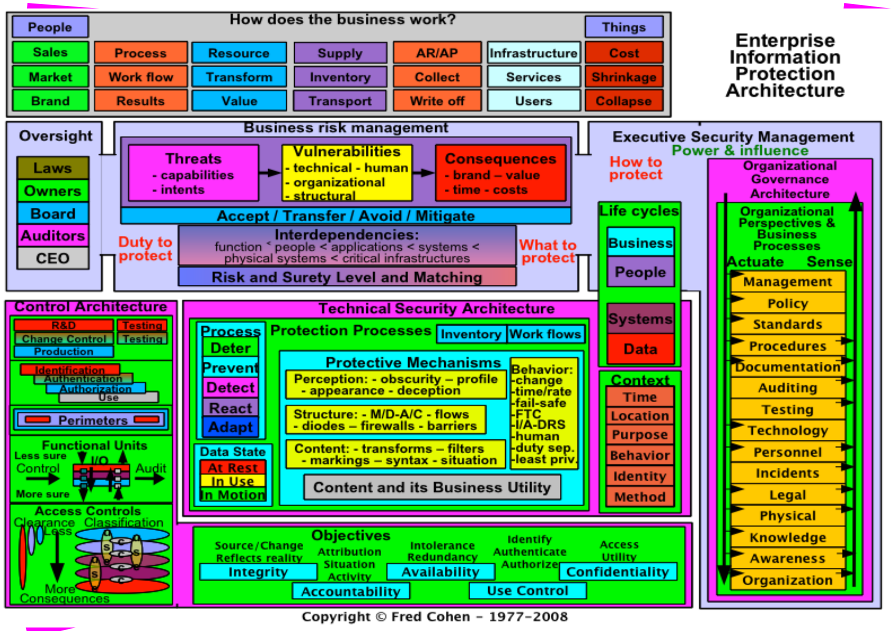
Fitting Information Security into the Business

An Issue of Governance

Fred Cohen
CEO – Fred Cohen & Associates
President – California Sciences Institute



Enterprise Information Protection Architecture

How does the business work?

People | Things

Sales | Process | Resource | Supply | AR/AP | Infrastructure | Cost
Market | Work flow | Transform | Inventory | Collect | Services | Shrinkage
Brand | Results | Value | Transport | Write off | Users | Collapse

Oversight: Laws, Owners, Board, Auditors, CEO

Business risk management

Threats - capabilities - intents → Vulnerabilities - technical - human - organizational - structural → Consequences - brand – value - time - costs

Accept / Transfer / Avoid / Mitigate

Interdependencies: function < people < applications < systems < physical systems < critical infrastructures

Risk and Surety Level and Matching

Duty to protect

What to protect

Executive Security Management
Power & influence

How to protect

Organizational Governance Architecture

Organizational Perspectives & Business Processes

Actuate | Sense

Management, Policy, Standards, Procedures, Documentation, Auditing, Testing, Technology, Personnel, Incidents, Legal, Physical, Knowledge, Awareness, Organization

Life cycles: Business, People, Systems, Data

Context: Time, Location, Purpose, Behavior, Identity, Method

Control Architecture

R&D | Testing
Change Control | Testing
Production

Identification, Authentication, Authorization, Use

Perimeters

Functional Units: Less sure, Control, I/O, Audit, More sure

Access Controls: Clearance, Classification, Less, More, Consequences

Technical Security Architecture

Process: Deter, Prevent, Detect, React, Adapt

Protection Processes: Inventory, Work flows

Data State: At Rest, In Use, In Motion

Protective Mechanisms

Perception: - obscurity – profile - appearance - deception

Structure: - M/D-A/C - flows - diodes – firewalls - barriers

Content: - transforms – filters - markings – syntax - situation

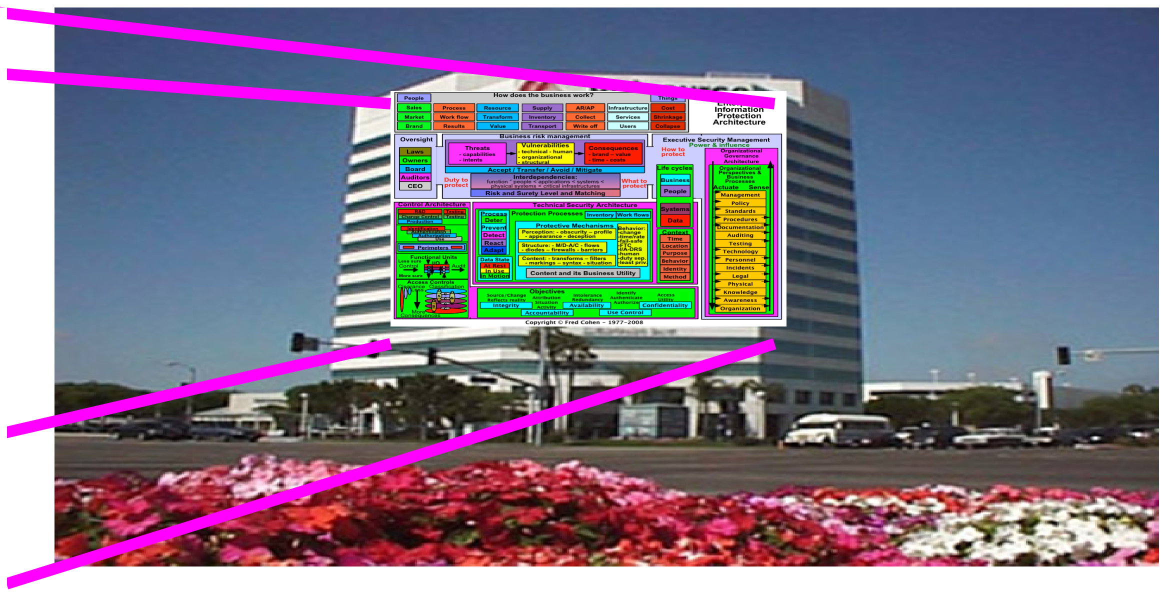
Behavior: -change -time/rate -fail-safe -FTC -I/A-DRS -human -duty sep. -least priv.

Content and its Business Utility

Objectives

Source/Change, Reflects reality: Integrity
Attribution, Situation, Activity: Accountability
Intolerance, Redundancy: Availability
Identify, Authenticate, Authorize: Use Control
Access, Utility: Confidentiality

Copyright © Fred Cohen – 1977–2008



Key issues

- It's about the business!
  - There are lots of vulnerabilities – so what?
    - We can always find technology weaknesses
    - We can always find people weaknesses
    - So what?
  - The issue: Potentially serious negative consequences
    - Unless vulnerabilities produce them, we cannot afford to care
    - But we may have to search for a long time
  - How do we find the problems that matter?
    - We have to model the business to figure this out
    - We have to know what's there, why, and how it works
  - How do we manage them effectively and efficiently?
    - Business models, inventories, and work flows

Outline

People	How does the business work?					Things
Sales	Process	Resource	Supply	AR/AP	Infrastructure	Cost
Market	Work flow	Transform	Inventory	Collect	Services	Shrinkage
Brand	Results	Value	Transport	Write off	Users	Collapse

- Background
- The Big Picture
- Business modeling
- Inventory
- Work flows
- An example
- Summary & Conclusions

Inventory	Work flows

Background of the Speaker

- Some career accomplishments
  - MS Information Science, Ph.D. EE
  - First examined “Computer Viruses” and defenses
  - First defined “Information Assurance” as used today
  - Critical infrastructure protection starting in 1992
  - 30+ years of research, development, consulting in the information protection arena
  - 150+ professional papers, 10+ books, hundreds of presentations and talks, and on and on
- President: “California Sciences Institute”
  - Non-profit post-graduate educational institution

Background of the Talk

- Ongoing development since the 1980s of a systematic comprehensive approach to enterprise information protection
  - 1984 – Technical underpinnings and TechSecArch
  - 1990 – IPPAs and organizational perspectives
  - 1992 – Interdependencies and risk aggregation
  - 1995 – Business risk management, life cycles
  - 2003 – Control architecture as a concept
  - 2004 – Oversight, duties, power and influence
  - 2006 – Business modeling and work flows
  - 2007 – Inventory control integration

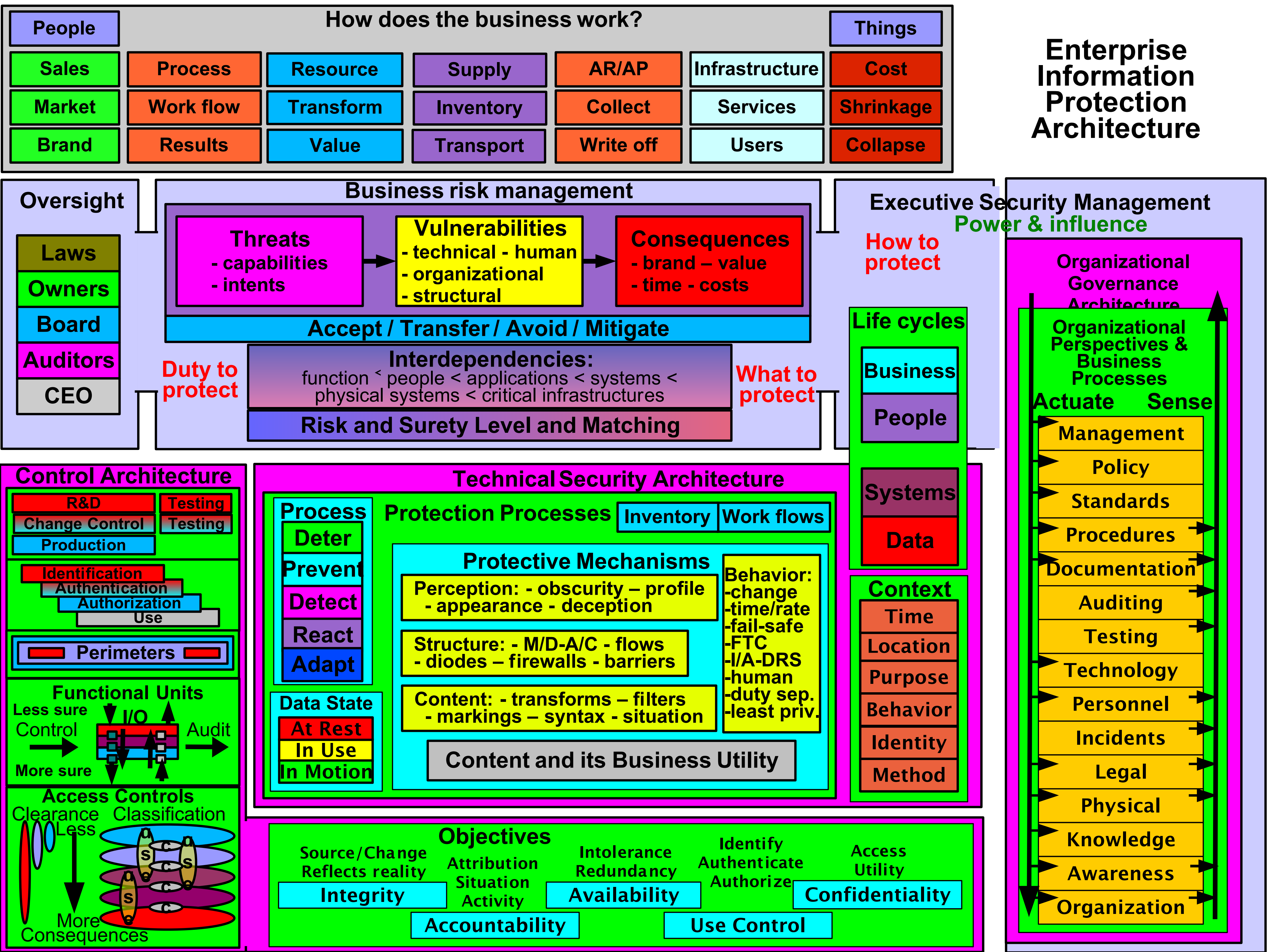
Outline

People			How does the business work?			Things
Sales	Process	Resource	Supply	AR/AP	Infrastructure	Cost
Market	Work flow	Transform	Inventory	Collect	Services	Shrinkage
Brand	Results	Value	Transport	Write off	Users	Collapse

- Background
- The Big Picture
- Business modeling
- Inventory
- Work flows
- An example
- Summary & Conclusions

Inventory	Work flows

Enterprise Information Protection Architecture



How does the business work?

People

Things

Sales | Process | Resource | Supply | AR/AP | Infrastructure | Cost

Market | Work flow | Transform | Inventory | Collect | Services | Shrinkage

Brand | Results | Value | Transport | Write off | Users | Collapse

Oversight

Laws

Owners

Board

Auditors

CEO

Duty to protect

Business risk management

Threats
- capabilities
- intents

Vulnerabilities
- technical - human
- organizational
- structural

Consequences
- brand – value
- time - costs

Accept / Transfer / Avoid / Mitigate

Interdependencies:
function ˂ people < applications < systems < physical systems < critical infrastructures

Risk and Surety Level and Matching

What to protect

Executive Security Management

Power & influence

How to protect

Life cycles

Business

People

Systems

Data

Control Architecture

R&D | Testing

Change Control | Testing

Production

Identification

Authentication

Authorization

Use

Perimeters

Functional Units

Less sure

I/O

Control

Audit

More sure

Access Controls

Clearance

Classification

Less

More

Consequences

Technical Security Architecture

Process

Deter

Prevent

Detect

React

Adapt

Data State

At Rest

In Use

In Motion

Protection Processes

Inventory | Work flows

Protective Mechanisms

Perception: - obscurity – profile - appearance - deception

Structure: - M/D-A/C - flows - diodes – firewalls - barriers

Content: - transforms – filters - markings – syntax - situation

Behavior:
-change
-time/rate
-fail-safe
-FTC
-I/A-DRS
-human
-duty sep.
-least priv.

Content and its Business Utility

Context

Time

Location

Purpose

Behavior

Identity

Method

Objectives

Source/Change
Reflects reality

Integrity

Attribution
Situation
Activity

Accountability

Intolerance
Redundancy

Availability

Identify
Authenticate
Authorize

Use Control

Access
Utility

Confidentiality

Organizational Governance Architecture

Organizational Perspectives & Business Processes

Actuate | Sense

Management

Policy

Standards

Procedures

Documentation

Auditing

Testing

Technology

Personnel

Incidents

Legal

Physical

Knowledge

Awareness

Organization

Outline

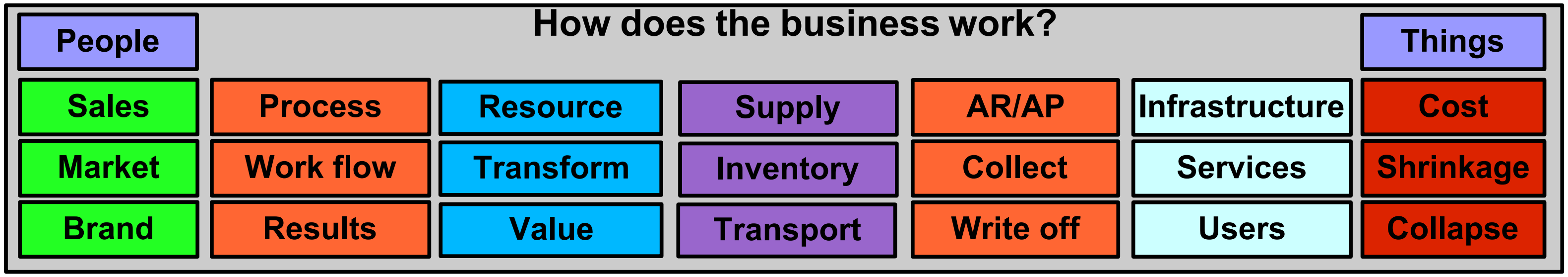
People			How does the business work?			Things
Sales	Process	Resource	Supply	AR/AP	Infrastructure	Cost
Market	Work flow	Transform	Inventory	Collect	Services	Shrinkage
Brand	Results	Value	Transport	Write off	Users	Collapse

- Background
- The Big Picture
- Business modeling
- Inventory
- Work flows
- An example
- Summary & Conclusions

Inventory	Work flows

Business modeling

- Information Security Starts with the Business
  - What does the business do?
  - How does the business do it?
  - How does the business interact with information?
  - What are the business implications of failures?
  - How does the protection program mitigate them?
    - **<u>The potentially serious negative consequences</u>**
    - NOT the failures – except as they produce business potentially serious negative consequences



How does the business work?

People						Things
Sales	Process	Resource	Supply	AR/AP	Infrastructure	Cost
Market	Work flow	Transform	Inventory	Collect	Services	Shrinkage
Brand	Results	Value	Transport	Write off	Users	Collapse

Why model the business?

So you can do proper risk management

- Risk management demands understanding business consequences of information technology failures
  - Loss of integrity, availability, confidentiality, use control, and accountability,
  - Induces liability, repetitional harm, loss, cost, etc.
- To do this, some kind of model of the business against which failures can be posited is necessary
  - The model may be in the heads of the team members
  - The model may be a computer model
  - The model may be the expertise of a group using spreadsheets and hand notes
- The results of risk management depend critically on this model

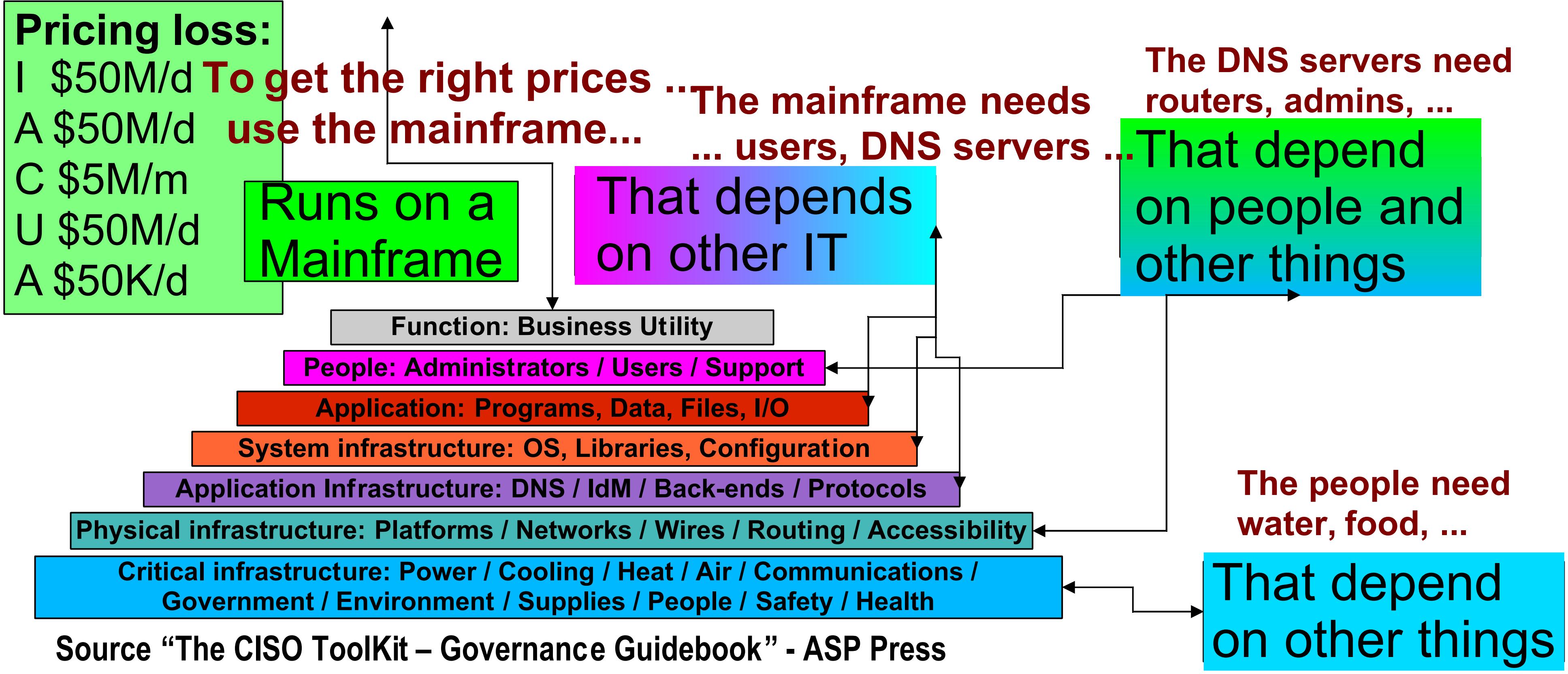
What might a model look like?

- Suppose I am in the shoe business (manufacturing)

To make shoes I have to... price orders ...

To price orders I have to... get right prices ... and if I don't...

People/Things		How does the business work?			People/Things	
Sales	Process	Resource	Supply	AR/AP	Infrastructure	Cost
Market	Work flow	Transform	Inventory	Collect	Services	Shrinkage
Brand	Results	Value	Transport	Write off	Users	Collapse



Pricing loss:
I $50M/d
A $50M/d
C $5M/m
U $50M/d
A $50K/d

To get the right prices ... use the mainframe...

Runs on a Mainframe

The mainframe needs ... users, DNS servers ...

That depends on other IT

The DNS servers need routers, admins, ...

That depend on people and other things

The people need water, food, ...

That depend on other things

Function: Business Utility

People: Administrators / Users / Support

Application: Programs, Data, Files, I/O

System infrastructure: OS, Libraries, Configuration

Application Infrastructure: DNS / IdM / Back-ends / Protocols

Physical infrastructure: Platforms / Networks / Wires / Routing / Accessibility

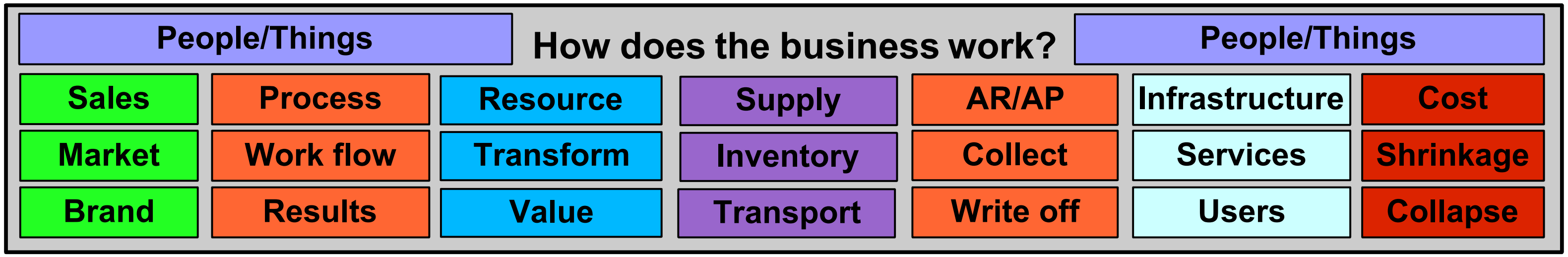
Critical infrastructure: Power / Cooling / Heat / Air / Communications / Government / Environment / Supplies / People / Safety / Health

Source “The CISO ToolKit – Governance Guidebook” - ASP Press

What does the model include?

A useful model from a standpoint of risk management encompasses three key things:

- It models how the business functions at a gross level
- It models specific key issues that interact with IT ranging from people to things:



People/Things			How does the business work?		People/Things	
Sales	Process	Resource	Supply	AR/AP	Infrastructure	Cost
Market	Work flow	Transform	Inventory	Collect	Services	Shrinkage
Brand	Results	Value	Transport	Write off	Users	Collapse

- It models the dependencies of these things on IT

•It would also be nice...

- If it could model malicious and accidental events

The model includes...

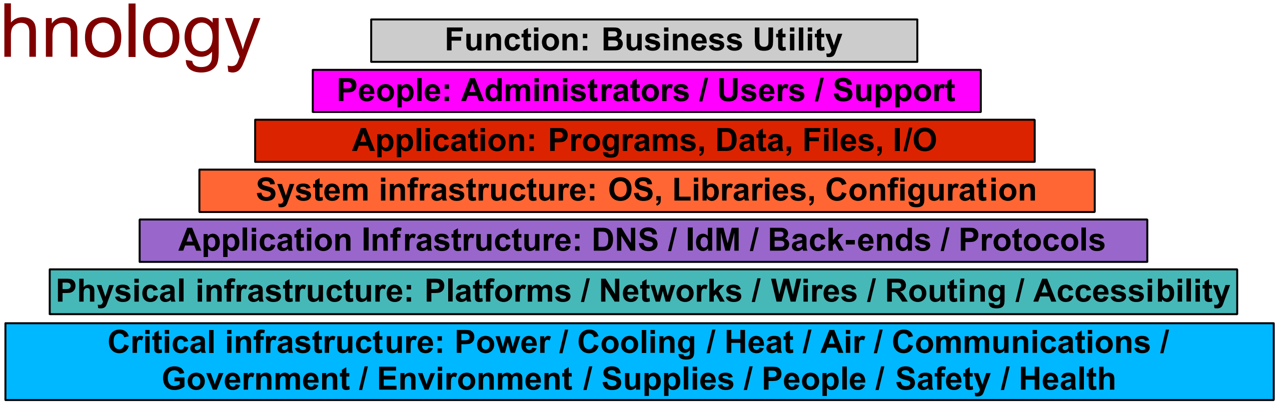
How does the business function?

- We make shoes and sell them at wholesale
  - To make them we need this...
  - To sell them we need this...
  - To deliver on the sales we need this...

There's a hole in my bucket
So fix it ...
With what...
With ...
... ... water ...
But there's a hole in my ...

It models interdependencies

- Starting with the business utility, there are a series of recursive dependencies associated with information and information technology
- And ... people
- Infrastructure
- Society ...



Function: Business Utility

People: Administrators / Users / Support

Application: Programs, Data, Files, I/O

System infrastructure: OS, Libraries, Configuration

Application Infrastructure: DNS / IdM / Back-ends / Protocols

Physical infrastructure: Platforms / Networks / Wires / Routing / Accessibility

Critical infrastructure: Power / Cooling / Heat / Air / Communications / Government / Environment / Supplies / People / Safety / Health

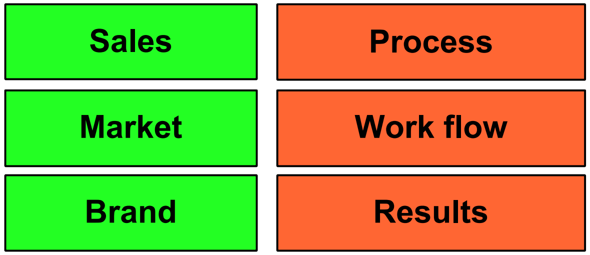
Elements you should consider

Key: Sales – Market – Brand

- How are leads generated, tracked, pursued etc.
- How does the enterprise fit into special niches
- How is the company presented, viewed, understood

Key: Process – Workflow – Results

- How is process defined?
- How does work get done, tracked, associated, etc.?
- How does process generate results?



Sales	Process
Market	Work flow
Brand	Results

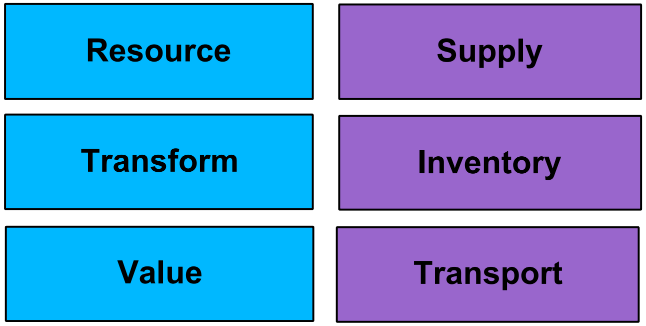
More elements to consider

Key: Resources – Transforms – Value

- What resources are required, how do we get them, etc.
- What do we do with them, using what mechanisms, etc.
- What is the resulting output, waste, utility?

Key: Supply – Inventory – Transportation

- Where does it come from, how much do we need, etc.
- How much do we store, for how long, where, etc.
- How do we fill and empty inventory, get and deliver, etc.



Resource	Supply
Transform	Inventory
Value	Transport

More elements to consider

Key: AR/AP – Collections – Write-offs

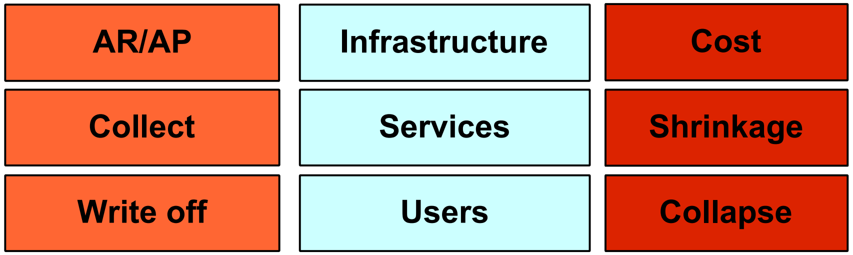
- How do we bill, get paid, get billed, pay, etc.
- What happens when they/we are late, after how long, etc.

Key: Infrastructures – Services – Users

- What do we provide to whom, via what paths, in what way, with what delivery parameters and implications?

Key: Cost – Shrinkage – Collapse

- What does it cost us, how do we lose things, how much can we lose and stay successful?



AR/AP	Infrastructure	Cost
Collect	Services	Shrinkage
Write off	Users	Collapse

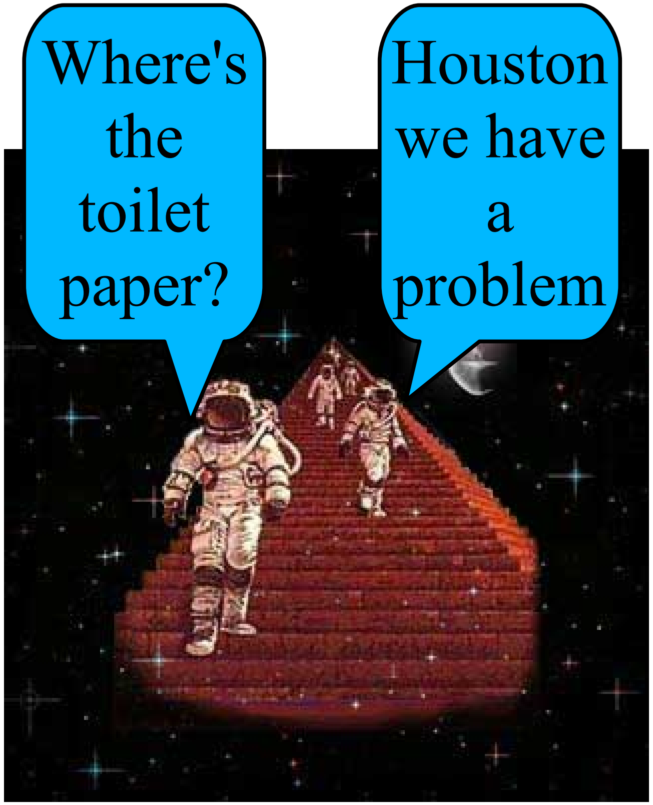
More elements to consider

Key: People

- Who do we need, where, why, when
  - In terms of capabilities and knowledge
  - Hopefully not in terms of individuals except for a startup

Key:Things

- What do we need, where, and when
  - Unique items? How so? Why so?
  - Commodity items?
  - When, how often, in what volume?



What and who not to put in?

What should not be in the business model?

- Some things do not belong
  - Lots of details do not belong
  - Trivial things do not belong
- But which things are those?
  - Executive management identifies it through COSO
  - Excessive details are eliminated by balancing the effort of data collection, entry, analysis, and presentation against the utility of the information to the process
  - Do the recursion to decide!

How deep you go depends on the business consequence

A governance issue

- Who's on the team?
  - People responsible for the consequences (business)
  - People who understand how technology supports business

How Do I Use the Model?

- The model allows systematic answers to questions about risks
  - What systems are how important and why?
  - How are threats likely to interact with systems?
  - What is important enough to protect how well?
  - What changed / changes when I do this?
  - What am I missing and how do I compensate for it?
- And when I create simulations of it...
  - What are the SPOFs and what fails?
  - What happens as this gets overloaded?
  - Which of these options will do better?

How Do I Use the Model?

Ideally, the model is an ongoing integrated view of enterprise information protection and business operations

How deep you go depends on the business consequence

- In practice
  - it is periodically revisited and elements of the model are used for analysis
  - the model is not integrated but a collection of parts pieced together
  - the model has limits on the cost of keeping it up to date
  - granularity and accuracy are limited

In practice, the model – as all models – is an approximation that helps us do our jobs better

Other business model benefits

- They provide a basis for measurement
  - So management can make meaningful decisions
  - So feedback can be identified and make sense
- To keep track of decisions and their implications
  - So changes over time can be tracked
  - So the justifications for decisions can be recorded
- To automate, systematise, and enhance analysis
  - So errors and omissions are reduced
  - So meaningful comparisons can be done

Summary of business models

Critical business functions mapped as processes

- To make shoes, I have to ...

•Processes mapped into information and IT

- To order the leather, I need Purchase Order systems, ..

•Loss of IACUA and business implications

- If I lose POs, in 3 days I will lose sales at rate of ...

•IT interdependencies analysed as a supply chain

- POs depend on Database, network infrastructure, ...
  - They depend on DNS, AD, ...
    - They depend on ...
- Content is driven by COSO or similar process

Outline

People			How does the business work?			Things
Sales	Process	Resource	Supply	AR/AP	Infrastructure	Cost
Market	Work flow	Transform	Inventory	Collect	Services	Shrinkage
Brand	Results	Value	Transport	Write off	Users	Collapse

- Background
- The Big Picture
- Business modeling
- Inventory
- Work flows
- An example
- Summary & Conclusions

Inventory	Work flows

Inventory

- You would think that inventory is an area that was long ago understood and addressed
  - You would be wrong if you thought that
  - Very few enterprises have ***useful*** inventory of
    - Hardware
    - Software
    - Content
    - Users
    - Uses and linkages
  - ***... from an information protection perspective***
- Why is this?

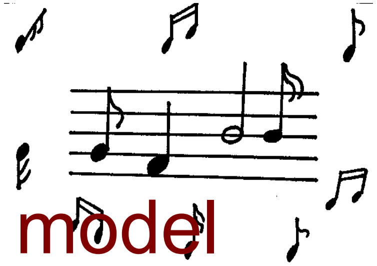
Inventory

What does inventory look like?

- From an information protection standpoint
  - There is a collection (database?) of
    - People and things
    - Properties associated with them
  - Where they are
    - Meaningful to business understanding
    - Usable in modeling, analysis, and simulation
    - Kept adequately up to date for the purpose
    - Accurate to the level required
    - Granular to the level desired
- Why do we need such an inventory?

Inventory

Inventory – what is it good for?



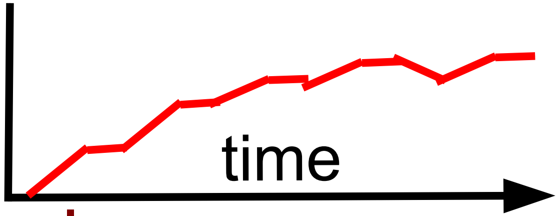
- Absolutely everything... sing it again...
  - Everything and everyone in the business model should be in the inventory
  - ... associated with oversight should be in inventory
  - ... risk management models
  - ... organizational models
  - ... control architecture should be linked to ...
  - Anything of significance that changes should be reflected in a change to the inventory
- The question I can't answer without inventory
  - Am I done yet?

How do I build one?

- Things you need to build a good inventory
  - A database of some sort with an extensible schema
  - A list of the things you want to know about
  - A list of the things you want to know about them
- How do you go about building the inventory?
  - Automated tools for collecting lots of things
  - Manual and semi-automated methods for filling in
  - A prioritized checklist driven by the business
- How do you maintain the inventory?
  - Change management should reflect everything in the inventory and business process should do it

Inventory doesn't just happen

- It takes time and resources to build up
  - Typically, you start at the highest level
    - COSO process drives business model drives inventory
  - Typically you back fill with automation
    - Scanners and automated collectors fill things in
    - Links to HR systems fill things in
    - Integration processes fill in over time



  - Data retention and disposition process helps
    - As things are disposed of you don't have to worry
    - As new acquisitions arrive, you inventory them in
    - A decreasing list of non-inventoried items remains
  - Change management links inventory and changes
- Eventually you get to stability of a sort

Outline

How does the business work?

People						Things
Sales	Process	Resource	Supply	AR/AP	Infrastructure	Cost
Market	Work flow	Transform	Inventory	Collect	Services	Shrinkage
Brand	Results	Value	Transport	Write off	Users	Collapse

- Background
- The Big Picture
- Business modeling
- Inventory
- An example
- Work flows
- Summary & Conclusions

Inventory	Work flows

Work Flows

- Solid work flows are at the heart of successful and effective protection programs over time
  - At the end of the day, anything that is going to work over time depends on a mature process
  - Mature processes ultimately end up codified in work flows for efficiency and effectiveness
- What work flows?

Work Flow

  - Periodic processes codified in time-based flows
  - Change management flows to control changes
  - Exception handling flows to manage incidents
  - Work flows to manage just-in-time protection inventory and supply chain issues

Implementation

- Typically integrate into other work flow systems
  - Incident management work flows with help desk
  - Ticketing systems augmented for security
  - Database integration with work flow engine
    - To turn generic processes into specifics
    - To allow the work flows to be independent of the details
    - Allow change management to change
      - Data associated with inventory in the database
      - Work flows associated with processes in the process engine
- Beware of risk aggregation and SOD issues
  - You have to analyze the work flow systems for risk

If it looks like a factory...

- And sounds like a factory...
  - The goal of a normalized and mature information protection program should be to run like a factory
  - The supply chain and inventory controls of a modern factory should be a good model to follow
  - Except that information protection is largely about informational things and people (the inventory)
  - But the processes should function on a regular, predictable, measurable basis
    - Inputs should be well defined and tracked
    - Outputs should be well defined and measured
    - Processes should be well understood and largely automated and measurable

Outline

People	How does the business work?					Things
Sales	Process	Resource	Supply	AR/AP	Infrastructure	Cost
Market	Work flow	Transform	Inventory	Collect	Services	Shrinkage
Brand	Results	Value	Transport	Write off	Users	Collapse

- Background
- The Big Picture
- Business modeling
- Inventory
- Work flows
- An example
- Summary & Conclusions

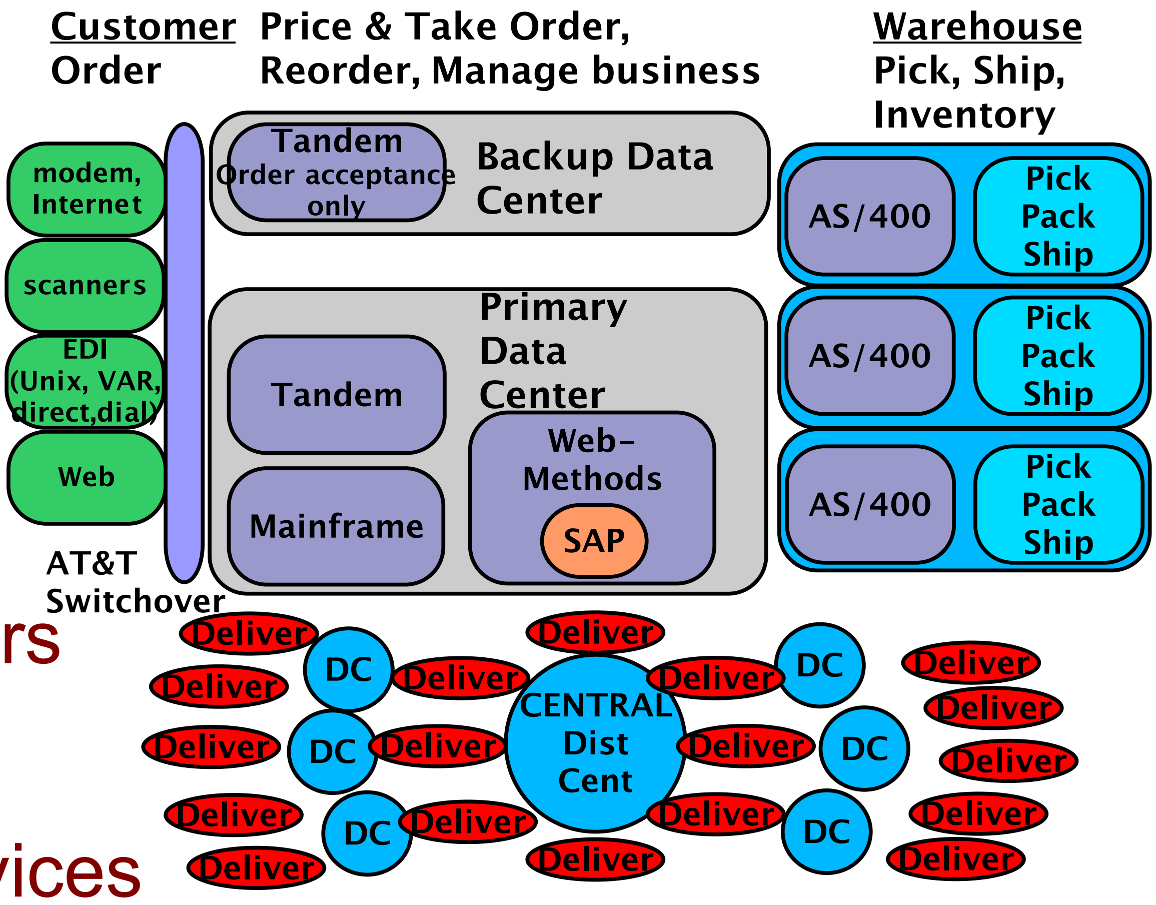
Inventory	Work flows

An example

- I do business modeling in most consulting gigs
  - I work predominantly on strategic enterprise protection architecture (and digital forensics)
  - How can I understand your situation without understanding your business? I can't!
  - It takes explanation in case after case
  - You came here to look at how we should architect
    - Sensitive data protection
    - Records retention and disposition processes
    - Enterprise security architecture
    - Cryptographic systems controls for the future
  - Why are you asking about the business?

A company in the X business

- A CEO asks to assess protection posture (IPPA)
- What business are you in and how does it work?
- Wholesale distribution: all of this must work or else...
  - Price and take orders
  - Analyze loads & lanes
  - Pick from warehouses
  - Ship to customers
  - Process returns
  - Replenish from suppliers
  - Collect money
  - Pay for goods and services

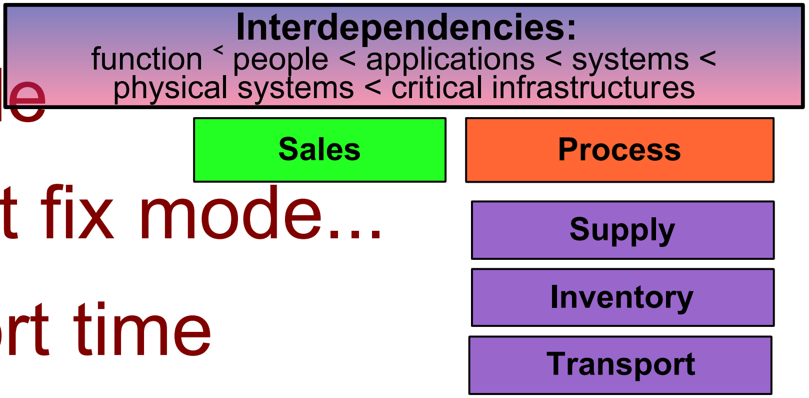


Or else what?

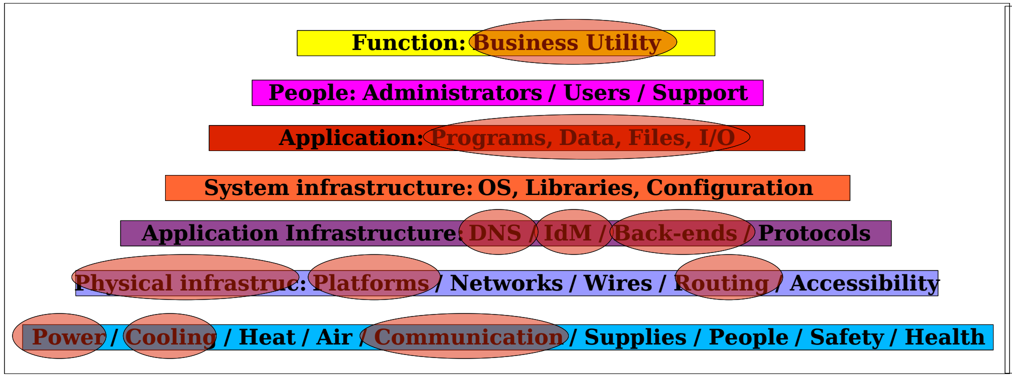
- They recently bought a competitor who had an information protection problem
  - The competitor couldn't turn orders into deliveries for several days (wholesale is a just-in-time business)
  - They started losing customers to others
  - They had partial restoration but ongoing problems
  - In a short time, they lost half of their valuation
  - They were bought for a song (a hit song - but still...)
- Lots of loss scenarios over acceptance thresholds
  - Model how the business works at the right level
  - Understand IT dependencies and failure modes
  - Get consequences from executives and analysis

Single Points of Failure

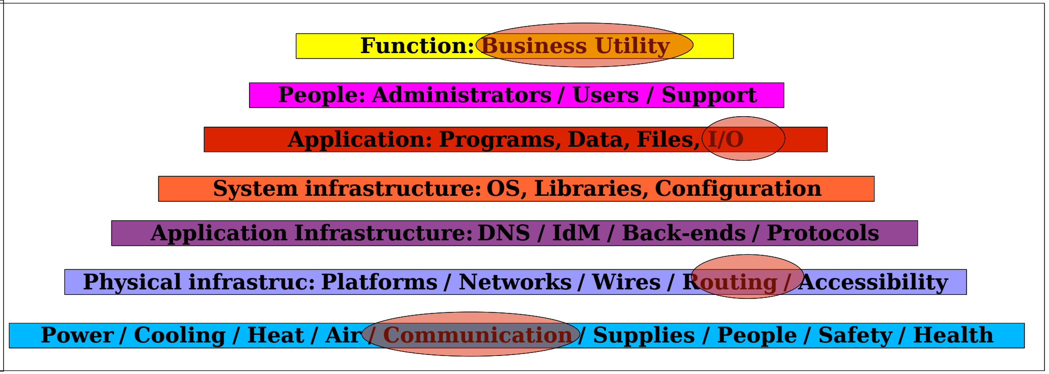
- Analysis showed that there were SPOFs
- These SPOFs could produce business collapse
- They knew of some of them and not of others!
  - They were in an urgent fix mode
  - They moved into a more urgent fix mode...
  - Accepted very high risk for short time
  - Paid millions of dollars over 3 months to mitigate



Interdependencies:
function < people < applications < systems < physical systems < critical infrastructures


Function: Business Utility
People: Administrators / Users / Support
Application: Programs, Data, Files, I/O
System infrastructure: OS, Libraries, Configuration
Application Infrastructure: DNS / IdM / Back-ends / Protocols
Physical infrastruc: Platforms / Networks / Wires / Routing / Accessibility
Power / Cooling / Heat / Air / Communication / Supplies / People / Safety / Health

The SPOFs they knew about


Function: Business Utility
People: Administrators / Users / Support
Application: Programs, Data, Files, I/O
System infrastructure: OS, Libraries, Configuration
Application Infrastructure: DNS / IdM / Back-ends / Protocols
Physical infrastruc: Platforms / Networks / Wires / Routing / Accessibility
Power / Cooling / Heat / Air / Communication / Supplies / People / Safety / Health

And the SPOFs they didn't

What's wrong with a SPOF?

- Nothing is wrong with a SPOF

Accept / Transfer / Avoid / Mitigate

  - Many businesses have them – including mine
  - Many decide that the cost of mitigation is too high
  - Many have no real choice – it's in the water...
- The problem is risk tolerance, aggregation, and SOD
  - If you don't know of a SPOF

Duty to protect

    - You are not managing risk – you're accepting without knowing it
    - You have aggregated risk beyond known levels
    - Separation of duties has failed (risk acceptance level exceeded)

What to protect

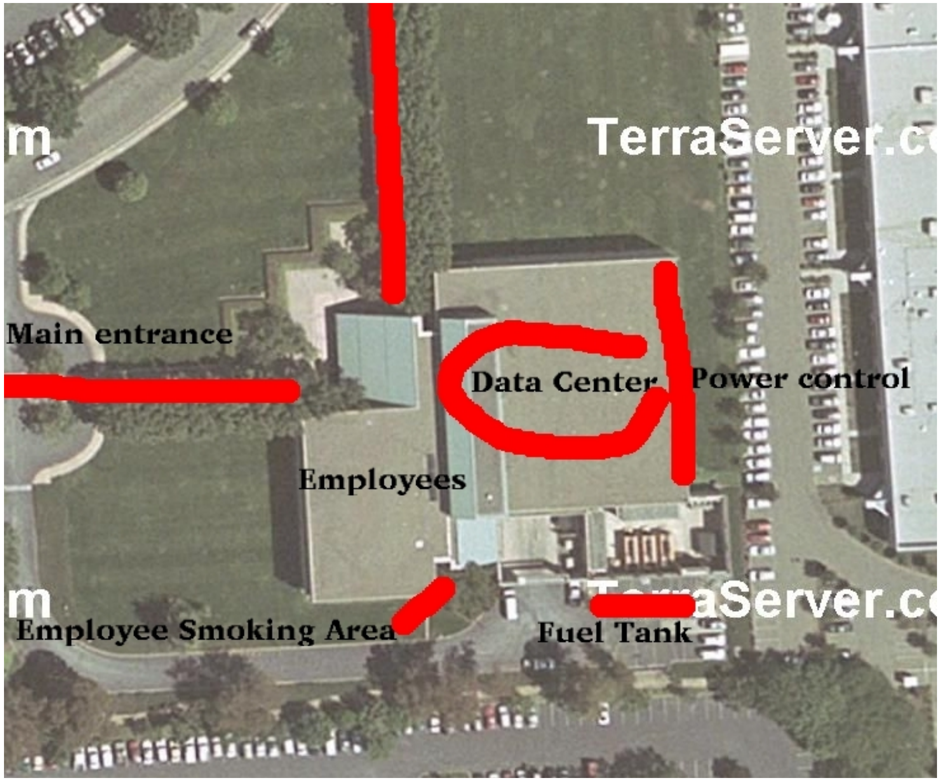
  - Who is authorized to allow a SPOF? Board/CEO!

Risk and Surety Level and Matching

  - Who can accept risks above what threshold? Policy!
  - Did it go into the COSO analysis for SOX? Liability!

They had lots of things in place

- They had some reasonably good things...
  - Some inventory and work flows
  - Policies, procedures, standards, documentation, ...
  - But no business modeling – which is why the SPOFs
- And some really bad ones
  - Fuel tanks at data center
    - Mad bomber supplies
  - EFT system problems
    - Large loss scenarios
  - Many others
    - Too numerous to list
- They didn't know!



What's the point?

- It's not that we found problems
  - We always find problems if we look for them
  - Because no human or human thing is ever perfect
- It's that the business issues drive the process
  - Technology exists to serve a (business) purpose
  - If you start with the technology you waste time/effort
  - If you start with the business you get the key issues
- To take orders we need prices (~20%/day loss)
  - Pricing is done by the mainframe
    - There is only one mainframe (SPOF)
      - The mainframe is located next to an external fuel tank
        - Disgruntled employees can reach the fuel tank and ignite ...

Another part of the example

- To refresh inventory we need... X$s/day of cash
  - Cash flow depends on payments, invoices, terms
  - Cash flow depends on money in accounts
    - Money has to be moved in and out of accounts
    - Money is moved via EFTs
      - EFTs depend on ... users ... computer in CFO area
        - Better be physically secured
        - Better have adequate protection from abuse
          - Needs ... adequate authentication
            - Depends on ...
- Somewhere down this stack we found a case of
  - Inadequate surety for separation of duties
  - One person – in the right circumstances - could empty the bank account (it's a really big balance)!

AR/AP

Collect

Write off

What's the point?

- It's not that we found problems
  - We always find problems if we look for them
- It's that the business issues drive the process
  - They might have 100,000 or more computers
    - Most or all of them have weaknesses
    - Only one does the high valued EFTs
  - If you start with the technology you waste time/effort
    - If we scanned the network we wouldn't even notice it
    - It's usually not turned on and never connected to the network
  - If you start with the business you get the key issues
- They didn't have an inventory that told us about it
- The workflows were strictly manual

Consequences
- value
- costs

Outline

People			How does the business work?			Things
Sales	Process	Resource	Supply	AR/AP	Infrastructure	Cost
Market	Work flow	Transform	Inventory	Collect	Services	Shrinkage
Brand	Results	Value	Transport	Write off	Users	Collapse

- Background
- The Big Picture
- Business modeling
- Inventory
- Work flows
- An example
- Summary & Conclusions

Inventory	Work flows

Are we measuring security?

- **You cannot** directly **measure security** anyway
  - How can you measure what didn't happen?
    - We didn't collapse today – attackers were out there trying
    - The security program saved the entire information value of the enterprise today – and every day... till we collapse
  - No real repeatable experiments can be done
    - No retries - after action reports (feedback) - red teaming - historical data of limited value and hard to get
- **You can measure the protection program**
  - The theory is:
    - With an effective system in place, and
    - Feedback for improvement with time,
    - Risks will be reasonably well controlled

Conclusions

We need business models

- To make sensible protection decisions
  - Formalise the models to gain understanding of business consequences of information technology failures
- Run the model against posited threats and failures
  - For review, design, and verification
  - Verify and improve the model against actual events
- Use the model to make risk management decisions
  - Spend the time and effort to get it right
  - Verify it with empirical data when available
- Integrate with other models for even better results
  - Threat models, other business models, etc.
- Integrate with inventory and work flows
  - To supply data and analyse failures

More Conclusions

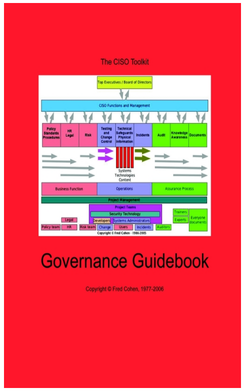
- We need inventory (systems)
  - To track what we do and why
  - So we can tell when we are done
  - (Efficiently and effectively at high volumes / time)
- We need work flow (systems)
  - To support repeatable protection processes
  - That can be measured and improved over time
  - (Efficiently and effectively at high volumes / time)
- And we don't have most of these today
  - Which is why it is hard to get to reasonably mature and measurable protection programs.

Caveats

- Watch out for risk aggregation and SOD
  - In business models, inventories, and work flows
- Technology support is not there today
  - Marginal for work flows (few libraries for infosec)
  - Inventory is somewhat business dependent
  - Business models are highly business dependent
- Some risk management systems are starting
  - They model the business at some level
  - The link resources to business issues
  - They allow limited automated analysis
  - But it's inherently complex and has a long way to go

Resources

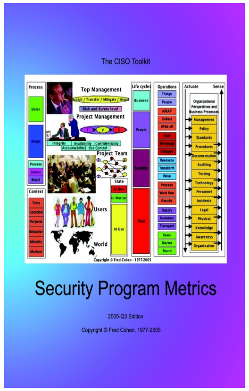
- On http://all.net/
- “Security Architecture”
- The CISO ToolKit
  - Governance Guidebook
  - Security Metrics
  - Security Governance Checklists
- Software to automate process
  - Management Analytics
- Risk Management
- Library ...



The CISO Toolkit

Governance Guidebook

Copyright © Fred Cohen, 1977-2006



The CISO Toolkit

Security Program Metrics

2005-Q3 Edition

Copyright © Fred Cohen, 1977-2005

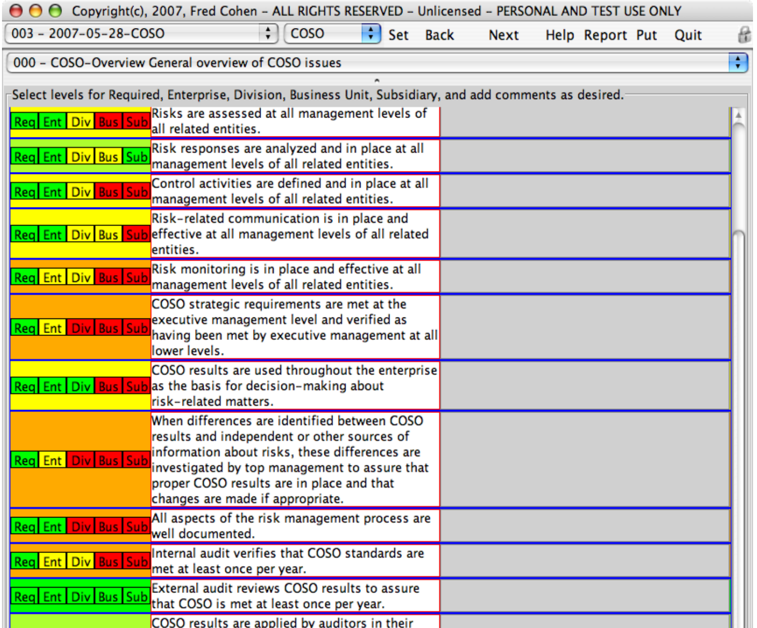
Security Checklists

Hitting your security targets

Security Governance:
Business Operations,
Security Governance,
Risk Management
and
Enterprise Security Architecture

by Dr. Fred Cohen

Copyright © Fred Cohen, 2005



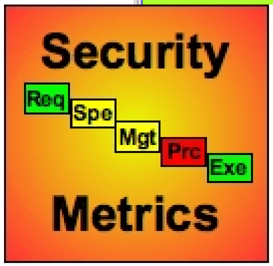
Copyright(c), 2007, Fred Cohen – ALL RIGHTS RESERVED – Unlicensed – PERSONAL AND TEST USE ONLY

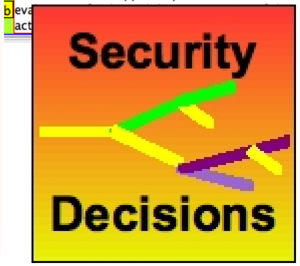
003 – 2007–05–28–COSO | COSO

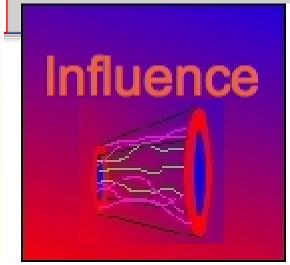
000 – COSO–Overview General overview of COSO issues

Select levels for Required, Enterprise, Division, Business Unit, Subsidiary, and add comments as desired.

Req Ent Div Bus Sub	Risks are assessed at all management levels of all related entities.
Req Ent Div Bus Sub	Risk responses are analyzed and in place at all management levels of all related entities.
Req Ent Div Bus Sub	Control activities are defined and in place at all management levels of all related entities.
Req Ent Div Bus Sub	Risk–related communication is in place and effective at all management levels of all related entities.
Req Ent Div Bus Sub	Risk monitoring is in place and effective at all management levels of all related entities.
Req Ent Div Bus Sub	COSO strategic requirements are met at the executive management level and verified as having been met by executive management at all lower levels.
Req Ent Div Bus Sub	COSO results are used throughout the enterprise as the basis for decision–making about risk–related matters.
Req Ent Div Bus Sub	When differences are identified between COSO results and independent or other sources of information about risks, these differences are investigated by top management to assure that proper COSO results are in place and that changes are made if appropriate.
Req Ent Div Bus Sub	All aspects of the risk management process are well documented.
Req Ent Div Bus Sub	Internal audit verifies that COSO standards are met at least once per year.
Req Ent Div Bus Sub	External audit reviews COSO results to assure that COSO is met at least once per year.
b	COSO results are applied by auditors in their eva act







Thank You

Questions?

Discussion?!

Dr.Cohen at Mac.Com

http://all.net/