

Data Security Management

Joseph R. Tolisano
Gene Kingsley
Holyoke Community College
Information Technology Division

Essential Criteria for Data Security

- **Build and Maintain a Secure Network**
 - Install and maintain a Firewall.
 - Do not use vendor-supplied defaults for system passwords and other security measures.
- **Protect Critical Data**
 - Segregate and store critical data in multiple secure locations.
 - Encrypt transmission of critical data across open, public networks.
- **Maintain a Vulnerability Management Program**
 - Use and regularly update anti-virus software.
 - Develop and maintain secure systems and applications

Essential Criteria for Data Security

- **Implement Strong Access Control Measures**
 - Restrict access to cardholder data by business need to know.
 - Assign a unique ID to each person with systems access.
 - Restrict physical access to information systems and critical data.
- **Regularly Monitor and Test Networks**
 - Track and monitor all access to network resources and critical data.
 - Regularly test security systems and processes.
- **Maintain Information Security Policy**
 - Maintain a policy that address information security and train employees on critical data security and operations.

What is the InfoSec Goal?

- To enable an organization to meet all of its mission/business objectives by implementing systems with due care consideration of IT-related risks to the organization, its partners and customers...

– (NIST, IRL, sp800-33, p. 6, December 2001)



 **WISER**

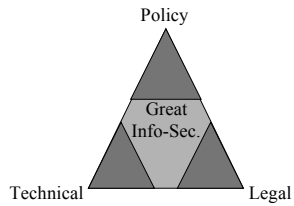
Security Objectives

- Availability
- Integrity
- Confidentiality
- Accountability
- Assurance

ISACA.org – COBIT 4.1

- **Why are we here?**
- **Management has rated information security as a top concern; however, CIO's have indicated insufficient budget as the number one obstacle in effective security management.**
- **There is a disconnect between the very high level of importance assigned to information security and the relatively low assessment among organizations.**

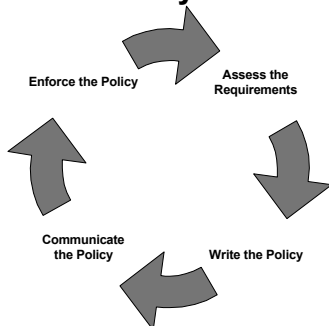
Balance Needed



Infosec Policies

- Must be maintained
 - Environmental changes affect us daily
- Departmental policies are fragmented
 - One Institutional set of policies is key
 - Collaboration is important.
- Security awareness of everyone in the organization is important to manage information security risks.
- A comprehensive, practical and documented security policy is a key starting point in an effective information security awareness program.

Policy Development LifeCycle



Why have a plan?



Why have a plan?

STOP&SHOP



Why have a plan?

STOP&SHOP



Why have a plan?

STOP&SHOP

PURDUE

TJX
THE TJX COMPANIES, INC.

KU

Why have a plan?

STOP&SHOP

PURDUE

TJX
THE TJX COMPANIES, INC.

KU

UMBC
AN HONORS UNIVERSITY IN MARYLAND

Why have a plan?

STOP&SHOP

PURDUE

TJX
THE TJX COMPANIES, INC.

KU

GEORGE MASON
UNIVERSITY

UMBC
AN HONORS UNIVERSITY IN MARYLAND

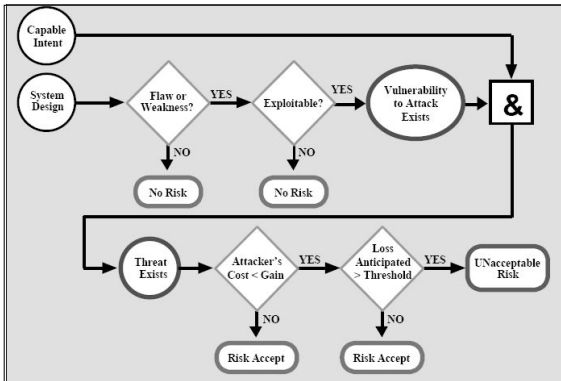


Figure 5-1 Basics of Risk Mitigation - "Attacks"

SWOT Analysis

	Positive	Negative
Internal	Strengths	Weaknesses
External	Opportunities	Threats

TOWS MATRIX

Strengths		Weaknesses	
S-O strategies		W-O strategies	
Strength:	Offers a high quality education to its service area.	Weakness:	Responsiveness to workforce needs.
Opportunity:	Local community relations and fundraising.	Opportunity:	Partner with business, industry and government.
Strategy:	Promote and market programs of distinction more aggressively to community.	Strategy:	Form workforce advising boards for each college, promote linkages with faculty and students.
S-T strategies		W-T strategies	
Strength:	Low cost.	Weakness:	Faculty and staff salaries.
Threat:	Increased competition from other and online providers.	Threat:	High cost of living and housing.
Strategy:	Media campaign to promote value of our education.	Strategy:	Consider university-sponsored housing.

How'd that happen?

- Trash is not inherently private
 - 1998 Supreme Court Ruled we have no expectation to privacy where our trash is concerned.
 - 1996 Economic Espionage Act makes it a federal offense to steal trade information
 - No protection for firms that do not take reasonable steps to protect data
