SearchFinancialSecurity.com
INFORMATION SECURITY
FINANCIAL
INFORMATION SECURITY DECISIONS

Lessons Learned

Applying Effective Information Security Governance Post Société Générale 2007

Keith White
Vice President Information Technology Risk
Credit Suisse

Lessons Learned - Introduction

- **Goals and Objectives**
  - Is the "success" of rogue traders the result of information security failures?
  - Who are the leadership and governance stakeholders in the IS and related risk measurement and management processes?
  - What are the roles and responsibilities of governance-management in the avoidance, detection, and response to the rogue trading events?
  - Are rogue trading events anomalies or do they reoccur?

Lessons Learned - Introduction

- **Goals and Objectives**
  - At an industry level should the processes for creating successful information security governance differ in light of recent rogue trading events?
  - In light of the SocGen events of 2007, are IS and other governance standards appropriate and sufficient?

Lessons Learned - Introduction

- **Workshop Leader**
  - Keith White, Vice President
    Information Technology Risk
    Credit Suisse
  - Member of the Board of the RMA Technology Risk subcommittee
  - Former member of multiple BITs subcommittees and contributor to several BITs standards
  - Published author on technology risk and related topics

Lessons Learned - Introduction

- **Structure and Agenda**
  - Introductions
  - Baseline Analysis – Industry Precedents
  - Baseline Analysis – Facts and Assumptions
  - Baseline Analysis – Regulatory Context and Applicable IS Standards
  - Governance Hypothesis
  - Open Summary Discussion
  - Wrap Up

Lessons Learned – Baseline Analysis

- **Baseline Analysis – Industry Precedents**

Financial Institution	BCCI	Barings	Sumitomo	LCTM
Year				
Approximate Total Loss (USD, bn)				
Loss as % of Capital				
Loss to Creditors				
Factors				
Perpetrator				
Crisis Trigger				
Risk Categories				
People				
Process				
Systems				

Lessons Learned - Baseline Analysis

- **Baseline Analysis – Sample Industry Precedents not Explored**
  - Metallgesellschaft 1993
  - Daiwa 1995
  - NatWest Markets 1997
  - Many multimillion dollar events

Lessons Learned - Baseline Analysis

- **Facts and Assumptions – Anatomy of the SocGen Incident (Based on research by Credit Suisse Information Security)**
  - Mr. Jerome Kerviel, joined SocGen in mid-2000 working in back-office and middle-office functions. In 2005, he became a Jr. trader.
  - Kerviel knew the timing of the nightly reconciliation process of the day's trades by Eliot (back-office trade booking system), so with his back-office credentials was able to delete and re-enter these unauthorized transactions without being noticed. He sometimes used fake counterparty information.
  - Kerviel took just four days of vacation in 2007.

Function	Trade Entry	Position Maintenance	Confirmations	Settlements	Accounting Entries	General Ledger	Valuation	Payments
Employee								
Access Standards and Controls								
Technology Layer	Trading System		Trade Processing System (like Eliot)			GL System	Trade Processing System (like Eliot)	SWIFT/EuroClear/ other
	Infrastructure							
Monitoring								

Lessons Learned - Baseline Analysis

- **Facts and Assumptions– Anatomy of the SocGen Incident**
  - Hypothetical trade-transaction function spectrum (HTTFS)

Function	Trade Entry	Position Maintenance	Confirmations	Settlements	Accounting Entries	General Ledger	Valuation	Payments
Employee								
Access Standards and Controls								
Technology Layer	Trading System		Trade Processing System (like Eliot)			GL System	Trade Processing System (like Eliot)	SWIFT/EuroClear/ other
	Infrastructure							
Monitoring								

Lessons Learned - Baseline Analysis

- **Task – Profile the Société Générale Event**

Financial Institution	BCCI	Barings	Sumitomo	LCTM	Societe Generale	Profile	
						Similarities	Differences
Year	1991	1995	1996	1998			
Approximate Total Loss (USD, bn)	10	1.3	2.6	4.4			
Loss as % of Capital	100%	100%	45%	44%			
Loss to Creditors	70%						
Factors	Fraudulent loans, fictitious deposits, money laundering	Unauthorised and concealed trading in options and futures; loss concealment;	Unauthorised commodity trades	Over leveraged, too dependent on model, exposed to liquidity and volatility risk			
Perpetrator	Top Management	Trader, subsidiary in Singapore	Branch office staff	Top Management Strategists			
Crisis Trigger	Regulatory audit report on massive fraud	Margin call	Document was mistakenly sent to finance office	Persistent unfavourable market			
Risk Categories							
People	Fraud by owner	Employee character; employer misjudgment	Fraud by staff member	Practical skills appropriate for assessing variable parameters			
Process	Regulatory and legal compliance; inadequate documentation	Internal policy; regulatory compliance; non segregated duties	Lax internal controls; passive audit deparment; inadequated management reporting systems	Market shift (sector weight/volumes); insufficient model adjustment and stress testing;			
Systems			Missing trade reporting links				

Lessons Learned - Baseline Analysis

- **Task – Develop Next Steps**
  - From a risk management view, what should FIs do immediately after discovery of a rogue trading event?
  - What risk management tools should have been and should be in place at FIs?
  - What changes should be made to the FI IS and other risk management frameworks?

Lessons Learned - Baseline Analysis

- **Task – Groups Present Next Steps for SocGen**
  - From where should an FI response to a rogue trading event be directed?
  - Who should be involved in the response?
  - Assign roles and responsibilities to CISO, Op Risk, Technology Risk?
  - What changes should be made to FI risk management frameworks going forward?

Lessons Learned - Baseline Analysis

- **Task - Standards and Regulations – ISO/IEC 27002:2005 (ISO/IEC 17799:2005) Code of Practices for Information Security Management**
  - Which ISO/IEC 27002:2005 sections contain applicable controls?
  - Which ones are violated in rogue training scenarios?
  - Which of the IS objectives (confidentiality, integrity, and availability) were not achieved in rogue training scenarios?

Lessons Learned - Baseline Analysis

- **Standards and Regulations – BIS Basel Consulting Paper 96 on Operational Risk**
  - People
  - Process
  - Systems
  - External Events

Lessons Learned - Baseline Analysis

- **Task – Standards and Regulations**
  - Compare the list of next steps developed earlier for SocGen with the applicable sections of ISO/IEC 27002:2005? Basel Consulting Paper 96?
  - Identify any gaps between practice standards, regulatory guidance, and the next steps.
  - Compare the next steps with the assigned roles and responsibilities developed earlier?
  - Identify any gaps between what needs to be accomplished and what responsibilities were assigned?

Lessons Learned - Baseline Analysis

- **Discussion – Standards and Regulations**
  - When comparing the list of next steps developed earlier for SocGen with the applicable sections of ISO/IEC 27002:2005 and Basel Consulting Paper 96, were any gaps identified between practice standards, regulatory guidance, and the next steps?
  - When comparing the next steps with the assigned roles and responsibilities developed earlier, were any gaps identified between what needs to be accomplished and what responsibilities were assigned?

Lessons Learned – Governance Hypothesis

- **Do rogue trading events like SocGen 2007 involve an**
  - Information security risk exposure?
  - Operational risk exposure? (People? Process? Systems?)
  - Technology risk exposure?
  - Who was responsible for identifying the scenario risk (Information Security? Operational Risk? Technology Risk?)

Lessons Learned – Summary Discussion

- **Discussion – How Would the Components of a Risk-Based Approach Impact the likelihood and magnitude of a rogue trading event?**
  - Cross functional governance
  - Comprehensive risk assessment methods
  - Dynamic risk measurement methods
  - Ownership and accountability
  - Effective communication
  - Ensuring ability to quickly respond
  - Meaningful reporting mechanisms

Lessons Learned - Summary Discussion

- **Discussion – How Would the Components of a Risk-Based Approach Impact the likelihood and magnitude of a rogue trading event?**
  - Cross functional governance
    - Develop Examples of how cross-functional governance could have dampened the impact of a rogue trading event

Lessons Learned - Summary Discussion

- **Discussion – How Would the Components of a Risk-Based Approach Impact the likelihood and magnitude of a rogue trading event?**
  - Comprehensive risk assessment methods
    - Approach 4 ways
      - Information systems
      - Electronic data
      - Physical files
      - Third parties
    - Focus on accountability
    - Some overlap, but each has distinct owners
    - Use self-assessments vs. loss data or scenarios

Lessons Learned - Summary Discussion

- **Discussion – How Would the Components of a Risk-Based Approach Impact the likelihood and magnitude of a rogue trading event?**
  - Dynamic risk measurement methods
    - What's at risk?
      - Customer, corporate, operational, prospect, third-party
    - What would be the impact?
      - Financial, operational, regulatory & reputation
    - What could be the source?
      - Internal, external & natural disaster
    - What can we mitigate?
      - Prevention, monitoring & recovery

Lessons Learned - Summary Discussion

- **Discussion – How Would the Components of a Risk-Based Approach Impact the likelihood and magnitude of a rogue trading event?**
  - Ownership and accountability
    - Should responsibility belong to IT or the business?

Lessons Learned - Summary Discussion

- **Discussion – How Would the Components of a Risk-Based Approach Impact the likelihood and magnitude of a rogue trading event?**
  - Effective communication
    - How can communication programs impact the likelihood of rogue trading events?

Lessons Learned - Summary Discussion

- **Discussion – How Would the Components of a Risk-Based Approach Impact the likelihood and magnitude of a rogue trading event?**
  - Ensuring ability to quickly respond
  - Meaningful reporting mechanisms
    - How can the "meaningfulness" of reporting in light of a rogue trading event be measured?

Lessons Learned - Summary Discussion

- **Discussion – What role should training play in decreasing the likelihood and magnitude of a rogue trading event?**
  - What works?
  - What does not work?