SECURITY RISK MANAGEMENT

FROM TECHNOLOGY VISION TO MARKET REALITY

Avi Corfas, VP EMEA – Skybox Security

FIRST 2007

Seville, Spain

skybox security

Topics

- The Risk Assessment Challenge
- What Is IT Security Risk Management?
- The technology
- The process – from dream to product to market leader

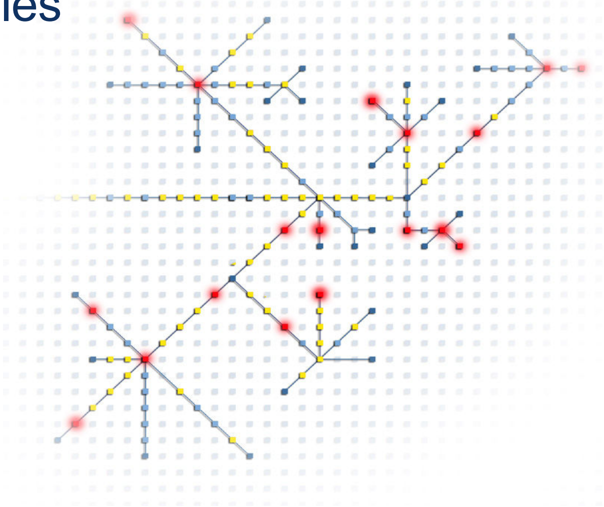
The Risk Assessment Challenge

*What you don't know **<u>can</u>** hurt you*

- *Measuring infrastructure risk is a security and a governance requirement.*
- *Despite fortunes invested, IT infrastructure security remains the **great unknown***
  - Lack of visibility – poor decisions
  - Too much information – need for automation

The Task is Significant

- Assessing IT infrastructure risk is more of an art
- Impossible to connect all the dots due to information overload
  - 10’s or 100’s of business applications
  - 1000’s of servers, routers & firewalls
  - 10,000’s security controls and access rules
  - 10,000’s of vulnerabilities
- Continuous state of change
  - New vulnerabilities published daily
  - Constant network changes



However…the Task Can Be Simplified

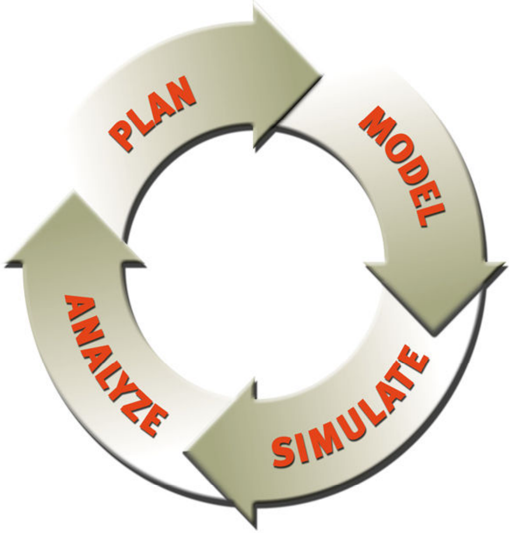
Through advanced analytics, performed on a virtual model, an organization’s security risk profile can be measured and risk exposure proactively reduced, while gaining insight into how effective security controls and access rules are.

We Call This….

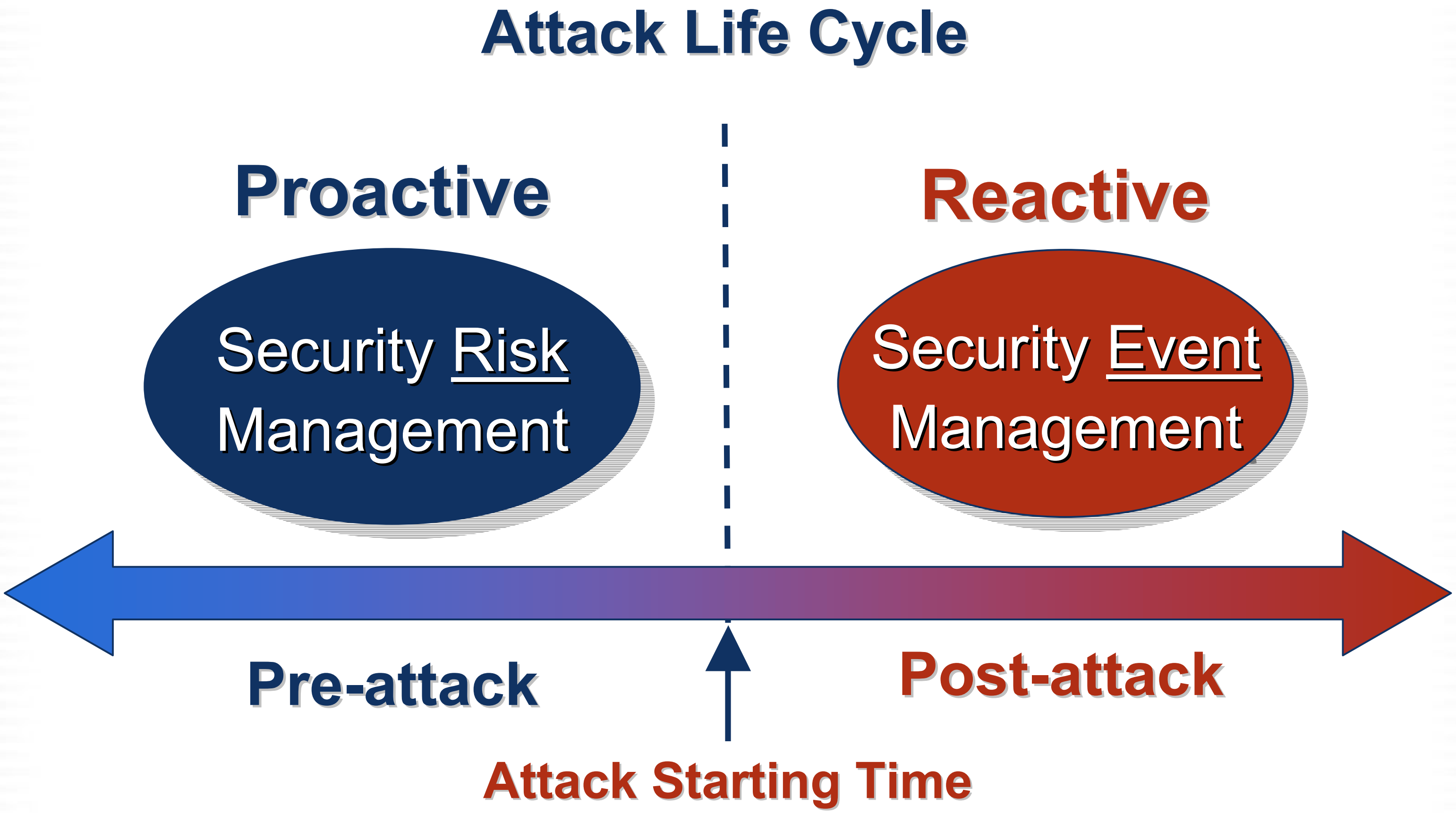
Security Risk Management for IT Infrastructures

What is IT Security Risk Management?

The complete process of understanding threats, prioritizing vulnerabilities, limiting damage from potential attacks, understanding the impact of proposed changes or patches on the target systems and the business, ***and measuring all of the above****.*



How is SRM Different Than SEM?



Attack Life Cycle

Proactive

Security Risk Management

Reactive

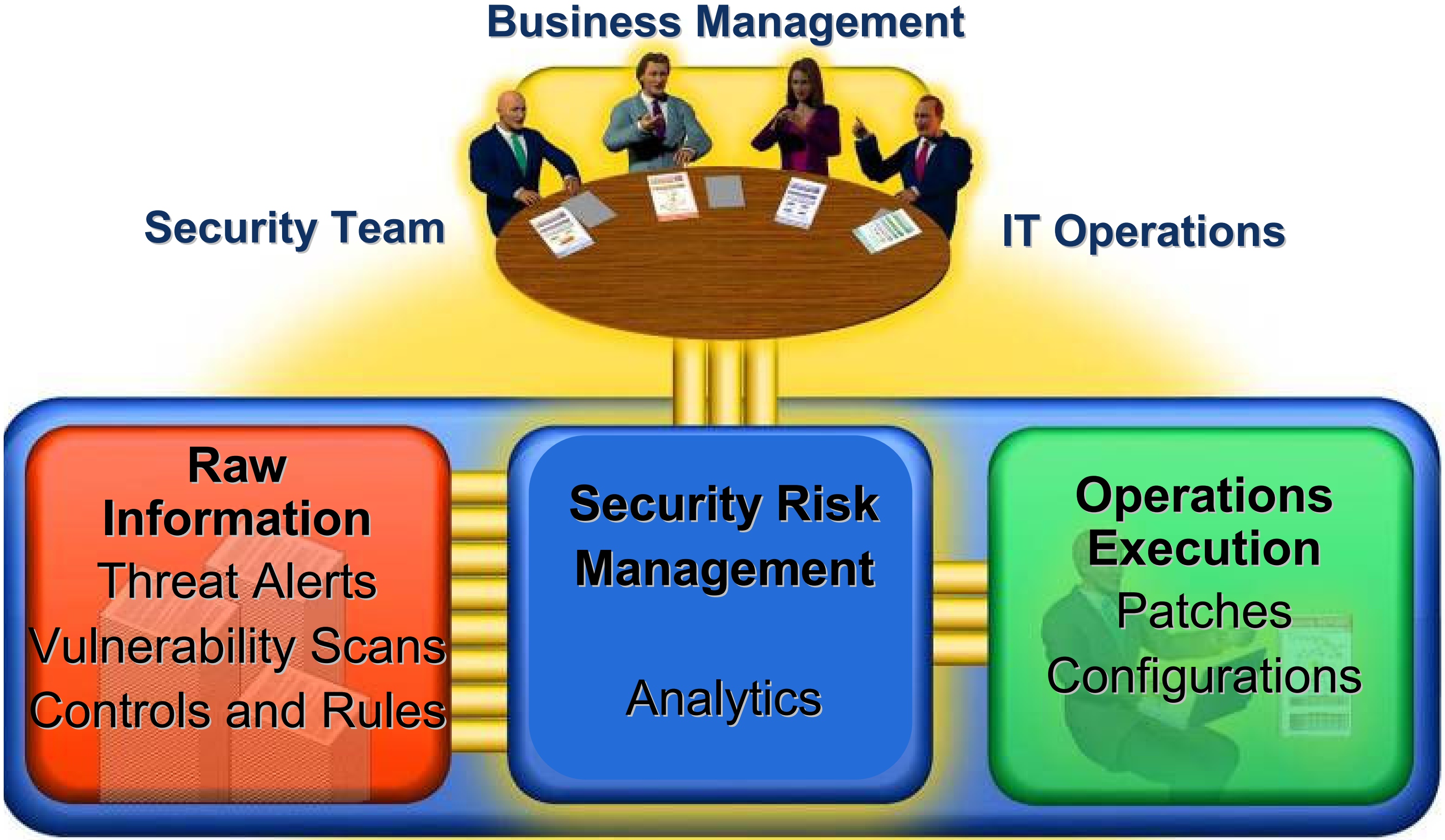
Security Event Management

Pre-attack

Post-attack

Attack Starting Time

Where Does SRM Fit?



Business Management

Security Team

IT Operations

Raw Information

Threat Alerts

Vulnerability Scans

Controls and Rules

Security Risk Management

Analytics

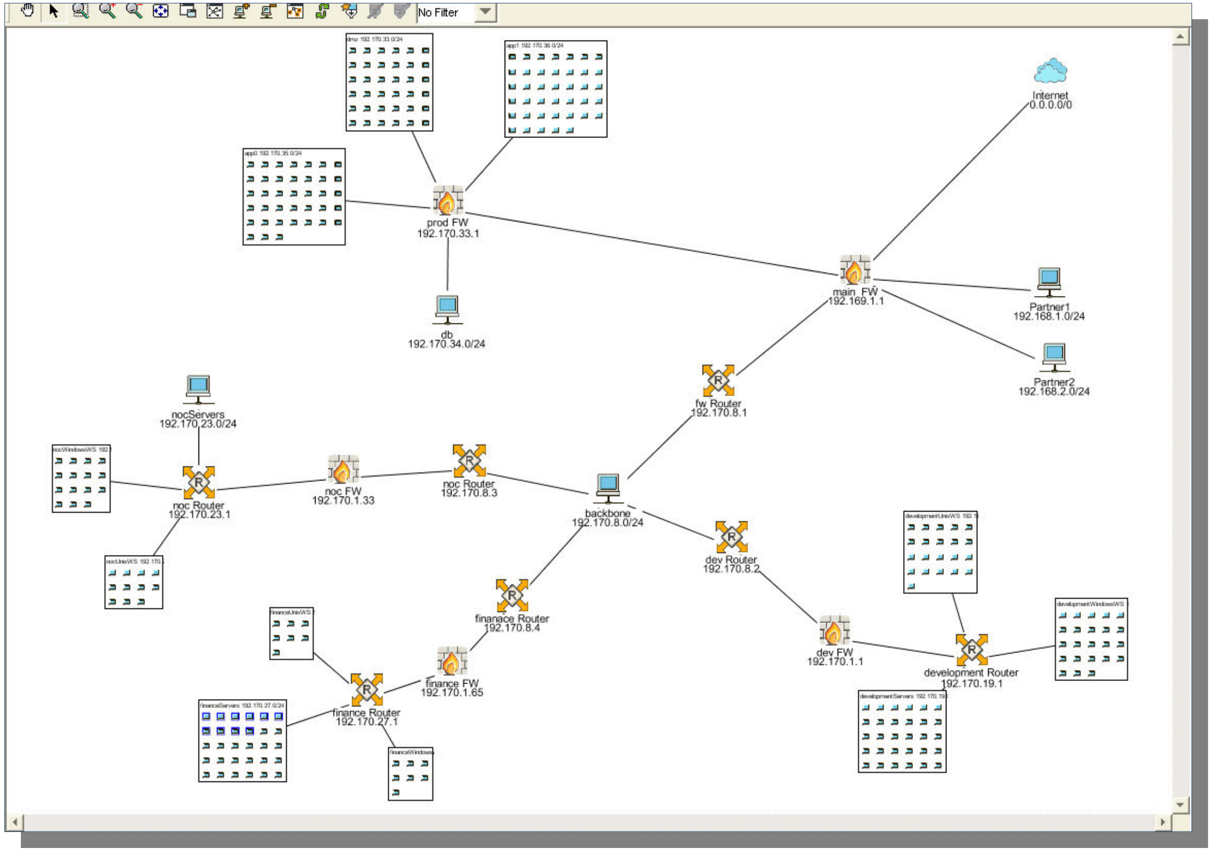
Operations Execution

Patches

Configurations

How Does SRM Work?

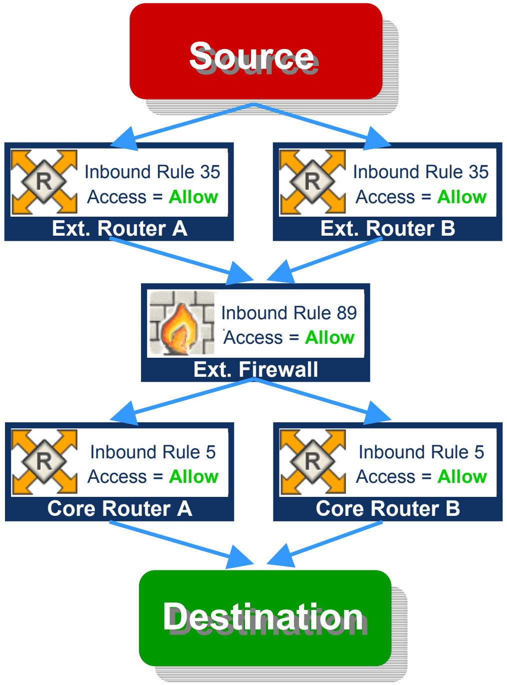
It All Starts With a Virtual Model



Single View of Threats, Controls and Policies

Simulation

Access Analysis



Source

Inbound Rule 35
Access = Allow
Ext. Router A

Inbound Rule 35
Access = Allow
Ext. Router B

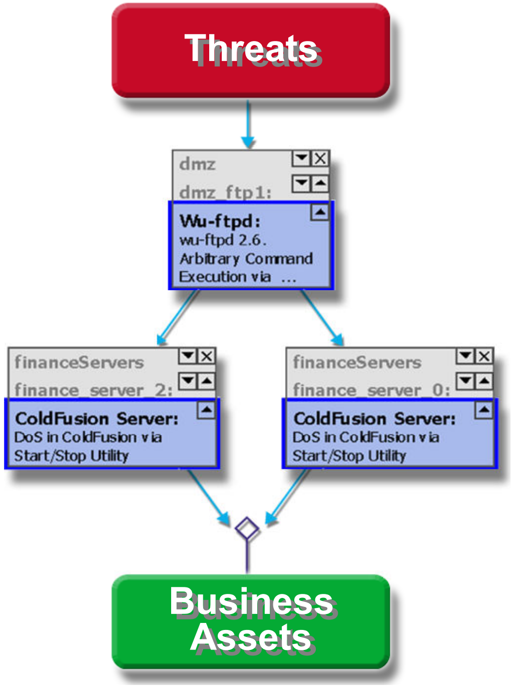
Inbound Rule 89
Access = Allow
Ext. Firewall

Inbound Rule 5
Access = Allow
Core Router A

Inbound Rule 5
Access = Allow
Core Router B

Destination

Attack Paths



Threats

dmz
dmz_ftp1:
Wu-ftpd:
wu-ftpd 2.6.
Arbitrary Command
Execution via ...

financeServers
finance_server_2:
ColdFusion Server:
DoS in ColdFusion via
Start/Stop Utility

financeServers
finance_server_0:
ColdFusion Server:
DoS in ColdFusion via
Start/Stop Utility

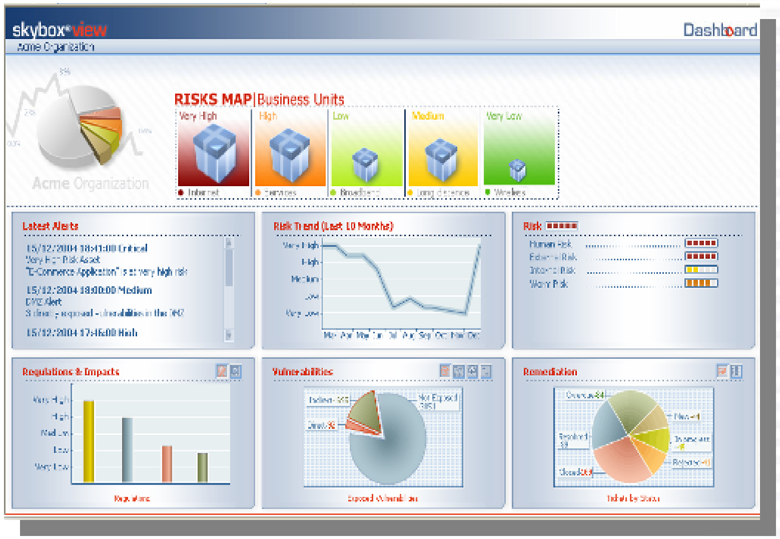
Business
Assets

War Games for Business

PLAN
MODEL
SIMULATE
ANALYZE

Analysis

- Business Impact Analysis
  - CIA (Confidentiality, Integrity, Availability)
  - Regulation (SOX, HIPAA…)
  - Damage levels
- Audit firewalls and uncover network policy violations



Latest Alerts

15/12/2004 18:41:00 Critical
Very High Risk Asset
"E-Commerce Application" is at very high risk

15/12/2004 18:00:00 Medium
DMZ Alert
3 directly exposed vulnerabilities in the DMZ

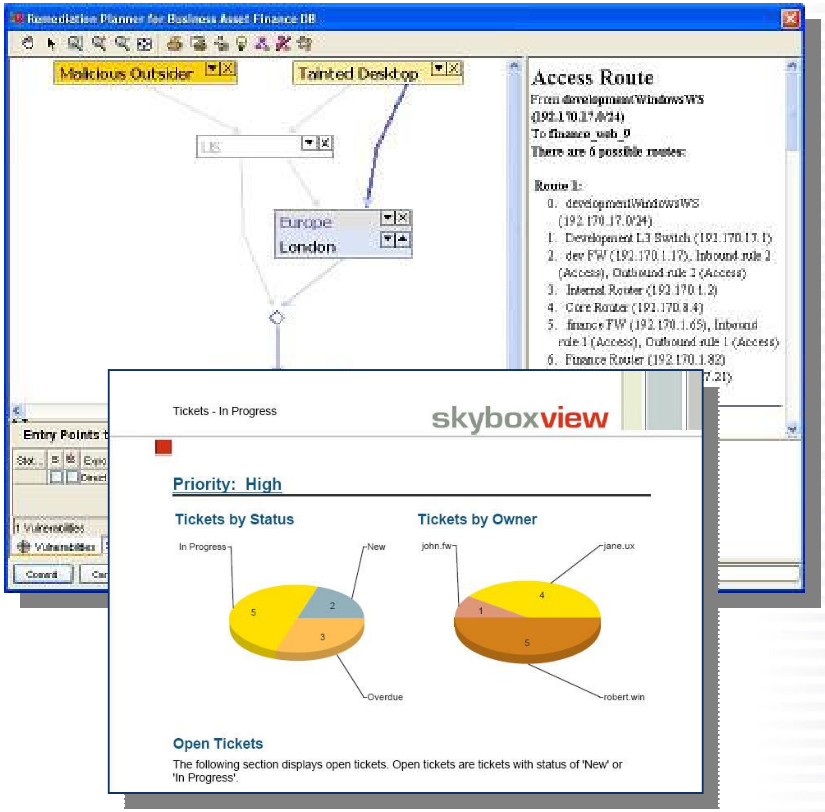
15/12/2004 17:46:00 High

- Test and validate network configuration before deployment

Managing the Risks That Matter

Mitigation Planning and Reporting

- Determine the most effective countermeasures
- “What-if” scenarios
- Workflow automation
- Reports geared for technical and business audiences



Access Route

From developmentWindowsWS (192.170.17.0/24)

To finance_web_9

There are 6 possible routes:

Route 1:

0. developmentWindowsWS (192.170.17.0/24)
1. Development L3 Switch (192.170.17.1)
2. dev FW (192.170.1.17), Inbound rule 2 (Access), Outbound rule 2 (Access)
3. Internal Router (192.170.1.2)
4. Core Router (192.170.8.4)
5. finance FW (192.170.1.65), Inbound rule 1 (Access), Outbound rule 1 (Access)
6. Finance Router (192.170.1.82)

Tickets - In Progress

Priority: High

Tickets by Status

Tickets by Owner

Open Tickets

The following section displays open tickets. Open tickets are tickets with status of 'New' or 'In Progress'.

Plan Optimal and Safe Countermeasures

SRM examples

Automating the Risk Assessment and Mitigation Planning Process

- **Challenge:** Annual IT risk assessment audit performed by a team of 10 people. Due to constant network change and daily influx of new vulnerabilities findings quickly became obsolete. **Goal:** Move to a continuous and automated process.

- **Challenge**: Information overload. Vulnerability Scanners discovered 8500 vulnerabilities with over 1600 ranked as severe or critical. Over 20,000 security controls and access rules. **Goal:** Prioritized security battle plan, based on understanding which vulnerabilities are directly or indirectly exploitable according to the network access rules in place.

- **Challenge**: Hundreds of network configuration changes processed weekly. Network engineers unable to validate if proposed changes expose the organization to unacceptable risk. **Goal**: Reduce change validation process from weeks to hours.

Other potential SRM use cases

- Calculate impact of changes on network resilience
- Calculate impact of authentication controls on security risk
- Calculate impact of changes on performance
- Integrate Security Risk with other forms of Operational Risk
- SRM on data, applications, etc.

Summary - SRM Can Help

1. Continuously measure your organization’s IT security risk profile
2. Build a defensible case for your security control set
3. Prioritize risk reduction projects based on their business impact
4. Deploy scarce resources on the risks that really matter (ROI)
5. Automate labor-intensive tasks and achieve operational efficiency
6. Measure and track the level of security and improvement

Entrepreneurial challenges

- Technology
- Culture
- The meaning of life

Technology Challenges

- Consistency
- Scalability
- Integrability
- Manageability
- Usability
- Maintainability

Cultural questions

- Conviction vs. communication
- Engineering vs. sales
- Local vs. global
- Hierarchy vs. cooperation
- Strong leadership vs. consensus

Fundamental questions

- Is it doable?
- Can we make a market?
- What exactly is that I am trying to sell?
- How fast should I run?
- Who are my constituents?
- Whose mistakes can I learn from?
- When should I let go?

A guide to the perplexed

- Do thorough research
- Surround yourself with experienced people you trust
- Make sure you can deal with failure and with success – and with a few years of not knowing the result
- Then, but only then, run as fast as you can to the goal!

skybox® security

MANAGING THE RISKS THAT MATTER