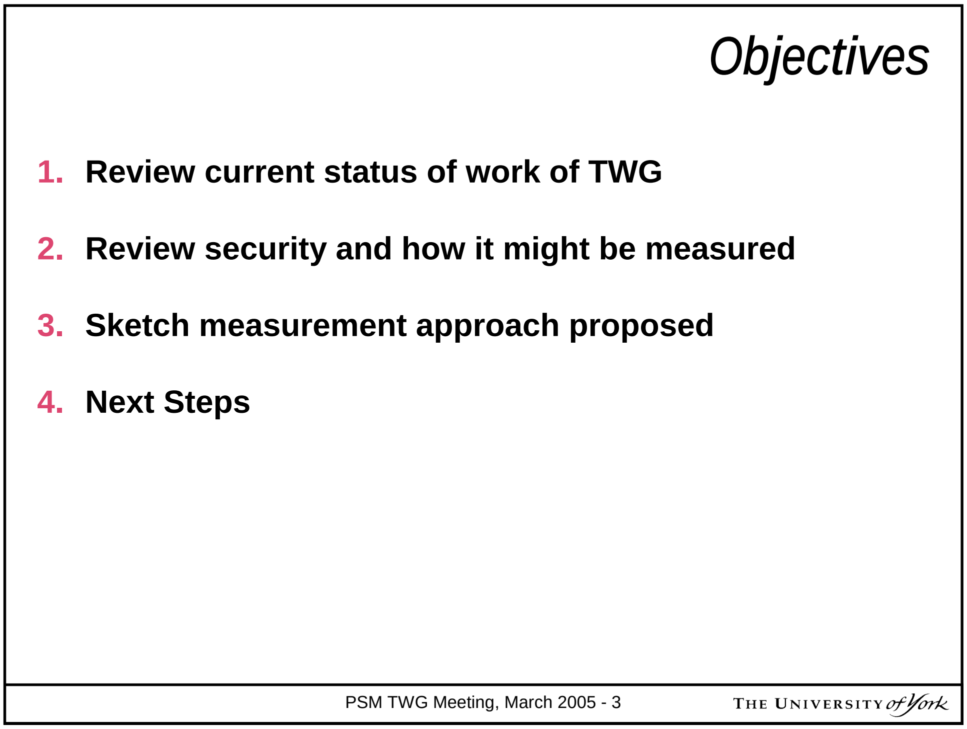
Security Measurement: Progress Report

PSM TWG Meeting
23 March 2005

John Murdoch
for the Security TWG

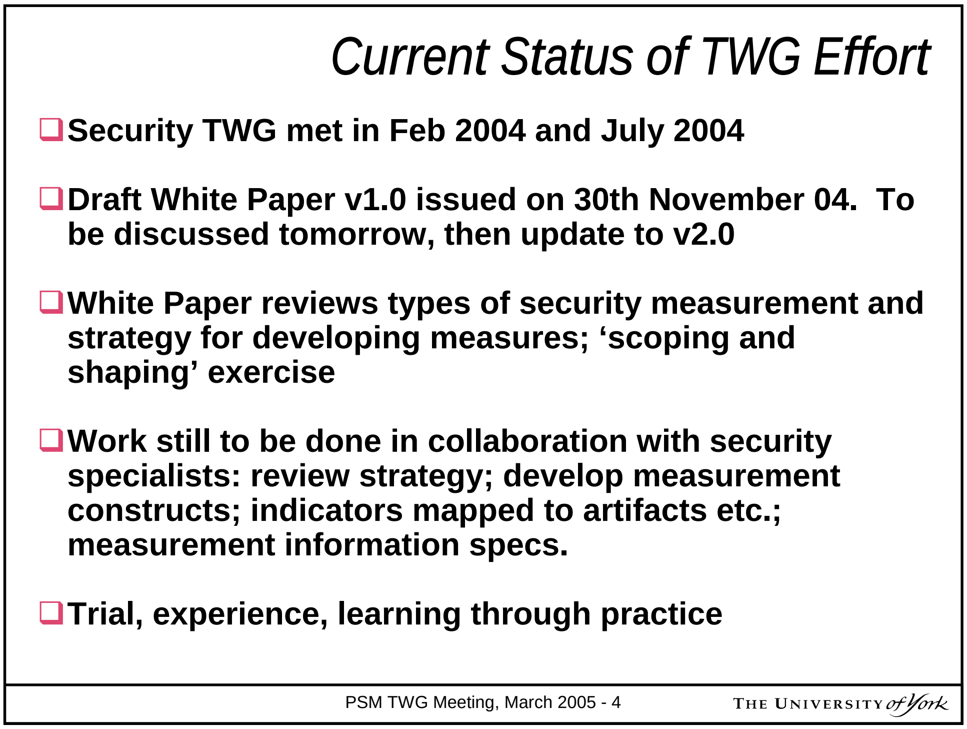
on behalf of the PSM Safety & Security TWG

Paul Caseley, John Gaffney, Joe Jarzombek, Cheryl Jones, John Van Orden, Don Reifer, Rob Robason, Amos Rohrer, David Seaver, Dave Zubrow



Objectives

1. Review current status of work of TWG
2. Review security and how it might be measured
3. Sketch measurement approach proposed
4. Next Steps



Current Status of TWG Effort

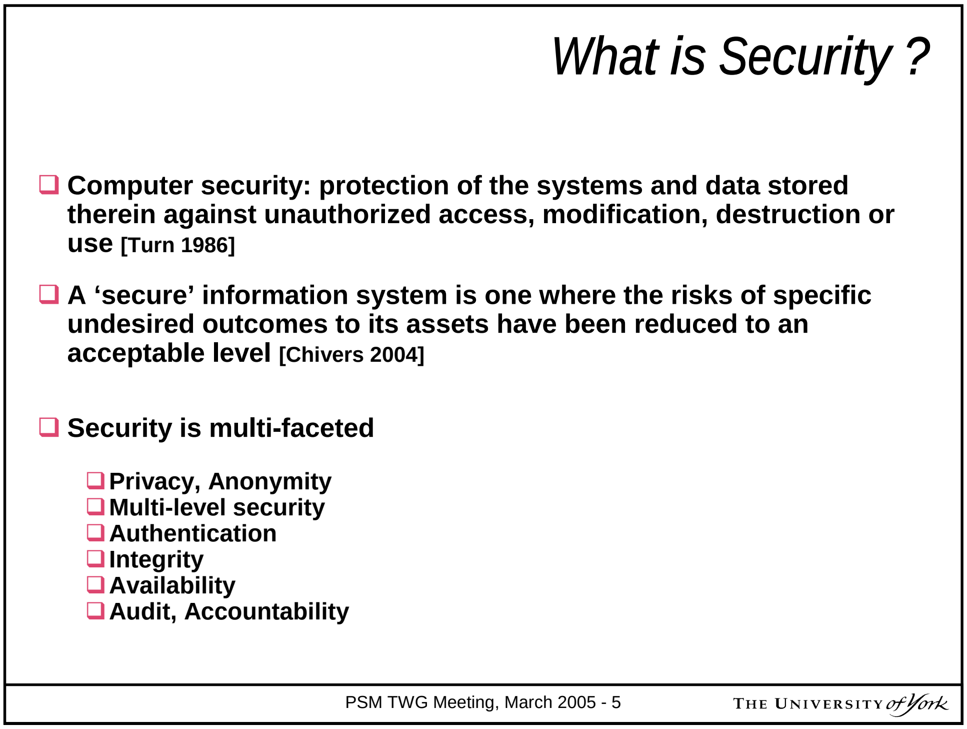
❑ Security TWG met in Feb 2004 and July 2004

❑ Draft White Paper v1.0 issued on 30th November 04. To be discussed tomorrow, then update to v2.0

❑ White Paper reviews types of security measurement and strategy for developing measures; ‘scoping and shaping’ exercise

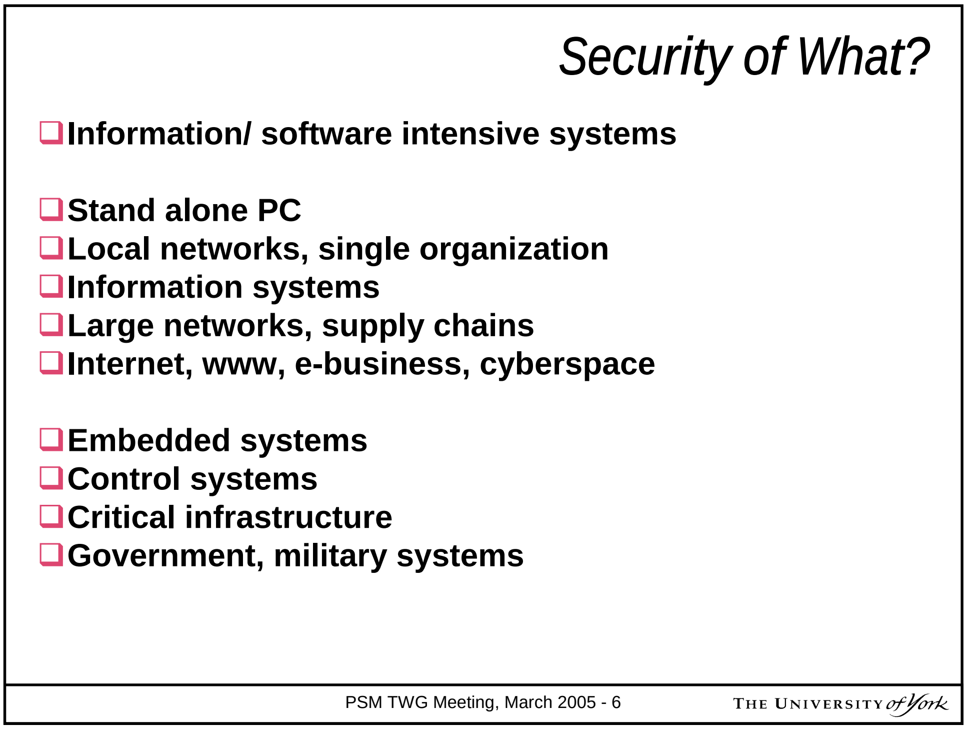
❑ Work still to be done in collaboration with security specialists: review strategy; develop measurement constructs; indicators mapped to artifacts etc.; measurement information specs.

❑ Trial, experience, learning through practice



What is Security ?

- **Computer security: protection of the systems and data stored therein against unauthorized access, modification, destruction or use [Turn 1986]**
- **A 'secure' information system is one where the risks of specific undesired outcomes to its assets have been reduced to an acceptable level [Chivers 2004]**
- **Security is multi-faceted**
  - **Privacy, Anonymity**
  - **Multi-level security**
  - **Authentication**
  - **Integrity**
  - **Availability**
  - **Audit, Accountability**



Security of What?

- **Information/ software intensive systems**

- **Stand alone PC**
- **Local networks, single organization**
- **Information systems**
- **Large networks, supply chains**
- **Internet, www, e-business, cyberspace**

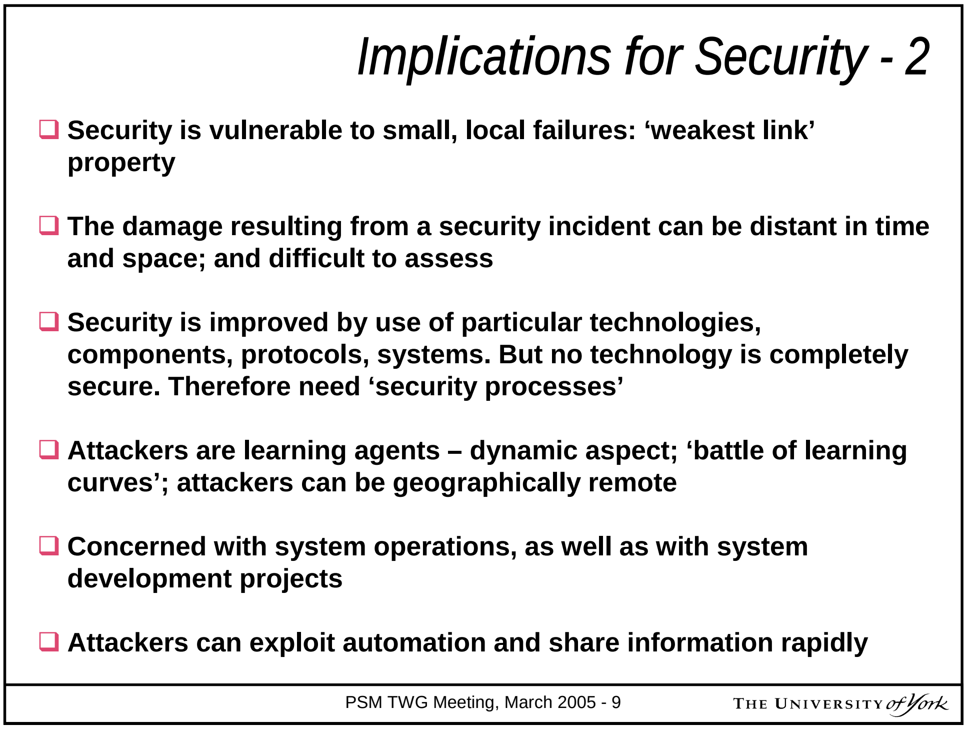
- **Embedded systems**
- **Control systems**
- **Critical infrastructure**
- **Government, military systems**

Current Trends

- ❑Stand-alone or isolated systems -> distributed, networked information systems, web-based services, cyberspace
- ❑Grid, pervasive/ ubiquitous, mobile, software agents
- ❑Hierarchical control - > collaboration, e-business, processes that cut through organizational structures
- ❑Critical systems & services increasingly dependent on cyberspace
- ❑Increasing complexity – systems not fully understood
- ❑Post 9/11, Enron - > increased risk perception

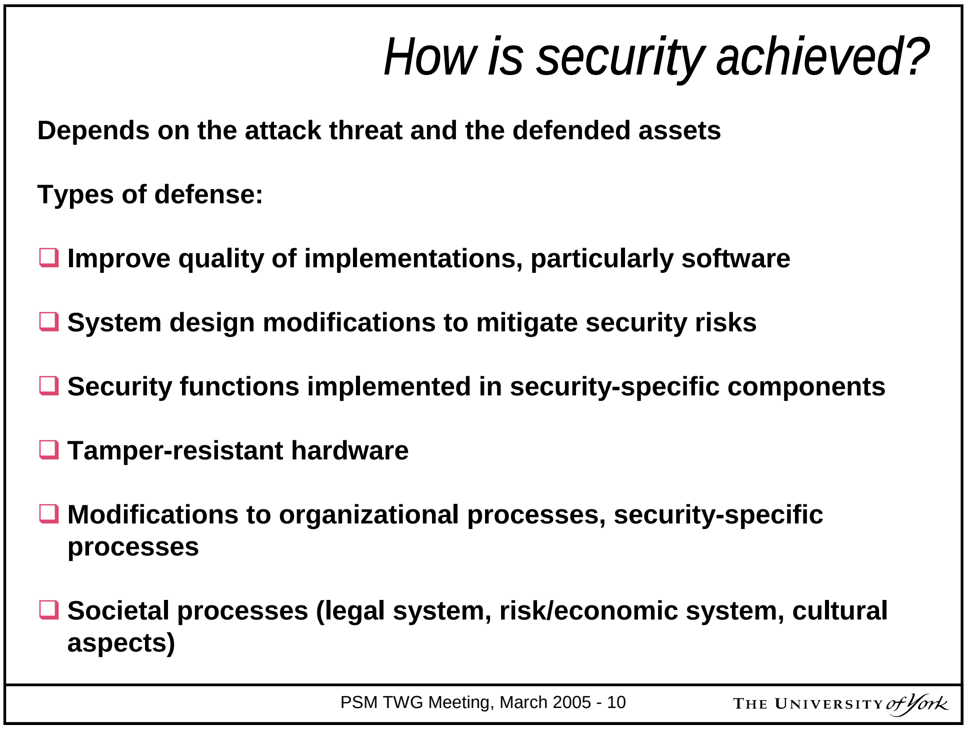
Implications for Security - 1

- ❑ Increasingly difficult to define and police ‘boundaries’
- ❑ Digital world is abstract – more difficult to authenticate, requires trust in supporting systems, services
- ❑ Attackers exploit all aspects of systems (especially human weaknesses), not only the digital
- ❑ Security a property of total systems (including organizations, communications, people), not only the computers
- ❑ Vulnerabilities associated with the interfaces, links, shared services, complexity
- ❑ Increasing overlap of safety and security in many sectors
- ❑ Historical development of the internet, sw/ hw technology has not prioritized security



Implications for Security - 2

- Security is vulnerable to small, local failures: ‘weakest link’ property
- The damage resulting from a security incident can be distant in time and space; and difficult to assess
- Security is improved by use of particular technologies, components, protocols, systems. But no technology is completely secure. Therefore need ‘security processes’
- Attackers are learning agents – dynamic aspect; ‘battle of learning curves’; attackers can be geographically remote
- Concerned with system operations, as well as with system development projects
- Attackers can exploit automation and share information rapidly

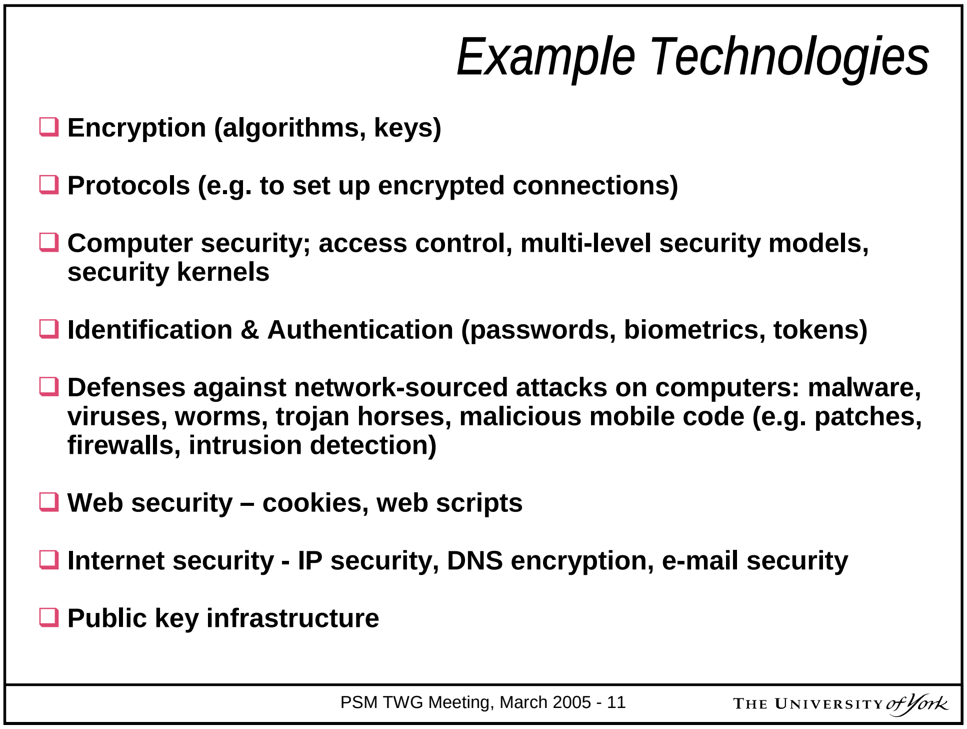


How is security achieved?

Depends on the attack threat and the defended assets

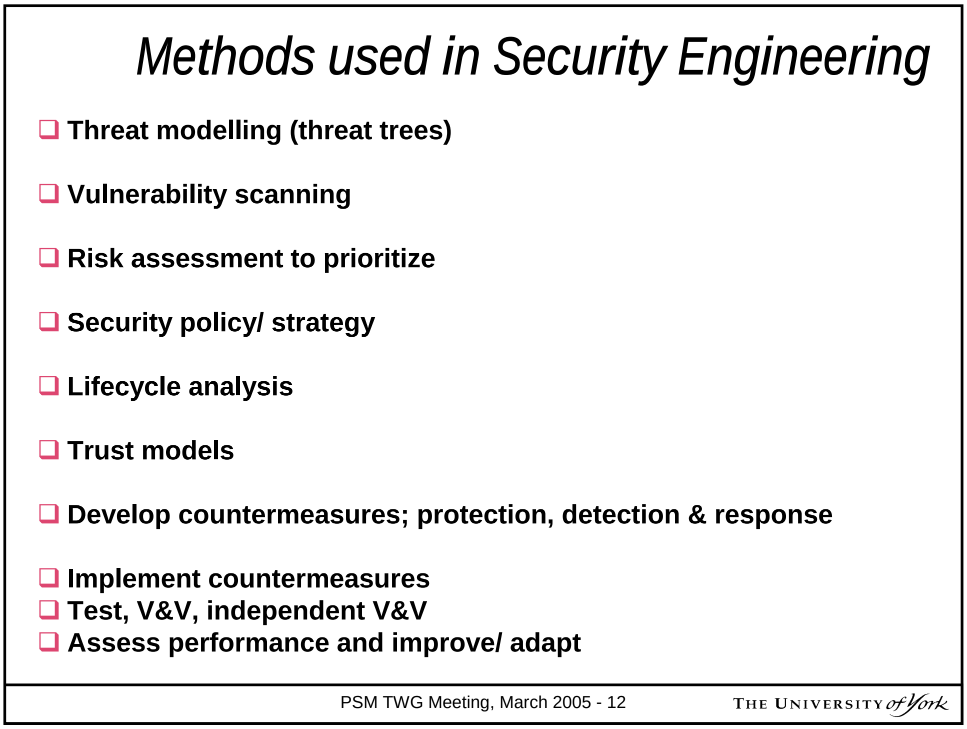
Types of defense:

- Improve quality of implementations, particularly software
- System design modifications to mitigate security risks
- Security functions implemented in security-specific components
- Tamper-resistant hardware
- Modifications to organizational processes, security-specific processes
- Societal processes (legal system, risk/economic system, cultural aspects)



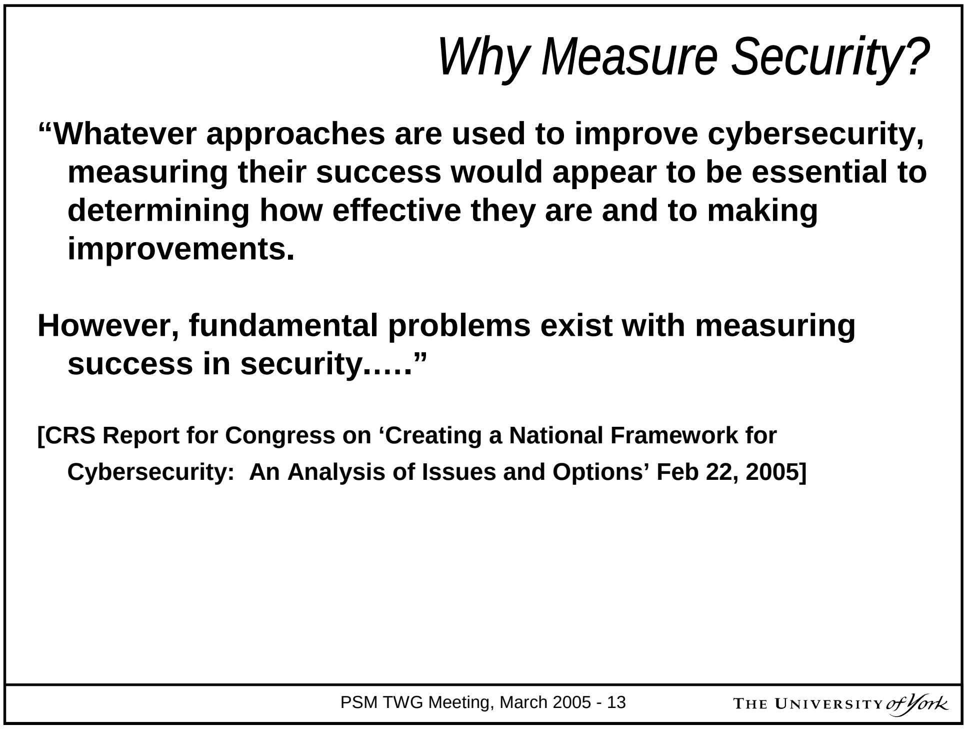
Example Technologies

- Encryption (algorithms, keys)
- Protocols (e.g. to set up encrypted connections)
- Computer security; access control, multi-level security models, security kernels
- Identification & Authentication (passwords, biometrics, tokens)
- Defenses against network-sourced attacks on computers: malware, viruses, worms, trojan horses, malicious mobile code (e.g. patches, firewalls, intrusion detection)
- Web security – cookies, web scripts
- Internet security - IP security, DNS encryption, e-mail security
- Public key infrastructure



Methods used in Security Engineering

- Threat modelling (threat trees)
- Vulnerability scanning
- Risk assessment to prioritize
- Security policy/ strategy
- Lifecycle analysis
- Trust models
- Develop countermeasures; protection, detection & response
- Implement countermeasures
- Test, V&V, independent V&V
- Assess performance and improve/ adapt

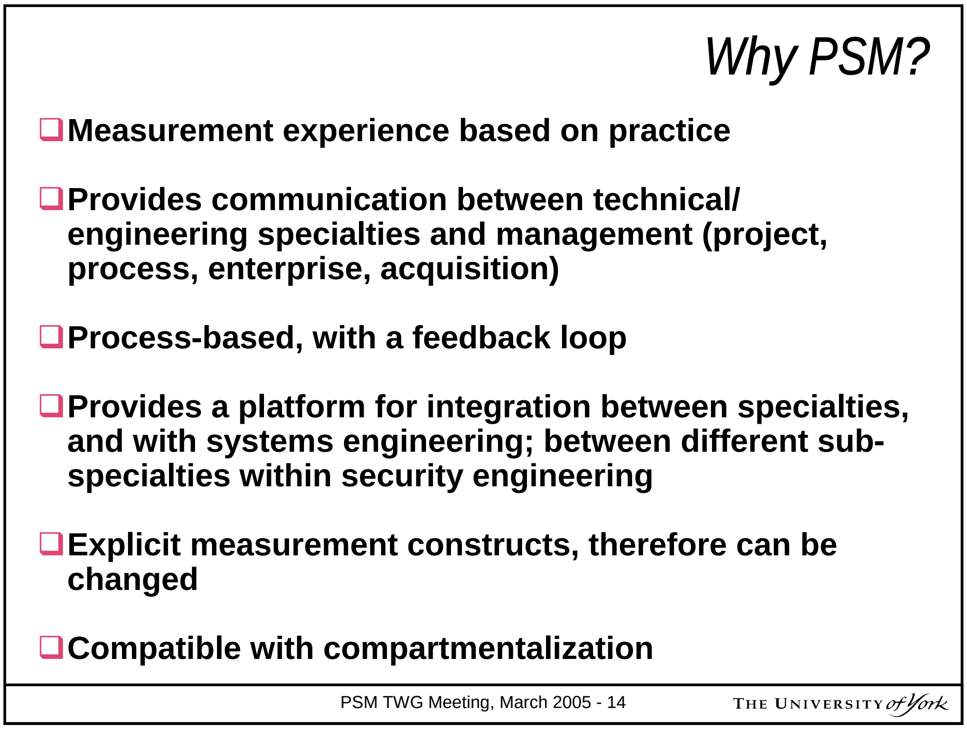


Why Measure Security?

"Whatever approaches are used to improve cybersecurity, measuring their success would appear to be essential to determining how effective they are and to making improvements.

However, fundamental problems exist with measuring success in security….."

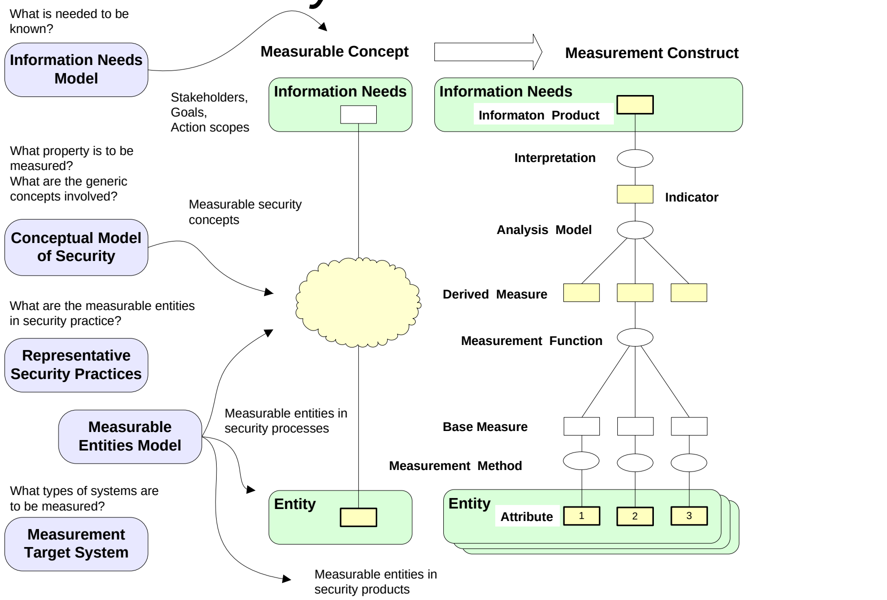
[CRS Report for Congress on 'Creating a National Framework for Cybersecurity: An Analysis of Issues and Options' Feb 22, 2005]



Why PSM?

- □ Measurement experience based on practice
- □ Provides communication between technical/ engineering specialties and management (project, process, enterprise, acquisition)
- □ Process-based, with a feedback loop
- □ Provides a platform for integration between specialties, and with systems engineering; between different sub-specialties within security engineering
- □ Explicit measurement constructs, therefore can be changed
- □ Compatible with compartmentalization

Security Measurement Constructs



What is needed to be known?

Information Needs Model

What property is to be measured?
What are the generic concepts involved?

Conceptual Model of Security

What are the measurable entities in security practice?

Representative Security Practices

Measurable Entities Model

What types of systems are to be measured?

Measurement Target System

Measurable Concept

Measurement Construct

Stakeholders,
Goals,
Action scopes

Information Needs

Measurable security concepts

Measurable entities in security processes

Entity

Measurable entities in security products

Information Needs

Informaton Product

Interpretation

Indicator

Analysis Model

Derived Measure

Measurement Function

Base Measure

Measurement Method

Entity

Attribute 1 2 3

Information Needs – First Level

Are the residual security risks assigned to a defined entity acceptably low, for defined security threats?

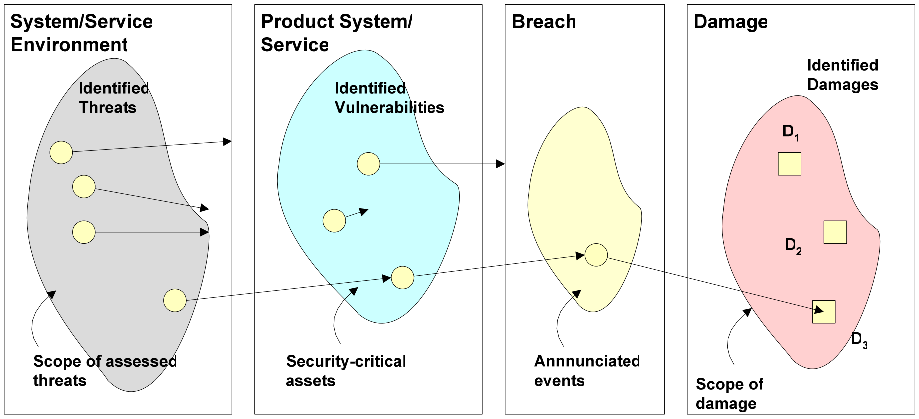
What is the Return on Security Investment (ROSI) ? relates the achieved integrated security performance of an entity (systems plus processes) with the total security costs incurred (development and operations)

At the next level of decomposition, we can ask the following questions:

Information Needs – Second Level

1. What is the capability/competence of the resources deployed on security?
2. Are security actions based on known best practice and in compliance with applicable standards and legal requirements?
3. How are security risks being managed?
4. What is the assurance evidence that defines our degree of confidence in likely future security performance?
5. What is the achieved performance of our systems in terms of managing threats, vulnerabilities, responding to events and recovering from & controlling damage?

Security Managed Domains

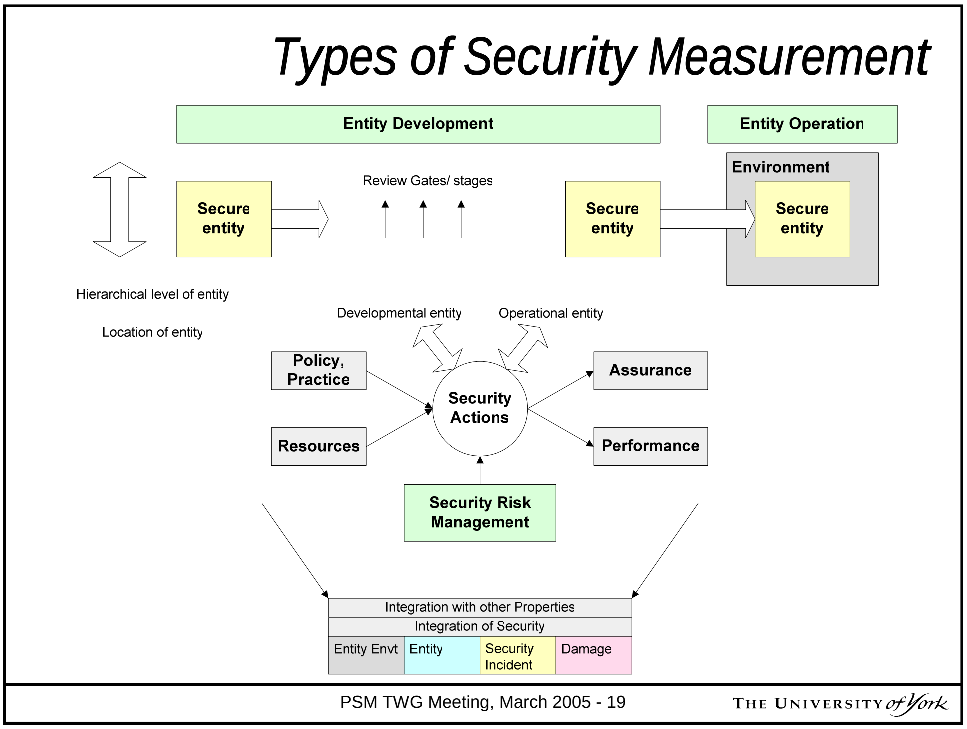


Threat: capability, intent
Threat type

Vulnerability
Vulnerability type
Vulnerability attack likelihood and severity

Security incident
Incident type
Incident likelihood

Damage severity
Damage likelihood



Types of Security Measurement

Entity Development

Entity Operation

Environment

Secure entity

Review Gates/ stages

Secure entity

Secure entity

Hierarchical level of entity

Location of entity

Developmental entity

Operational entity

Policy, Practice

Resources

Security Actions

Assurance

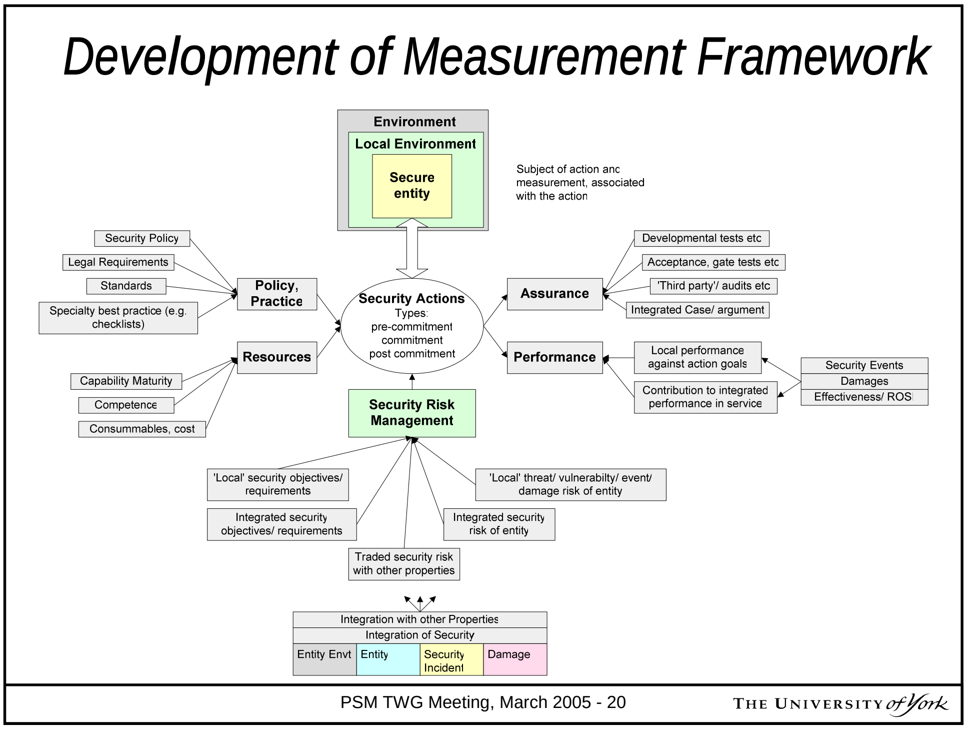
Performance

Security Risk Management

Integration with other Properties			
Integration of Security			
Entity Envt	Entity	Security Incident	Damage

PSM TWG Meeting, March 2005 - 19

THE UNIVERSITY of York



Development of Measurement Framework

Environment

Local Environment

Secure entity

Subject of action anc measurement, associated with the action

Security Policy

Legal Requirements

Standards

Specialty best practice (e.g. checklists)

Policy, Practice

Capability Maturity

Competence

Consummables, cost

Resources

Security Actions
Types:
pre-commitment
commitment
post commitment

Assurance

Developmental tests etc

Acceptance, gate tests etc

'Third party'/ audits etc

Integrated Case/ argument

Performance

Local performance against action goals

Contribution to integrated performance in service

Security Events

Damages

Effectiveness/ ROSI

Security Risk Management

'Local' security objectives/ requirements

Integrated security objectives/ requirements

Traded security risk with other properties

Integrated security risk of entity

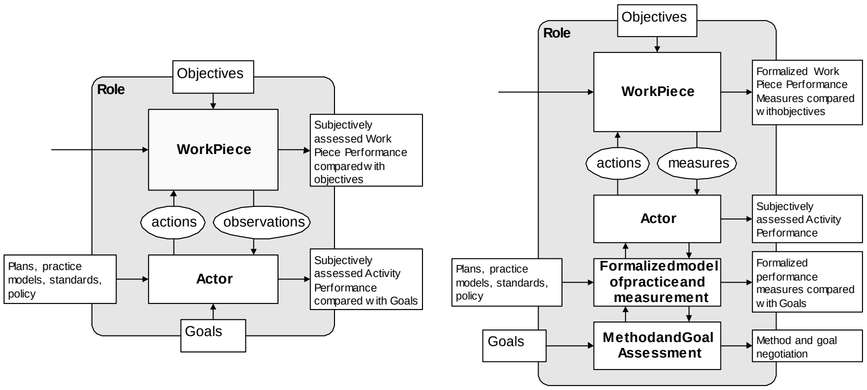
'Local' threat/ vulnerabilty/ event/ damage risk of entity

Integration with other Properties			
Integration of Security			
Entity Envt	Entity	Security Incident	Damage

PSM TWG Meeting, March 2005 - 20

THE UNIVERSITY of York

Measurement Development



Role

Objectives

WorkPiece

Subjectively assessed Work Piece Performance comparedw ith objectives

actions

observations

Plans, practice models, standards, policy

Actor

Subjectively assessed Activity Performance compared w ith Goals

Goals

Role

Objectives

WorkPiece

Formalized Work Piece Performance Measures compared w ithobjectives

actions

measures

Actor

Subjectively assessed Activity Performance

Plans, practice models, standards, policy

Formalizedmodel ofpracticeand measurement

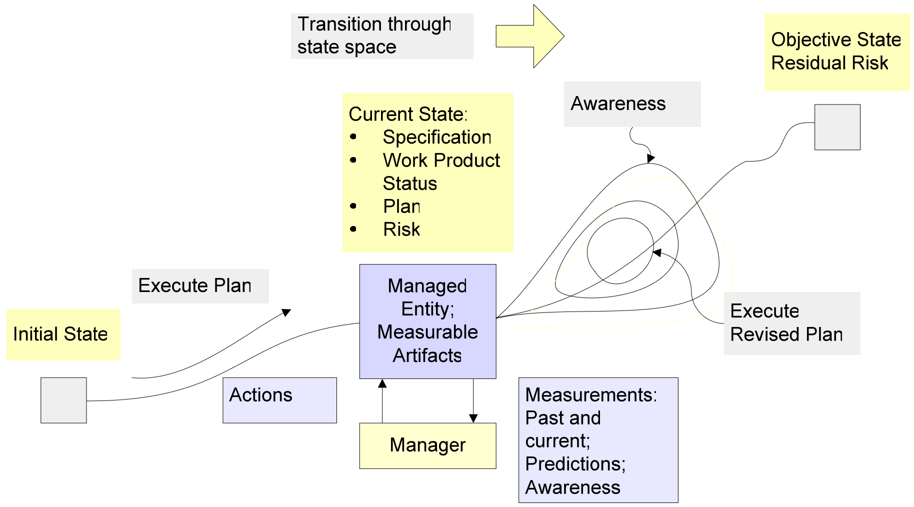
Formalized performance measures compared w ith Goals

Goals

MethodandGoal Assessment

Method and goal negotiation

Project



Transition through state space

Objective State
Residual Risk

Awareness

Current State:
- Specification
- Work Product Status
- Plan
- Risk

Execute Plan

Initial State

Managed Entity; Measurable Artifacts

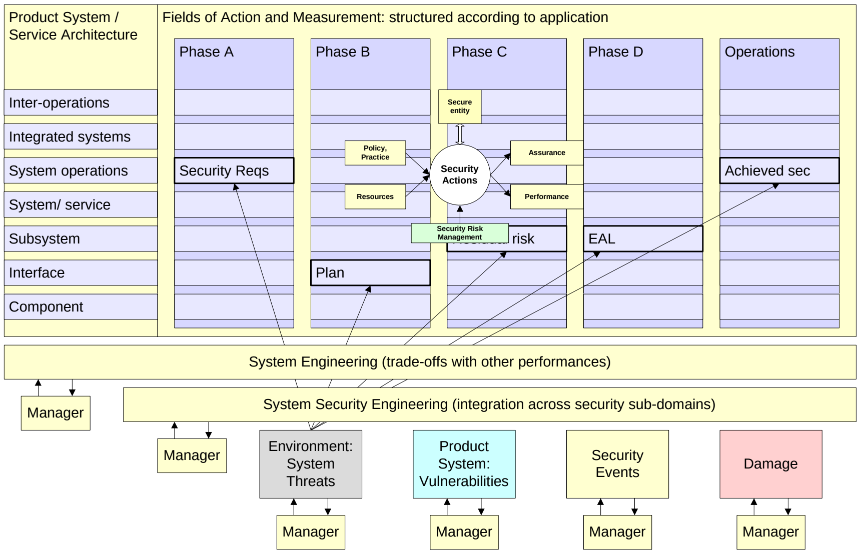
Execute Revised Plan

Actions

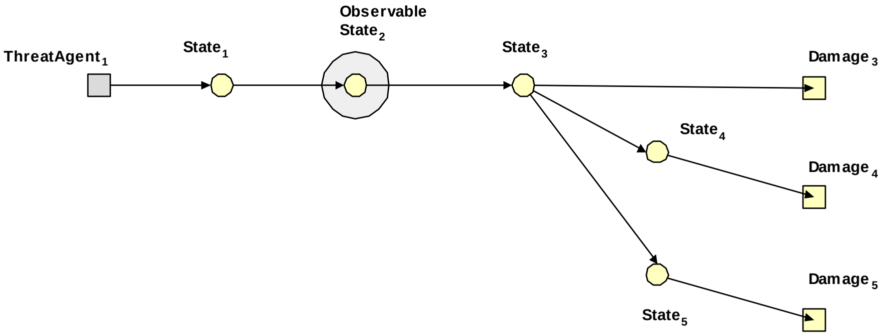
Manager

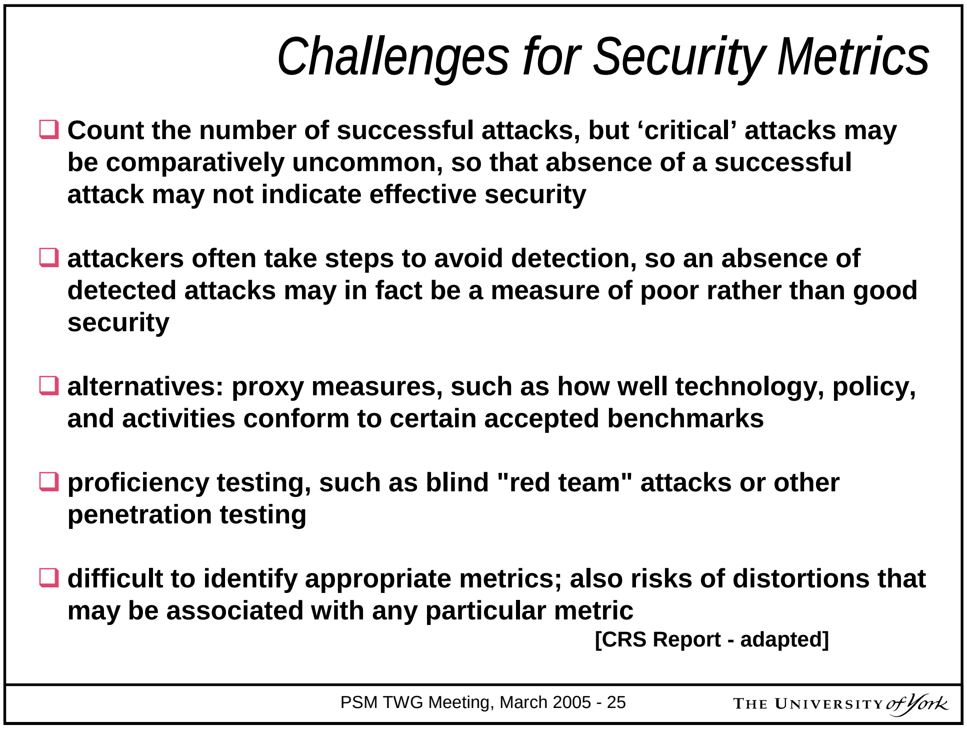
Measurements:
Past and current;
Predictions;
Awareness

Security Measurement & Complex Projects



Measurement against Attack Scenarios

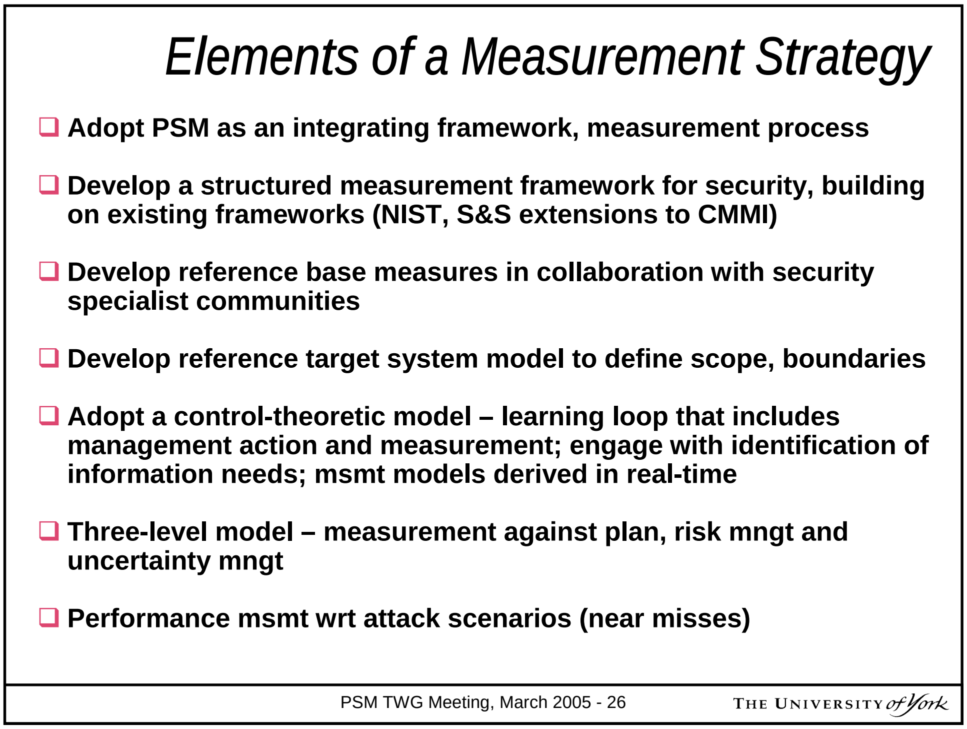




Challenges for Security Metrics

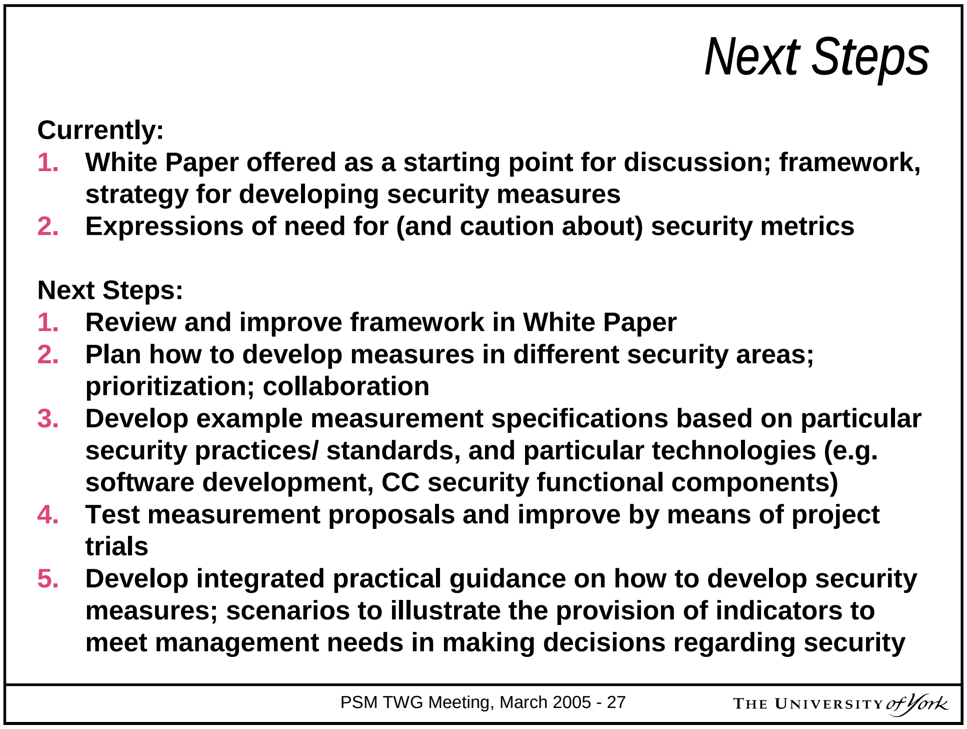
- ❑ Count the number of successful attacks, but ‘critical’ attacks may be comparatively uncommon, so that absence of a successful attack may not indicate effective security
- ❑ attackers often take steps to avoid detection, so an absence of detected attacks may in fact be a measure of poor rather than good security
- ❑ alternatives: proxy measures, such as how well technology, policy, and activities conform to certain accepted benchmarks
- ❑ proficiency testing, such as blind "red team" attacks or other penetration testing
- ❑ difficult to identify appropriate metrics; also risks of distortions that may be associated with any particular metric

[CRS Report - adapted]



Elements of a Measurement Strategy

- ❑ Adopt PSM as an integrating framework, measurement process
- ❑ Develop a structured measurement framework for security, building on existing frameworks (NIST, S&S extensions to CMMI)
- ❑ Develop reference base measures in collaboration with security specialist communities
- ❑ Develop reference target system model to define scope, boundaries
- ❑ Adopt a control-theoretic model – learning loop that includes management action and measurement; engage with identification of information needs; msmt models derived in real-time
- ❑ Three-level model – measurement against plan, risk mngt and uncertainty mngt
- ❑ Performance msmt wrt attack scenarios (near misses)



Next Steps

Currently:

1. White Paper offered as a starting point for discussion; framework, strategy for developing security measures
2. Expressions of need for (and caution about) security metrics

Next Steps:

1. Review and improve framework in White Paper
2. Plan how to develop measures in different security areas; prioritization; collaboration
3. Develop example measurement specifications based on particular security practices/ standards, and particular technologies (e.g. software development, CC security functional components)
4. Test measurement proposals and improve by means of project trials
5. Develop integrated practical guidance on how to develop security measures; scenarios to illustrate the provision of indicators to meet management needs in making decisions regarding security