Architecting Security

NERCOMP

9/24/2007

Mark Poepping
Head IT Architect
Computing Services
Carnegie Mellon

Outline

- Drivers, History, Measures of Success
- Perspective: IT Charter; IT Infrastructure
- IT Security

Drivers

The Security Glass Really **IS** Half-Empty

- Negative Drivers
  - Crisis Response
  - Risk Avoidance
  - Death of a Thousand Cuts
- Where's the "Yippee!"?
  - Security is not an end-user feature
  - Security is an enterprise imperative
- Find, Organize, Serve *YOUR* Drivers

History

- IT is young – 1960, 1970, 1980
- IT Security is younger – 1988
- Growing a *Discipline*
  - Between, among, in spite of, but ultimately for Applications, Systems, Networking...
  - All in service of those wondrous *customers*
  - *Necessity is the mother of invention*
    - But it's nice to think ahead…

Reference

- EDUCAUSE Leadership Strategies, Volume 8: “Computer and Network Security in Higher Education”, Luker and Peterson, 2003 EDUCAUSE
  - IT Security and Academic Values
  - Organizing for Security
  - Risk
  - Liability
  - Policy
  - Architecture
  - Security Education

Success

- Structural – *Drain the Swamp*
  - Integrated Discipline: *build Security in*
  - Defined, Sustained Activity
    - Prevent, Detect, Remediate, Investigate
  - Managed Risk - *Limiting Loss*
    - There will always be surprises
- Tactical – *Fight off the Alligators*
  - Handle the Priorities
  - Functioning with Security
    - We still get the work done, just more safely

Perspective: IT Charter

- Facilitate and Automate
  - Needs of the Business
    - In: Manufacturing, Instruction, Research
    - For: ERP, Financials, HR, SIS
    - On: Marketing (CRM, Web, CMS)
  - Needs of Users
    - Communications, Documents, Presentation
    - Entertainment, Personal Expression

IT Infrastructure Leverage Commonalities

- Enterprise and IT-focused reasons
  - Technical - Efficiency of effort/investment
  - Functional - Policy and control
    - Audit, regulation, asset management
- User-focused reasons
  - Common user information across applications
  - One way to do each thing
  - One person to call

IT Infrastructure (15 years ago)

- Networks
  - Voice
  - Data – Dialup, Local, Wide Area
- Systems
  - Server platforms; Hardware, OS (proprietary)
  - Maybe NOS or File Systems – Accounts
- Applications
  - Business – ERP, Fin, HR
  - Computer Labs
  - Personal Productivity - Email, Doc/Presentation
- Operations – Machine Rooms, backups
- Help desk

New IT Infrastructure

- Networks
  - Wireless, VPN, Mobility
  - Network Access Control
  - VoIP Services, E911
  - International/Multi-home connectivity
- Systems
  - Open source servers and services
  - Virtualization – platforms + storage
  - Client Diversity
- Middleware
  - Identity Management
    - Authn/r
    - Internal/External Federation
    - Entitlement/service provisioning
  - Unified messaging
    - Anti-messaging (A/spam,A/Virus)
  - Sharing/collaboration
  - CMDB, Monitoring, Logging
- Information Security, Compliance
  - Firewall/IDS/IPS, Defense-in-depth
  - Data Classification, Policy
  - Incident response, Forensics
  - SOX, E-Discovery, FERPA, HIPAA, CALEA
- Application Infrastructure
  - Web delivery (portal/SaaS)
  - Enterprise Data/Service (SOA/ESB)
  - Data Warehouse, Document Mgmt
  - Course Management, Repositories
  - Research – Data/Cycles/Storage
  - IT-Enabled (e.g. Keycards, HVAC)
- Operations/Support
  - DR/BC; Emergency Response
  - 24x7x360 (global operation)
  - Insource, Outsource

Networks

- Wireless, VPN, Mobility
- Network Access Control
- VoIP Services, E911
- International/Multi-home connectivity

Systems

- Open source servers and services
- Virtualization – platforms + storage
- Client Diversity

Middleware

- Identity Management
  - Authn/r
  - Internal/External Federation
  - Entitlement/service provisioning
- Unified messaging
  - Anti-messaging (A/spam,A/Virus)
- Sharing/collaboration
- CMDB, Monitoring, Logging

Information Security, Compliance

- Firewall/IDS/IPS, Defense-in-depth
- Data Classification, Policy
- Incident response, Forensics
- SOX, E-Discovery, FERPA, HIPAA, CALEA

Application Infrastructure

- Web delivery (portal/SaaS)
- Enterprise Data/Service (SOA/ESB)
- Data Warehouse, Document Mgmt
- Course Management, Repositories
- Research – Data/Cycles/Storage
- IT-Enabled (e.g. Keycards, HVAC)

Operations/Support

- DR/BC; Emergency Response
- 24x7x360 (global operation)
- Insource, Outsource

Secure that Infrastructure

- Boiling the new ocean
  - Structural
    - A lot of people to teach
    - Can't *Bolt it on*
    - Need a *system*
  - Tactical
    - A lot of software/productivity to protect
    - Need some tools
    - They will evolve as structure co-informs

IT Security

- Bottom-up – security immediacies, practice
  - Examples, situations, remediation
  - Issues, use cases, policy
- Top to Bottom
  - Security Architecture
  - Evolve development process – Build Securely
- Top-upward
  - Business architecture and goals
  - Risk assessment, enterprise priority, high-level policy

Top-Upward

- Uh

Top-Upward

- Conditions
  - Reporting Structure
  - Situational History
    - Crisis or foresight
  - Organizational Self-awareness
  - Geo-Political, Financial, Social Conditions
  - Alumniacal Realities and Retention of Faculties
  - Not just a *Security* issue
- Potential Action
  - ~~Head-on~~
  - Supporting
    - Engage your CIO - help with models, translation, timing
  - Wait-n-see
    - Build perspective, look for opportunities

Top to Bottom - What

- Model Security Architecture
  - Principle, Practice, Control, but further…
  - Value Measures in line with Organization
    - Buy a new server or a faster firewall?
- Establish Security Operations
  - Prevent, Detect, Remediate, Investigate
  - Policy, Training/Awareness
- Integrate Security into Processes
  - Security consideration early in project cycle
    - Standard processes - proposal, decision, review
    - *Security Profile* as software service attribute (portfolio)
  - Periodic review of standard operational practice
    - Manage changes, evolution

Top to Bottom - How

- Define an Agenda
  - Path to improvement
    - Can't "do everything now"
    - Focus on Total Value
  - Functional roadmap
    - Tactical – stuff for you
    - Structural – helping others
    - With the rest of the organization
      - Shouldn't mandate what we can't sustain
      - Expose, Support new work for others

Bottom-Up

- Acquire and use tools based on:
  - What your bosses want
  - What your peers do
  - What you believe you can achieve
    - Can't live without
    - Can't live with
    - Simplest to do at the time
  - *Best of breed?*
    - What they'll sell you
    - What you can afford
    - What you can sustain
- Filling Time or Creating Value
  - Beware of *diminishing returns* (i.e. the deadly rathole)
  - "Must I be in this business? Can I ever get out?"

Architecting Security

NERCOMP

9/24/2007

Mark Poepping
Head IT Architect
Computing Services
Carnegie Mellon