December 23 2007 18:13 | Last updated: December 24 2007 01:35

Gordon Brown was facing further political embarrassment over the government's handling of personal data after the Department of Health confirmed that nine National Health Service trusts had admitted losing patient records.

BBC NEWS WATCH LIVE BBC News 24

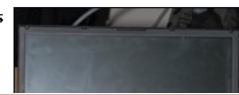
NEWS SERVICES Your news when you want it

Last Updated: Saturday, 19 January 2008, 18:41 GMT

E-mail this to a friend Printable version

MoD to be quizzed over lost data

The information watchdog is to grill the Ministry of Defence over its data protection policies after it lost the personal details of



VIDEO AND AUDIO NEWS
Details of the lost information
WATCH

WATCH LIVE BBC News 24

Last Updated: Tuesday, 20 November 2007, 19:51 GMT

E-mail this to a friend Printable version

UK's families put on fraud alert

Two computer discs holding the personal details of all families in the UK with a child under 16 have gone missing.



TJX breach could top 94 million accounts

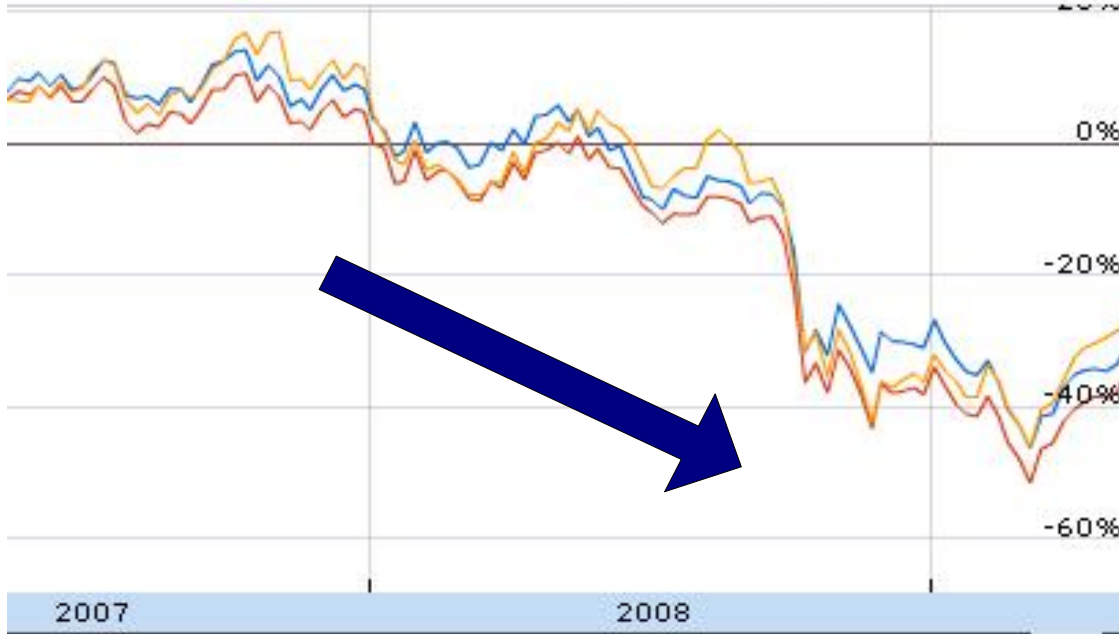
Filings in case involving Visa cards alone as much as \$83 million

bank accounts

Security Transformation

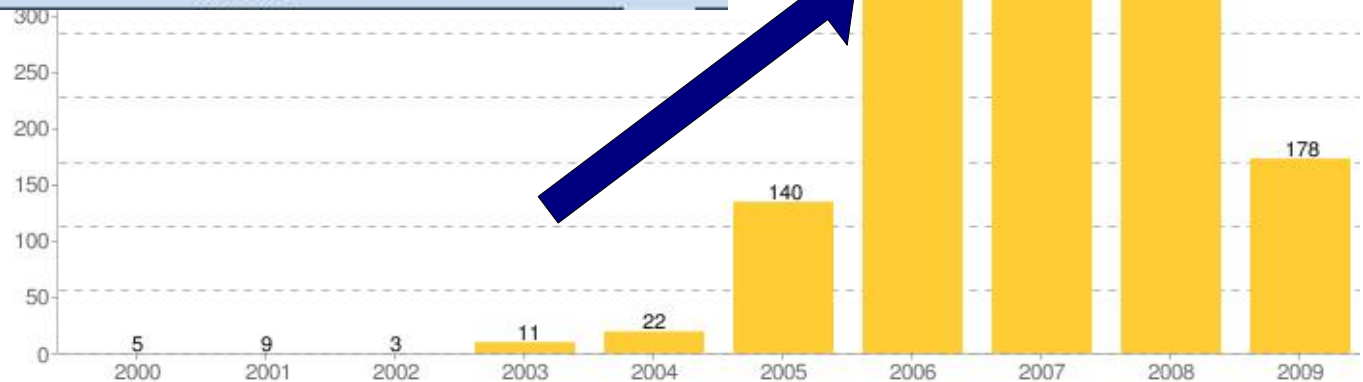
Current Market vs. Security Incidents

● Dow -32.39% ● S&P500 -36.59% ● Nasd -29.60%



- Pressure to reduce operational overheads
- Increasing regulation
- Increased risk of fraud

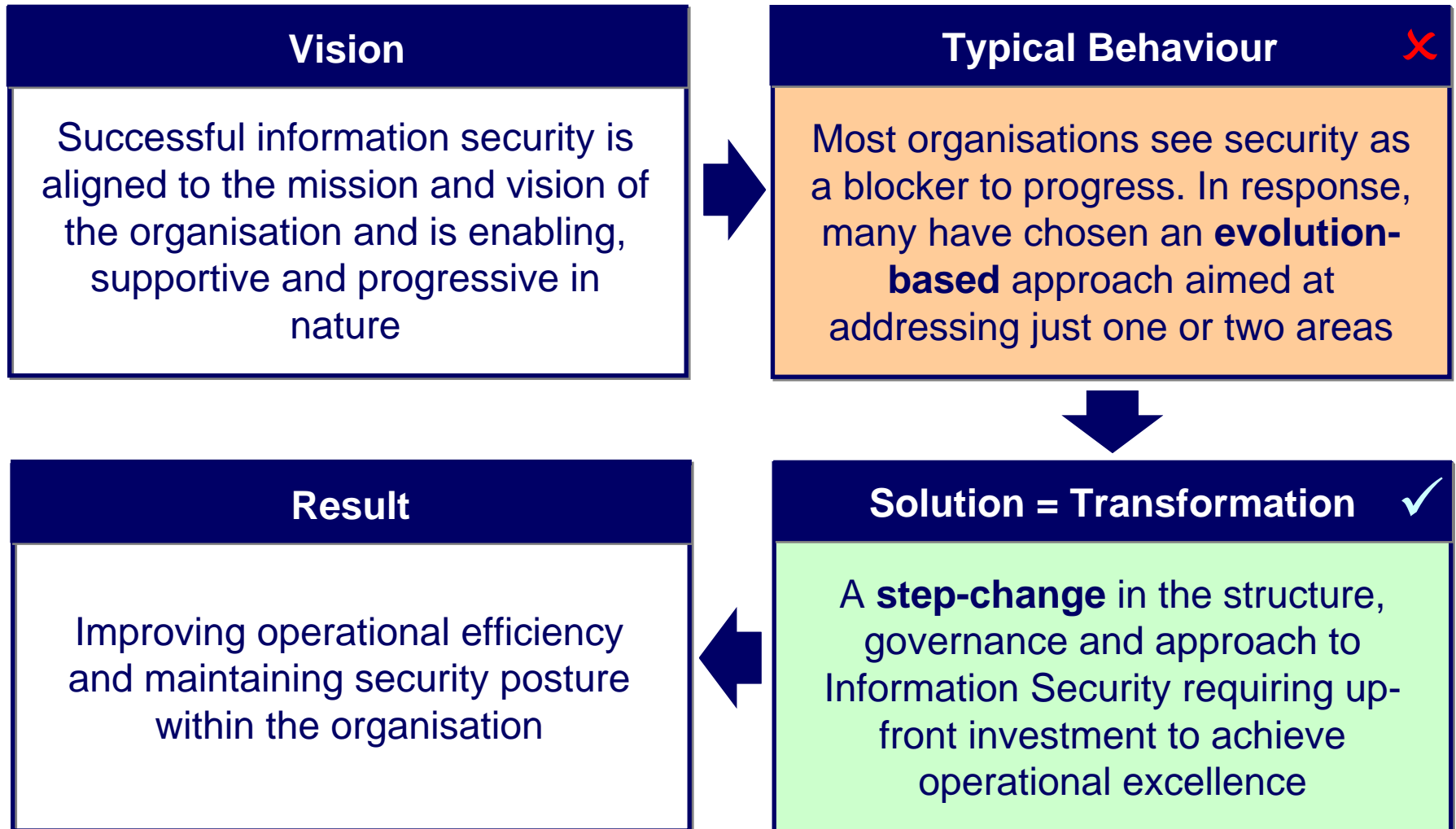
Source: Google Finance (May 2009)



Source: DataLossDB.org (May 2009)

Security Transformation

What is Security Transformation?



Security Transformation

Case Study - Large Global Retail Bank: Challenges

Challenges

- Negative publicity and industry reputation
- Historically, typical investment had been <1% of IT budget
- Control weaknesses
e.g. logical access management, encryption and data privacy
- Internal audit findings
- Rising number of security-related incidents escalated to the Board
- Overseas acquisitions
- Ongoing compliance with industry, legal and regulatory requirements
- Rising costs for security BAU-activities due to operational inefficiencies stemming from:
 - manual processes
 - no product standardization

Security Transformation

Case Study - Large Global Retail Bank: Challenges (cont.)

No Clear Security Strategy

Lack of consensus of where the organisation wants to be regarding information security and how to get there

✓ **Created one!**

Lack of Support

Lack of buy-in from stakeholders to support organisation wide change – security is often seen as a “blocker” to business

✓ **Did a roadshow**

Inability to Execute Change

Immature delivery capabilities within the Information Security function – lack of skills and capacity to manage change

✓ **Contracted with 3rd-party specialists**

Don't know where to Invest

Lack of management information which hinders the Executive's ability to make informed investment decisions

✓ **Benchmarked security against ISO27001 to see weak spots**

Security Transformation

Case Study - Large Global Retail Bank: Approach

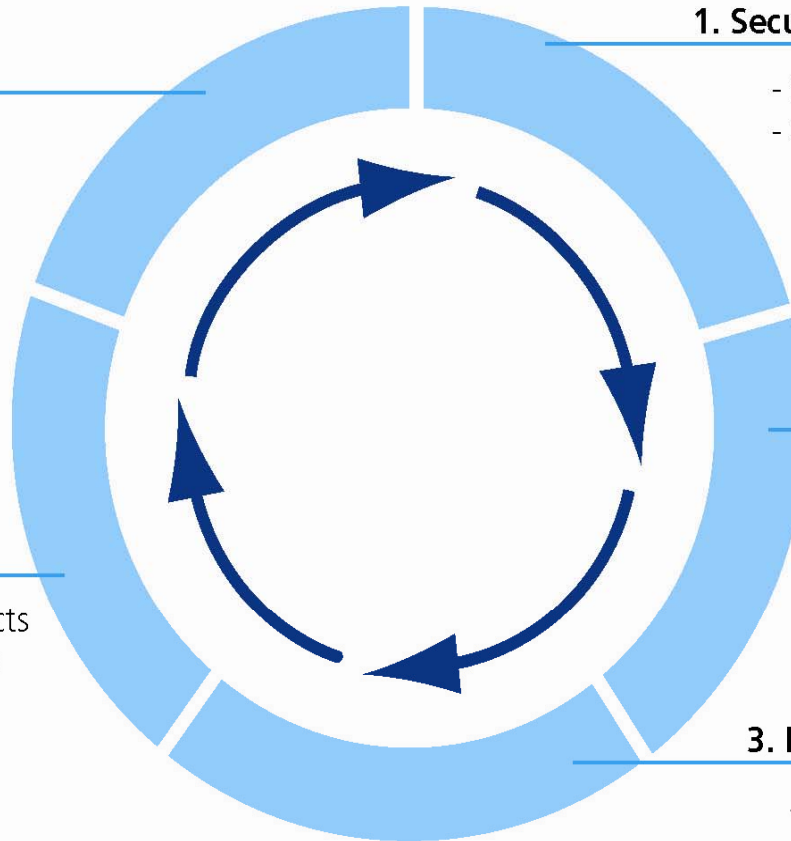
Life cycle of Security transformation project

5. Implementation

- Onboard resources
- Implement intelligent PMO
- Project management
- Technical delivery support
- Education & training
- Review impact on capabilities

4. Strategic roadmap

- Propose and plan new projects
- Create programme roadmap
- Engage stakeholders



1. Security framework

- Select baseline (e.g. ISO 27001)
- Select maturity model (e.g. CoBit)

2. Current state analysis

- Measure current maturity
- Identify key challenges

3. Future state vision

- Define guiding principles
- Define desired future state
- Identify capability gaps

Security Transformation

Case Study - Large Global Retail Bank: Benefits

Regulatory Compliance

Compliance with internal and external requirements through controls remediation

Cost Reduction

Cost reduction through automation and security service / licence consolidation

Organisation Integration

Integration of regional security functions inherited through recent banking acquisitions

Management Information

Mature MI of Information Security risks through deployment of cross-team and platform monitoring solutions

Security Transformation

Case Study - Large Global Retail Bank: Example Projects

Example Projects

1. *ISO27001 certification* achieved for one of the bank's online banking platforms
2. *Data leakage prevention* solution to monitor and block personal and sensitive data leaving the organisation without adequate protection
3. *Encryption key management* solution to allow encryption keys to be stored centrally and management to be securely automated
4. Group-wide *security baseline controls* and multiple layers of security standards
5. The programme is ongoing and further projects are being delivered, including:
 - *Security compliance monitoring* and
 - *Security metrics / KPI reporting*

Security Transformation

Types of Firms Transforming their Security Function

Client Description	Primary Driver for Security Transformation
Financial Services	
Global Retail Bank	Reputation
Card Bureau	Regulatory
Public Services	
Government Agency	Security Breach
Technology, Media, Telecoms	
Online Gaming Company	Regulatory
Consumer Business	
Retail Chain	Customer Service
Retail Chain	Regulatory
Beverage Manufacturer	Operational Efficiency

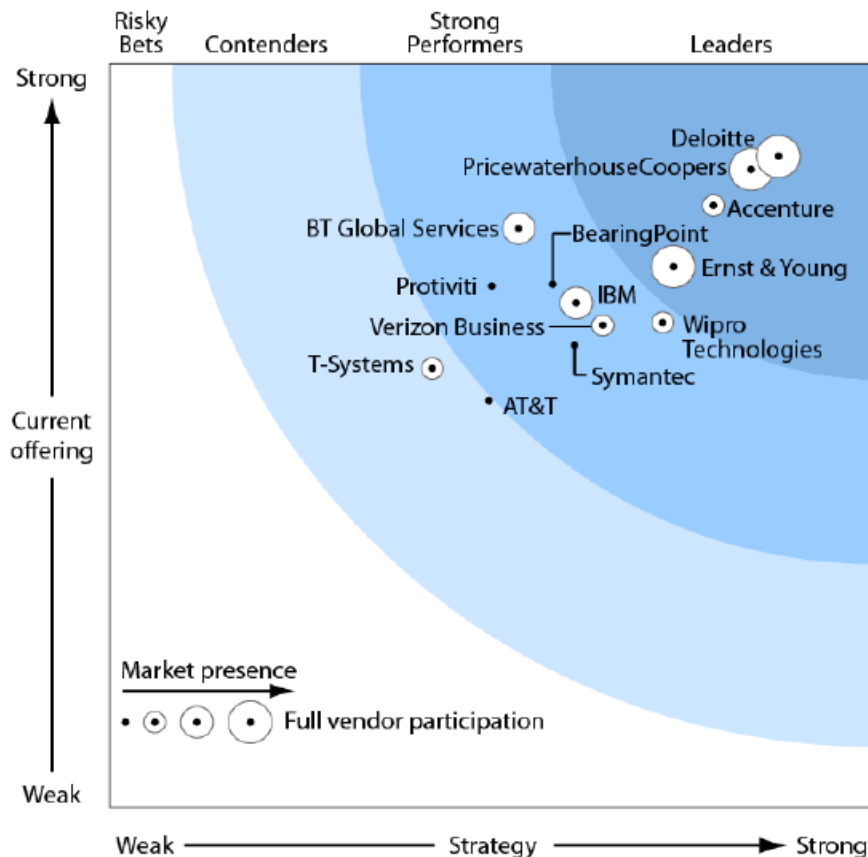
Security Transformation

Why Deloitte?

Scale to support large programmes of change

Skills to advise on the whole spectrum of information security competencies

Experience to help clients do what we preach – strong market presence



“Deloitte led the pack with established methodologies, thought leadership, and exceptional talent.”

Forrester Wave™: Information Security and Risk Consulting , Q1 2009”, Khalid Kark

Forrester Wave™: Information Security and Risk Consulting , Q1 2009”, Khalid Kark



This document is confidential and prepared solely for your information. Therefore you should not, without our prior written consent, refer to or use our name or this document for any other purpose, disclose them or refer to them in any prospectus or other document, or make them available or communicate them to any other party. No other party is entitled to rely on our document for any purpose whatsoever and thus we accept no liability to any other party who is shown or gains access to this document.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Deloitte LLP is the United Kingdom member firm of Deloitte Touche Tohmatsu ('DTT'), a Swiss Verein, whose member firms are legally separate and independent entities. Please see www.deloitte.co.uk/about for a detailed description of the legal structure of DTT and its member firms.