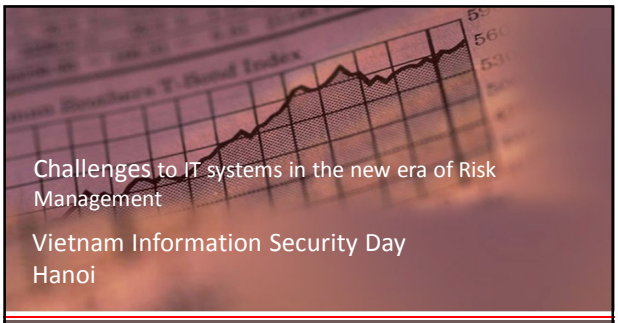

Challenges to IT systems in the new era of Risk Management

Vietnam Information Security Day
Hanoi

23RD NOVEMBER, 2011

Pavel Dvorak, Nicholas Davies

InfraRisk

Current Macro Enviroment

Global events impacting the Banking sector include:

- Post GFC 1, we saw Basel 3 rushed through with extra *Capital & Liquidity* impacts being key changes.
- In addition to these Regulatory initiatives – national government considerations are driving improved *Governance and Reporting*
- With the current GFC 2, borrowing costs for Sovereigns are increasing – and this has a knock on effect to global liquidity and *cost of funds*

These have (will) impact Vietnam as:

- State Bank has raised capital requirements already in both a minimum dollar amount and as a % of Risk Weighted Assets. More initiatives rumuored….
- Liquidity and cost of funds for liabilities, whether domestic or offshore – is a key management issue
- Market consolidation is already proving to be a by product of the more demanding environment and competition

If that is not enough, banks are also contending with major Technology changes

InfraRisk

Technology Implications

New developments, whilst challenging, also provide the opportunities to manage the new challenges…

Development	**Opportunity for business**
New computing platforms aimed to serve explosion of requirements rapid and often disruptive changes which redefine the enterprise IT landscape - virtualization of operating environments, - removal of physical boundaries for data and systems	Leverage IT for greater effectivness Expand total organisational capabilities Cost advantage Operational fexibility
Mobility and consumer technology - Expansion of end-users capabilities and needs - Addition of new information channels - Consumerisation of enterprise	Reach new customers with new products Extend customer services and redefine them from transaction to customer interaction Empower bankers to reach out to customers in their new online social space

Often paradoxical challenges
Representing new factors from the risk management perspective

InfraRisk

InfraRisk Experience

InfraRisk serves top tier banks in Australia, Asia & the Middle East - delivering risk management solutions for both back-office and front-office users

CVX – Credit Value Maximizer – deliveres the critical functionalities needed to effectively manage credit risk and optimise Risk/Return

InfraRisk

System robustness

InfraRisk systems respond to many of these new opportunities for banking.
To address the challenges coming with these opportunities our systems been regularly exposed to maximum scrutiny according to the highest standards for information security.

Systems must be **robust**
preventing failure in all anticipated situations
engineered for success

Robustness is evaluated through

- Standards and policies
  Follow prescriptive process how to avoid failure
- Maturity – validated by practice and exposure to real conditions
  - Systems established in existing relevant production deployments
  - Accellerate by applying testing tools – penetration tests, repeated automated UI tests etc.

InfraRisk

System resillience

Systems must be **resillient**
providing such change management, early detection of failure and swift correction so that fail is safe
engineered for failure

- Experienced staff, who can invent solution to unforseen problems
- Agile process to react flexibly

Examples of benefit:

1. Preventing security breach of Gizmodo site – incorrect use of data model and encryption algorithm led to exposure of passwords – described as OWASP known vulnerability "Weak cryptography"
2. Citibank 2011 hacking attack via URL rewrite error – described as OWASP known vulnerability "Session fixation"
3. CERT Australia 2010 reported 50 serious security incidents – one/week , some requiring military oversight

Hardly forseen circumstances

InfraRisk

System scrutiny

Bank established an internal CERT team
- Evaluation of technical risk
- Responsible for security testing
- Trained and certified team of security specialists

Some concrete tasks in a typical system review:
- Evaluation of the deployment environment status (up-to-date patching from vendor)
- Code review against a set of known vulnerabilities
- Best practices in development and robustness against common vubnerabilities
- Testing resillience by threat risk modelling techniques to address unknowns

Approach to Infromation Security review
- Evaluate areas according to STRIDE categories of vulnerabilities
- Produce a DREAD report
- Standard AS/NZS ISO/IEC 17799:2006 [included into ISO/IEC 27002:2005]
  - Section 12 – Information Systems Acquisition, Development and Maintenance
  - Sec. 13 – Security Incident management
  - Sec. 11 - Access control, business continuity management, compliance
- ISO/TR 13569:2005 - Financial services -- Information security guidelines industry-specific implementation of above 27002

InfraRisk

System scrutiny

Internal standards defined and mapped to
- ISO provisions
- COBIT framework developed internally, Delivery and Support domain

Prescribe for example concrete:
- code development practices
- data validation requirements
- cryptographic algorithms and keys management practices
- source code management practices

Alternative approaches:
- applying OCTAVE method – Carnegie-Mellon developed
- Microsoft Threat Modelling framework for security development
- IT governance frameworks include security concerns (COBIT, TOGAF)

InfraRisk

Conclusion

- Current environment brings unprecedented challenges to IT including security
- The prize is the opportunity to transform business
- IT will become business partner and leader in responding to the change

InfraRisk