



# A Practical Security Infrastructure

NERCOMP

October 28th, 2007

Kevin Amarin

Network Security Manager

Harvard Kennedy School

# [Topics]

---

- My/Your Current IT Security
  - Budget
  - Security Tools
  - Bottom-up
  - IT 'Coopetition'
- Information Security Program
  - Strategy
  - Top Down
  - Risk Controls

# [About Me - Kevin Amarin]

- Network Security Manager  
Kennedy School of Government
- Duties
  - Security policy and enforcement
  - Security awareness
  - Security design & implementation
  - Risk assessment, VPN, DMCA Officer, Unix Servers (& other random stuff)

# [ Slides ]

---

Slides will be available on  
nercomp.org media archive

Also available at:

<http://amorin.org/talks>

# [ Information Security in Higher Ed ]

- Program is often not formalized
  - Security group is most often a part of IT / NOC
  - Admin that is Jack of all trades
- Limited
  - Limited personnel resources
  - Limited budget
  - Limited influence at C-level

# [ Information Security Budget ]

- VM labs, testing facilities, software/hardware
- Staff
  - Full Time, part time, consultants
- Measured industry averages
  - Per unit revenue
  - Info Sec staff number per total employees
  - % of IT budget
- *US 4-6% of IT budget*

# [ Security Projects ]

---

- System lock down practices
  - Windows 2003/XP, Linux, Switches, Handhelds..
- Firewall/VPN
  - ACLs, ASA
- Pen testing
  - System Scanner
  - Web Scanner

# [ Security Projects ]

- IDS
  - Snort, Dragon..
- NAC
  - Registration, Detection, Isolation, Remediation
- Encryption
  - Full Disk
  - USB Thumb drive/HDD

*Security Currently is a lot of Projects and not a lot of Strategy*

# [ Planning Bottom Up ]

- Grass-roots effort of Admins securing the environment

## Pros:

- Technical Expertise
- InDepth-Knowledge
- Understanding the threats

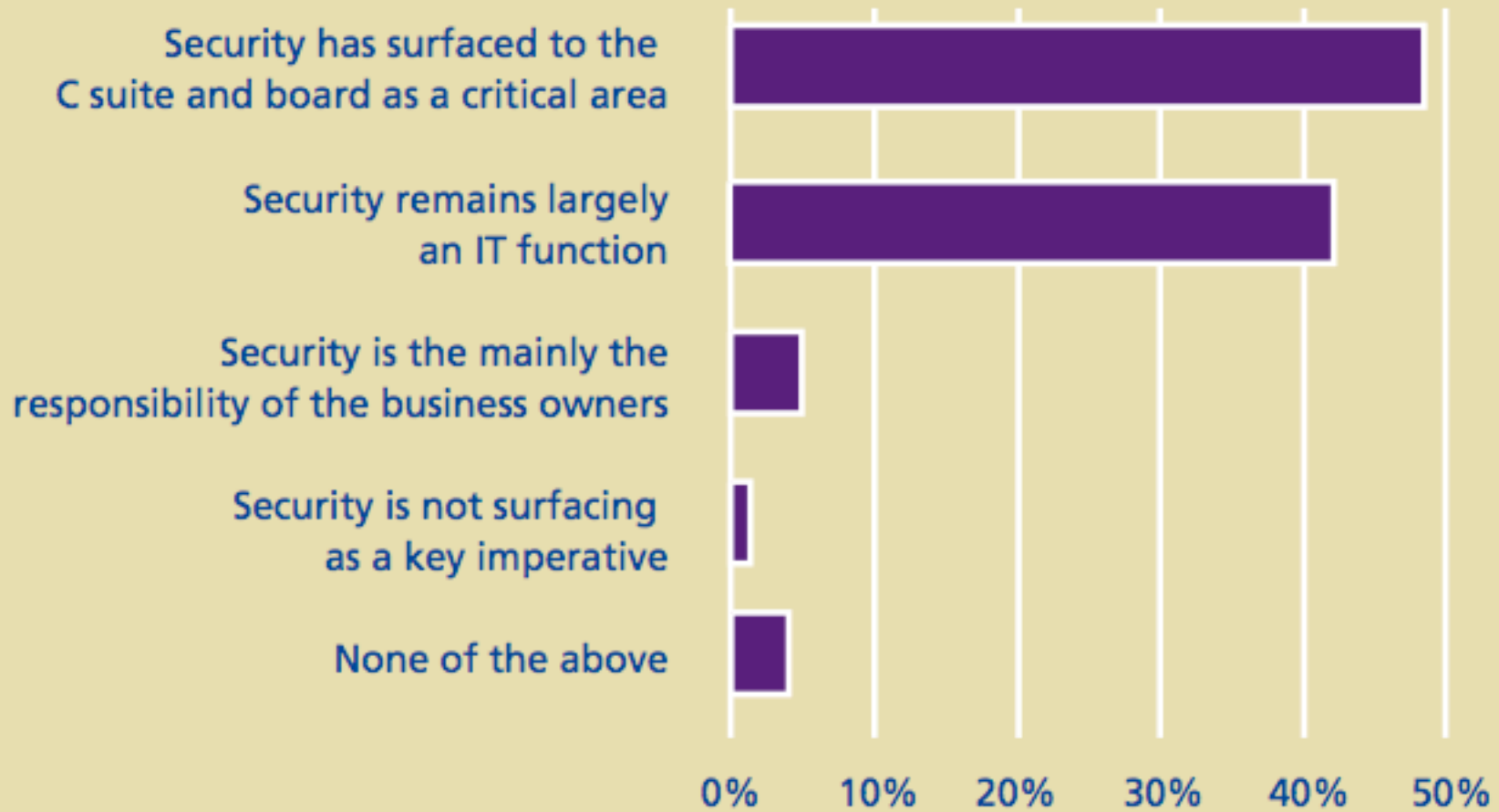
## Cons:

- Seldom works
- Coordinated planning between departments
- Resources
- Coordinated planning from management

# [ IT - Security 'Coopetition' ]

- Availability vs. Security
- Security being stream rolled
  - Get it up and running, disable the firewall
- OSI Layer 8+
  - Culture, influence, budget, politics
- Example: Financial Aid App
  - Web UI open to world
  - VPN, only on campus, ...

## Where security is surfacing



# [ How do you fix this mess? ]

## Formalize Security Program

- Focus on the mission, values, vision, and strategy of University/College
- Integrate security with CIO strategy
- Differentiate Information Security from IT
- Kick start top down planning
- Kick start risk management

# [Components of a Security Program]

- Policy, Practices, Guidelines
- Security Software Development Life Cycle (SecSDLC)
- Risk Management
  - Assessment
  - Analysis
  - Controls
- Security Awareness, Training, Education (SETA)
- DR/BC
- Incident Response
- IDM

# [ Re-examining Strategy ]

- Foundations are Values, Vision, Mission Statements
- Flows from Top to bottom
- Long term direction, Guides all levels
- Focus resources to defined goals

*Goal: Security Program integrated as part of the CIO Strategic Plan*

# [ Find Support - Top Down Planning ]

- Strong upper management support

## Pros:

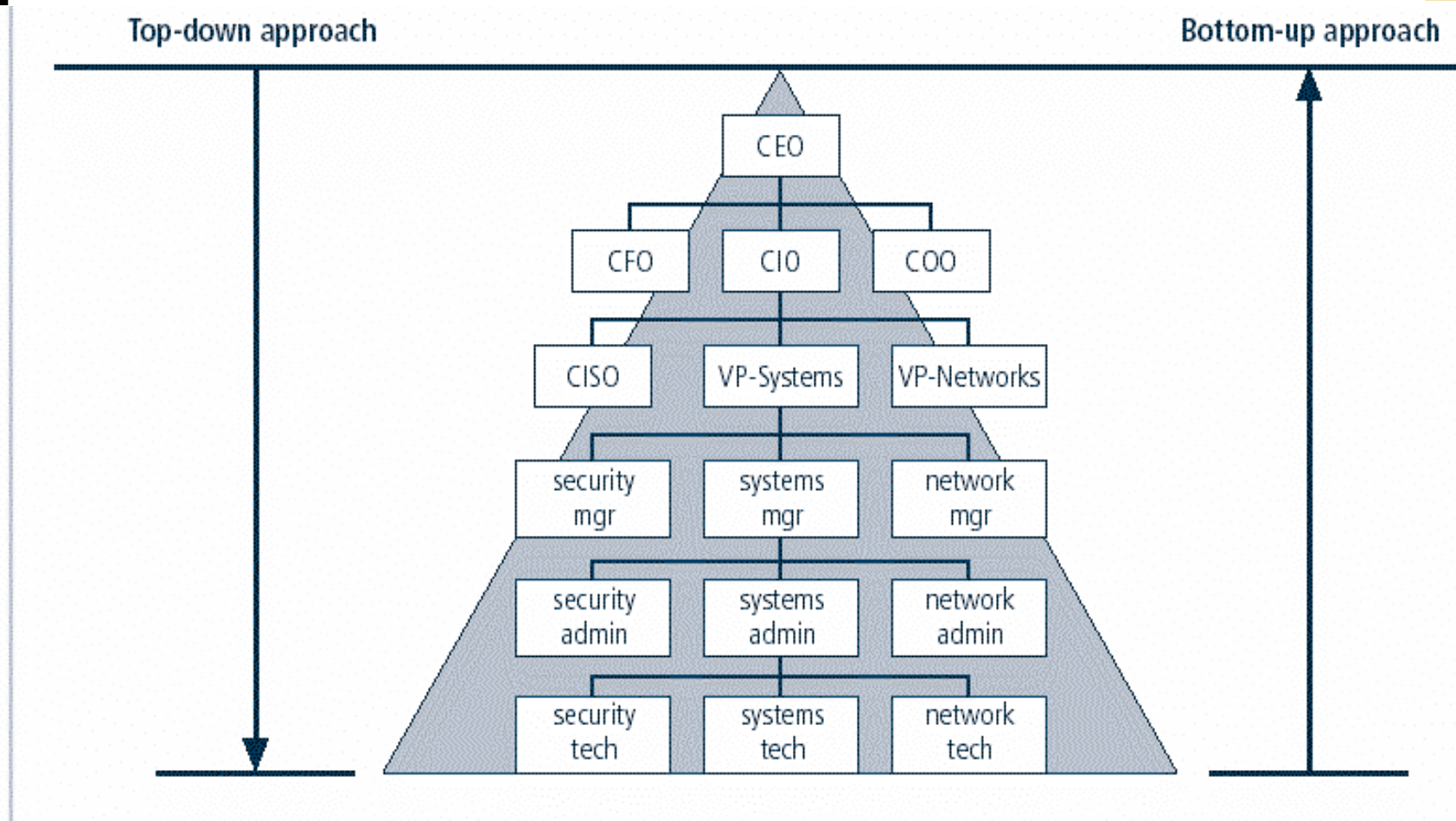
- 'Champion'
- Funding
- Influence
- Define policy, process, procedures for organization
- Direction
- Accountability

## Cons:

- Management must buy into the effort
- Full support to all departments
- Finding a champion

*Goal: Find a champion, kick start top down planning*

# Security Focused Org Chart



**FIGURE 1-8** Approaches to Information Security Implementation

# Differentiate Information Security from IT

- Reorg or new program
  - Goals and objectives in conflict
  - Understand the Pros/Cons in your environment
  - Research possibilities and create memo
- Management of Information Security  
M. Whitman and H. Mattord

*Goal: separate/differentiate InfoSec from IT*

# [ Kick start Risk Management ]

- Application Inventory -> Risk Assessment
  - Identify server/apps and classify the data
  - Identify business owners, application contacts
- Security Tools -> Risk Controls
  - Identify and describe the threat
  - Describe how threat is mitigated with tool

*Goal: Security Program integrated as part of the CIO Strategic Plan*

# Application Inventory -> Risk Assessment

---

- SNMP Polling & Discovery App
  - NeDi
  - Nagios
  - Solarwinds Orion
- System Scanner
  - Server list with application
  - Threats, Vulnerabilities
- Web/Application Scanner
  - Additional detail
- Classify Applications & Data and order by threat level

# [ Security Configs -> Best Practices ]

- Use existing documentation (ya right)
- Create them with IT
  - Champion must help in prioritizing
- Security Best Practices
  - OS's, Network Devices, Encryption, VMs

*Goal: Security Best Practices blessed by CIO, integrated into IT culture and strategy*

# [ Risk Controls - Practices ]

- Windows 2003/XP, Linux, Switches, Routers
  - SANS reading room
  - DOD checklist - <http://iase.disa.mil/stigs/checklist/>
  - SANS Security 505 - Securing Windows
- VMWare
  - Center for Internet Security (CIS) Docs
  - Console OS (Redhat 3), VMs
  - Virtual Machine checklist DOD

# [ Risk Controls - Firewall/VPN ]

- Port and protocol inventory
  - Existing ACLs
  - Use new server & application list
  - VLAN or segment by data type
- Cisco ASA 5505
  - SSL VPN, IPSec, Firewall, Content Filtering, IDS/IPS,...

# [ Risk Controls - IDS ]

---

Coming up next:

Scalable Snort Infrastructure

Phil Deneault

Network Security Officer, WPI

# [ Risk Controls - Pen Testing ]

- Network Scanners
  - Nmap, Nessus, Foundstone, Retina
- Web Scanners
  - Appscan, watchfire, webinspect
  - Acunetix, Hailstorm
  - Network Computing Web-Applications-Scanners

# [ Risk Controls - NAC ]

- Registration
  - 802.1.x, captive portal, passive
  - one time, session, period based
- Detection
  - IDS, SIM, NetFlow, host scan, host agent
- Isolation
  - VLAN, DHCP, ARP, agent, ACL/Route injection
- Remediation
  - Agentless, one time, full agent

# [ Risk Control - PacketFence NAC ]

- Network World - 'This is the best open source NAC available'
- Registration
  - Once, Period interval, session
- Detection
  - Snort, SOAP API
- Isolation
  - ARP, DHCP, VLAN option add on
- Remediation
  - Violation specific instructions
- Commercial Support Offering - [Inverse.ca](http://Inverse.ca)

# [ Risk Controls - Encryption ]

## USB Thumb drive/HDD

No public Partition

Fast 24M/Sec Read 10M/Sec Write

Hardware 256bit AES Encryption

Waterproof

Windows Only

10 Attempts Lock out

Password Hint

DataTraveler Secure  
Privacy Edition



# [ Overview of a Security Program ]

- Risk Assessment
  - Inventory, Server & Application Scanning
- Layered Risk Controls
  - Firewall/VPN/IDS/IPS/SIM
- Security Education, Training & Awareness (SETA)
  - Cyber security month, awareness web site/training
- SDLC
  - Development, Staging, Pen Testing, Production, Maintenance (repeat)

*Goal: tie all the projects together with strategy*

# [ My Goals ]

---

## **Former Security**

- A lot of projects and not a lot of strategy
- Planning bottom up
- Part of IT
- Many Tools

## **Security Program**

- Integrated security strategy with vision
- Top down
- Security Department
- Risk Management

# [ Questions ]

