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

<table>
<thead>
<tr>
<th>Financial Institution</th>
<th>ECCI</th>
<th>Barings</th>
<th>Gurnitomo</th>
<th>LCTM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approximate Total Loss (US$ bn)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss as % of Capital</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss to Creditors</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Factors</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perpetrator</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crisis Trigger</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Categories</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>People</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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)**
  - 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.
Lessons Learned - Baseline Analysis

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

<table>
<thead>
<tr>
<th>Function</th>
<th>Trade Entry</th>
<th>Position Maintenance</th>
<th>Confirmations</th>
<th>Settlements</th>
<th>Accounting Entries</th>
<th>General Ledger</th>
<th>Valuation</th>
<th>Payments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Standards and Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology Layer</td>
<td></td>
<td>Trading System</td>
<td></td>
<td></td>
<td>Trade Processing System (like Elliot)</td>
<td>GL System</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Trade Processing System (like Elliot)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SV/IFT/EuroClear/other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Lessons Learned - Baseline Analysis

• Task – Profile the Société Générale Event

<table>
<thead>
<tr>
<th>Financial Institution</th>
<th>DCCI</th>
<th>Darroch</th>
<th>Suriombo</th>
<th>LCTM</th>
<th>Société Générale</th>
<th>Similarities</th>
<th>Differences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year</td>
<td>1991</td>
<td>1995</td>
<td>1999</td>
<td>1999</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approximate Total Loss (USD, bn)</td>
<td>12</td>
<td>8.2</td>
<td>28</td>
<td>44</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss as % of Capital</td>
<td>10%</td>
<td>10%</td>
<td>59%</td>
<td>84%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location of Trade</td>
<td>Asia</td>
<td>Asia</td>
<td>Asia</td>
<td>Asia</td>
<td>Asia</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Institution</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Profile</td>
<td>Fraud, money laundering, unauthorized trading</td>
<td>Loss of confidence in options and futures, loss of confidence in the market, derivative trading losses</td>
<td>Loss of confidence in options and futures, loss of confidence in the market, derivative trading losses, profit</td>
<td>Over leveraged, too dependent on model, exposed to liquidity risk, volatility risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perpetrator</td>
<td>Top Management</td>
<td>Trader, subsidiary in Singapore</td>
<td>Branch office staff</td>
<td>Top Management Strategies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case Trigger</td>
<td>Regulatory audit report on massive fraud</td>
<td>Margin call</td>
<td>Document was mistakenly sent to wrong clients, Persistent unfavorable market</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
</tr>
<tr>
<td>Fraud by owner</td>
</tr>
<tr>
<td>Employee</td>
</tr>
<tr>
<td>Fraud by staff</td>
</tr>
<tr>
<td>Practical skills appropriate for assessing variable parameters</td>
</tr>
<tr>
<td>Process</td>
</tr>
<tr>
<td>Regulatory and legal compliance, regulatory compliance, non-compliance</td>
</tr>
<tr>
<td>Market risk (credit, market, liquidity)</td>
</tr>
<tr>
<td>Systems</td>
</tr>
<tr>
<td>Missing trade reporting roles</td>
</tr>
</tbody>
</table>
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

  - 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?
  - 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?