Metricon 4 The “Ugly, The Bad, The Good”

August 11 2009
Montreal, Canada
Lloyd Ellam
Vice President
Risk Science and Innovation
Table of Contents

- Security as Risk
- SigmaRisk Perspective
- Value of Security
- Industry Observations
Meet the Team Leader

Lloyd Ellam
Vice President, Risk Science and Innovation

Experience
- Cyber risk assessment and control specialist
- Team Leader for secure semiconductor solution and first successful chipset
- Experienced in many mixed technology processes and test methodologies
- Team Leader for high speed and secure data collection satellite and ground-based systems. Developed verification and control system for seismic monitoring and control
- Engineering and service leader for “mission critical” computer control systems for a global computer supplier. Developed modeling, simulation, and training for “hard down” utility controls
- NATO and NORAD line officer specializing in Electronic Warfare. Crisis control training in nuclear, chemical, and biological disasters. Liaison to civilian authorities on national and international infrastructure

Education
- Bsc.Eng., The Royal Military College
- MSc (Physics) Strathclyde
The mission of SigmaRisks is to deliver highly valuable enterprise risk management professional services to large enterprise and government customers.

SigmaRisks uses a combination of proprietary and industry standard practices to:
- Identify
- Quantify
- Mitigate and
- Transfer risk.
The Proposition today

- Expand on previous presentation area to show examples of business value of security. Yes this is the back up presentation.

- Technology for quantification of complex scenarios based on the Precautionary Principle.

- Review three examples of client scenarios where security ranged from non existent to a true business enabler.
Good Enough Security

- You have heard this from Dan before

- Good Enough is Good Enough

- Good Enough always beats perfect

- The difficult part is determining what is good enough
What is Security?

- Security is a “State”.
  - As a “state” Security is most often an intangible asset.
  - However Security is an asset and can be valued.

- Security as a “State” is obtained by integrating to the enterprise.
  - Best Practices
  - Technology Solutions
  - Human Factor Interactions
    - Cultural Myopia
What Security is Not

- Security is not Static. By definition therefore it must be Dynamic.
- Static solutions to a Dynamic problem will fail.
- There is no Silver Bullet.
- One Size Doesn’t fit all.
SigmaRisks delivers ERM services around the four key pillars of business risk:
- Strategic
- Financial
- Hazards
- Operational

**Identify**
- Enterprise threat/risk assessments
- Program/project threat/risk assessments
- Scenario facilitation
- Compliance assessments to a variety of policies, standards and regulations
- Privacy impact assessments
- Risk mapping and prioritization

**Quantify**
- Risk Modelling
- Digital asset valuation
- Process valuation
- Financial model development
- Prioritized risk mapping
- Scenario facilitation

**Mitigate**
- Crisis management consulting
- Business recovery planning
- Disaster recovery planning
- Risk operations and monitoring solutions
- Service level agreements
- Identity and access consulting and systems integration
- Security event management systems
- Integration of security and compliance tools

**Transfer**
- Service Level Assurance program development and operation
- Service level identification, measurement and monitoring solutions
- Technical warranty programs
- Insured solutions
- Underwriting submissions
Lack of Security

- Under funded Security
- Misrepresented Benefits - Today
- Reduced Credit Rating
- Inefficient Operation
- Errors in operations
- Limited Audit
- Fraud & Employee Theft
- Less Money to Pay Employees
- Misrepresented Benefits - LT
- Errors within Client
- Inefficient Operation
- Misrepresented Benefits - LT
- Unhappy Politicians
- Unhappy Employees
- Unhappy Clients
- Unhappy Retirees
- Unhappy Politicians
- Unhappy Employees
- Unhappy Clients
- Unhappy Retirees
- Bad Press
- Law Suit
- Reduced Funding

Stakeholders

- Good Internal Communication
- Good Board Direction
- Trust = Contract Commitment
- Accountability
- Knowledge Management
- Data Integrity
- Internal Reporting
- Knowledge Management
- Compliance
- Portfolio Concentration
- Ability to Influence Outcome
- Matching Assets to Liabilities

- Reduced Funding
- More Taxes
- Write-off Acct Receivables
- Over Paying Suppliers
The External Environment is driving the need for higher standards of corporate governance. Public companies are subject to increasingly higher standards of corporate governance in today’s post Enron environment. Regulation is growing more visible & powerful: Sarbanes Oxley, SEC, NASD, OCC, Federal Reserve, OTS, Basel II. Increasing standards for Audit Committees and Internal Auditors & now General Counsels who increasingly will report directly to the Board. Financial reporting transparency mandates greater risk disclosure & reduces the time cushion to disclose. European Accounting approach may revive use of the Pro Forma to estimate earnings with a confidence range. S&P and ISS broaden their Rating Process to include SOX considerations. Stakeholders are more demanding with suits larger and voting for Directors more open. Hardening of the insurance markets is leading to reduced cover, increased costs and greater risk retention especially for D&O coverage.
Quantification

Define Success and the appropriate Risk Evaluation Criteria

Identify the Most Critical Risks

Understand the Consequences of each Critical Risk

Understand what Drives each Critical Risk

Identify common Drivers among the Critical Risks

Identify common Consequences among the Critical Risks

Identify the Critical Questions that must be answered using External Data

Quantify each risk’s Adverse Impact

Quantify each risk’s Likelihood of Occurrence

Compute & Net the Inter-dependencies

Lay out The Options for the Risk Management Strategy

External Data

Proprietary External Data

Internal Company Interviews & Workshops

Internal Company Data
The key to quantification is External Data Gathering which often requires data from outside the company.
Meet a Team Member

Mark Braverman, Ph.D.
Human Impact Leader

Experience

- President, Crisis Management Group, Inc.—providing corporate crisis management, employee assistance, and organizational consulting to corporations and public agencies
- Provided training, case management, and acute crisis response to over twenty Fortune 500 companies and to numerous Federal Agencies, including the United States Postal Service
- Instructor, Harvard University School of Medicine Department of Psychology
- Co-Founder, Harvard University Center for Psychological Trauma Studies
- Developed innovative approaches to the prevention of traumatic stress across diverse groups
- Specialist in intervention with groups in community and workplace settings in the aftermath of a trauma or disaster
- Widely published, lectures and trains internationally on workplace violence, crisis intervention, and occupational mental health

Education

- PhD, Clinical Psychology, Boston University
- Ed.M, Human Development, Harvard University
- BA, English and Comparative Literature, Columbia University
Frank P. Terzuoli
Financial Compliance

Experience
- Financial management at Citibank (Division CFO), Wells Fargo
- Mergers & Acquisitions specialist at Ford Financial
- Supervising Engineer at AT&T-conduit distribution planning
- Principal at Arthur Andersen & Accenture’s financial institutions practice — enterprise risk, financial & strategy consulting
- Responsible for the development of sophisticated financial and economic models designed to determine shareholder value of unique operations
- California regional bank — small business Hispanic Market evaluation and credit risk analysis
- Large Credit Card company — credit risk modeling and forecasting
- Large California bank — trust regulatory-compliance analysis. Customer relationship manager data mapping
- Large Southern bank — distribution economic model for branch network; site evaluation modeling; consumer surveying

Education
- Graduate studies in finance, New York University
- MBA, Adelphi University
- BS, Rensselaer Polytechnic Institute (Physics)
Example One…. The Ugly

- Merger banking institution retained us for 5 company merger and acquisition.
- Had heard all of the warning signs.
  - No Security plan
  - No history of events or logs
  - Unidentified security responsibility

- It was worse..
  - Software still in shrink wrap
  - Firewall turned off
  - Policies that existed were not enforced.
The Cost...

- About one billion in assets under management
- Buyout not approved
  - Security was not the sole factor but major.
  - Loss to investors of 19% value in holdings

- Aftermath.
  - Inbound spoof campaign diverted funds to Belize corporation
  - Customer list had been compromised
  - First four claims exhausted all available funds.
  - Company non existent
The Bad….

- Financial Institution
- Ongoing Security spend was not matched to enterprise exposure
- Management identified the need but were unable to support internal funding requirements.
- With security identified response to event was able to occur
The event....

- Personal records were sent to public domain through human error.

- Response began on a Sunday afternoon....

- Legal advised all exposures complete by Monday afternoon.

- Cost saving to organization. $17,000.00 per file
The Good.....

- Retail Outlet

- Had completed an Enterprise wide assessment.

- Security had been funded and incorporated into all strategies from production to backup and recovery.
The event:

- Alternate data centre was compromised physically.
- Data was encrypted.
- Backup was effective for operation
- Recovery was complete in 48 hours.
- Insurance paid the claim
- Reconstructed the valuable data as asset had been scheduled.
- Savings of 3 million due to complete payout of loss.
In Security there are constants……never enough money and

Never enough time...

Thank you for yours
SigmaRisks CORPORATION

- Tel: (613) 216 2271
- www.SigmaRisks.com

- Email: info@SigmaRisks.com
- Email: Lloyd.Ellam@sigmarisks.com