Purpose Driven Security

- Ideas, thoughts, opinions and tips on information security's relevance to business
- What are some common standards & how to approach them
- Why process & purpose are great partners
- Why adopting standards matters more than ever
- The crystal ball (prognostications)

The purpose of information security?

- How do we (security people) talk?
  - Confidentiality, Integrity, Availability (CIA)
  - Advanced persistent threats, hacktivists….
- What do executives & managers hear?
  - Blah, blah, blah …….
  - Cognitive dissonance or something else?
- "… if we want to make significant, quantum change, we need to work on our basic paradigms.." – Steven Covey

Great, but what do we DO!?

- "Secure stuff" ... yes, but....
- WHY?
  - Because we're cool (knowledge of the black arts:)
  - It's the right thing to do (noble cause)
  - Someone pays us to
- What do “non magic” folk think of us?
  - Befuddle the masses with dramatic practices of intellectual kung-fu?
- Short answer is, we may not really know
  - Do you see dead people? ☺

Security paradigm? (buzzword alert)

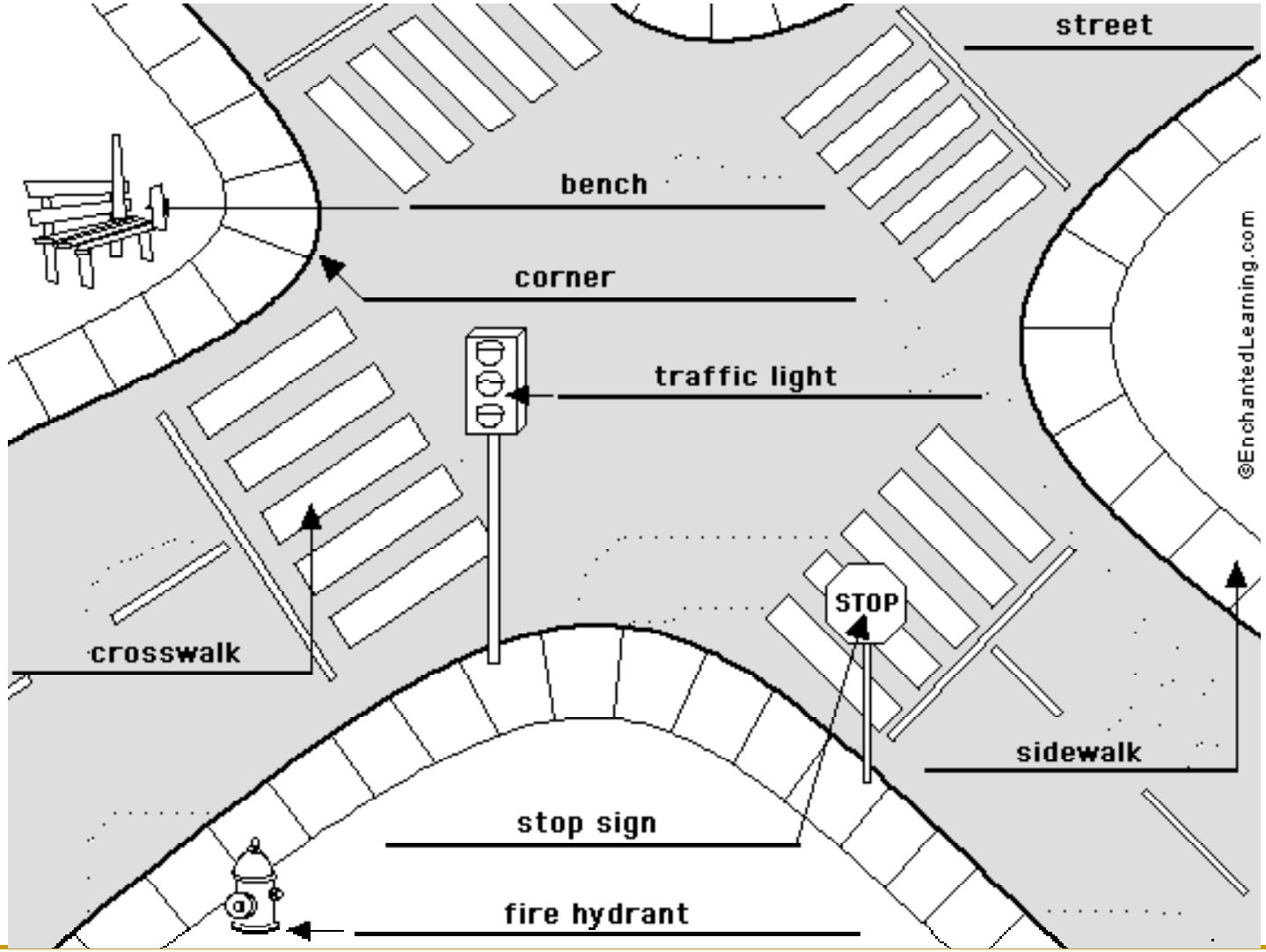
- Paradigm: Way of seeing, interpreting, seeing the world
- Infosec; we study carefully… intently
  - But everything looks like an issue
    - Dr. No syndrome
- An "aha!" moment

Me: Blaine I need help communicating to executives why tool X is critical!
Blaine: Dave, you've talked about tools a lot
Me: Yeah! They're great!
Blaine: Have you talked to them about trucks?
Me: Trucks? Why would I talk about trucks?
Blaine: Your company has trucks, will tool X help them move freight?
Me: Um…
Blaine: You need to talk their language not about tech tools

What If….

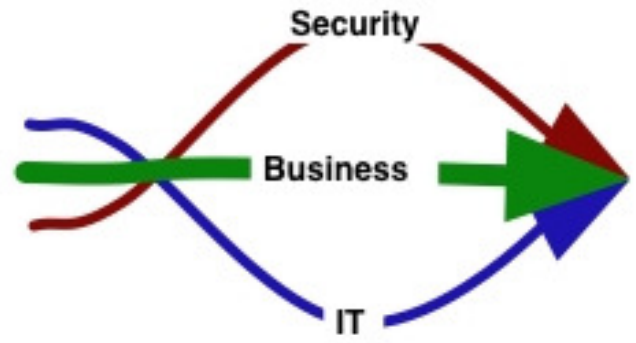
- We talk about increasing productivity?
- Werner Example, we move freight
  - How can information security move a pallet?
- What if controls can be shown to make IT and thereby business perform – better?
  - IT Process Institute study of IT top performers
- How do we do that?
  - Consider the crosswalk

Crosswalk Security Model



Purpose

- Every organization has SOME purpose
  - No… really it does…
- What is purpose driven security?
  - Adapted from Rick Warren's book, "The Purpose Driven Church"
  - Leaving theology out of it, there are business lessons in it (Karlgaard 02/04)



Being Purpose Driven

- The goal (purpose) of the business must be clear and concise
- Everything must be dedicated in support of that purpose
  - Organization, staffing, communications, calendaring, budgeting, evaluations (personal & programmatic)
- The skills of key contributors are important, but don't overshadow purpose
- Have a process, but keep proper flexibility
  - Process shouldn't overshadow purpose
  - Begin with the end in mind (another Covey-ism)

Purposeful Security & IT

- Security must be a key part of corporate planning
- Security must be properly aligned within the company
- Security must be accountable for deliverable products/results
- Security must understand how it supports company mission (purpose)
- Every company has a risk model
  - It may not be written
  - Someone, somewhere is making risk decisions

IT/Security Alone is Flawed

- History shows that:
  - Technology can innovate
    - Has to have vision/purpose
- Enron had great technology
  - The people processes were flawed

> "*If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology*." - Bruce Schneier
>
> "Secrets and Lies"

IT Doesn't Matter

- Purpose does
- IT Doesn't Matter by Nicholas G. Carr
  - Three main points:
    1. Spend less
    2. Follow don't lead
    3. Focus on vulnerabilities
  - Its not that IT doesn't matter, but the emphasis is changing as technology matures

> "... When a resource becomes essential to competition but inconsequential to strategy, the risks it creates become more important than the advantages it provides."
>
> - Nicholas G. Carr

Soooo….

- How do we apply “purpose” in a structured way?
- How do we minimize risk without retarding our organizations?
- How can IT/Security be consistently utilized?

The "F" Word :)

- Not that one! Framework!
- Established standards for IT practices
  - I know... the other "f" word comes to mind ;)
  - But... "common sense" doesn't necessarily scale
- What do we think of when the word framework comes up? – BLOAT!

Watch the Bath Water

- There may be a baby in it
- Don't let framework overtake purpose
- Any organization has something it DOES
  - Any framework should be a reference for DOING something better
- How many failed TQM & ISO9000 projects have there been?
  - Why?

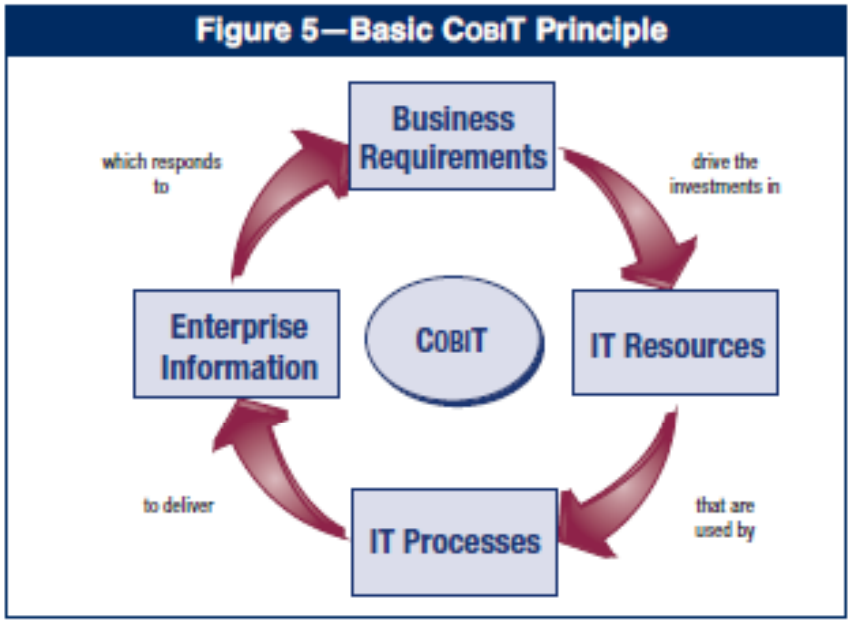
IT/Security Management Frameworks

- COBIT
  - Comprehensive (huge actually)
  - Cool buzzword "IT governance”
  - Very accessible
- ISO Standards
  - ITIL (ISO 20000)
    - Strong, process oriented ITSM approach
  - ISO 27001 & 27002
- Most major standards have common factors
  - Careful strategy aligned with business
  - Security is strong element
  - Adopting best practices for managing IT

CoBiT Principles

- **Four phases**

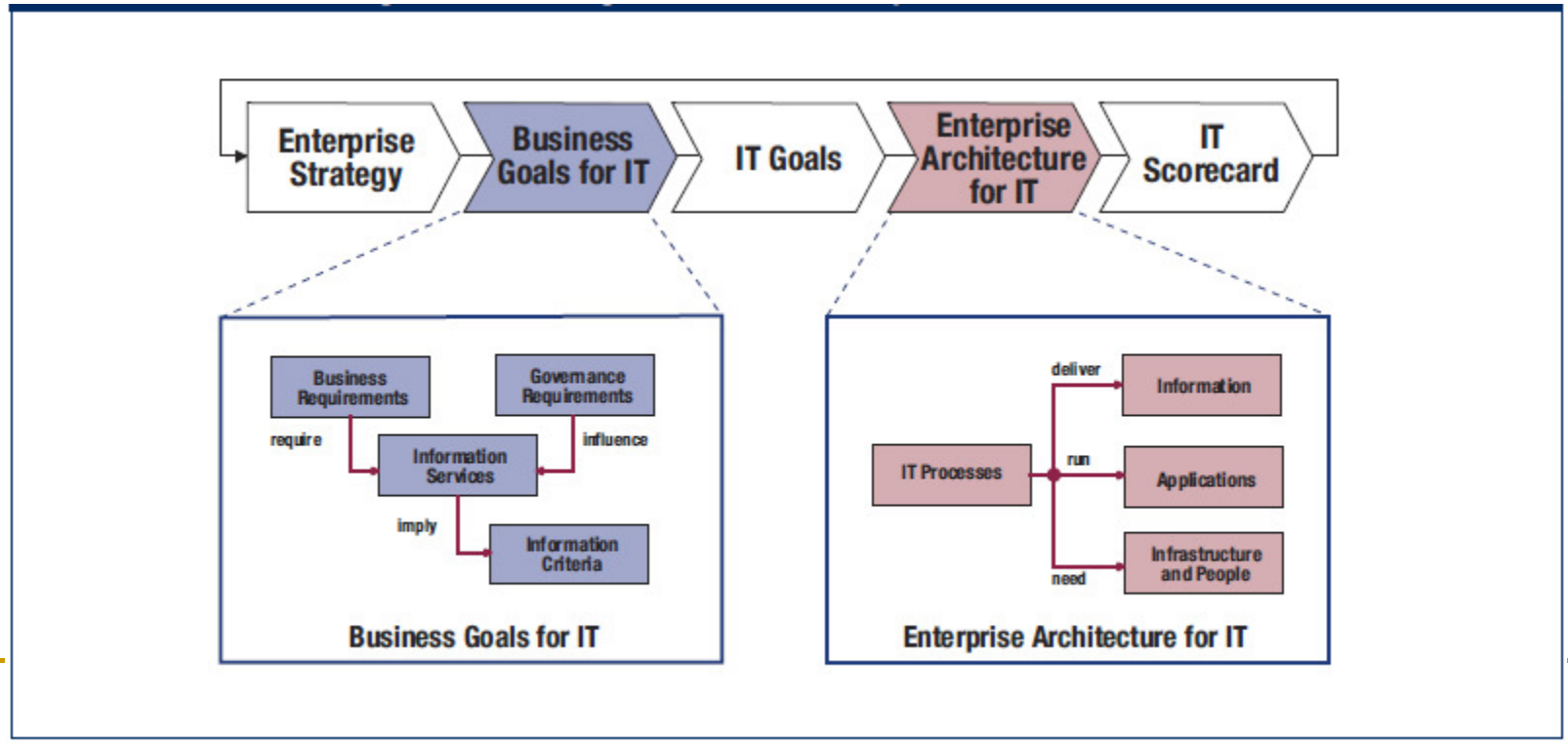
1. Plan & Organize
2. Acquire & Implement
3. Deliver & Support
4. Monitor & Evaluate



In their own words: “COBIT® provides good practices across a domain and process framework and presents activities in a manageable and logical structure”

CoBiT From 30,000 Feet

- Strong process orientation
  - 34 IT processes
- Strong “business” support
  - IT processes must support business requirements



An Auditor's Clipboard Dream ☺

Legend:

Information Criteria
- **Blank** = No impact
- **P** = Primary impact
- **S** = Secondary impact

IT Resources
- **False** = Not used
- **True** = Used

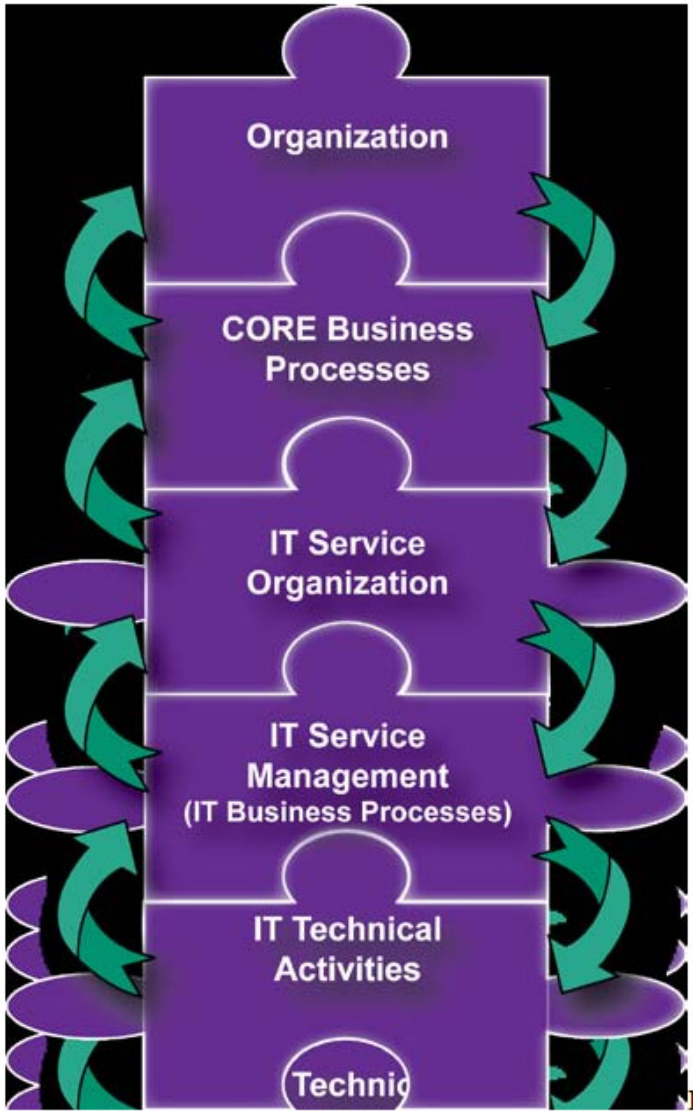
	Information Criteria							IT Resources				
	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	People	Applications	Technology	Facilities	Data
Plan and Organise												
PO1 Define a Strategic Information Technology Plan	P	S						✓	✓	✓	✓	✓
PO2 Define the Information Architecture	P	S	S	S					✓			✓
PO3 Determine Technological Direction	P	S								✓	✓	
PO4 Define the Information Technology Organisation and Relationships	P	S						✓				

Issues with CoBiT

- What would happen if you implemented its entirety?
  - You might be great at CoBiT but go out of business ☺
  - It is extremely exhaustive
- Reminds of OSI model for networking
  - Great reference is it too bloated to really “do”
  - Is the bible for IT auditors

ITIL Basics

- Emphasis on “service management”
  - Operation & maintenance of current systems
  - New systems development
  - Adjustment of services to meet business requirements
- Core of ITIL management
  - Service delivery
  - Service support



ITIL "Starter Kit"

- ITIL can be started quickly
  - Not as complex as CoBiT
  - Can be implemented in phases
- The Visible Ops Handbook
  - Gene Kim, George Spafford, Kevin Behr
  - Tied to work at the IT Process Institute
  - Studied hundreds of organizations
    - Categorized high & low performers

Visible Ops Approach

- Four phases
  1. Stabilize the patient
     - Start the road to recovery
  2. “Catch & Release”, “Find Fragile Artifacts”
     - Create & maintain production inventory
     - Note the fragile “don’t touch” infrastructure
  3. Create repeatable build library
     - Stress on reducing mean time to repair (MTTR)
     - Make infrastructure easier to rebuild than repair
  4. Continual improvement
     - “The better you get, the better you’d better get” – David Allen

Fruit of "Visible Ops"

- Did you know that high performers:
  - Have a higher ratio of servers to admins? (around 100:1 or higher)
  - Plan which controls they use in support of business
  - Roll out patches less often than others
  - Have most outages linked to planned change requests
  - Generally fix incidents without "logging in"
  - Spend 15% or less of their time on unplanned work
  - Spend less time on audits than others
- Low performers:
  - Have higher ratios of servers to admins
  - Spend 50% or more of their time on unplanned work
  - Use scattered sets of controls & live in audit hell

Security Standards

- ISO17799 & BS7799
  - International standard for security policy
    - ISO17799:2000 - Provides a well rounded look at all areas of policy
    - BS7799:2002 - Augments code of practice in ISO17799:2000
      - Plan, Do, Check, Act model
- NIST (Treasure trove of material)
  - SP800-53: Recommended controls
  - SP800-64: Security & software life cycle planning
- Other sources (primarily technical level)
  - SANS, Charles Cresson Wood

My $.02 on Standards

- ITIL makes sense to me
- But pick a card… any card
- Standards without purpose won't solve anything
- Understand your controls
  - A business risk model is the rosetta stone
  - Document your controls against *some* major standard
  - A process oriented program for consistency

Fuzzy Pumper Barber Shop

- Now we have:
  - The idea that IT is changing
  - Legal issues are mounting
  - The security world is collapsing like a black hole
    - Zero day security flaws
    - Huge exposures of private data
    - Online fraud epidemic
  - Processes are needed
- What's the magic solution?
- Just squeeze the handle?

Prognostications!

- This my own personal crystal ball (take with grain of salt)
  - Standards will matter more, not less
    - Over 80% of public favors national privacy legislation
    - Laws mean… (drum roll) compliance
    - Compliance requires using approved practices
  - I believe we will see a PCI style standard for personal data
    - There will be legal and civil liabilities for companies, IT & security professionals
    - You will need to demonstrate due diligence
  - Security professionals split into two camps
    - Those who administer
    - Those who produce compliance reports

No More Scary Monsters

- IT/Infosec leaders must cease to be wizards
- Commoditization makes management more important
  - IT is arguably a commodity, what are "difference makers"?
  - Top performers have common factors
- A defined process that supports purpose is understandable and capable of constant improvement
- Standards & frameworks don't guarantee security
  - You can't PCI the stupid out of people ☺

Wait… Hold the Presses

- We left out something important
  - Measurements, aka metrics
- A metric isn't security, it is visibility into the security **process**
- Can you demonstrate what you can't measure?
- **Omaha ISSA Security Metrics Workshop**
  - Tuesday August 30, 3:00 -> 4:30PM
  - Featured speaker Dr. Lance Hayden
  - **RSVP communications@issa-omaha.org**
  - **http://issa-omaha.org**

Omaha ISSA

- ISSA well known, international affiliation of information security professionals
- Local chapter being formed
- Multiple speakers/sessions in the works
  - Dr. Lance Hayden: Information Scientist & IT Security Professional for Cisco Corporation and author of "IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data"
  - Dr. Kevin Kealy - Interim Chief information Security Officer for Select Comfort and Security Scientist at AT&T Labs
  - Eric Cowperthwaite - Chief Information Security Officer at Providence Health & Services.
  - Mike Rothman - President of Securosis and author of "The Pragmatic CSO"
  - Alex Hutton: Sprint Research & Intelligence Principal