

# Bringing A New Operational Discipline to Network Security

**Transforming today's labor-intensive efforts of guesswork into predictable, automated, risk-driven business processes.**

**Christofer L. Hoff**  
**Chief Architect, Security Innovation**  
**Unisys**

# Topics For Discussion

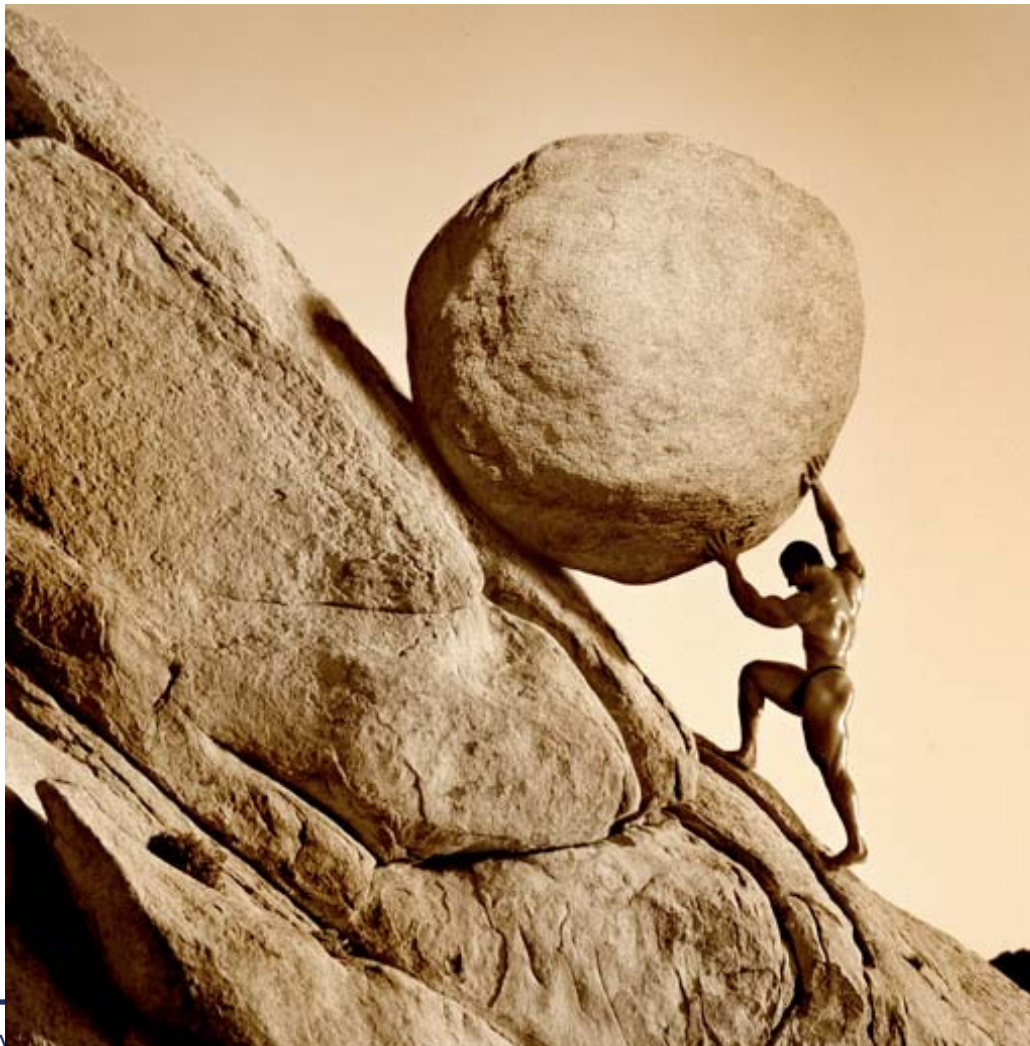
- **The Hamster Wheel Of Pain & Why Security Is Like Bell-Bottom Pants**
- **Managing Risk Is a Business Problem**
- **Transforming guesswork into predictable, automated, risk-driven business processes**
- **Risk Analytics & Modeling: Because Hope is Not a Strategy**
- **A Practical Roadmap for Managing Risk, Assuring and Improving Service Delivery**



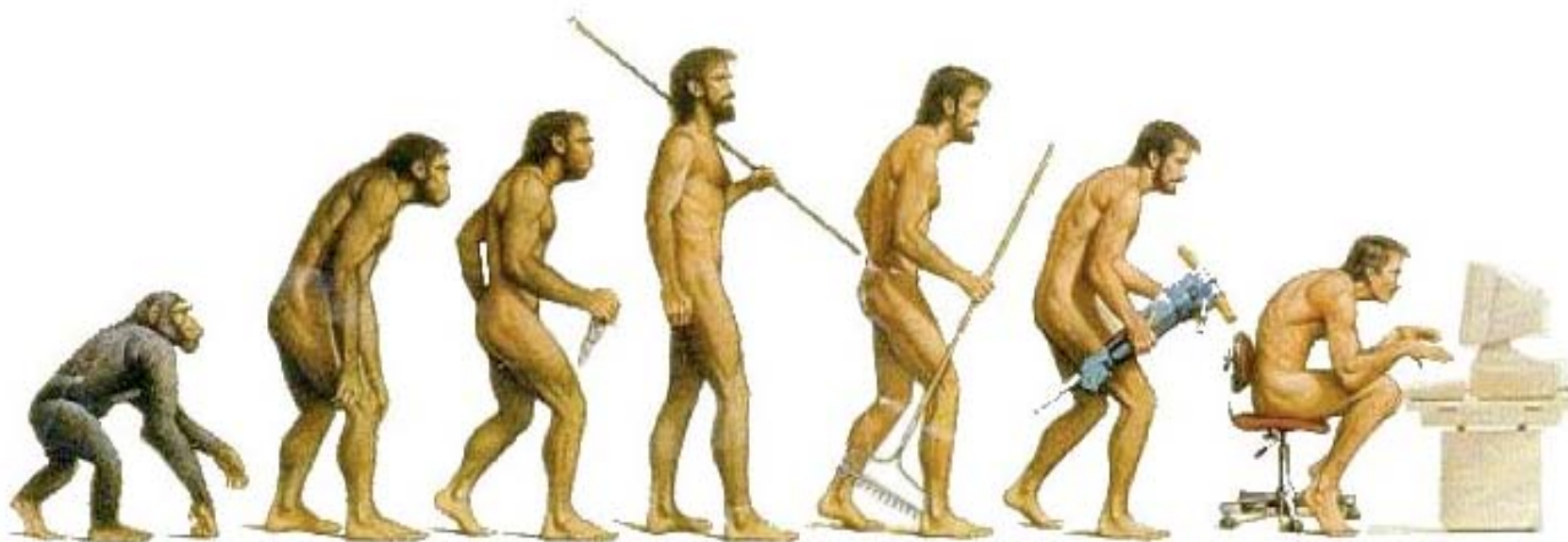
# InfoSec – Where Every Day Is A Holiday!



# The Network/Information Security Sisyphean Challenge

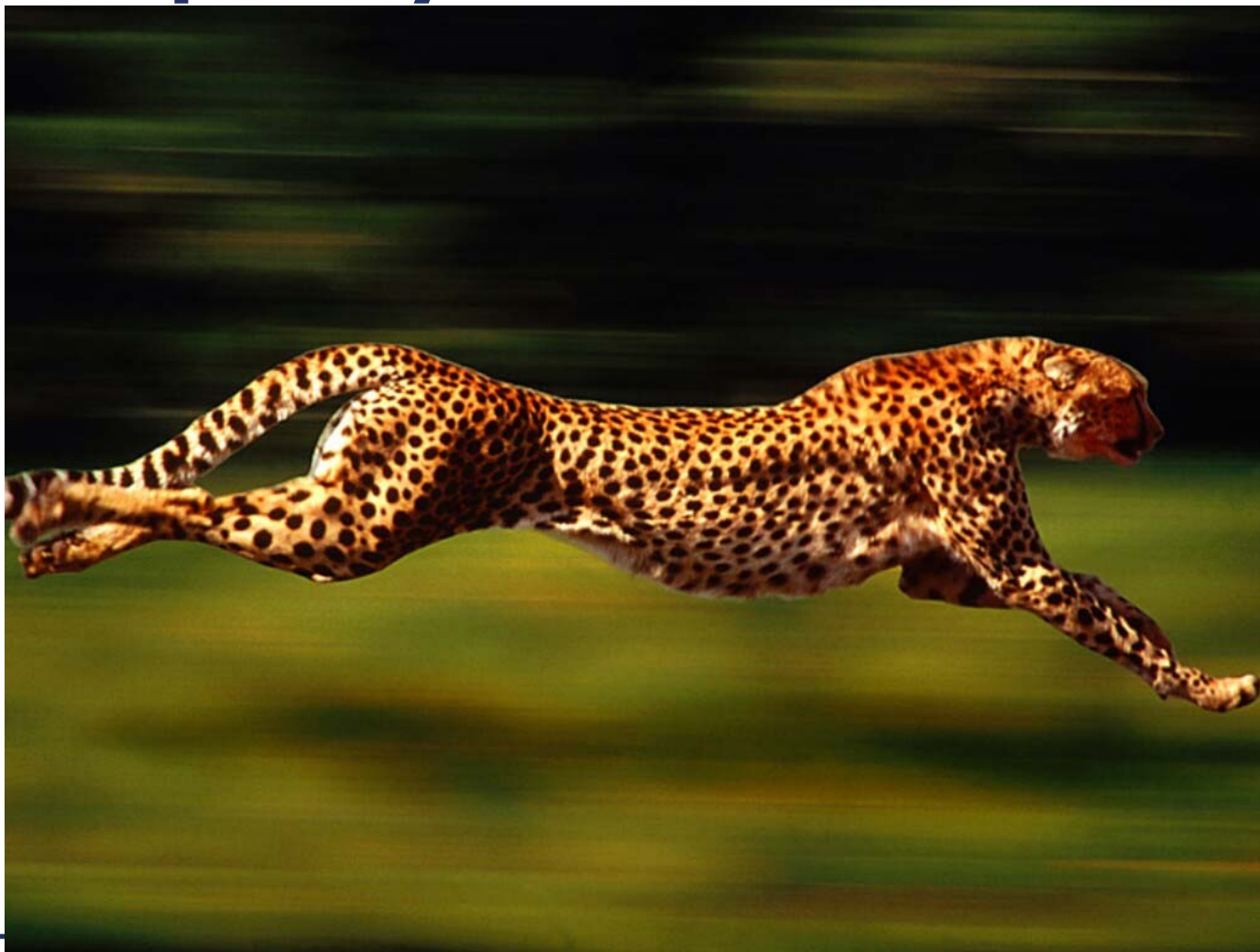


# Change Happens...





# ...and quickly



# A Tool for Every Job



# Everything Is Connected

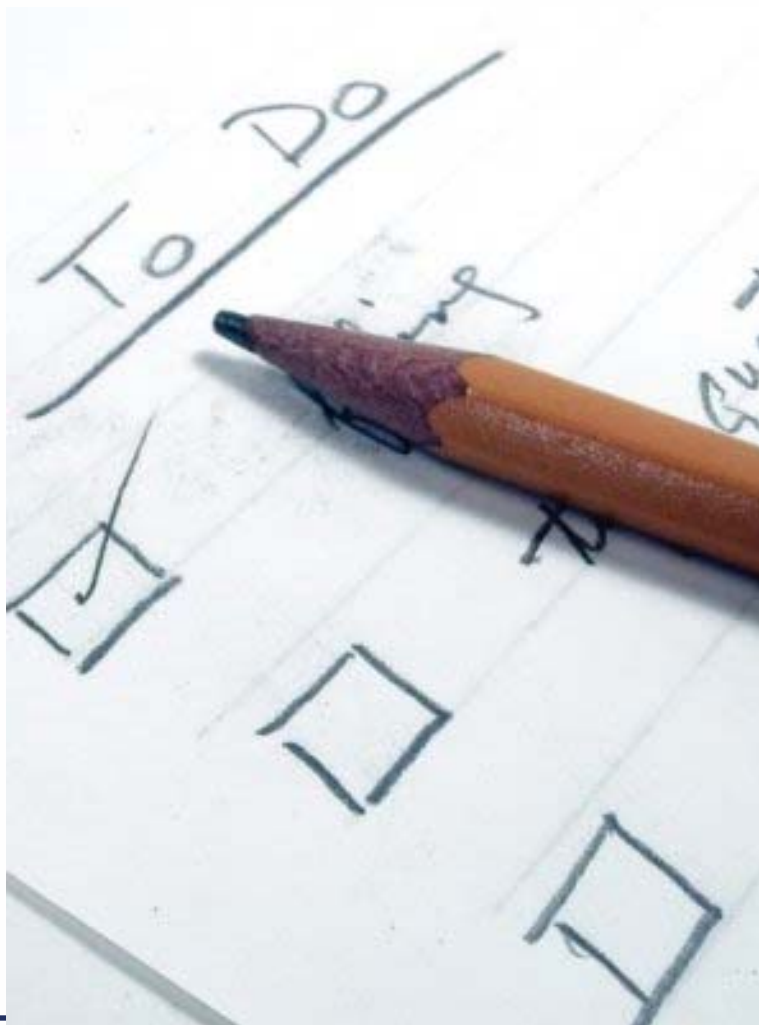




# Lots of Folks Along for the Ride



# Maintain Alignment to the Business



# Provide Transparency & End-to-End Visibility



# Maintain Service Levels



# Keep Business Impact in Context





# Use Consistent Language



# Maintain Compliance & Satisfy Governance



# ...Manage Risk For the Things That Matter Most



# **Ideally, Our Solutions To These Problems Would...**

# Bolt-on / Integrate With Existing Machinery





# Provide a Single Pane of Glass

Change Management

Risk

Compliance

Audit

Governance

IT

Business

Security



# Deliver Actionable Intelligence



# Be Timely & Not Temporally Inaccurate



# Function In An Automated Fashion



# Allow For Predictive What-If Modeling





# Communicate Business Impact & Risk



# Whilst Avoiding the Hamster Wheel Of Pain...



# **A Guided Tour**

**Observations from the Front Lines  
From the Perspective of a CISO, a  
Vendor and an Integrator**

**(Who all happen to be me)**

# Our “Security” Challenges

- **Allow the business to do what they need in a manner consistent with appetite for risk in a “secure” and “compliant” state**
- **Reduce costs, do more with less**
- **Recognize we are a service delivery function & accept that our role & function needs to radically change**
- **Deliver a consistent way of measuring and communicating**
- **Manage risk to focus on the things that matter most while still tactically handling threats and mitigating vulnerabilities**

# What We Really Wanted to Answer

- Are we more/less “secure” than we were last week/month/quarter/year?
- How do we stack up next to our peers or competitors?
- ■ Are we getting value for our security investment and spending on the right things?
- Can we communicate this with appropriate measures and metrics that are quantifiable, informative and actionable?
- Can we measure, model and manage our **risk?**



# Our Navel Gazing Showed...

- We had lost the language that defined what we did
- We were perceived as a grudge purchase and a cost center that was not aligned to the business
- Thought of as reactive and focused on solving the wrong sets of problems
- We provided a narrowly-focused, technology-centric view of the enterprise
- Our models were flawed, our metrics worse
- **Threats & vulnerabilities did not represent the business problem, but managing risk did...**

# Our Goals -- “There Is No Try, Only Do!”

- Make “securing” the business a business problem
- Describe modeling, measuring, managing and expressing risk as something the CxO understands
- Integrate business processes and technology with an automated information-centric perspective of managing risk, not solely threats and vulnerabilities
- **Present a holistic view of enterprise risk as expressed as a function of business operations, not just compliance or security**



# Five Digestible, Bite-Sized Chunks.



- 1. Get Control of the Estate**
- 2. Provide a Unified & Consistent Model of Assets and Infrastructure**
- 3. Take Control of the Change Assurance Problem**
- 4. Transition from Managing Threats & Vulnerabilities to Managing Risk**
- 5. Align to Measurable Externally-Referenced Frameworks & Metrics**

# Phase 1: Get Control Of the Estate

## ■ Device Focused:

- Construct the asset portfolio
- Document the supporting infrastructure
- Baseline, globalize, standardize and optimize configuration standards
- Determine & correct the RCA of defects
- Stop the bleeding

# Phase 2: Provide a Unified & Consistent Model of Assets and Infrastructure

## ■ Model-Focused:

- Employ modeling/analytics solution to integrate & visualize the assets, infrastructure, and controls into a single model
- Integrate assets, network and control portfolio into SLA reporting along with “compliance”
- Define policies for service assurance, compliance, and governance
- Provide a single “Looking Glass” view
- Automate the process



# Phase 3: Take Control of the Change Assurance Problem:

## ■ Process Focused:

- Institutionalize Governance and Risk Assessment Processes
- Use modeling/analytics solution to manage & assure change across controls & network; planned or unplanned
- Complete the quality and validation feedback loop
- Proactively manage and measure security elements & cascading impact before they go Boom!
- Measure against policies & SLA's

# Phase 4: Transition From Managing Threats & Vulnerabilities to Managing Risk

## ■ End-to-End Service & Risk-Centric Focus:

- Integrate & institutionalize risk assessments as a business process
- Integrate business impact, threat origins, attacker skill into model; unite infrastructure with intelligence
- Drive fact based and objective decision making
- Focus on protecting the services that matter, not the platforms
- Dial up / down controls vs. resulting cost base
- Support future business decisions using modeling
- Migrate to quantitative versus qualitative measures
- Present one version of the truth

# Phase 5: Align to Measurable Externally Referenced Frameworks & Metrics

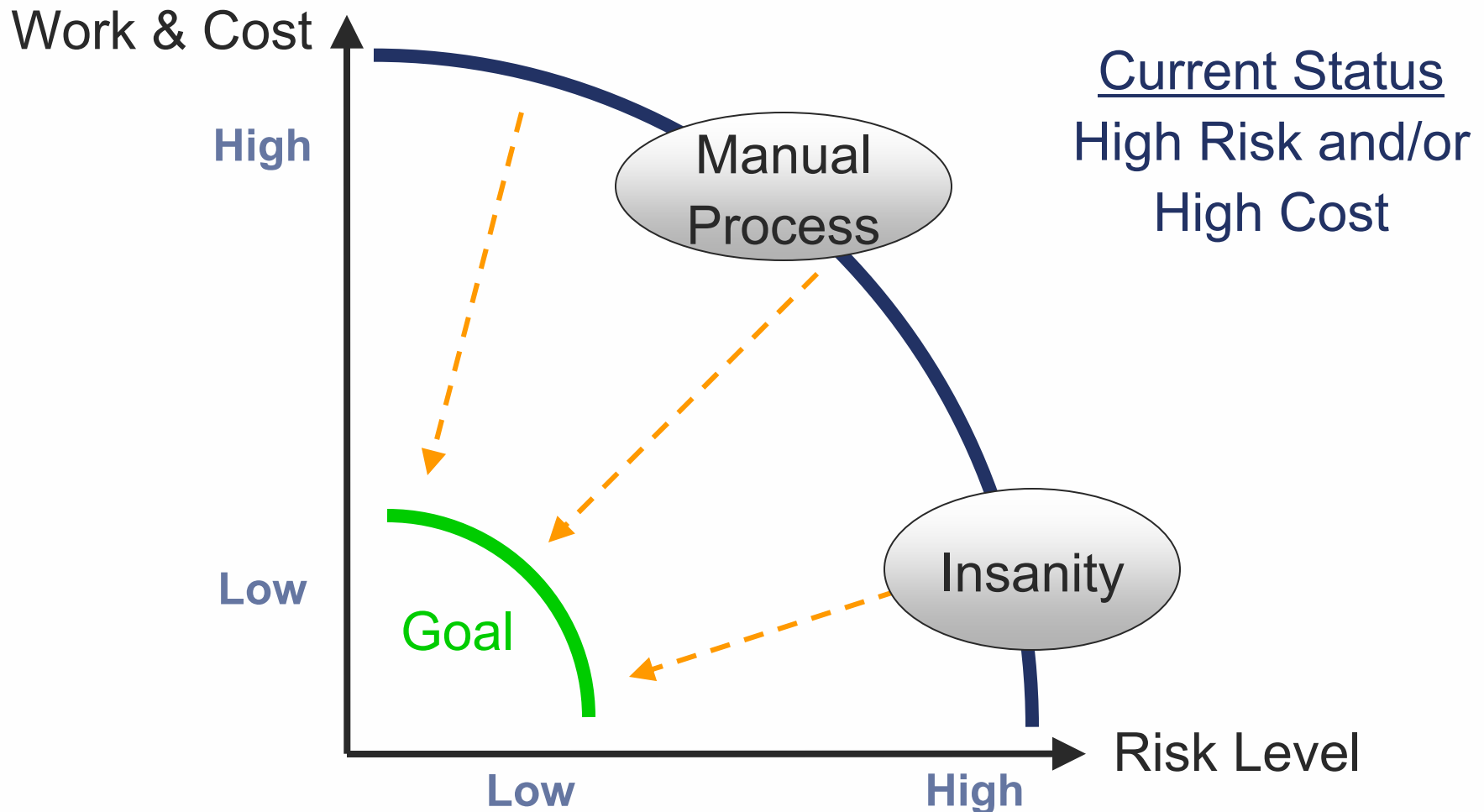
## ■ Measure and Compare

- Provide consistency in measurement that can be shared and compared externally
- Utilize standards-based frameworks CoBIT, ITIL, ISO for measurement alignment
- Communicate capability maturity as a function of risk posture
- Demonstrate compliance through transparency
- Measure effectiveness in terms of service assurance

# **Improving Our Operational Discipline By Deploying a Better Mousetrap**

## **Using Modeling & Risk Analytics To Level the Playing Field**

# Risk vs. Work Load Trade-off



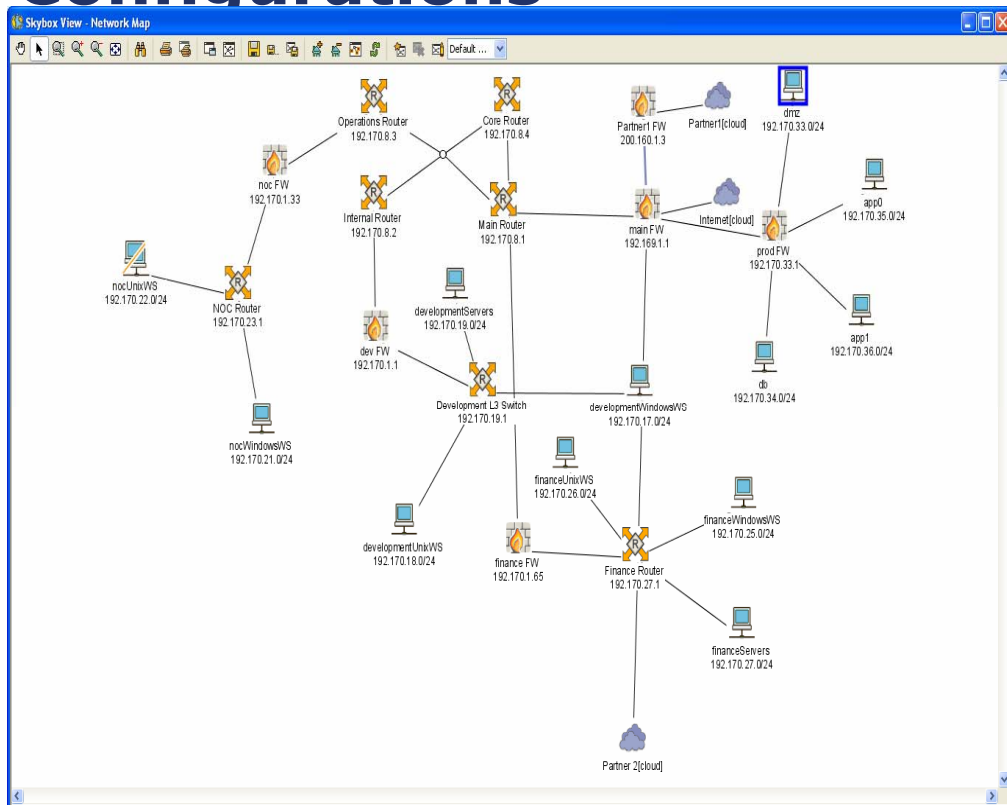


# The Value Proposition By Tactical Example

- **69,384 Total Vulnerabilities (Sev. 1-5)**
- **1,116 Directly Exposed Vulnerabilities with no compensating controls (regardless of threat)**
- **384 Single-Step Exploitable Assets w/threats**
- **16 of which impact your most important assets by increasing risk to an unacceptable level**
- **Mitigated by deploying 2 patches on 4 hosts and**
- **Instantiating 3 Firewall/ACL rules 2 firewalls...**

Which brings your exposure, once managed/mitigated, from  
\$670,000 down to \$240,000

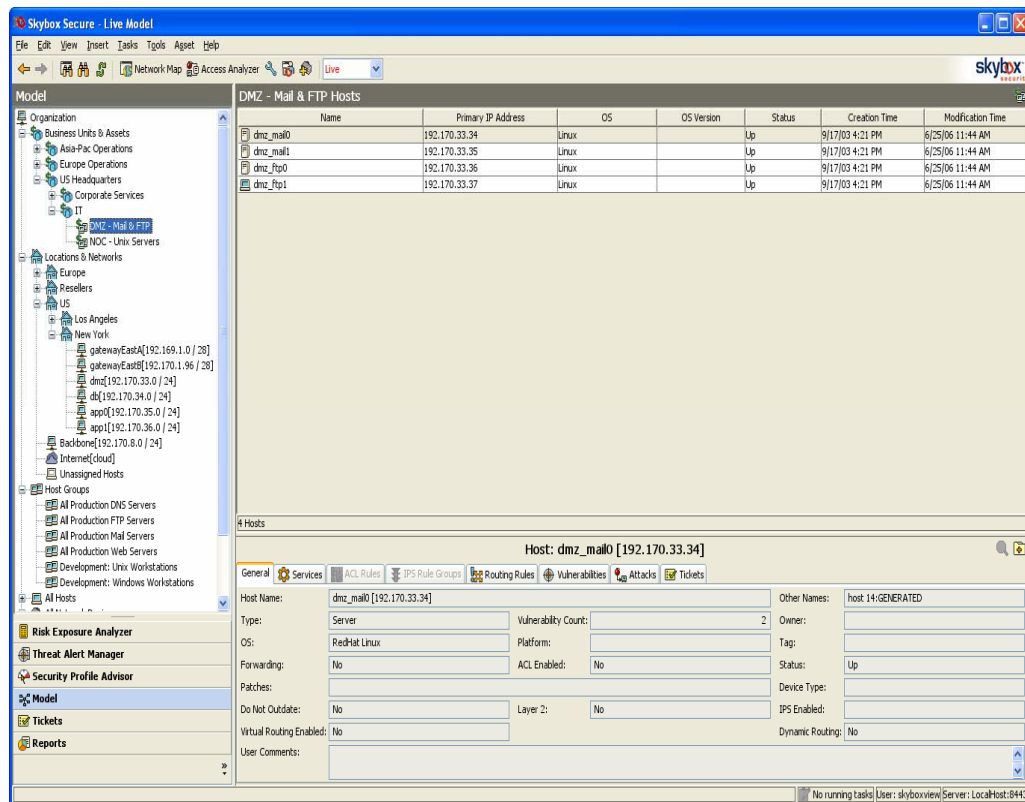
# Import Controls & Network Element Configurations



- Import configurations of controls and network elements including:
  - Firewalls
  - IPS
  - Routers
  - Switches, etc.
- This includes routes, ACL's, rules, physical/logical interfaces, NAT, etc...

This allows modeling/analysis of every path to/from any networked entity to another; this provides logical and physical paths to any networked asset

# Import the Inventoried/Managed Assets



- Import networked hosts from CMDB or asset discovery toolsets
- Create asset groups based on business units, function, geography
- Model Assets that conform to how your organization is structured, connected or administered

Since the network infrastructure and controls are already established, the assets are automatically populated into the network segments that house them and there is now context of the security policies protecting them.

# Import the Vulnerabilities Associated With Inventoried Assets

The screenshot displays the Skybox Secure - Live Model interface. On the left, a tree view shows the asset inventory structure, including Corporate Services, IT, DMZ - Mail & FTP, and various servers. The main pane shows a list of vulnerabilities with columns for Title, ID, CVE, Host, OS, Service Ports, Service Name, Status, and Has Tickets. Below this list, a detailed view of a specific vulnerability is shown, including its title, description, host, service, status, and risk level.

Title	ID	CVE	Host	OS	Service Ports	Service Name	Status	Has Tickets
Buffer Overflow in BIND...	SBV-00034	CVE-1999-0833	dmz_dns1 [192.170.33.33]	Linux	53/TCP	BIND (domain_1)	Found	
Buffer Overflow in BIND...	SBV-00034	CVE-1999-0833	dmz_dns0 [192.170.33.32]	Linux	53/TCP	BIND (domain_1)	Found	
wu-ftpd 2.6.0 and HP-UI...	SBV-00153	CVE-2000-0573	dmz_ftpd [192.170.33.36]	Linux	21/TCP	wu-ftpd (ftp)	Found	
Altaire ColdFusion Allows...	SBV-00405	CVE-1999-0477	finance_server_0 [192.170.27.2]	ADX	8500/TCP	ColdFusion Server...	Found	
DoS in ColdFusion via St...	SBV-00720	CVE-1999-0756	finance_server_0 [192.170.27.2]	ADX	8500/TCP	ColdFusion Server...	Found	
wu-ftpd 2.6.0 and HP-UI...	SBV-00153	CVE-2000-0573	dev_ftpd [192.170.19.20]	Linux	21/TCP	wu-ftpd (ftp)	Found	
[MS03-026] Buffer Over...	SBV-01655	CVE-2003-0352	app_4_server_8 [192.170.36.10]	Windows Server 2003	135/TCP	Windows (loc-srv)	Found	
Oracle 9iAS PL/SQL Apa...	SBV-00846	CVE-2001-1217	app_4_server_8 [192.170.36.10]	Windows Server 2003	443/TCP	Oracle9i Applicati...	Found	
Oracle 9i Application Se...	SBV-00845	CVE-2001-1216	app_4_server_8 [192.170.36.10]	Windows Server 2003	443/TCP	Oracle9i Applicati...	Found	
DoS in Oracle 9iAS Apa...	SBV-00861	CVE-2002-0566	finance_db_1 [192.170.27.23]	ADX	443/TCP	Oracle9i Applicati...	Found	
DoS in Oracle 9iAS Apa...	SBV-00861	CVE-2002-0566	finance_db_0 [192.170.27.22]	ADX	443/TCP	Oracle9i Applicati...	Found	
[MS00-086] IIS 5.0 Ena...	SBV-00262	CVE-2000-0886	finance_web_9 [192.170.27.21]	Windows 2000	80/TCP	IIS (http)	Found	
Apache Chunked-Encodi...	SBV-00926	CVE-2002-0392	dev_web5 [192.170.19.31]	Solaris	80/TCP	Apache (http)	Found	
[MS03-026] Buffer Over...	SBV-01655	CVE-2003-0352	developmentWin82 [192.170.17.84]	Windows XP	135/UDP	Windows XP (loc-s...	Found	
[MS03-026] Buffer Over...	SBV-01655	CVE-2003-0352	developmentWin81 [192.170.17.83]	Windows XP	135/UDP	Windows XP (loc-s...	Found	
[MS03-026] Buffer Over...	SBV-01655	CVE-2003-0352	developmentWin8 [192.170.17.10]	Windows XP	135/UDP	Windows XP (loc-s...	Found	
[MS03-026] Buffer Over...	SBV-01655	CVE-2003-0352	app_7_server_8 [192.170.36.40]	Windows Server 2003	135/TCP	Windows (loc-srv)	Found	
Buffer Overflow in Oracl...	SBV-00833	CVE-2001-0836	app_4_server_9 [192.170.36.11]	Solaris	3128/TCP	Oracle9iAS Web C...	Found	
Oracle 9iAS PL/SQL Apa...	SBV-00846	CVE-2001-1217	app_4_server_9 [192.170.36.11]	Solaris	443/TCP	Oracle9i Applicati...	Found	
Buffer Overflow in Oracl...	SBV-00833	CVE-2001-0836	app_4_server_8 [192.170.36.10]	Windows Server 2003	3128/TCP	Oracle9iAS Web C...	Found	
Buffer Overflow in Oracl...	SBV-00833	CVE-2001-0836	app_4_server_7 [192.170.36.9]	Solaris	3128/TCP	Oracle9iAS Web C...	Found	
Oracle 9iAS PL/SQL Aps...	SBV-00846	CVE-2001-1217	app_4_server_7 [192.170.36.9]	Solaris	443/TCP	Oracle9i Applicati...	Found	

**Vulnerability: Buffer Overflow in BIND 8.2 via NXT Records**

General Host Service Tickets Risk Profile

Title: Buffer Overflow in BIND 8.2 via NXT Records ID: SBV-00034 CVE: CVE-1999-0833

Description: Buffer overflow in BIND 8.2 via NXT records due to improper validation of those records by the server. This could enable a remote attacker to achieve root compromise of the host.

Host: dmz\_dns1 [192.170.33.33] Exposure: Direct Has Tickets: No

Service: BIND (domain\_1) (53/TCP) Commonality: Medium Severity: Critical (10)

Status: Found Detection Reliability: Normal

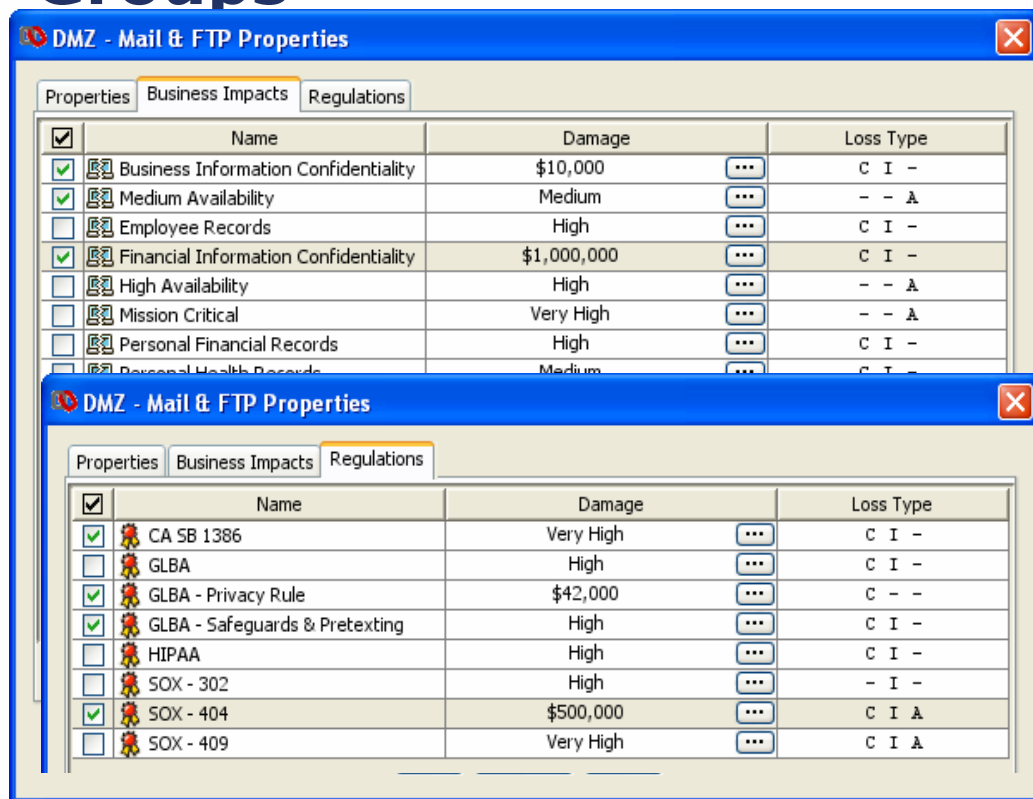
Imposed Risk: High Status Explanation: Vulnerability was found by a scanner or by Early Warning Analysis

Discovery Method: Nessus

- Import vulnerabilities from VA/VM tools that have run internally and externally
- Based upon IP addresses, the vulnerabilities are allocated automatically to the appropriate asset
- Criticality/Severity is reflected in rankings

This capability provides a device-focused, vulnerability-centric view of the asset inventory, regardless of compensating controls or topology. This is raw vulnerability data without the context of threat or impact but ranked solely by criticality.

# Define Business Impact & Regulatory Compliance Requirements Based Upon Asset Groups



The screenshot shows the 'DMZ - Mail & FTP Properties' dialog box with the 'Business Impacts' tab selected. It displays a table of business impacts with columns for Name, Damage, and Loss Type. The table is as follows:

<input checked="" type="checkbox"/>	Name	Damage	Loss Type
<input checked="" type="checkbox"/>	Business Information Confidentiality	\$10,000	C I -
<input checked="" type="checkbox"/>	Medium Availability	Medium	- - A
<input checked="" type="checkbox"/>	Employee Records	High	C I -
<input checked="" type="checkbox"/>	Financial Information Confidentiality	\$1,000,000	C I -
<input type="checkbox"/>	High Availability	High	- - A
<input type="checkbox"/>	Mission Critical	Very High	- - A
<input type="checkbox"/>	Personal Financial Records	High	C I -
<input type="checkbox"/>	Personal Health Records	Medium	C I -

The screenshot also shows a second instance of the same dialog box with the 'Regulations' tab selected. It displays a table of regulations with columns for Name, Damage, and Loss Type. The table is as follows:

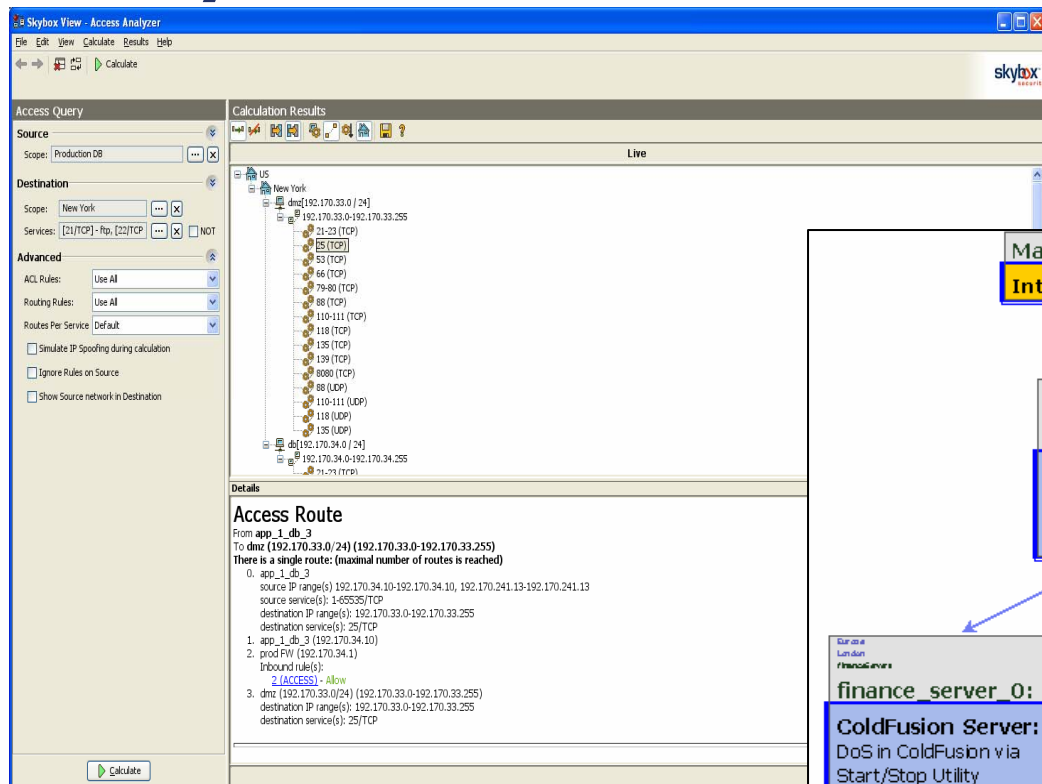
<input checked="" type="checkbox"/>	Name	Damage	Loss Type
<input checked="" type="checkbox"/>	CA SB 1386	Very High	C I -
<input type="checkbox"/>	GLBA	High	C I -
<input checked="" type="checkbox"/>	GLBA - Privacy Rule	\$42,000	C - -
<input checked="" type="checkbox"/>	GLBA - Safeguards & Pretexting	High	C I -
<input type="checkbox"/>	HIPAA	High	C I -
<input type="checkbox"/>	SOX - 302	High	- I -
<input checked="" type="checkbox"/>	SOX - 404	\$500,000	C I A
<input type="checkbox"/>	SOX - 409	Very High	C I A

- Business impact & loss types are defined based upon confidentiality, integrity and availability
- Define regulatory compliance requirements and impacts
- Impacts can be defined either qualitatively or quantitatively

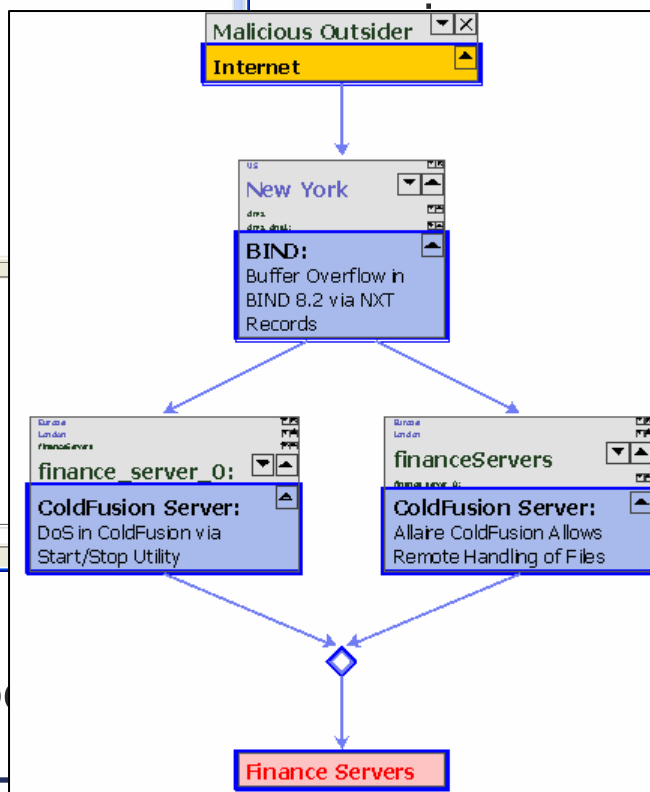
Now that we understand how assets are interconnected, what compensating controls are in place, how the assets are vulnerable, we need to define the business impact to help us prioritize what we mitigate based upon importance not purely vulnerability severity.



# Provide What-If Modeling and Access Path Analysis



- Model and analyze access paths to and from any networked entity using any



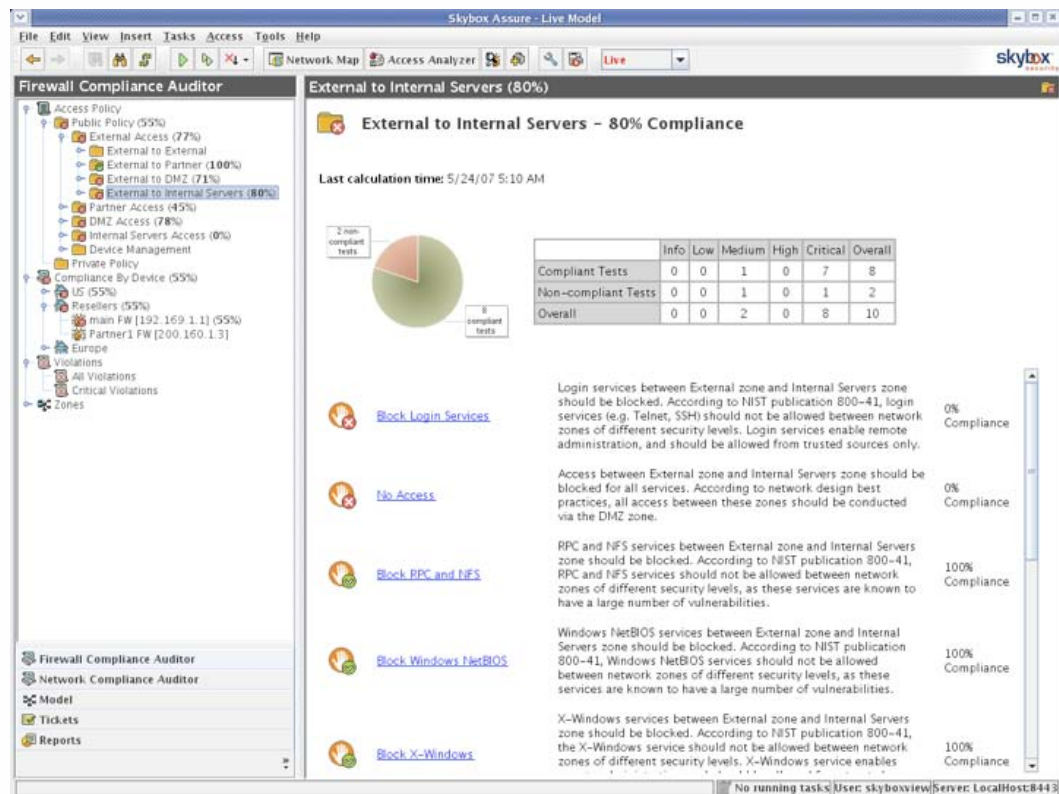
which network  
control policies

prospective  
effect access as  
ance & risk

ch  
nd in order

Understanding how assets can be  
compensating controls allows us  
to understand the current environment and how change will affect us.

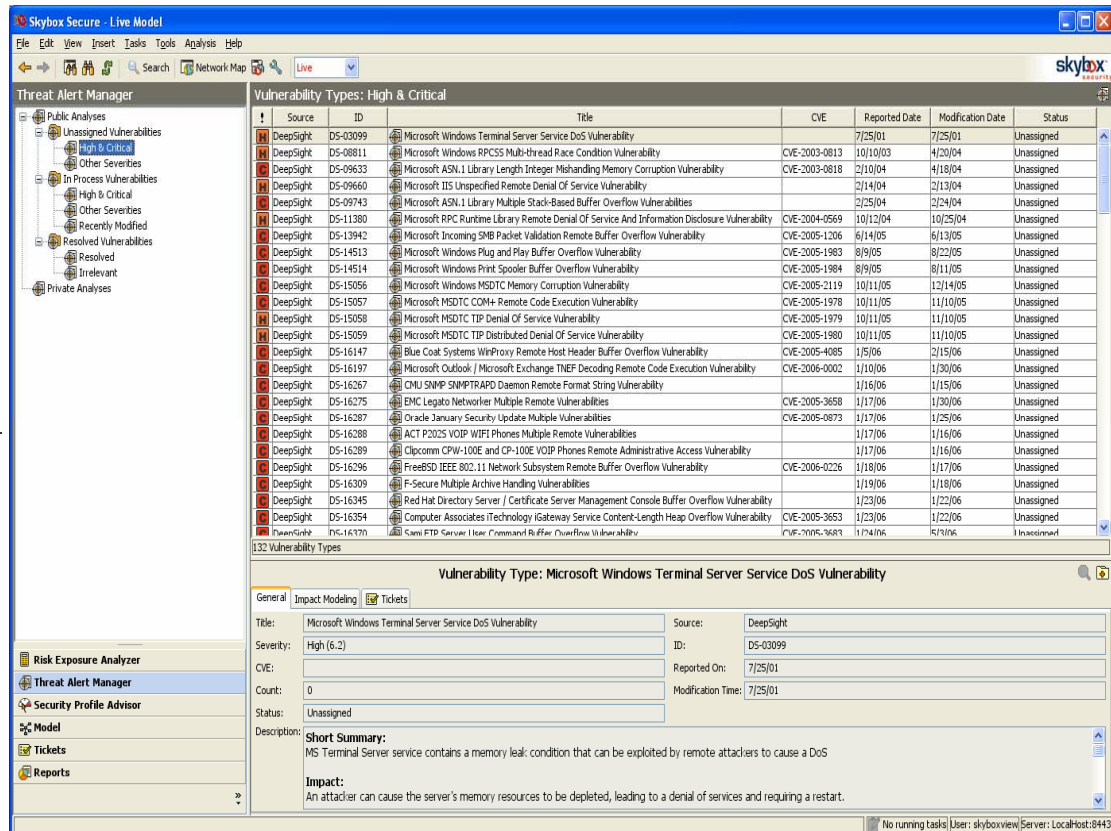
# Define Control and Network Policies In Accordance With Existing Corporate Governance Guidelines Based Upon Access



- Create policies that are easy to understand and measure based upon asset groups and zones
- Optimize rulebases based on usage/non-usage
- Manage Compliance based on a per-device or global perspective as aligned to best practice

This allows us to start managing network and control device configurations and change assurance to ensure compliance on a per device or access basis.

# Threat Management - Understand Current Threat Conditions



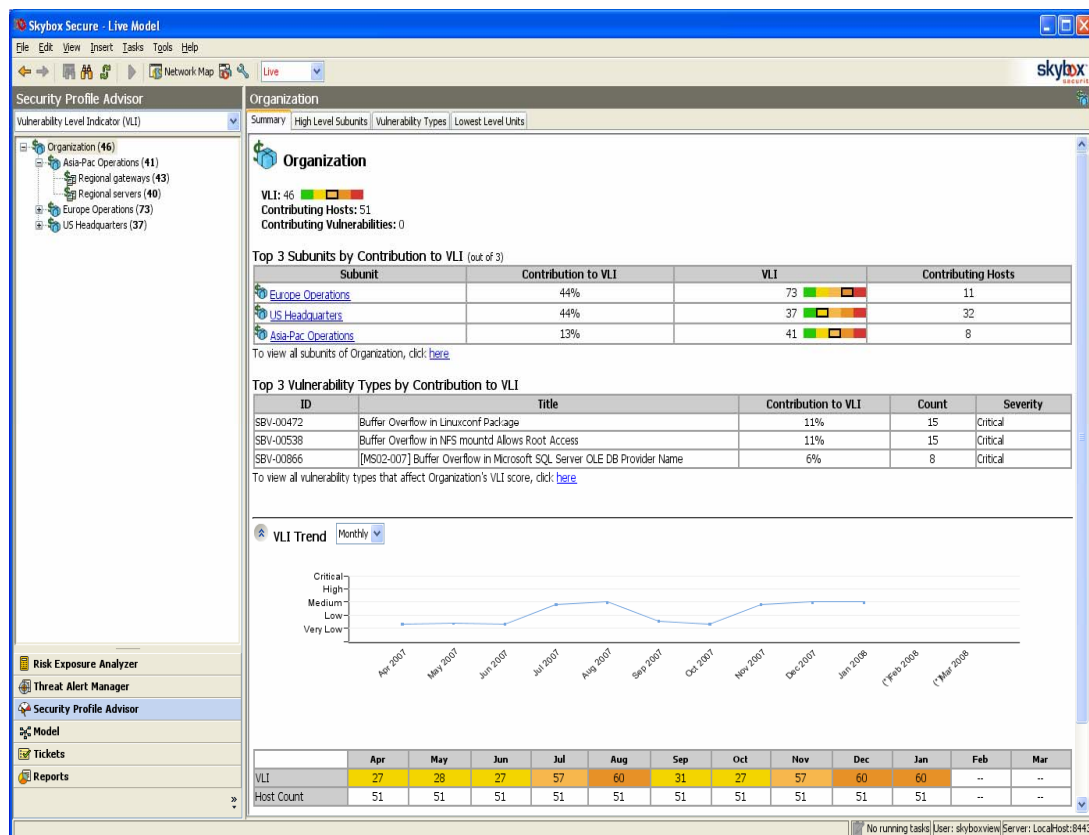
The screenshot displays the Skybox Secure Live Model interface. The main window shows a list of vulnerability types under the 'Threat Alert Manager' tab. The list includes columns for Source, ID, Title, CVE, Reported Date, Modification Date, and Status. The first entry is 'Microsoft Windows Terminal Server Service DoS Vulnerability' with ID DS-03099 and CVE CVE-2003-0813. The status is 'Unassigned'.

Below the list, the 'Vulnerability Type: Microsoft Windows Terminal Server Service DoS Vulnerability' details are shown. The 'General' tab is selected, displaying the title, severity (High (6.2)), CVE (0), count (0), status (Unassigned), and a short summary: 'MS Terminal Server service contains a memory leak; condition that can be exploited by remote attackers to cause a DoS'. The impact is described as: 'An attacker can cause the server's memory resources to be depleted, leading to a denial of services and requiring a restart.'

- Normalizes and correlates threat feeds from numerous sources (e.g. DeepSight)
- Provides threat rankings based upon product and technology repositories, threat properties, counts and locations of vulnerability instances
- Allows for threat-centric view of the organization

The Threat Alert Manager correlates threat and alert feeds, patch management details, and VA/VM scanner data to provide a threat-based perspective that allows staff to examine, investigate and research each alert, and decide on the appropriate course of action.

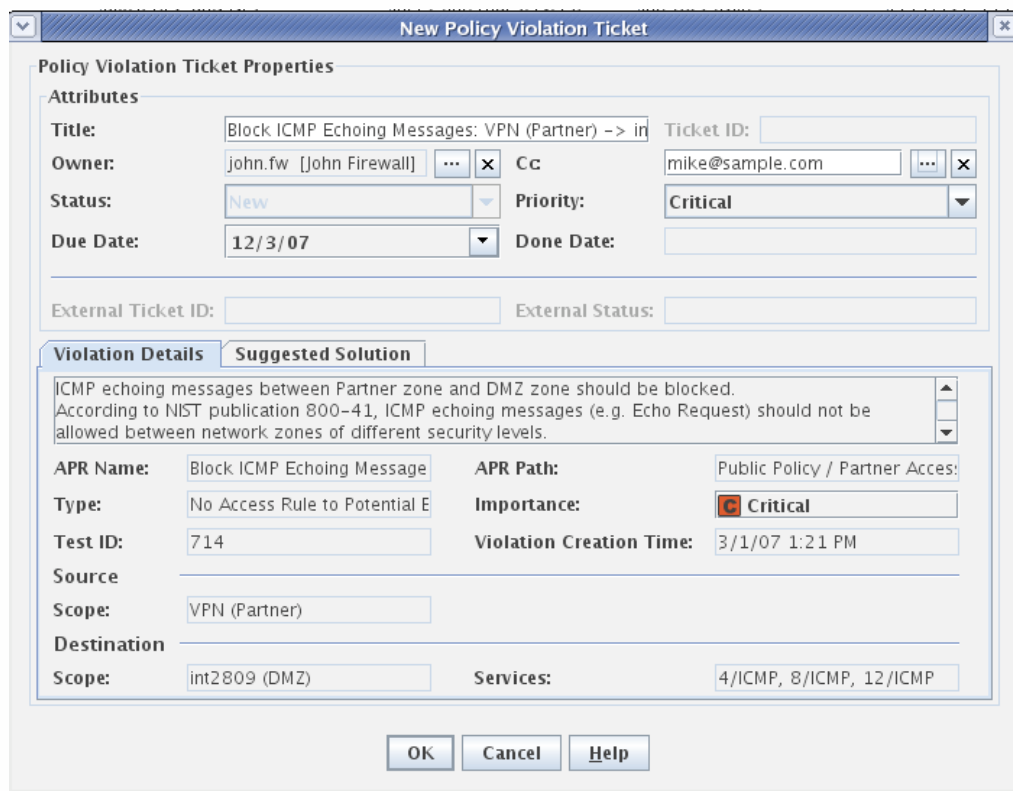
# Vulnerability Management - Measure the Organization's Security Profile



- Visualize the organization's security profile based upon contributed vulnerabilities
- Automates collection of risk and compliance data from multiple disparate systems
- Calculates Key Performance Indicators (KPI) and presents security advisories

Provides threat indicators for the organization and enables the security team to help management understand which threats pose the greatest harm and what the organization is doing about them. Security projects can thus be better aligned with the needs of the business

# Automate Mitigation Efforts and Change Assurance



**Policy Violation Ticket Properties**

**Attributes**

Title: Block ICMP Echoing Messages: VPN (Partner) -> in Ticket ID:

Owner: john.fw [John Firewall] ... x Cc: mike@sample.com ... x

Status: New Priority: Critical

Due Date: 12/3/07 Done Date:

External Ticket ID:  External Status:

**Violation Details** **Suggested Solution**

ICMP echoing messages between Partner zone and DMZ zone should be blocked.  
According to NIST publication 800-41, ICMP echoing messages (e.g. Echo Request) should not be allowed between network zones of different security levels.

APR Name: Block ICMP Echoing Message APR Path: Public Policy / Partner Acces:

Type: No Access Rule to Potential E Importance: Critical

Test ID: 714 Violation Creation Time: 3/1/07 1:21 PM

Source

Scope: VPN (Partner)

Destination

Scope: int2809 (DMZ) Services: 4/ICMP, 8/ICMP, 12/ICMP

OK Cancel Help

- Policy violations and non-compliance automatically generate violation tickets
- Violation details as well as suggested resolution is included in ticketing.
- Resolution is tracked across the ticket lifecycle

Ensures compliance not just based upon reactive reporting but by generating assigned ticketing with tracking across the lifecycle to resolution.



# Risk Management – Managing Risk Via Exposure Analysis

- Measure risk across the organization by asset, vulnerability, threat origin, business unit, business impact or regulations

The screenshot shows the Skybox Secure - Live Model interface. The left pane displays a tree view of 'Risk Exposure Analyzer' with categories like 'Public Analyses', 'Risks', 'Vulnerabilities', 'Threats and Attacks', and 'Worms'. The main pane shows 'Business Assets Analysis: Business Assets by Risk' with a table listing assets like 'Finance DB', 'Finance Servers', and 'Production DB' with associated risk levels. Below this, there's a 'Business Assets' section with tabs for 'General', 'Vulnerabilities', 'Attacks', 'Risk Profile', and 'Tickets'.

Attacks Analysis: All Attacks

Threat Origin	Target	Risk	Step Count
Internet Hacker	Finance DB	High Risk	1
Internet Hacker	Finance Servers	Medium Risk	2
B2B Threat	Production DB	Medium Risk	1
B2B Threat	Finance Servers	Medium Risk	2
Current Worm Thr...	Production DB	Medium Risk	1
Corrupted Insider	Finance Servers	Medium Risk	2
Corrupted Insider	Finance DB	Medium Risk	1
Internet Hacker	DMZ - Mail & FTP	Medium Risk	1
Current Worm Thr...	Finance DB	Medium Risk	1
Current Worm Thr...	Finance Servers	Medium Risk	2

198 Attacks

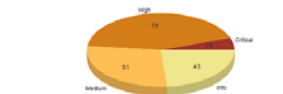
By analyzing risk exposure, we can identify the most critical threats, security controls, and vulnerabilities. This allows us to understand the most cost-effective remediation alternatives.

# Reporting & Dashboards

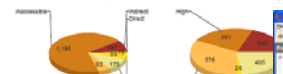
## 1. Vulnerabilities - Severity, Risk and Exposure

This section displays the Vulnerabilities distributed by Severity, Risk and Exposure level. "Exposed Vulnerabilities" are Vulnerabilities that can be accessed from Threat Origins in one step (Direct or more Indirect), while "Not Exposed Vulnerabilities" are mitigated Vulnerabilities that are inaccessible from the defined Threat Origins.

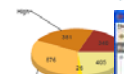
### Exposed Vulnerabilities - Severity



### All Vulnerabilities - Exposure



### All Vulnerabilities - Severity



Severity	Direct	Indirect	Not Exposed	Exposure	Count
High	1	1	1	High	3
Medium	1	1	1	Medium	3
Low	1	1	1	Low	3

Rules: Unused  
Rules which were not used, or whose hit count was below the defined candidates for removal.

Rule ID	Original Rule ID	Source	Target	Severity	Action	Hit Count
1	1	Any	Development_Network	High	Deny	1

Rules: Contains Unused Objects  
Rules whose hit count was above the defined threshold, but one or more rule has a hit count below the defined "unused" threshold.

Rule ID	Original Rule ID	Source	Target	Severity	Action	Hit Count
2	1	Any	DMZ	High	Deny	1537

Rules: Not Logged  
Rules which are part of the firewall, but not enabled for logging.

Rule ID	Original Rule ID	Source	Target	Severity	Action	Hit Count
1	1	Any	Any	Any	Deny	1

Objects: Unused  
Objects that are referenced in one or more rules, but have hit counts below the defined threshold. These objects may indicate entities that no longer exist and can probably be removed.

Object Type	Object Name	Addresses	Parent Objects	Referenced in Rules (logs)
IP	any	-	-	211
Domain	any	-	-	211

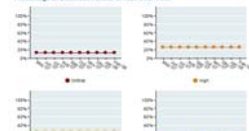
## 4. Business Assets at Risk - Count over Time

This section displays the number of Business Assets at each risk level for each specified time period (quarter or month).

### Number of Business Assets at Risk over Time



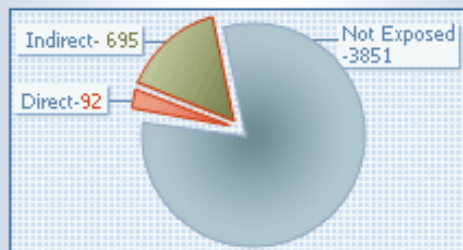
### Percentage of Business Assets at Risk over Time



## Risk Trend (Last 10 Months)



## Vulnerabilities

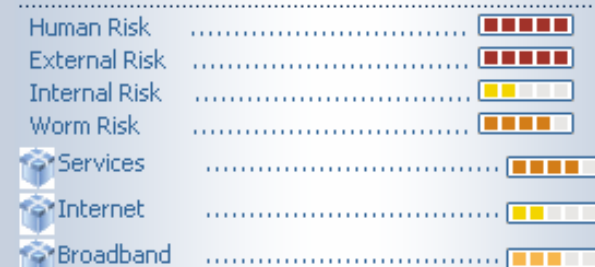


Exposed Vulnerabilities

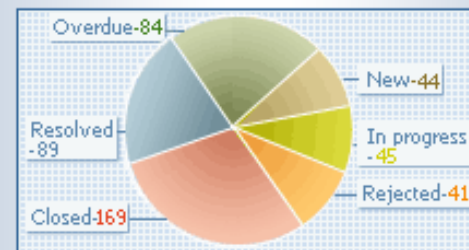
- Comprehensive and customizable reporting capabilities

- Web-based dashboard

## Risk



## Remediation



Tickets by Status

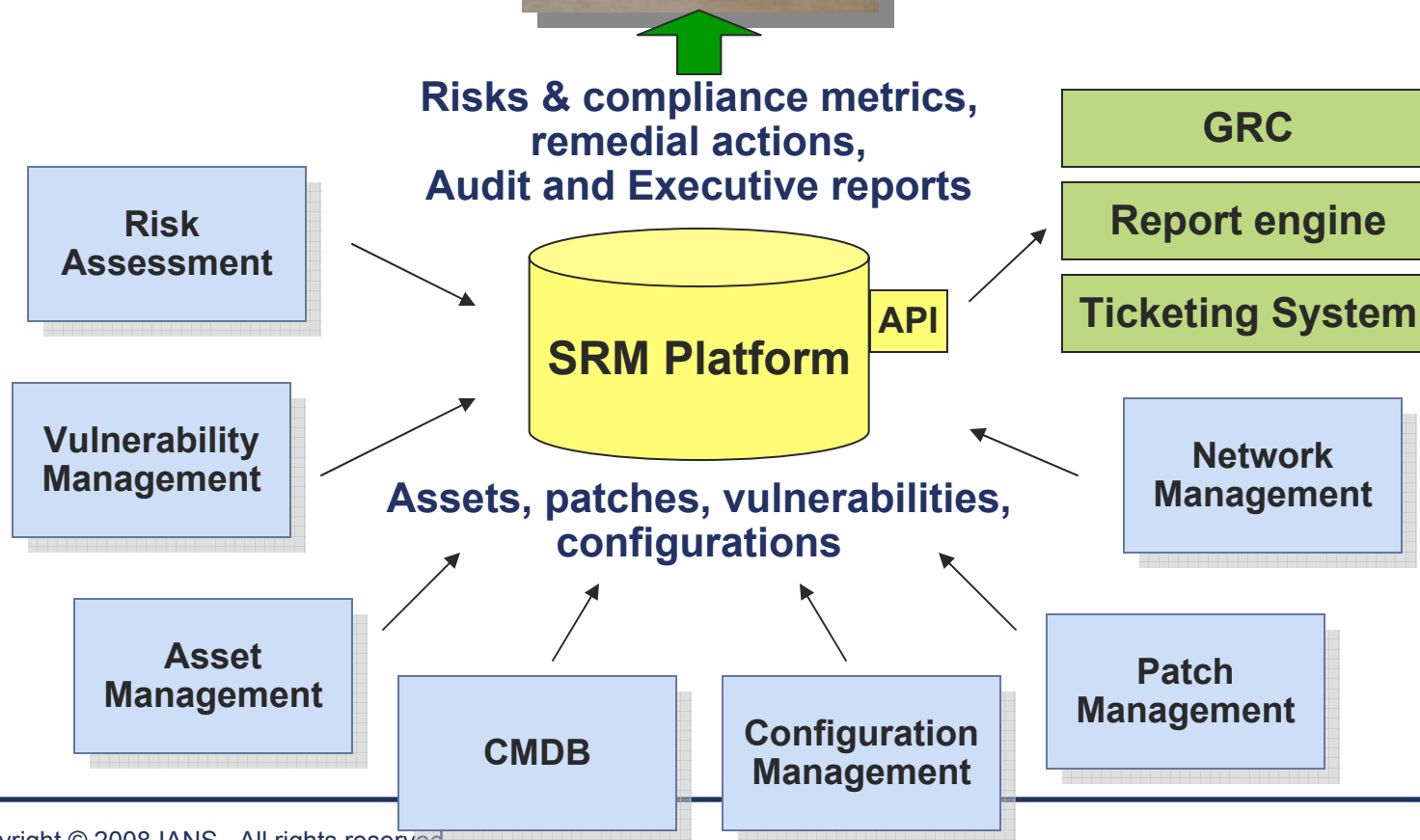
Provides rep  
Compliance,

# Integrates With Existing Organization/Organization

Compliance officer  
Risk officer



Executives  
Auditors



# What Did We Achieve?

- Platform standardization and compliance measurable and enforceable
- Change is manageable and accountable
- Defects due to previously undetected change substantially decreased
- Security posture is quantifiable and (IT) risk measured and trended
- Lowered costs, reduced labor; from manual to automated
- Security seen as more responsive/proactive
- Service availability increased; less business disruption
- Business Units, Audit, Management, Network, Server Admins & Security all have skin in the game
- Audits and compliance from months to minutes
- Improved and quantifiably-measured risk posture

# In Summary

- **Start Small, Think Big; this takes time and evangelism**
- **Get a grip on the basics**
- **Demonstrate value and gain trust in the model**
- **Opening the kimono can be ugly.**
- **The risk models are very much GIGO...you must get your risk assessment methodology squared away**
- **Start with qualitative business impacts and move to quantitative when you have confidence in the numbers**
- **It will be hard for some teams to let go of managing by risk rather than vulnerability severity**
- **The business units will start to compete with one another, be prepared for challenges**

# Thank You For Your Attention

**Christofer L. Hoff**  
**Chief Architect, Security Innovation**  
**Unisys**

**[Christofer.Hoff@Unisys.com](mailto:Christofer.Hoff@Unisys.com)**

**Blog - <http://RationalSecurity.typepad.com>**  
**+1.978.631.0302**