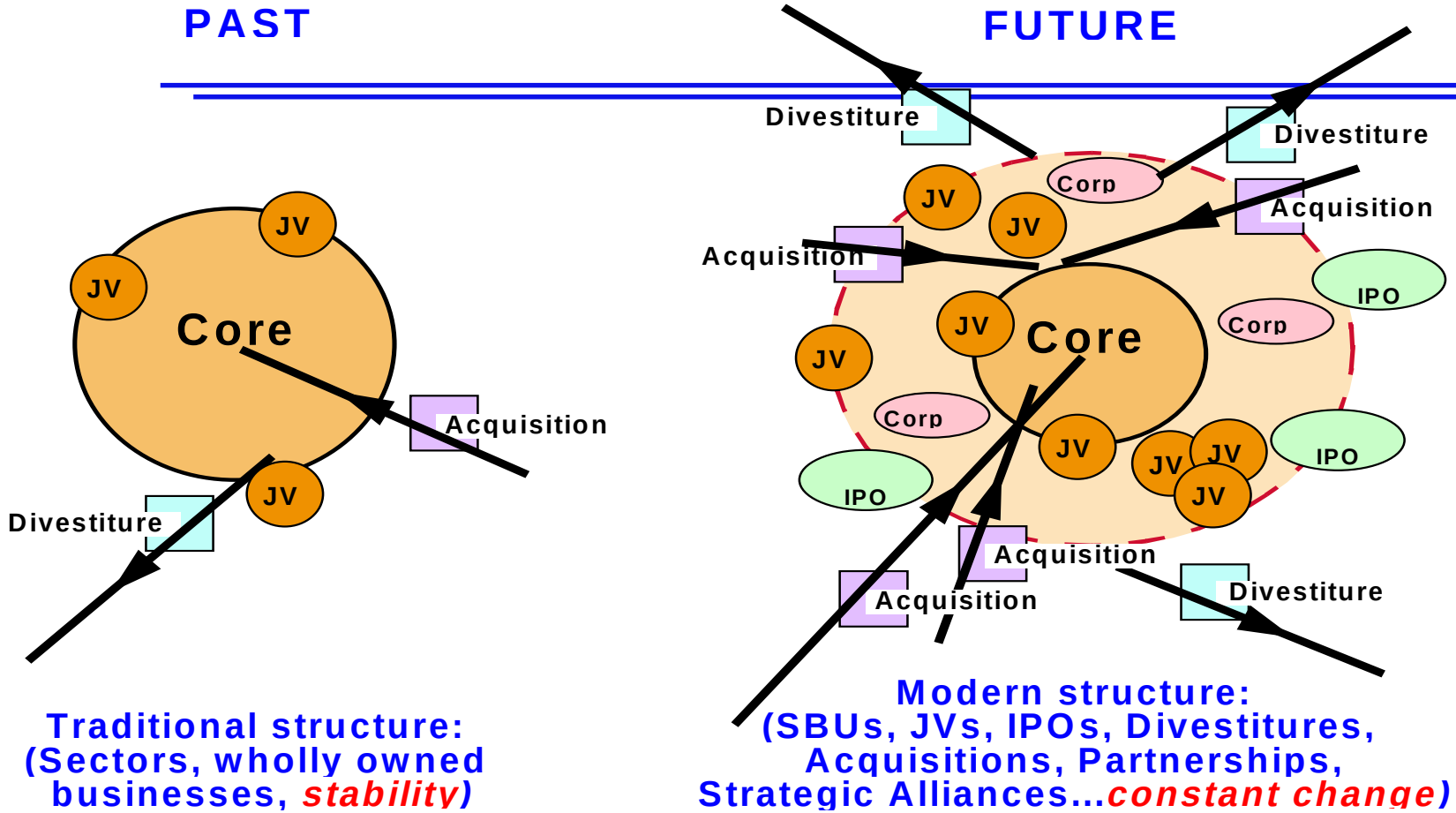
Building Effective, Tailored Information Security Policy

John Pescatore

Trusted Information Systems

301-947-7153 johnp@tis.com

Changing Business Model



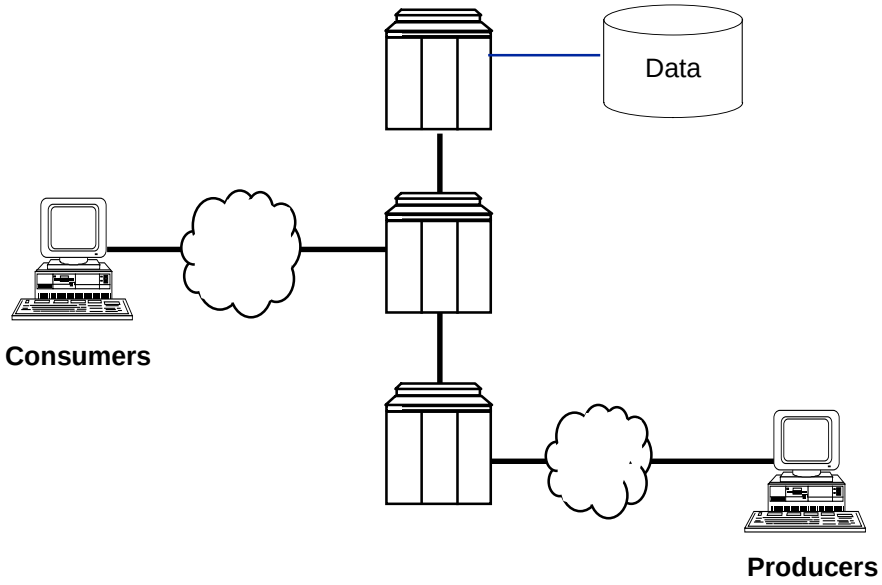
Traditional structure:
(Sectors, wholly owned businesses, *stability*)

Modern structure:
(SBUs, JVs, IPOs, Divestitures, Acquisitions, Partnerships, Strategic Alliances...*constant change*)

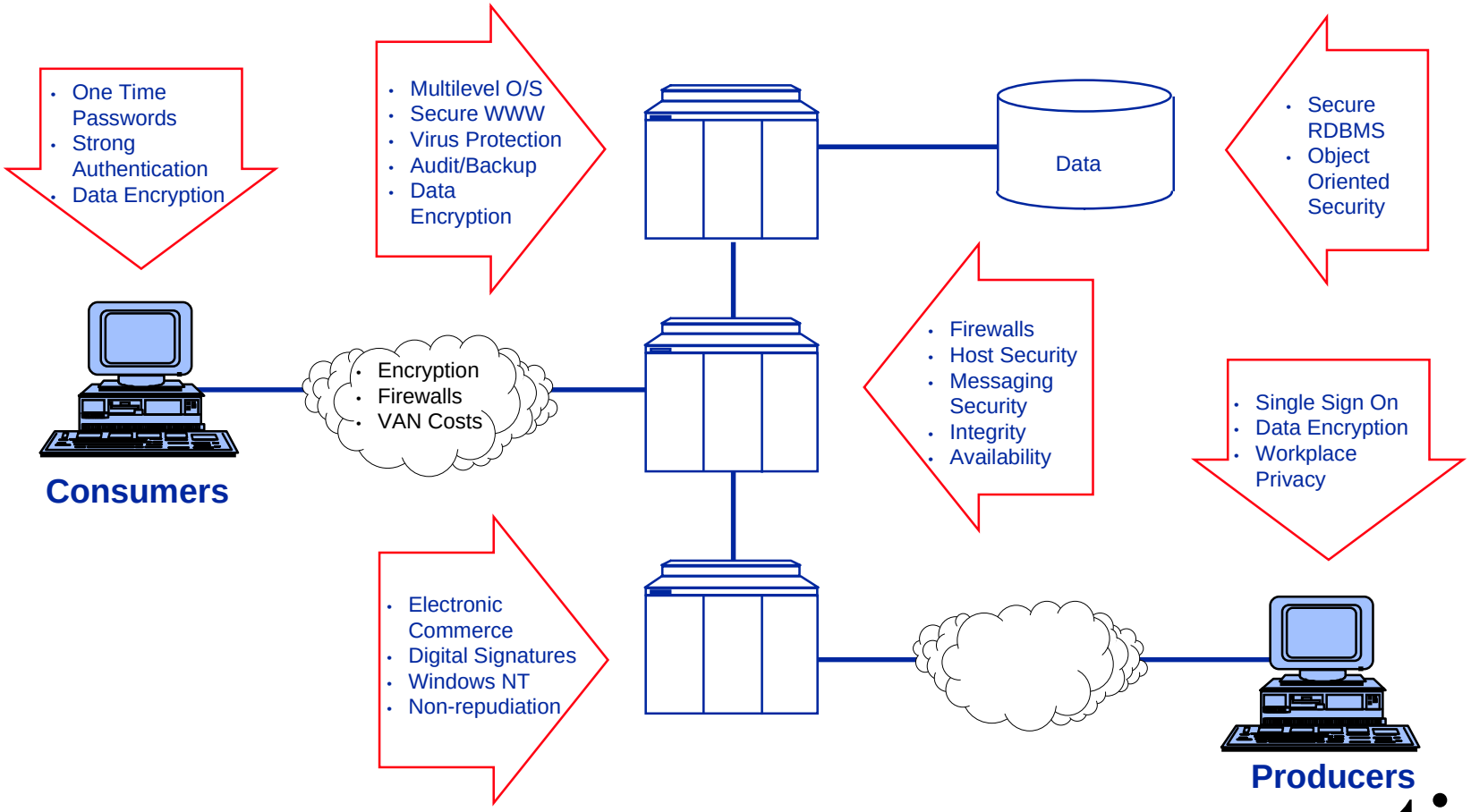
Need for flexibility will increase

Electronic Business Relationships

- **To be successful businesses need the ability to create rapid setup/teardown electronic business relationships with customers, suppliers, and partners. Security will need to be distributed throughout the computing enterprise**



Enterprise-wide Security



Infrastructure Impacts

- **Changing business model leads to:**
  - Growth by acquisition
  - Strategic alliances
  - Constant change
- **Infrastructure needs to support:**
  - Virtual Offices
  - Virtual Enterprises
  - Virtual Workgroups
- **Security enables business to use the Internet to keep up with pace of change**
  - Encryption
  - Authentication
  - Access Control

Growth by Acquisition

- **Security Impacts:**
  - Security Policy inconsistencies
  - Interoperability of Security Controls
  - Level of security sinks to lowest common denominator
- **Policy Demands:**
  - Frequent, often unplanned, updates needed
  - Must address multiple cultures
  - Drive to select best-of-breed approach

Strategic Alliances

- **Security Impacts:**
  - Team today, compete tomorrow
  - Need for international secure connectivity
  - Varying levels of trust
- **Policy Impacts:**
  - Focus on business-critical data
  - Need to address export issues
  - “One size fits all” no longer works

tis

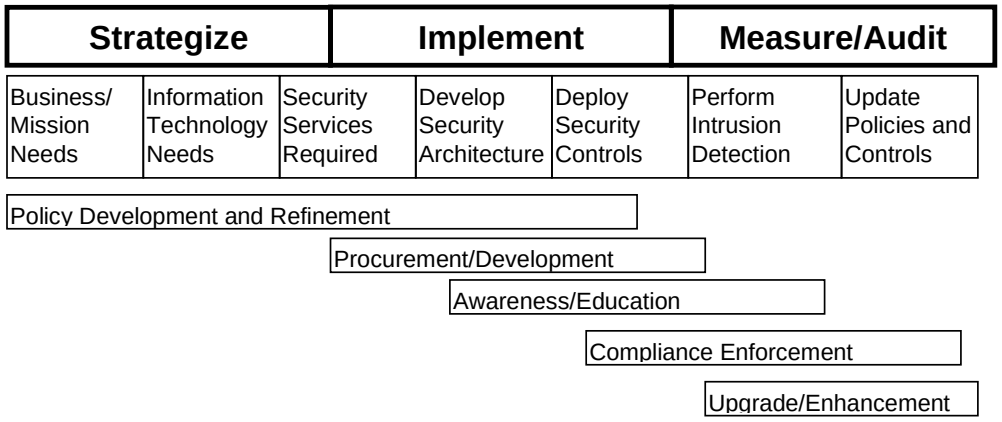
Constant Change

- **Security Impacts:**
  - Vulnerabilities follow transitions
  - Breakdown of informal policies
  - High administrative load for access control
- **Policy Impacts:**
  - Need for intrusion detection, updates, audits
  - Need to accessible formal policy
  - Policy needs to drive affordable solutions

tis

Integrated Security Planning

- **Treat security like an investment**
  - **Strategic planning**
  - **Business-driven**
  - **ROI or Cost/Benefit Analysis**
- **Legal and regulatory issues**



Tailored Security Policy

- Goal is to influence behavior
- Need to enable, not just to deny
  - Users can route around controls all too easily
  - Become cost of sales, not just overhead
- Focus on the business needs
  - What data will be handled?
  - How can that data be accessed?
  - What is your organization's paranoia level?
  - What controls are required on that data?

Data Categorization

- Define broad classes of information created, stored and/or delivered by your business
- Logical groupings based on impact to business
  - Customer data - financial records, medical records, orders
  - Business data - financial, competitive, intellectual property
  - Employee data - salary, benefits, home phone

tis

Data Categorization

- **Assign sensitivity levels, eg:**
  - **Unrestricted**
  - **Restricted**
  - **Controlled Distribution**

Unrestricted	Restricted	Controlled Distribution
Meeting notes	Memos for the record	Salary data, personnel files
Internal telephone directory	Organizational directories with home addresses and/or phone numbers	Customer databases, privacy or medical-related information
Corporate publicity	Financial reports	Data on mergers or potential acquisitions
User IDs		Passwords, encryption keys
Most internal policies and procedures	Incident response plans	Results of risk assessments
Functional information about a major application	Source code for a major application	Information that is the major product of a major application: loan approvals, flight plan data, public safety information, calculations, etc.

Data Access

- How could an attacker get to your data?
  - How is it created?
  - Where is it stored?
  - How is it transmitted?
- Typical client/server/Internet scenario
  - Created on a Windows 95 PC
  - Stored locally, on a file server, on an internal Web server, in a database, external Web server
  - Sent over LANs, WANs, over Internet via http, ftp and email

tis

Data Access

- Identify Data Owners and Data Maintainers
- Identify business needs to provide access to the data
  - Internal employees
  - External employees
  - Business partners
  - Customers
  - Other third parties
- Identify exposure points and threats

Paranoia Level

- Getting to “good enough security”
- Security policy needs to match the risk acceptance profile of an organization
  - What are the realistic threats?
  - How visible is your organization?
  - What are the consequences of an incident?
  - How sensitive is your organization to the intangible costs of an incident?
- Regulatory and legal issues

Risk Profiling Matrix

Risk Profiling Matrix				
Threats:	Rating	Visibility	Rating	Sco
None identified as active; exposure is limited	1	Very low profile, no active publicity	1	
Unknown state or multiple exposures	3	Middle of the pack, periodic publicity	3	
Active threats, multiple exposures	5	Lightning rod, active publicity	5	
Consequences	Rating	Sensitivity	Rating	Sco
No cost impact; well within planned budget; risk transferred	1	Accepted as cost of doing business; no organization issues	1	
Internal functions impacted; budget overrun; opportunity costs	3	Unacceptable Business Unit management impact; good will costs	3	
External functions impacted; direct revenue hit	5	Unacceptable Corporate Management impact; business relationships affected	5	
	Total Score:			

Security Controls

- Match the required controls to the organizational value of the data, the risk tolerance of the organization, and the investment required to meet the policy
  - Sounds easy, huh?
- Security policy can have wide ranging impact
  - Business-wide review
  - End result will be a compromise between security goals and business realities

Security Controls

	Information Category		
Protection Required	**Restricted**	**Unrestricted**	**Controlled Distribution**
Identification	Identify as Organization Property	Identify as Organization Property, with category shown on initial page of record	Identify as Organization Property, with category shown on each page of record
Disclosure Restrictions	None inside the Organization	Based on need to know	Only when approved by the information owner
Access Controls	Access limited to within the organization	Access limited to those authorized by the information owner	Access limited to those authorized by the information owner. All access must be logged
Transmission over networks	No restriction	Internal networks only	Must be encrypted before transmission over any network
Storage	No restriction	Locked storage, physical secure computer area.	Locked storage, encrypted when stored on computer connected to network

Writing the Policy

- Match your organization's culture
- Use the "real" information channels
- Several sources for templates
  - NIST/TIS - http://csrc.nist.gov/isptg
  - Charles C. Wood - http://www.baselinesoft.com
  - Outside consultants
- Involve Legal, HR, Public Affairs
- Policy should be issued from as high in the organization as possible

Awareness and Education

- **Standard approaches:**
  - **Part of new hire training**
  - **Yearly signed awareness statement**
  - **System banners**
  - **Internal newsletters**
- **Direct Marketing approach**
  - **Pay stub messages**
  - **Online quizzes with awards**
  - **Self assessment tools**

Trusted Information Systems

- Since 1983, computer, network, and information security
- Customers in industry and federal, state, and local governments, worldwide
- Security products, security consulting, and world-respected research and development
- RecoverKey encryption technology
- TIS offices in Maryland, Virginia, California, UK, Germany
- TIS Business Partners in North America, South America, Europe, Asia, Africa, and Australia