



Assessing and Managing Security Risk in IT Systems: a Technology-independent Approach

John McCumber

Software Assurance Forum

October 15, 2008

IT Risk Assessment

Find out the cause of this effect,
Or rather say, the cause of this defect,
For this effect defective comes by cause.

- *William Shakespeare, Hamlet*



Why is Risk Management Necessary?

"When you can measure what you are speaking about, and express it in numbers, you know something about it;

But when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind:

It may be the beginning of knowledge, but you have scarcely in your thoughts advanced to the stage of science."



***William Thomson
Lord Kelvin
1824 - 1907***

IT Risk Management

The process of designing, developing, sustaining, and modifying operational processes and systems in consideration of applicable risks to asset confidentiality, integrity, and availability.

**Applicable risks are those reasonably expected to be realized and to cause an unacceptable impact.*

IT Risk Management

- Incorporates an analytical, systems approach into the entire operational and support cycle.
- Provides systems and operational leaders a reliable decision support process.
- Encourages protection of only that which requires protection.
- Manages cost while achieving significant performance benefits.

Vulnerability Trends

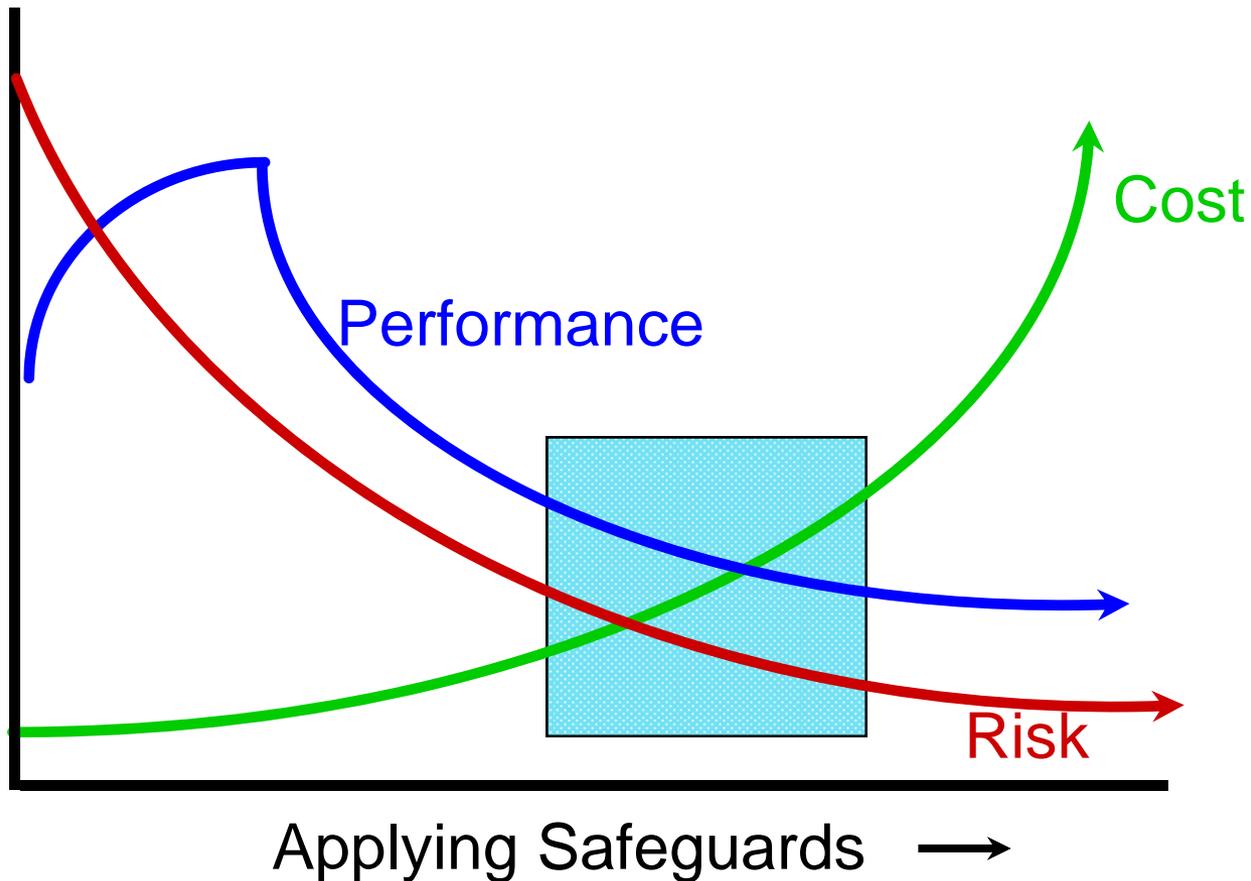
Volume: 2001 - 2007

- 2001 – approximately 1400 new technical vulnerabilities documented
- 2007 – over 4000
- Requirement for automated tracking and remediation

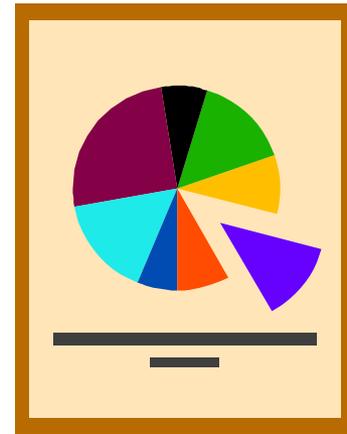
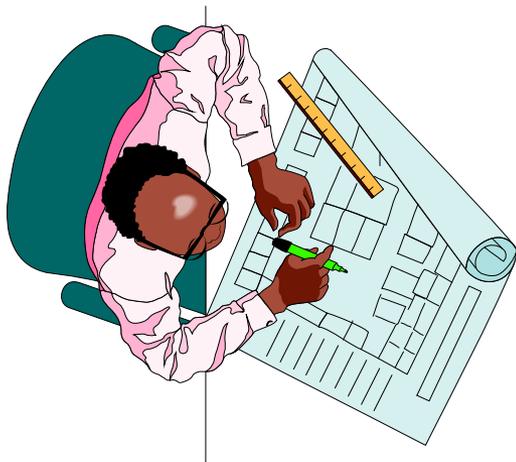
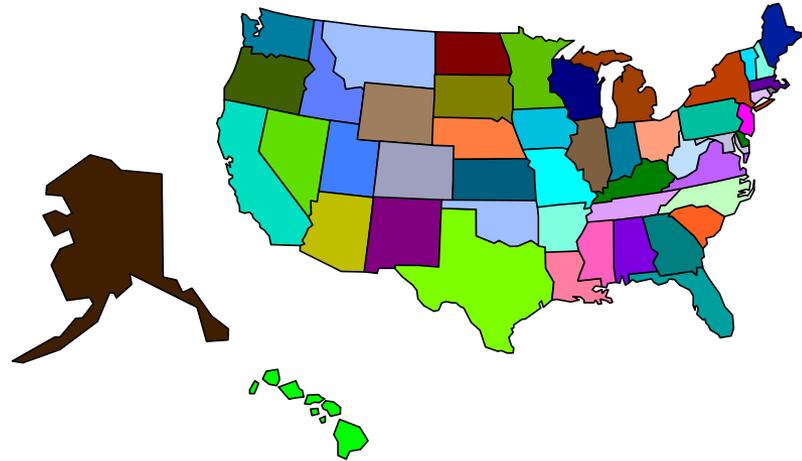
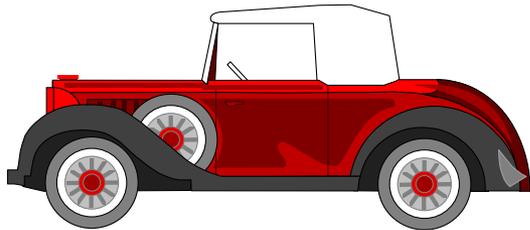
Vulnerability Management

- Vulnerabilities are specific technical weaknesses which can be exploited to impact an asset
 - System and network hardware
 - System and network operating systems
 - System and network applications
 - Network protocol
 - Connectivity
 - Current safeguards
 - Physical environment
- It is necessary to identify and rank vulnerabilities

Empirical Objective

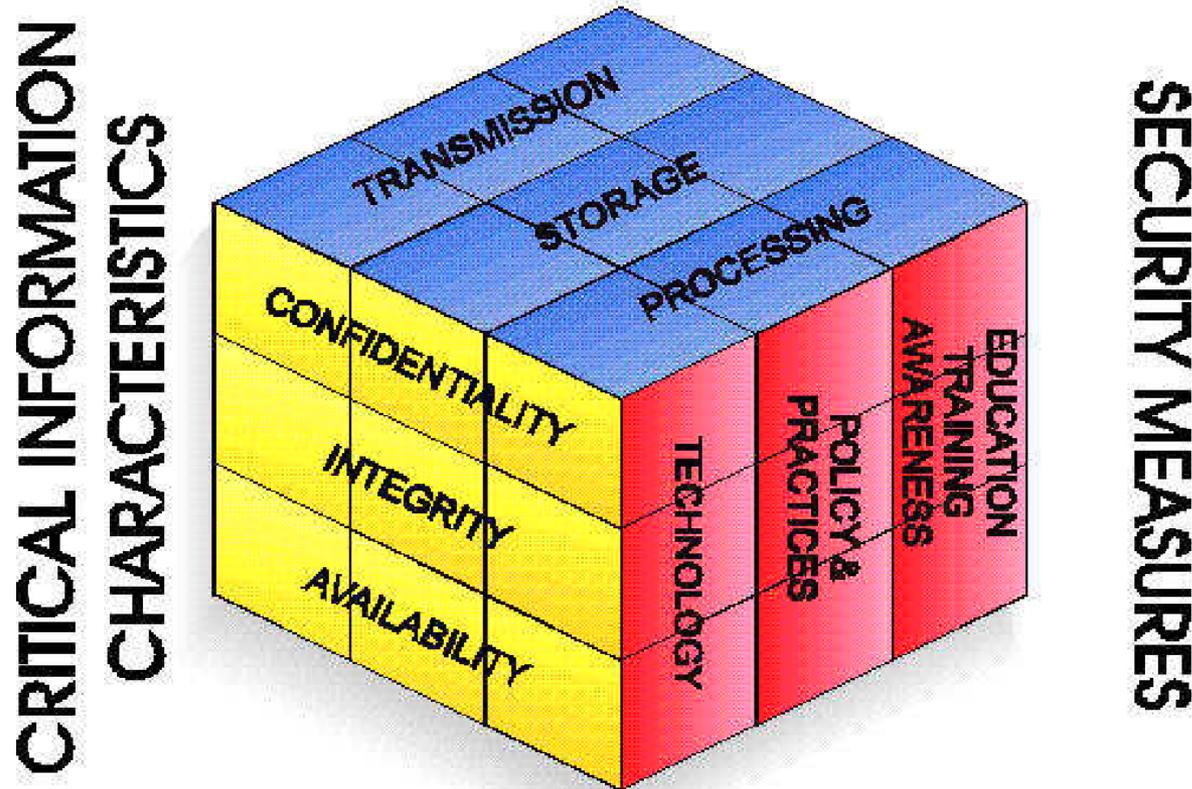


Uses and Types of Models

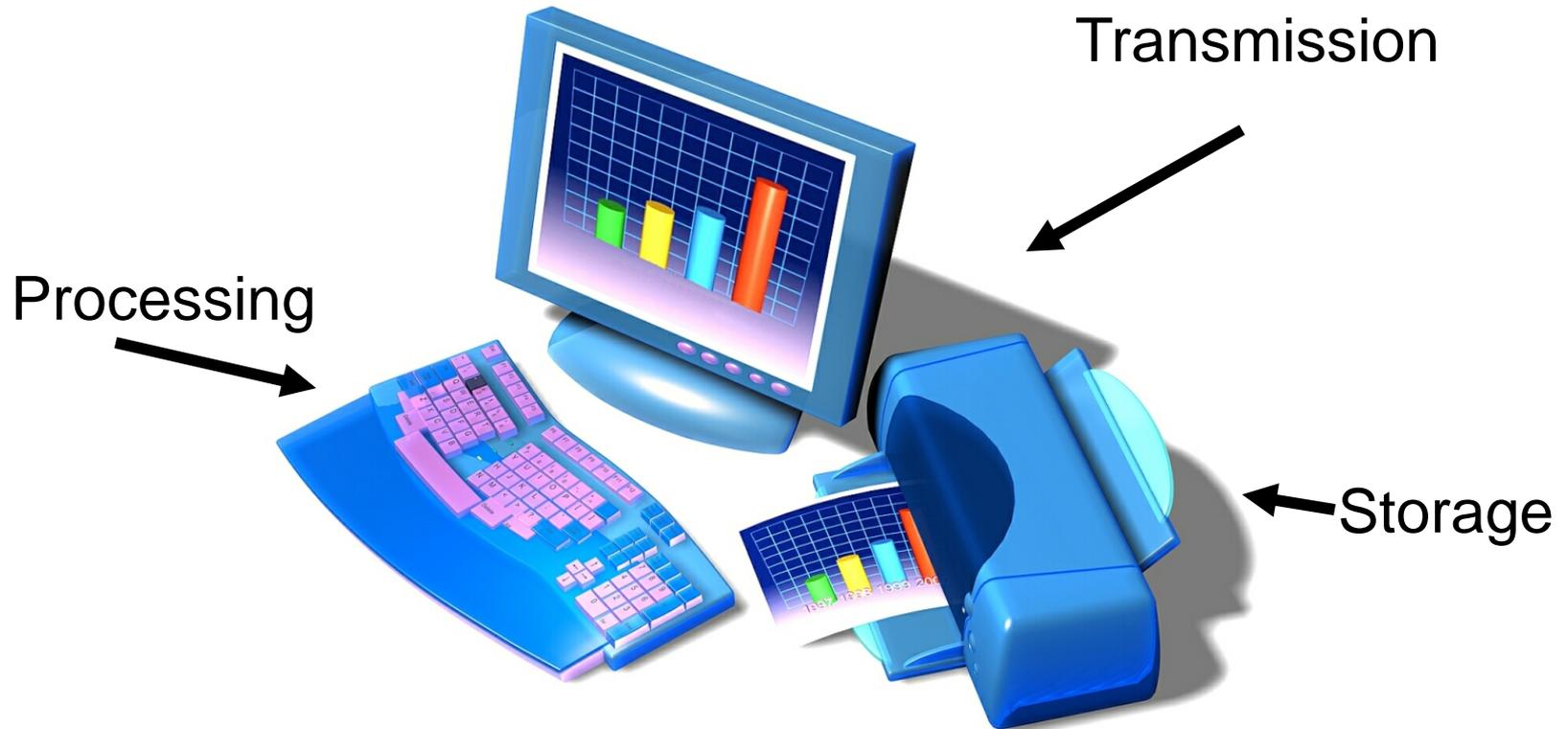


McCumber Cube Model

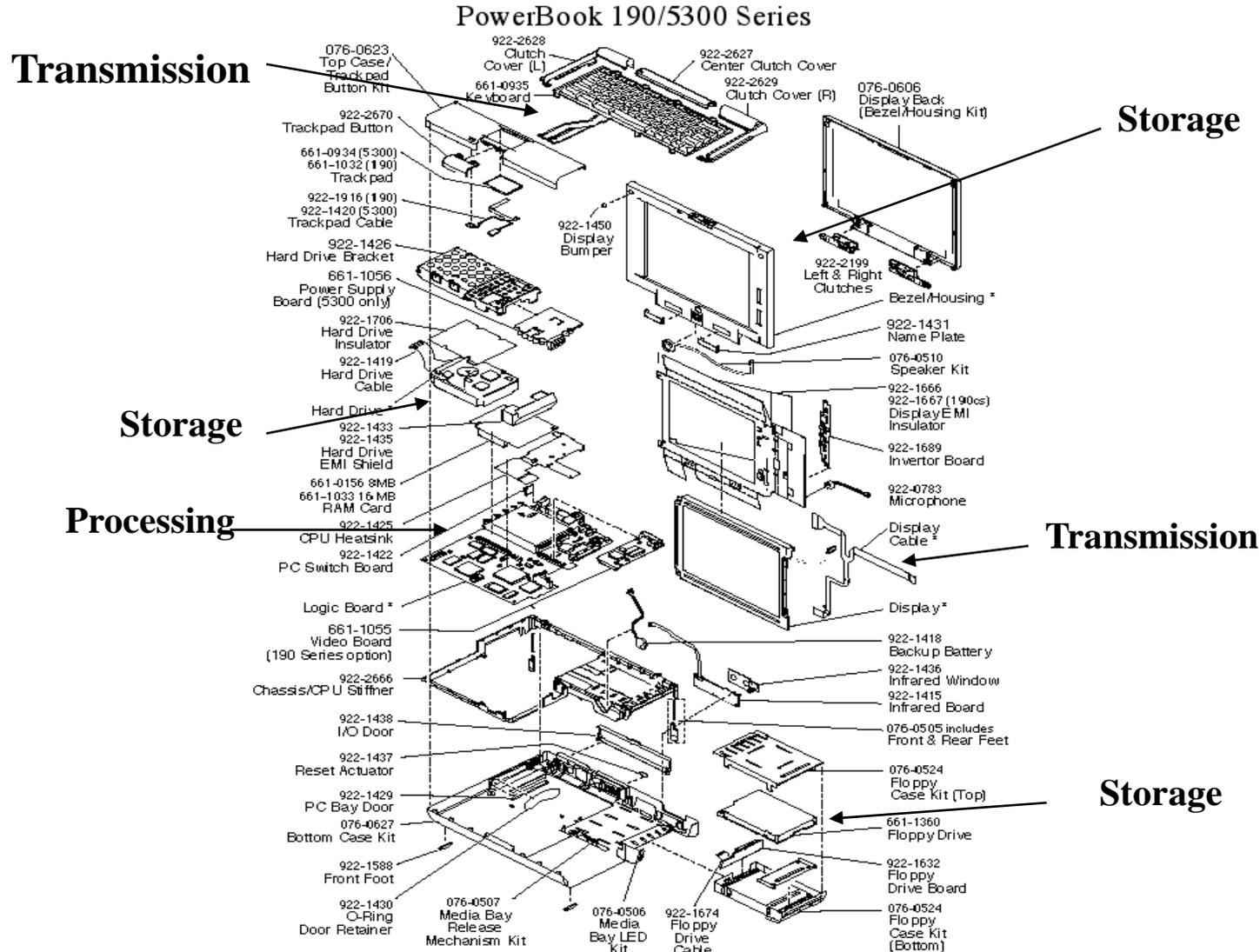
Information States



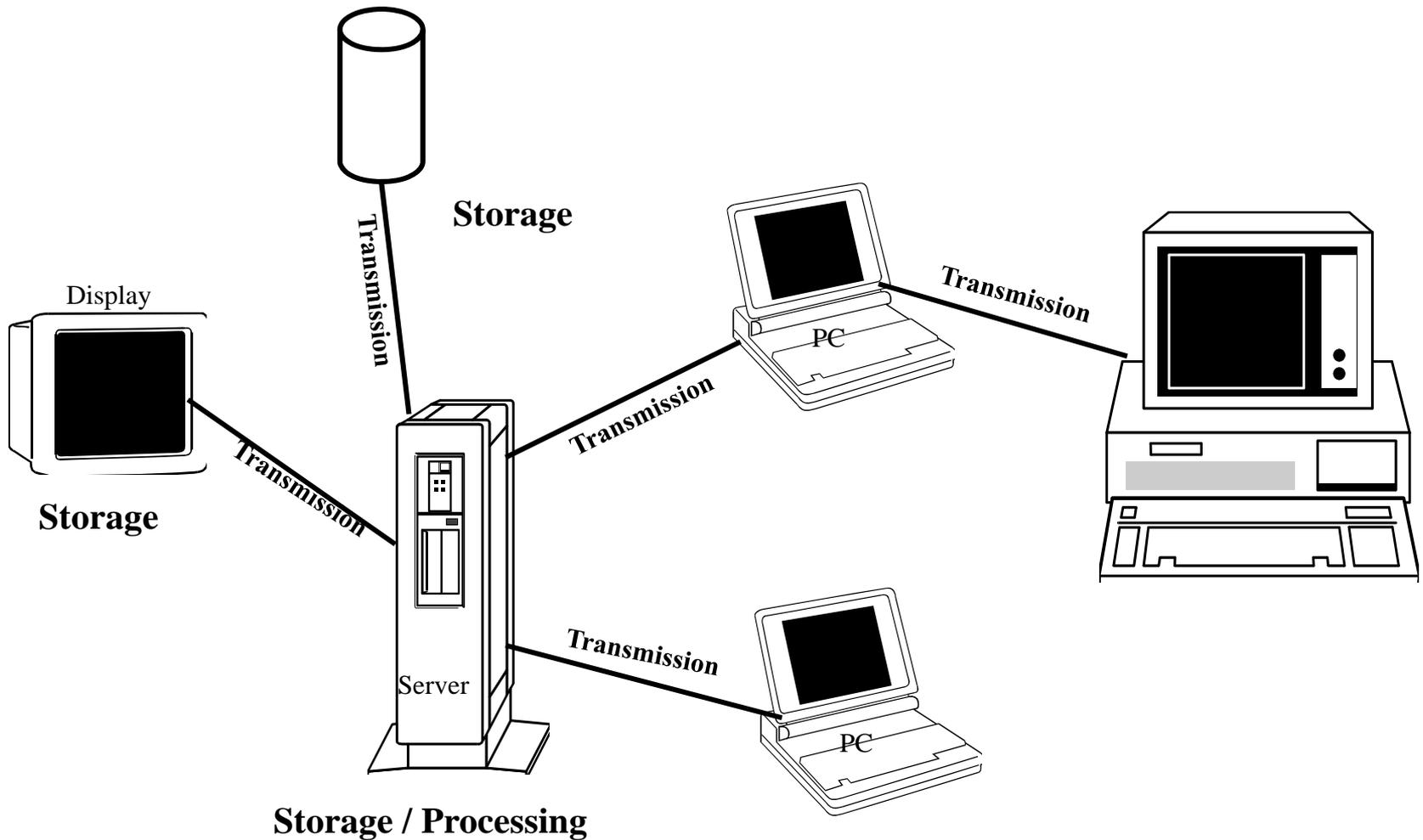
PC Information States



Component State Mapping

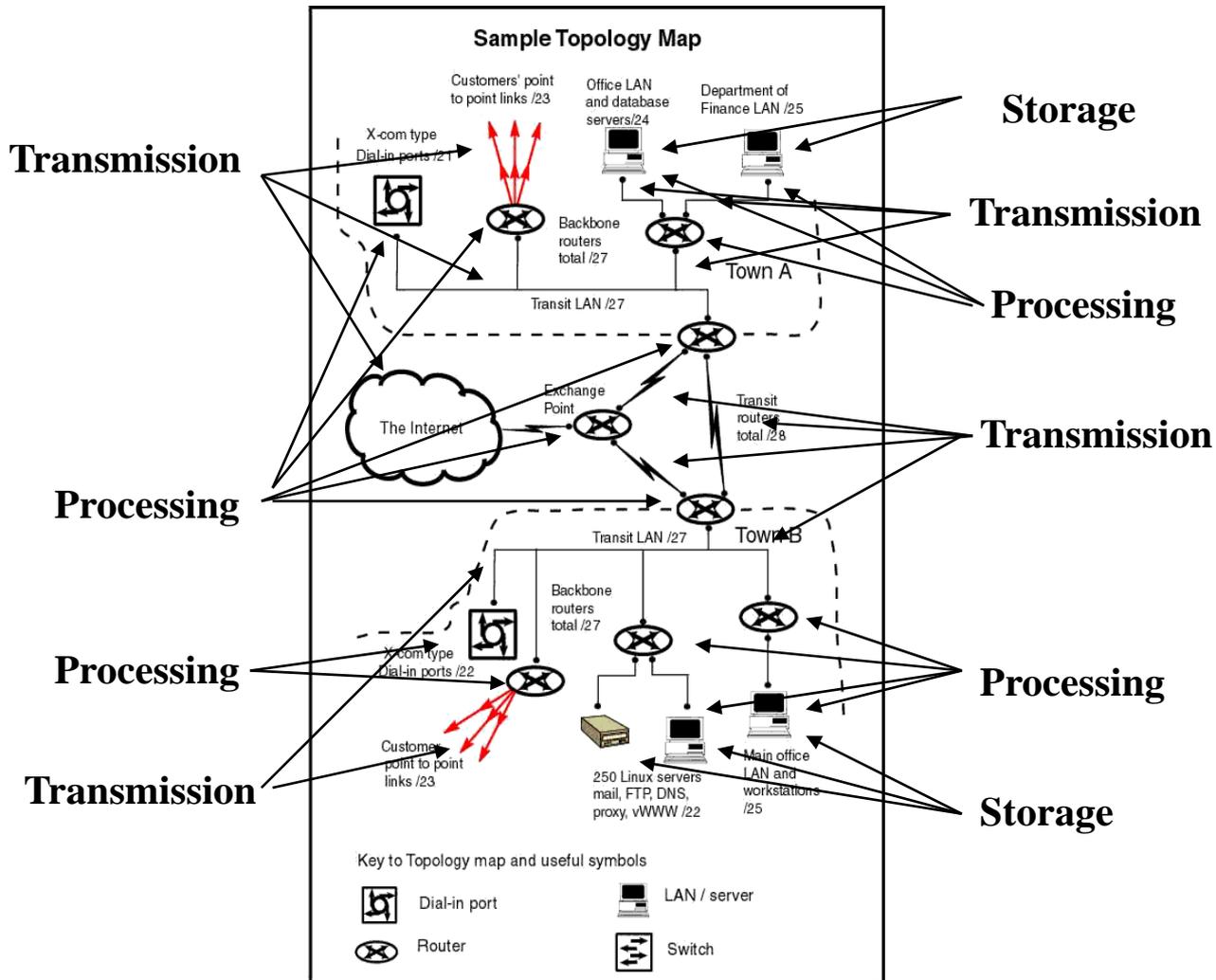


Modeling Information Systems



Information State Mapping

Example

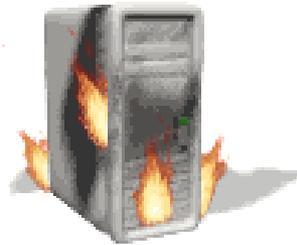


Security Attributes

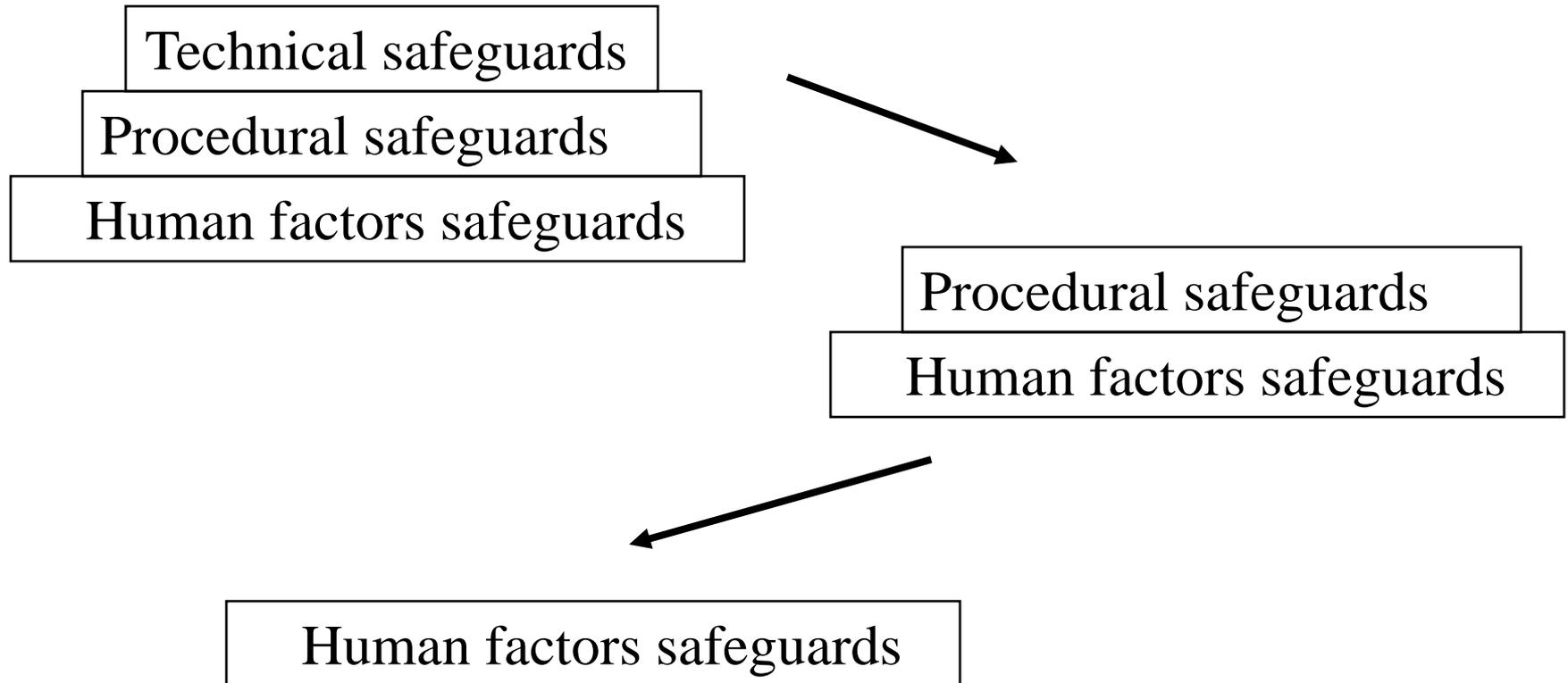
- Confidentiality
 - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity
 - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- Availability
 - Ensuring timely and reliable access to and use of information.

Safeguards and Countermeasures

- Technology
- Policy and Procedures
- Human Factors



Hierarchical Dependency of Safeguards



Hierarchical Dependency Example

Safeguard: Intrusion detection system

Technical: software, hardware, enforcement capabilities, etc.

Procedural: security policy, configuration, technology management, etc.

Human Factors: security management, training, audit & review, user awareness, etc.

Safeguard: Login warning banner

Technical: None

Procedural: None

Human Factors: user awareness, affect on external threats, legal support, etc.

Safeguard: Password development and management requirements

Technical: None (other than system enforcement)

Procedural: security policy, password assignment procedures, etc.

Human Factors: user awareness, password management oversight, human-based anomaly detection, training,

Vulnerability-Safeguard Pairing

Vulnerability

CVE-2002-0043

Sudo (superuser do) allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root or another user while logging the commands and arguments.

sudo 1.6.0 through 1.6.3p7 does not properly clear the environment before calling the mail program, which could allow local users to gain root privileges by modifying environment variables and changing how the mail program is invoked.

Safeguards

Technical:

None

Procedural:

Do not install and use Sudo 1.6.0 through 1.6.3p7;
upgrade to Sudo 1.6.4 or higher which runs the mail program with a clean environment. Admins wishing to run the mailer as the invoking user and not as root should use the *--disable-root-mailer* configure option in Sudo 1.6.5.

Human Factors:

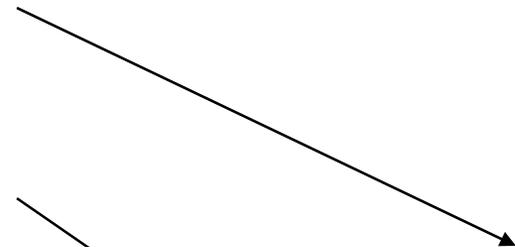
Ensure technical staff and BSD UNIX system administrators are aware of this requirement.

Expanded Vulnerability- Safeguard Pairing

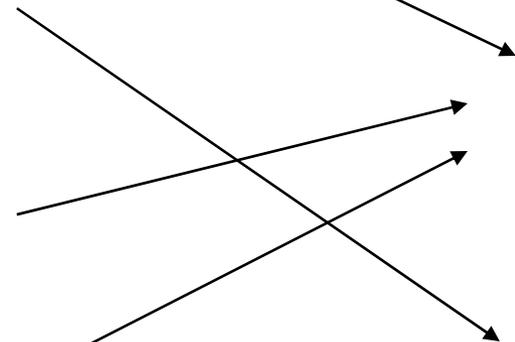
Vulnerability

Safeguards

CVE-XXXX-0043
Description:



CVE-XXXX-0044
Description:



CVE-XXXX-0049
Description:



CVE-XXXX-0052
Description:

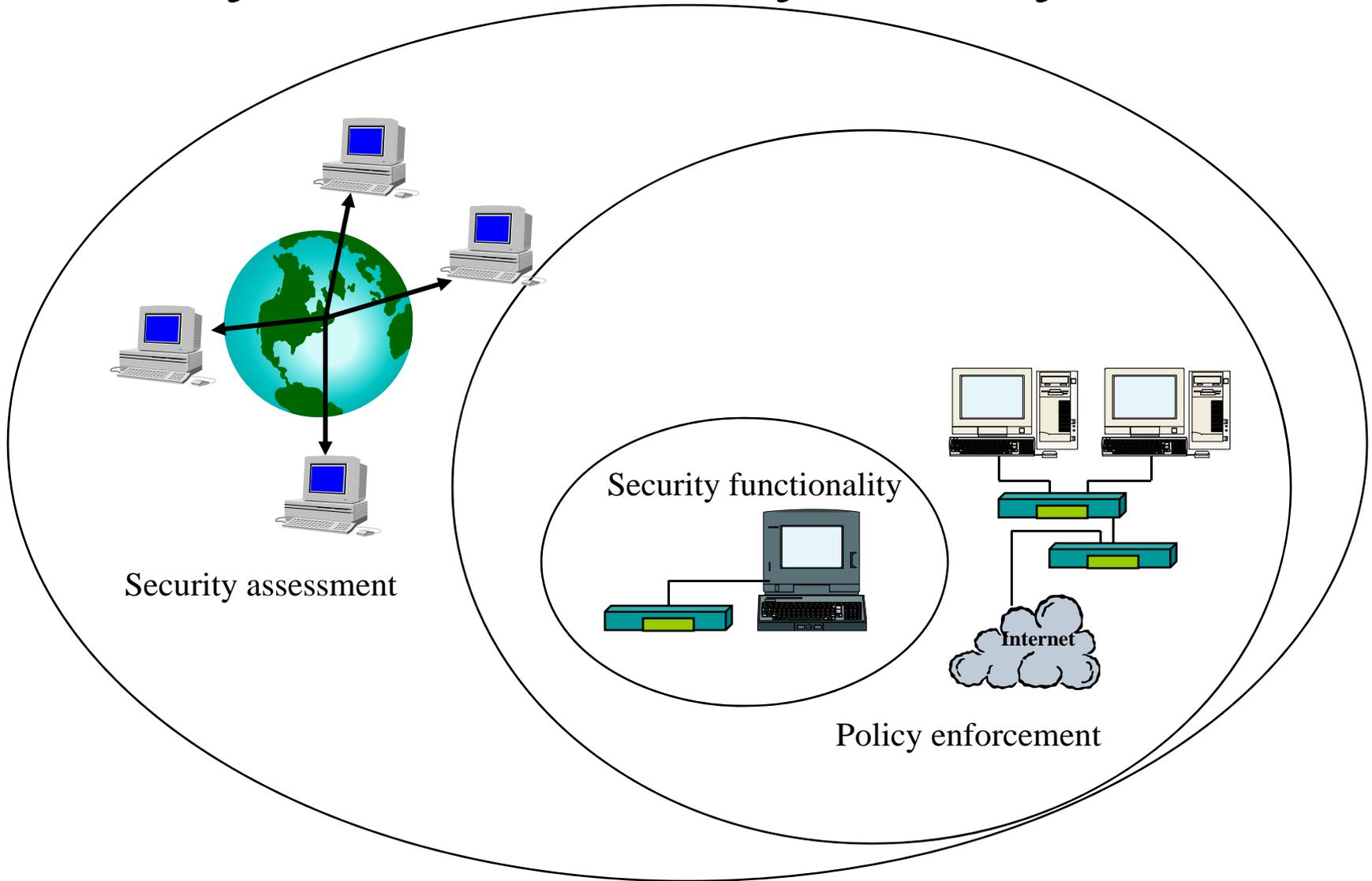


Safeguard A
Technical:
Procedural:
Human Factors:

Safeguard B
Technical:
Procedural:
Human Factors:

Safeguard C
Technical:
Procedural:
Human Factors:

Layered Security Analysis



Essential Elements of Risk

- Threats
- Assets
- Vulnerabilities
- Safeguards
 - Products
 - Procedures
 - People

The Risk Equations

$$1: \quad T \times V \times A = R_{\text{baseline}}$$

$$2: \quad \frac{T \times V \times A}{S} = R_{\text{reduced}}$$

Measuring Security Risk

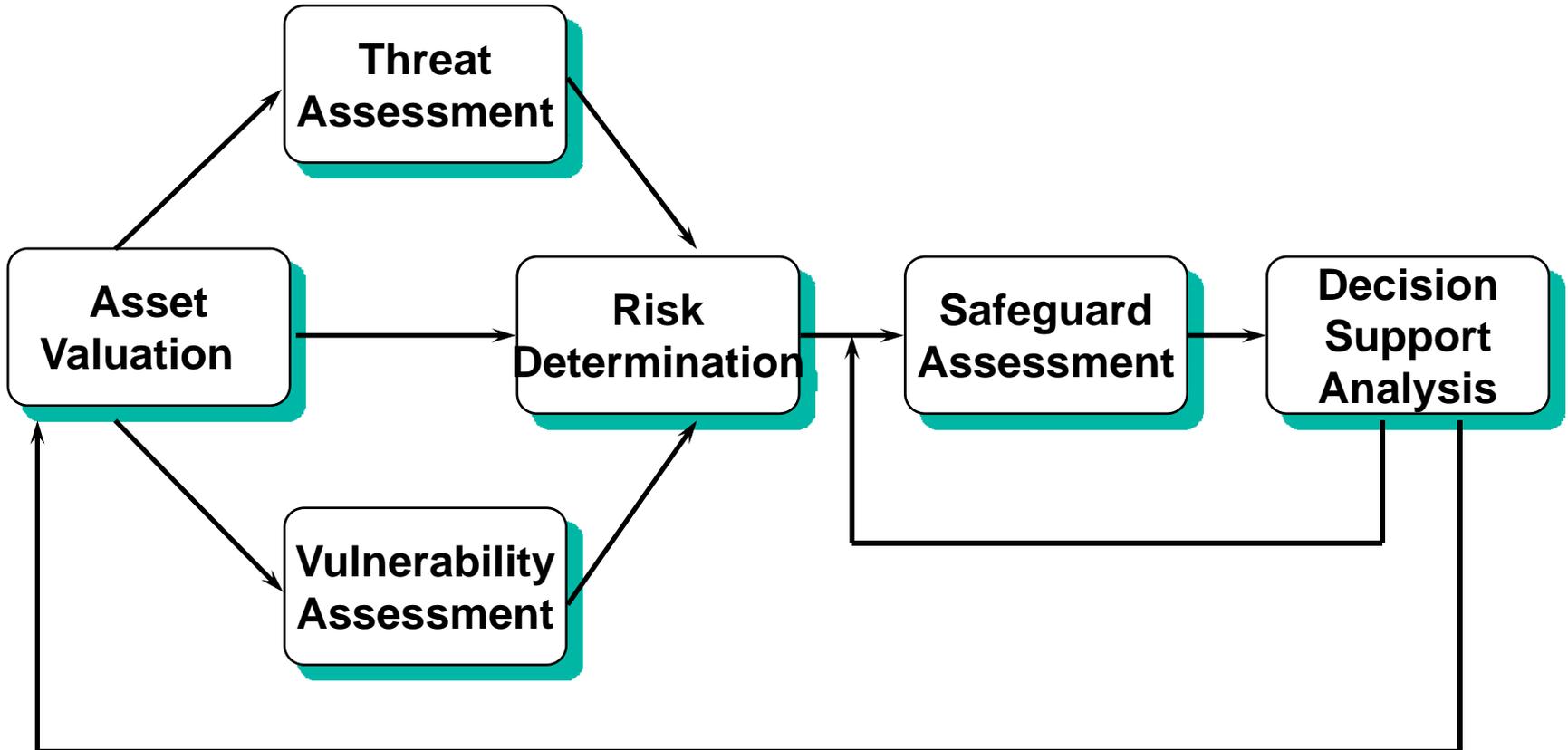


Baseline Risk



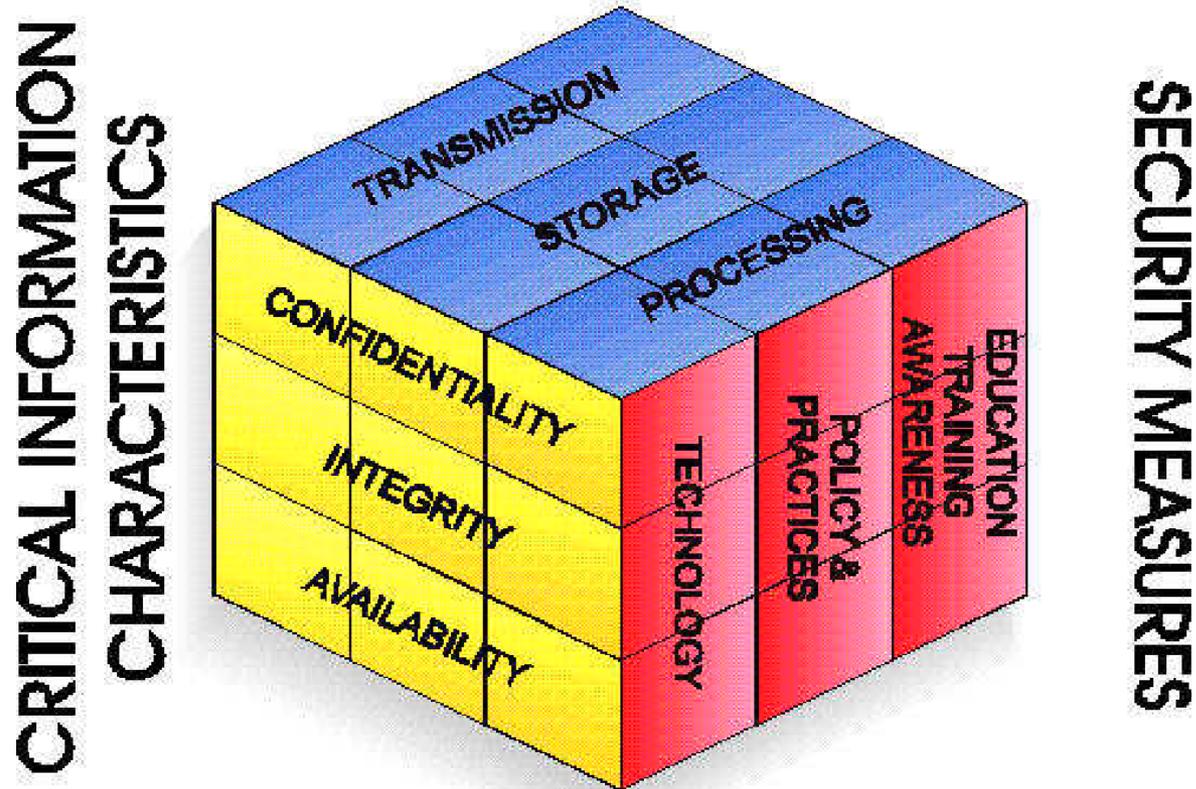
Residual Risk after Safeguards Applied

Risk Assessment Process



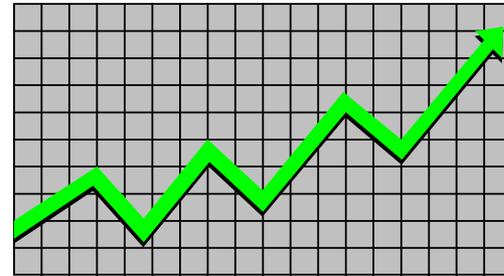
McCumber Cube Model

Information States



Conclusion

- If you can measure, you can:
 - justify
 - target
 - control
 - predict



- If you can **measure**, you can **manage**, and move information assurance from art to science.



symantec™

Thank You!

John McCumber

Assessing and Managing Security

Risk in IT Systems: a Structured Methodology

Auerbach, New York, NY 2004