Business Modeling for Risk Management

Fred Cohen

Consulting Principal Analyst

Thursday June 15, 2006

Business Modeling for Risk Management

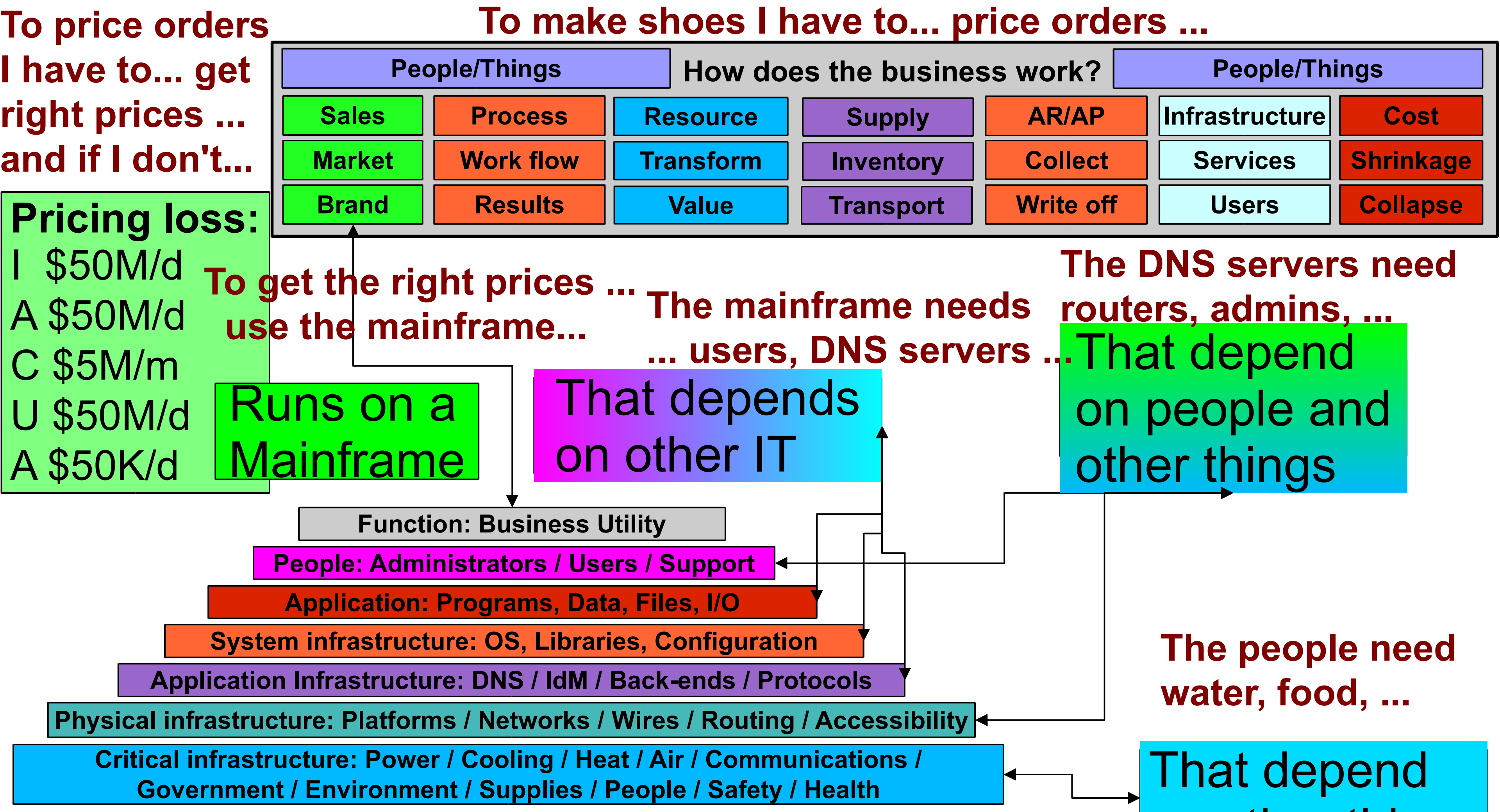
Thesis

- Risk management demands understanding of business consequences of information technology failures
  - Loss of integrity, availability, confidentiality, use control, accountability
- 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

Business Modeling for Risk Management

What might part of a model look like?

Monster shoe company as an example



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

- 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

The people need water, food, ...

That depend on other things

Source "The CISO ToolKit – Governance Guidebook" - ASP Press

Agenda

- Why do we need a business model?
- What does a business model look like?
- How do I use it?
- Technology support for business modeling
- Recommendations

Agenda

- *Why do we need a business model?*
- What does a business model look like?
- How do I use it?
- Technology support for business modeling
- Recommendations

Why do we Need a Business Model?

Four good reasons

- To associate risk with the business
  - Mapping business consequences to technology risks
- To provide a basis for measurement
  - So management can make meaningful decisions
- To keep track of decisions and their implications
  - So changes over time can be tracked
- To automate, systematize, and enhance analysis
  - So errors and omissions are reduced

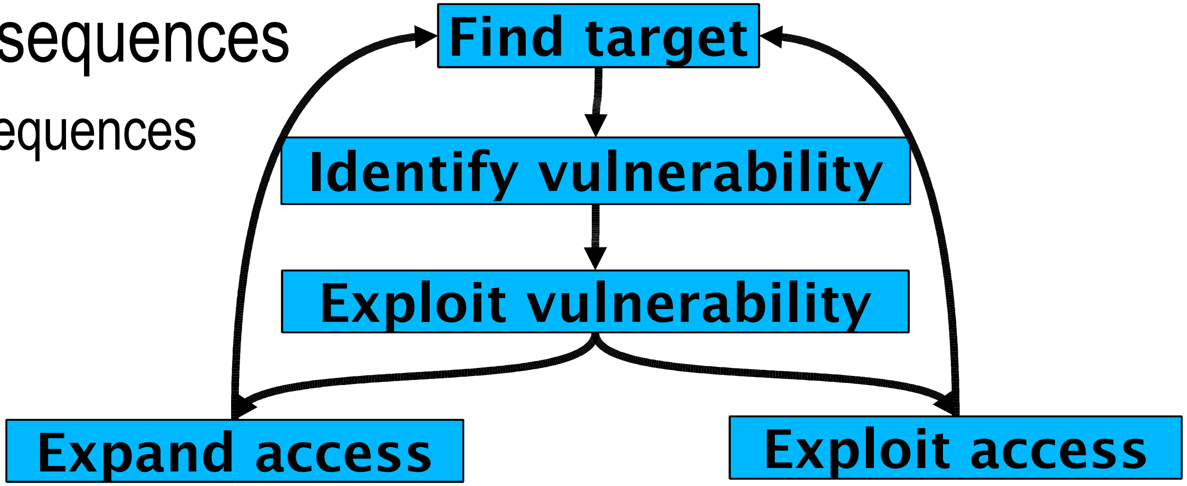
BCP / DRP / COSO / Risk Management all have models

- These models have things in common
- Perhaps the efforts should be unified?

Why do we Need a Business Model?

To associate risk with the business

- Need to associate consequences to protection failures in order to be able to assess risks of those failures
- Not just individual technology failures – combinations and sequences induced by threats (people, groups, & nature)
- A model against which we can run threats
  - For more details, see the previous talk on threat modeling
- But not for IT consequences
  - For business consequences



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

Why do we Need a Business Model?

To provide a basis for measurement

- We need to measure technical consequences against some business standard
  - If a server fails in the data center and nobody notices the crash, has it had a business impact?
- A matter of definition
  - Is a business impact the rippling effect on other processes, lost revenues, increased competition, and the eventual side effects when a second server crashes?
  - Is the business impact the instantaneous unavailability of a service that serves many people?
- It's a management decision as to which definition
  - But without understanding business consequences, how can they decide?

Why do we Need a Business Model?

To keep track of decisions and their implications

- Models aren't static representations
  - They must change as the business changes to stay accurate
  - They are typically used to “run scenarios” against
- Models include the data added to them on decisions
  - They may track the decisions and reasons for those decisions
  - They may track the changes back to the decisions to identify the need for updated decisions with updated business situations
- Models, at a minimum, allow manual revaluation
  - With changes in the business or technology, those making the changes and controlling the decisions can revisit the model to update decisions
  - Models are more necessary as complexity rises to the level where individuals cannot remember everything ever done

Why do we Need a Business Model?

To automate, systematize, or enhance analysis

- Even relatively simple models allow automation to replace manual analysis and reduces omissions
  - A spreadsheet that tracks and totals things dramatically reduces time to make better decisions and models the implications
  - A database that provides a list of things to check dramatically reduces the number of omissions typically made
  - A checklist that is used offers the hope of not missing things that are known to be at issue
  - The elements of the model themselves provide the basis for a systematic method for checking things
  - The business model helps to prioritize activities

Agenda

- Why do we need a business model?
- *What does a business model look like?*
- How do I use it?
- Technology support for business modeling
- Recommendations

What Does a Business Model Look Like?

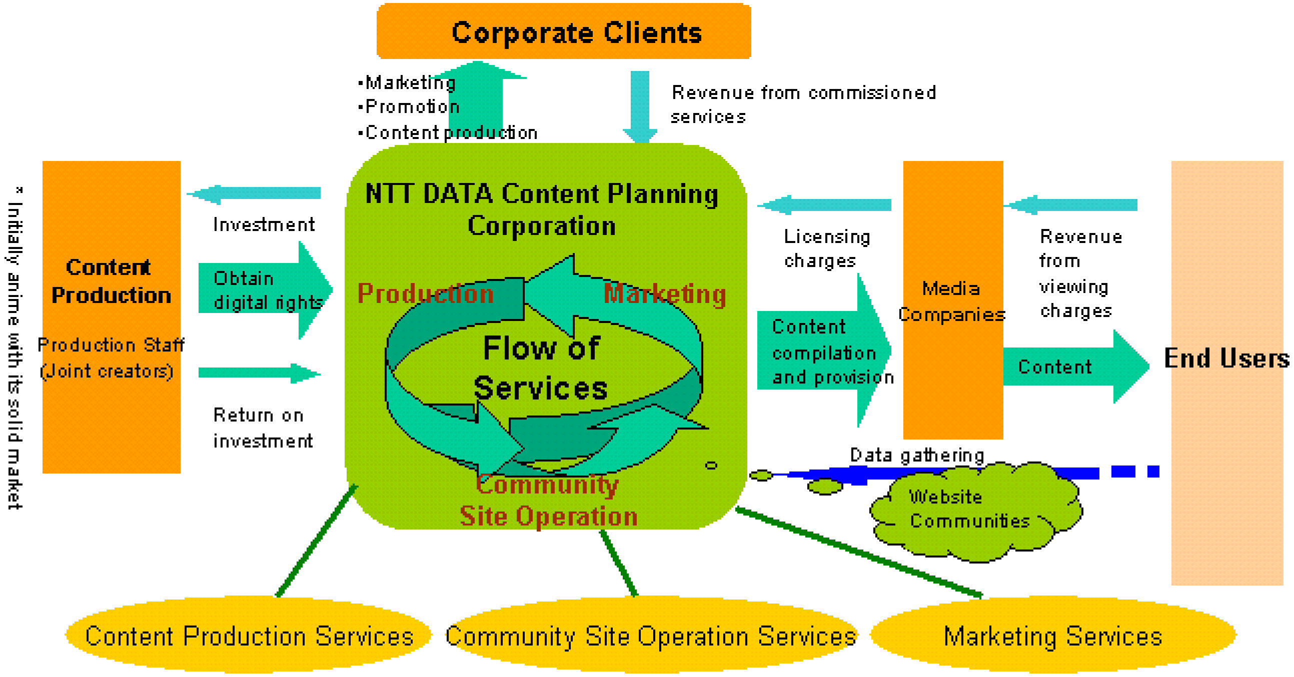
Sort of like this... but not really...

- This is not a great business model for our purposes
  - But it looks nice...

Business Model and Operations Overview

■Analyze data obtained from Web communities and assigning numerical ratings of content value (establishing rating indices).

■Through closely coordinated efforts in the three areas of services below, raise the accuracy of content appraisal, conduct precisely targeted marketing, produce quality content, and obtain digital rights.



Corporate Clients

・Marketing
・Promotion
・Content production

Revenue from commissioned services

* Initially anime with its solid market

Content Production

Production Staff (Joint creators)

Investment

Obtain digital rights

Return on investment

NTT DATA Content Planning Corporation

Production

Marketing

Flow of Services

Community Site Operation

Licensing charges

Content compilation and provision

Media Companies

Revenue from viewing charges

Content

End Users

Data gathering

Website Communities

Content Production Services

Community Site Operation Services

Marketing Services

Obtain digital rights/Reflect indices
*Joint production and purchase
*Business rollout planning
*Digital rights handling
(including legal and accounting)

Gather data
*Planning, building, and operation of community Websites

Analyze data/Establish indices
*Data mining analysis
*Establishment of indices for content appraisal

Source: NTT DATA Content Planning Corporation

What Does a Business Model Look Like?

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

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

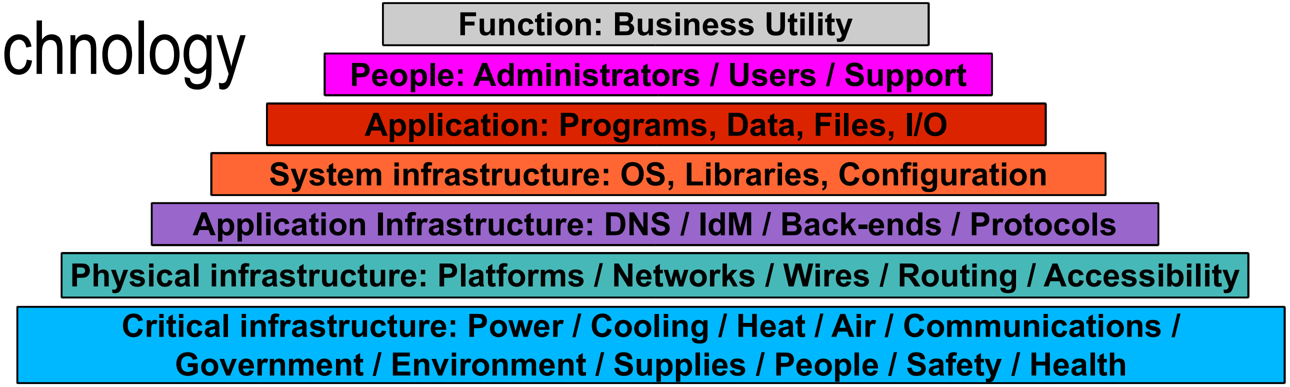
What Does a Business Model Look Like?

It models how the business functions at a gross level

- How does the business function?
  - e.g., 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...

It models dependencies on IT

- Starting with the business utility, there are a series of dependencies associated with information and information technology



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 a Business Model Look Like?

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, etc.

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

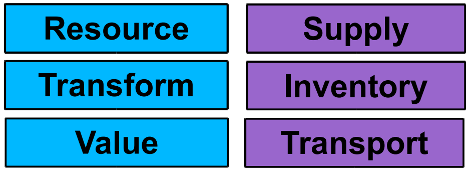
What Does a Business Model Look Like?

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

What Does a Business Model Look Like?

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

What Does a Business Model Look Like?

What should not be in the business model?

- Some things do not belong
  - Lots of details do not belong
  - Trivial things do not belong

How deep you go depends on the business consequence

- But which things are those?
  - Executive management identifies what is important through COSO
    - See the COSO and Risk Management tutorial (time travel tours: booth T)
    - See references...
  - Excessive details are eliminated by balancing the effort of data collection, entry, analysis, and presentation against the utility of the information to the process

A governance issue

- Who's on the team?

What Does a Business Model Look Like?

Summarizing

- Critical business functions mapped as processes
  - To make shoes, I have to ...
- Processes mapped into information technology
  - To order the leather, I need the Purchase Order system and ...
- Loss of IACUA associated with monetary implications
  - If I lose availability of POs after 3 days I will lose sales at rate of ...
- IT interdependencies analyzed to weigh criticality of IT and supporting infrastructure as a “supply chain”
  - POs depend on Database, network infrastructure, PCs of users
  - They depend on DNS, AD, ...
  - They depend on ...
- Content is driven by COSO or similar process

Agenda

- Why do we need a business model?
- What does a business model look like?
- *How do I use it?*
- Technology support for business modeling
- Recommendations

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?

How Do I Use the Model?

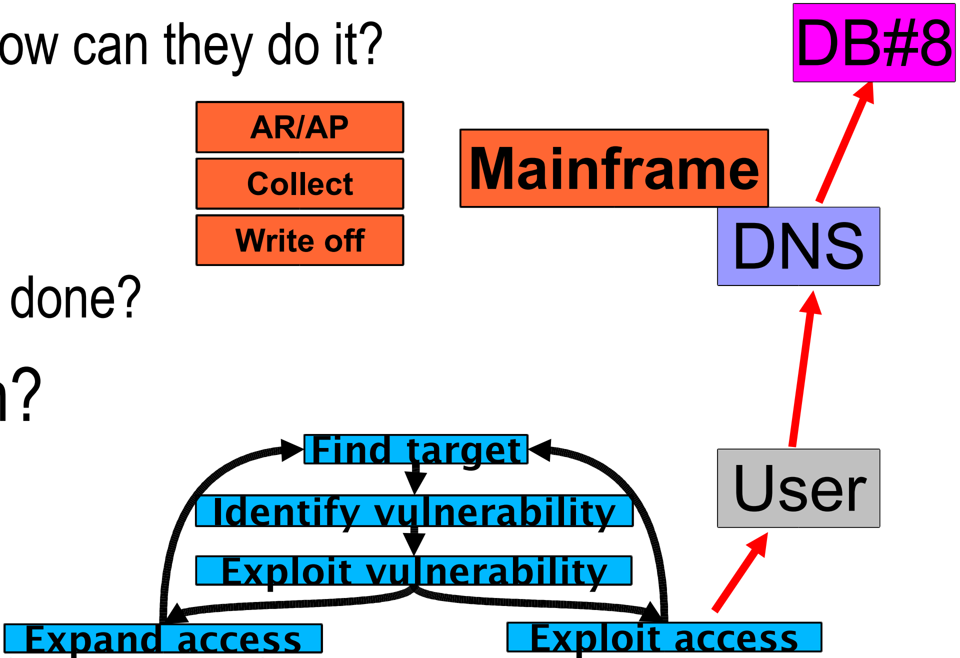
What systems are how important and why?

- Identification of systems involved in business processes
  - A business person can understand what systems are required in order to make a function work and why the systems are needed
  - A business person can understand what happens how soon if something fails and how important response or recovery at a pace is
- Identification of systems/people/things they depend on
  - Analysts can follow the interdependency chain to understand what depends on what
  - Business people can follow the analysis meaningfully and decide how indirect an implication is
- Identification of criticality of IACUA
  - The business need is directly related to the IACUA of specific systems and business decisions can be made about what is how important

How Do I Use the Model?

How are threats likely to interact with systems?

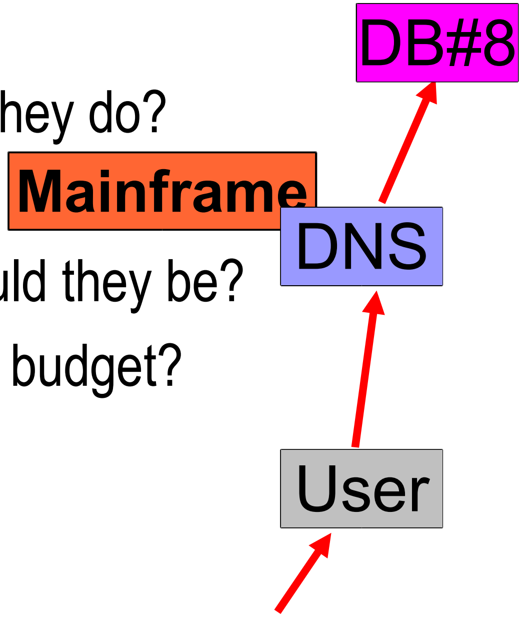
- Given the threat models, which of the systems are what threats likely to be able to take advantage of and when?
  - If a threat wants to do X, how can they do it?
  - How long will it take?
  - How long will it last?
  - How much damage will be done?
- Do I need risk reduction?
- What are my options?
  - Is prevention adequate?
  - Is detection and response fast enough?
  - What event sequences with potentially serious negative consequences should I cover?



How Do I Use the Model?

What is important enough to protect how well?

- The model leads business people to make business decisions based on identified IT issues
  - How can things go wrong and how bad is it when they do?
  - Where should I use redundancy?
  - Where should I have controls and how strong should they be?
  - How should I prioritize controls based on available budget?
- When have I gone too far?
  - How much redundancy am I willing to pay for?
  - How far should I go before credibility drops below my believability point?
  - Can I detect in time to not have to spend all the money on prevention?
  - What should I only protect minimally and what should I work hard on?



DB#8

Mainframe

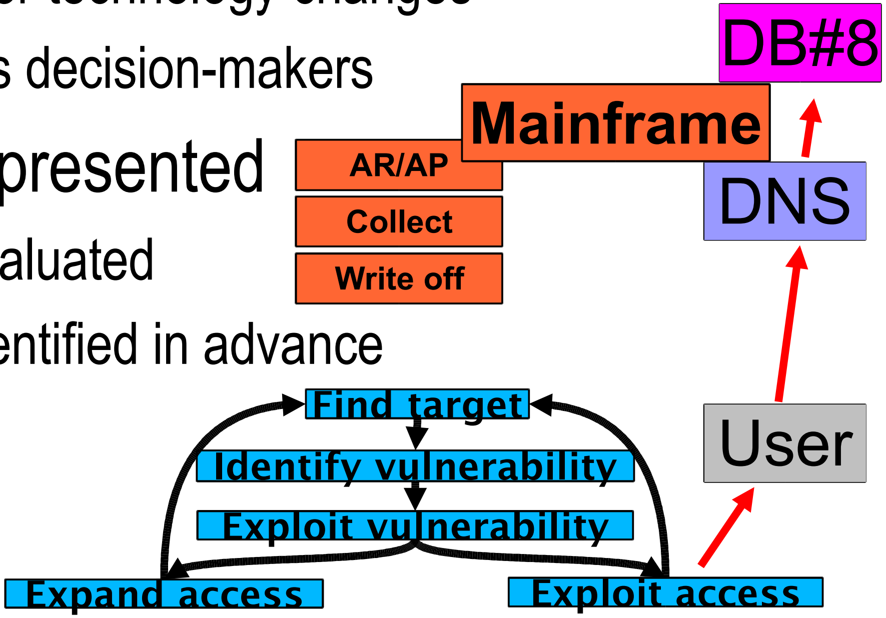
DNS

User

How Do I Use the Model?

What changed / changes when I do this?

- Changes over time can be tracked
- The implications of change can be identified
  - Business implications of security changes
  - Security implications of business changes
  - Implications of threat changes
  - Implications of infrastructure or technology changes
  - In financial terms for business decision-makers
- What-if scenarios can be presented
  - Proposed changes can be evaluated
  - Mitigation changes can be identified in advance



How Do I Use the Model?

What am I missing and how do I compensate for it?

- So errors and omissions are reduced
  - People forget things or fail to fully address known collections
  - People have problems tracking their analysis processes
  - A systematic approach per a model provides a check on process
- So analysis can be performed meaningfully
  - Without a model, what do we measure against?
  - With a model, we can measure against the model
  - Limited by the model's fidelity and accuracy
  - Costs are associated with keeping models up to date
- But without a model I am worse off

How Do I Use the Model?

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

- 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

How deep you go depends on the business consequence

Agenda

- Why do we need a business model?
- What does a business model look like?
- How do I use it?
- *Technology support for business modeling*
- Recommendations

Technology Support for Business Modeling?

Support is fragmented at best

- SOX compliance has driven accounting firms to build better – still minimal tools for documenting process
- Some process documentation tools
  - IBM, OpenPages, etc.
- Elements of tools are borrowed from elsewhere and applied to meet specific needs
- Uniqueness of each business plays a vital role in the difficulty of making good modeling software
- Technology support is and will remain fragmented for now
- But there are some tools that can help out

Technology Support for Business Modeling?

SOX compliance has driven accounting firms to build better – still minimal tools for documenting process

- A simple process diagramming approach is a good example:
  - Identify participants in a process
  - Document the protocol used to get the job done
  - Use it for analysis of controls

Who	T1	T2	T3	T4
Admin			Notified	
IT staff			Implemented	
Manager		Approve		
CFO			Notified	
User	Make request			Available

Technology Support for Business Modeling?

Elements of tools are borrowed from elsewhere and applied to meet specific needs

- Database example
  - A database that tracks business assets including IT inventory
  - Used as a tool to store access control information
  - IT builds tools to extract information from systems for database
  - Database compared to previous state for changes and reconciled
- Spreadsheet example
  - Spreadsheet of all major enterprise applications
  - Column for each indicating criticality
  - Added columns for loss from IACUA
  - Spreadsheets for each application with dependencies listed
- Graphics program example
  - Used to depict network structure and interdependencies

Technology Support for Business Modeling?

Uniqueness of each business plays a vital role in the difficulty of making good modeling software

- For any given business, creating a custom collection to manage and manipulate this data is not extremely hard
  - But it is a substantial effort
- Creating a generic software package to handle arbitrary business modeling and simulation is really building a language
  - But who do you sell this specialized language to and for how much?
- There are modeling and simulation languages available but that are hard to use for the range of tasks involved
  - Simula is inexpensive – programming it will take a while

Technology Support for Business Modeling?

Technology support is and will remain fragmented for now

- Until a strong business case can be made for the large investment of building the tool, only zealots will create such tools
- They will likely create them for themselves first
- Rather, tools used for other purposes will be applied
  - Spreadsheets, databases, graphic programs
  - Graph theory-based analysis tools
  - Network intelligence tools for the technical side of it
  - Existing modeling and simulation environments

Sorry – there is no saving technology available to unify this today

Technology Support for Business Modeling?

But there are some tools that can help out

- Your favorite spreadsheet, SQL database, graphical presentation language or GUI
- Business Continuity Planning (BCP) tools
  - Sungard has a decent one - So do others
  - But they are all limited and only facilitate certain aspects of risk management and tracking
- Consulting services offer it
  - IBM/PWC, others have put out offerings
  - None have taken hold – ahead of their time?
- Existing tools for limited interdependencies

You've already done parts of it for BCP/DRP/COSO

Agenda

- Why do we need a business model?
- What does a business model look like?
- How do I use it?
- Technology support for business modeling
- *Recommendations*

Recommendations

Like it or not – you have to model the business for security

- Will the model be informal in the heads of key workers?
- Will it be the result of a COSO/BCP/DRP/other process?
- Will it be haphazard or a single unified enterprise effort?

Burton Group recommends a unified effort

- Build on what you have
- Take care to separate regulatory from others

A documented, formalized part of official business processes

- Top management involvement via the COSO process
- COSO data collection should feed the model
- Additional efforts to create sensible looking depictions that can be used for description and clarity

Recommendations

The model should

- Clarify the rationale for business risk management decisions
- Readily differentiate the import of systems
- Allow decisions about when to stop spending money
- Allow threats and their capabilities and intents to be understood in terms of business effects
- Allow decisions between prevention and response to be made on a rational basis
- Provide supporting documentation for the reasonableness of decisions

Business Modeling for Risk Management

Conclusion

- We can and must build models to make sensible decisions
    - Formalize the process to gain understanding of business consequences of information technology failures
    - Loss of integrity, availability, confidentiality, use control, accountability
- Run the model against posited failures
    - For review
    - For design
    - For verification
- Use the model to make risk management decisions
    - Spend the time and effort to get it right
    - Verify it with empirical data when available

Business Modeling for Risk Management

References

- Burton Group Security and Risk Management Strategies
  - Risk Aggregation: The Unintended Consequence
  - Pulling up your SOX: IT Impacts and Compliance
  - IT Risk Management and COSO
  - Business Continuity Planning for IT
- Burton Group Application Platform Strategies
  - Business Process Modeling: Adding Value or Overhead?
- Other Sources
  - The CISO ToolKit – Governance Guidebook, ASP Press