Recap of RSA April 2008 Executive Security Action Forum

NEbraska CERT Conference 2008

Computer Security and Information Assurance

Mike Hoesing CISSP, CISA   402 981-7747

m-hoesing@cox.net

Personal observations and recollections from the forum, any content is anecdotal, adoption of any content by the viewer should be preceded by sufficient testing within your organization’s environment, viewer accepts all liability resulting from adoption of any content within their organization . Don’t sue me, I have no money.

What is ESAF?

- 100 of the Fortune 500 CISO’s
- One day forum encouraging transparency (with confidentiality)
- Interactive Polling on Topics of the day
- Break out sessions on:
  - App Security, Seat at the Exec Table, Isec Metrics,
  - Consumer Devices, Insider Threat, Public Private Partnership, Virtualization ☺ , Compliance to Governance, Web 2.0

Polling - #1 Concern

- **31% a) The insider threat**
- **17% b) Organized crime**
- **12% c) Corporate/government espionage**
- **6% d) Hackers**
- **8% e) New threats from Web 2.0**
- **5% f) New threats from consumer devices**
- **13% g) Risks of non-compliance**
- **3% h) Other**

Polling - Industry

- **1% a) Energy**
- **23% b) Financial Services**
- **16% c) Government**
- **4% d) Healthcare**
- **25% e) High Tech/Telecom**
- **10% f) Information services/Media/ Publishing**
- **7% g) Manufacturing/Automotive**
- **6% h) Retail/Hospitality**
- **8% i) Other**

Polling - Who

- 70% CISO’s
- 17% Exec (Risk Management)
- 52 % report to the CIO, 20% higher, 28% lower
- 87% are within 3 layers from the Board
- 41 % IS shops had less than 25 staff, 37% had 26-100 staff, 15% had 100-500 staff, 7% had over 500 staff

Polling - Scope

- Scope – 24% just policy & governance, 5 % just operations, 49% both P&G + Ops, Remainder have two ISec Executives
- Early ISec Involvement in New Initiatives, 15% always, 39% major projects, 39% yes but not early enough, 7% no
- Early ISec Involvement in New Initiatives, documented process 56%, 44% no

Polling – ISec Metrics

- Use External Benchmarks 51%
- Dedicated Metrics Staff Person 33% yes

Polling – Pen Tests, Consumer Devices, Insider Threat, Virtualization

- Perform their own internal testing 52%
- Use External Testers 38%, 10% no
- Policy covering consumer devices , 40% ban, 38% restrict, 13% allow employee choice, 9% none
- Task Force to reduce insider threat 57%
- Virtualization, 33 % have a policy (67% don’t)

Polling – Compliance

- Are you more secure with Compliance? 92% no or don’t know
- Frustrations – Resources, Focus on wrong things, Security driven by assessment cycles not strategy

Polling – Policy Items

- IP Mail Policy? (gmail, yahoomail) 42% yes
- Social Site Policy? (facebook, youtube) 41% yes
- Instant Messaging Blocked? 55% yes
- App Scans for Purchased of Outsourced Software, 34% always perform their own testing, 36% will accept vendor’s test, 20% nothing
- Code Reviews (internal development) 41% automated, 19% manual, 32% don’t
- Security Policy Education – 63% yes, **37% not ☹**

Polling – Money

- How does ISec “sell” itself to the C suite – 33% threats, 26% Compliance or Contracts, 22% reducing Risk, 12% Competitive Advantage or Business Strategy Alignment,
- 81% of ISec budgets are part of the CIO budget
- Percent of ISec $ of IT Budget – 29% 0-3 %,
  18% 3-5%, 24% 5-10%, 4% over 10%, 26% don’t know??
- 83% of ISec budgets also include some

Polling – Money (cont)

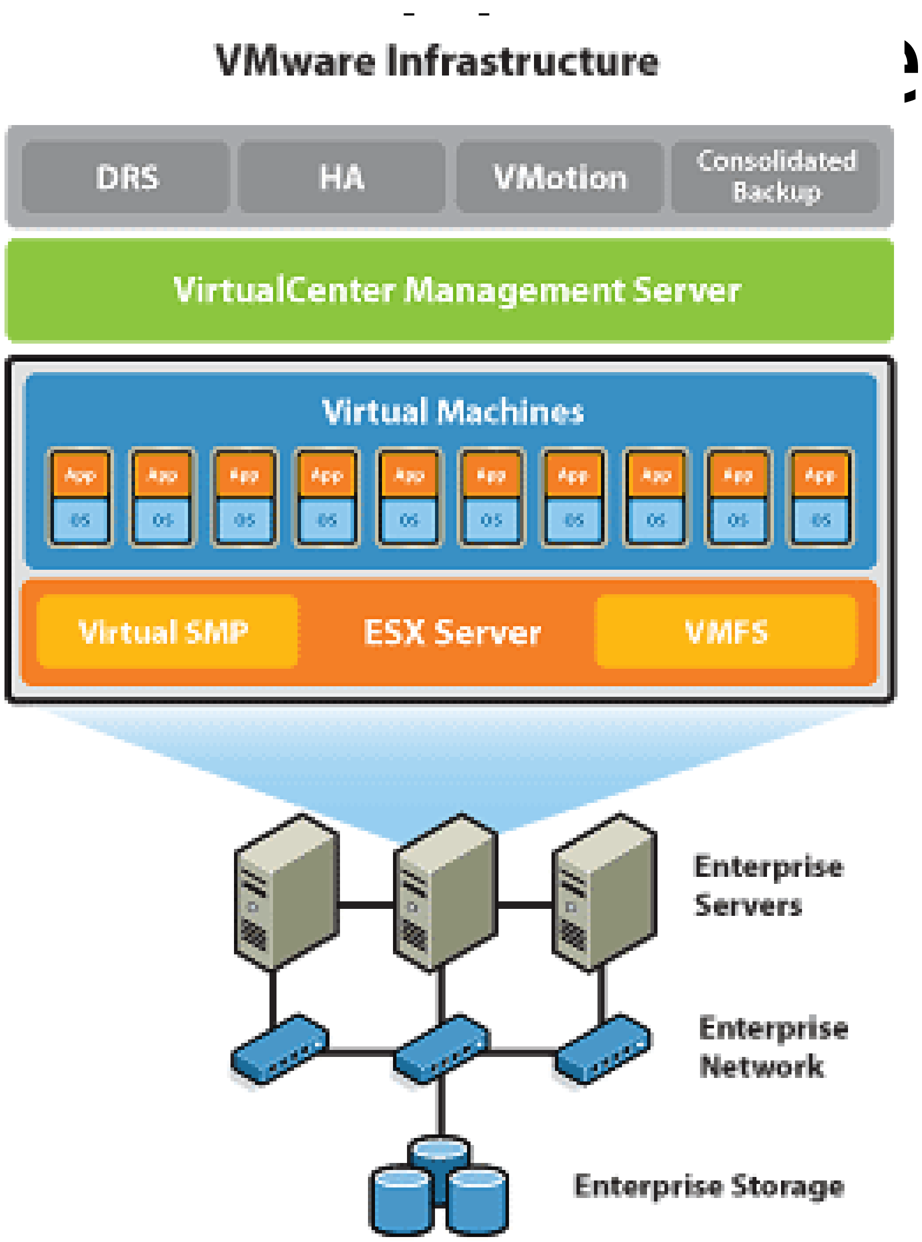
- ISec Budget Change for Next Year
  - 19% no change
  - 19% 1-10% increase
  - 8% 11-20% increase
  - 6% over 20% increase
  - 28% 1-10% Decrease
  - 11% 11-20% Decrease
  - 8% unknown

Polling – #1 Focus

- **20% 1. Alignment with business strategy**
- **6% 2. Metrics**
- **18% 3. Application Security**
- **8% 4. Managing risks posed by consumerization**
- **16% 5. Insider Threat**
- **18% 6. Regulatory compliance**
- **8% 7. Operational efficiencies**
- **6% 8. Other**

Virtualization Panel at ESAF April 2008

What is Virtualization? (source: VMware)

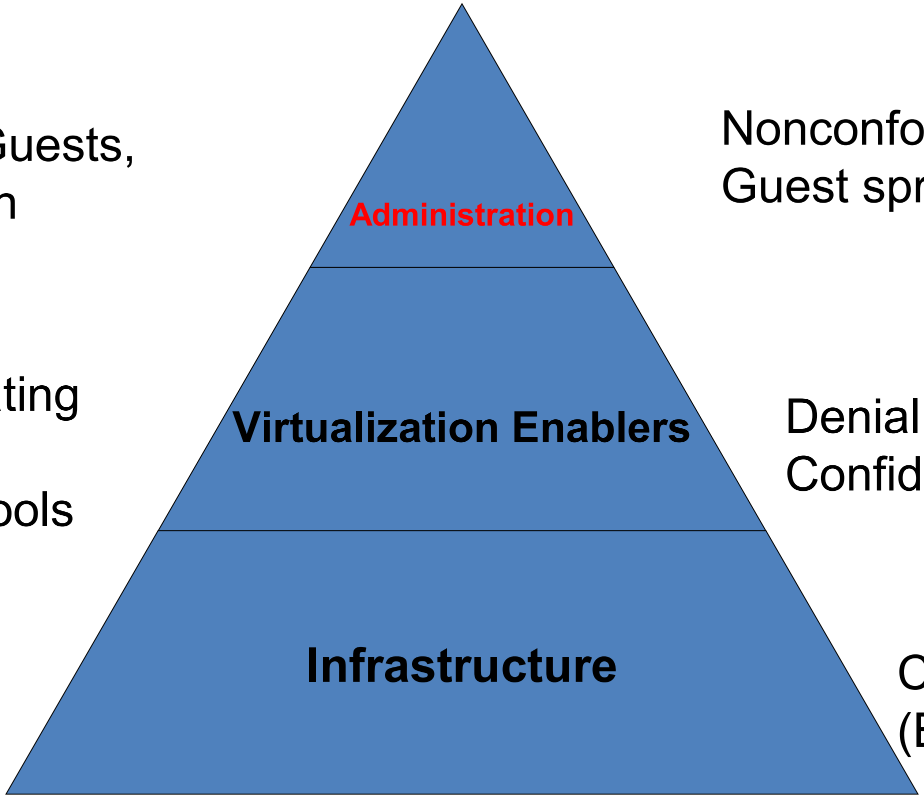


COS & VMkernel

ESX Host & Possibly Guest Storage

Guest Storage

Virtualization Security – Top Level View



Examples		***Risks***
Movement of Guests, Network Design	Administration	Nonconforming Configurations, Guest sprawl , Confidentiality
VMM Kernel, Console Operating System, Management tools	**Virtualization Enablers**	Denial of Service, Confidentiality
HVM CPUs, Storage	**Infrastructure**	CPU Ring Attacks (Blue Pill)

10 Risks of Virtualization

- Rogue Guests
- Network Segmentation
- Roles
- Infrastructure Integration
- Internal Skills
- Misconfigured Hosts
- Misconfigured Guests
- Remote Access
- Single Point of Failure, Additional Point of Failure
- CPU (Blue Pill)

There is Help

- Strategy, Planning
  - Read Ron Oglesby’s book
- Vendor documentation is good
- Standards and Benchmarks
  - Center for Internet Security
  - DISA STIG
- General Security (ISO 17799/27002, PCI)
- Engage Additional Skills

10 Positive Things About Virtualization

- Security Designed In
- Good Documentation
- Enables DR, BCP
- VAR Knowledge
- Flexibility, speed to deployment
- 96% PCI Compliant
- Docs Describe Fixes
- Open (VMsafe and scripting)
- Network Tiers
- Roles

(btw, u may save $$)

VMware ESX Server - PCI Big 3

- Protect root access to the ESX host COS
  - Strong password, use SUDO
- Protect remote access
  - “High” in ESX 2.x, don’t change ESX 3 defaults (i.e. no telnet, no root access via ssh)
- Tiered Networks, ensure you can show your assessor the following:
  - Ingress – patches, AV updates can be pushed to the guests
  - Egress – monitoring alerts, log files can be pulled out of the guests

ESX Server Close to PCI Compliant

- No password history for the COS (modify PAM)
- No warning banner on the COS, nor management server , nor web interface (add these)
- SNMP default community string is “public” (change to “password”) [1]
- NTP is not enabled (enable this)

» [1] auditor levity