Presentation

Getting Started With Measuring Your Security

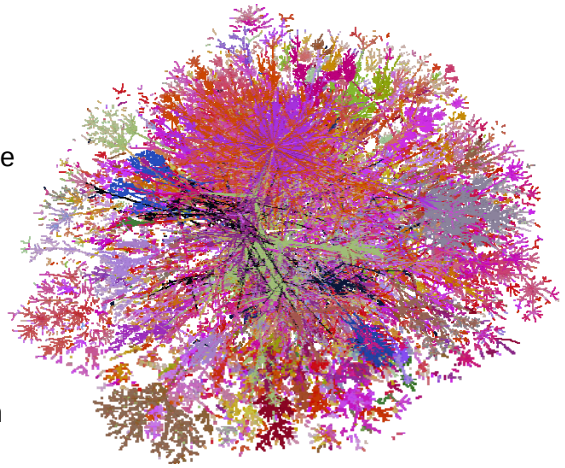
PSM Conference
Vail, CO
July, 2006

This document is confidential and is intended solely for the use and information of the client to whom it is addressed.

Booz | Allen | Hamilton

Security Needs are Continuously Evolving, Which Makes Security Implementation Increasingly Challenging

- Global interconnection
- Massive complexity
- Release of beta versions of software
- Exploitable vulnerabilities in technology
- Holes at the application layer
- Organizations and critical infrastructure increasingly rely upon the Internet for operations



Courtesy of: LUMETA CORPORATION

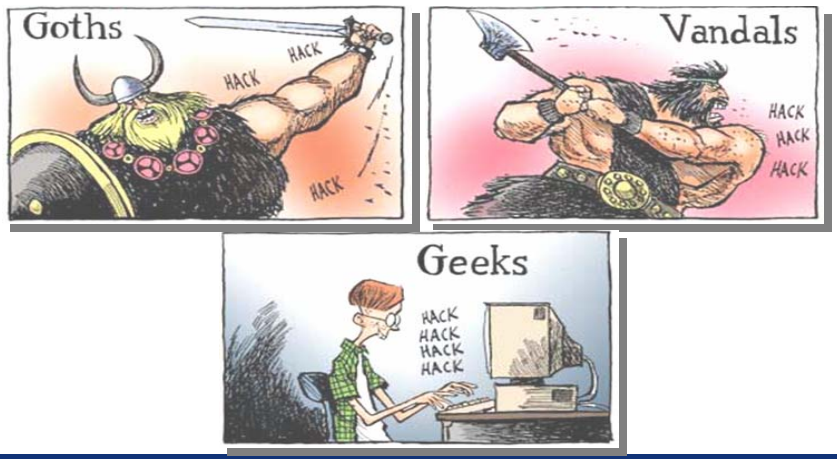
Booz | Allen | Hamilton

1

What is the impact of a security risk becoming a reality?

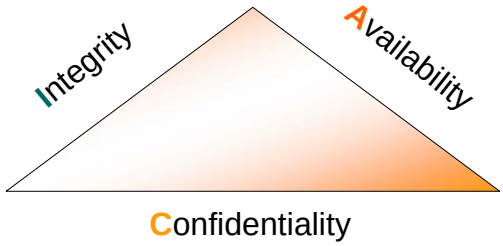
- **Reputation**
  - Confidence and credibility of clients, partners, investors
- **Litigation**
  - Business interruption, confidentiality
- **Compliance**
  - GLBA, SOX, HIPAA, NERC, etc
  - Directors, management, auditors
- **Service**
  - Capacity to serve customers and maintain confidential data
- **Productivity**
  - Employee dependency
- **Technology**
  - IT Staffing, expertise, infrastructure

Do we really know who developed the software we are using?



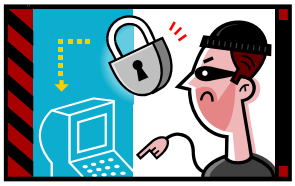
What is Security and what is adequate?

"The protection of computer hardware and software from accidental or malicious access, use, modification, destruction, or disclosure. Security also pertains to personnel, data, communications, and physical protection of computer Installations." [IEEE]



Defining and collecting meaningful quantitative information security metrics is a challenge

- Value is perceived to be what didn't happen and we can't measure that!
  - How many attacks did we prevent?
  - How many lives did we save?
- And more unintended consequences
  - We've had fewer incidents – we can cut the funding



These efforts are often compliance driven with pre-defined performance measures

	2005	2004		2005	2004
AGENCY FOR INTERNATIONAL DEVELOPMENT	A+	A+	DEPARTMENT OF COMMERCE	D+	F
DEPARTMENT OF LABOR	A+	B-	DEPARTMENT OF JUSTICE	D	B-
SOCIAL SECURITY ADMINISTRATION	A+	B	NUCLEAR REGULATORY COMMISSION	D-	B+
OFFICE OF PERSONNEL MANAGEMENT	A+	C-	DEPARTMENT OF TREASURY	D-	D+
ENVIRONMENTAL PROTECTION AGENCY	A+	B	DEPARTMENT OF ENERGY	F	F
NATIONAL SCIENCE FOUNDATION	A	C+	DEPARTMENT OF VETERANS AFAIRS	F	F
GENERAL SERVICES ADMINISTRATION	A-	C+	DEPARTMENT OF HEALTH AND HUMAN SERVICES	F	F
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	B-	D-	DEPARTMENT OF THE INTERIOR	F	C+
SMALL BUSINESS ADMINISTRATION	C+	D-	DEPARTMENT OF DEFENSE	F	D
DEPARTMENT OF TRANSPORTATION	C-	A-	DEPARTMENT OF STATE	F	D+
DEPARTMENT OF EDUCATION	C-	C	DEPARTMENT OF HOMELAND SECURITY	F	F
HOUSING AND URBAN DEVELOPMENT	D+	F	DEPARTMENT OF AGRICULTURE	F	F

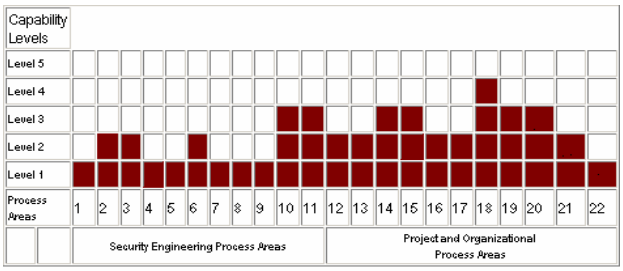
Is this the intended result of FISMA legislation?

Booz | Allen | Hamilton

6

Software measurement techniques can be applied to security measurement within individual project and organization context

- Capability based assessments
  - Capability Maturity Model Integration (CMMI)
  - System Security Engineering Capability Maturity Model (a.k.a., ISO/IEC 21827)
- Measurement and Analysis Process Area
- Goal Question (Indicator) Measure (GQ(I)M)
- Practical Software and System Measurement



Booz | Allen | Hamilton

7

A CMM can be used as a measurement tool to identify risks related to an organization's ability to deliver

- Basis for evaluation of organizations to establish organizational capability-based confidence in results
  - Continuity
  - Repeatability
  - Efficiency
  - Assurance
  - Sustainability
- Standard mechanism for customers to select appropriately qualified security engineering providers

Security Engineering: www.sse-cmm.org

Systems/Software Engineering: www.sei.cmu.edu/cmmi/cmmi.html

The purpose of the CMMI Measurement and Analysis Process Area is to develop and sustain a measurement capability that is used to support management information needs

- SG 1 Align Measurement and Analysis Activities
  - SP 1.1 Establish Measurement Objectives
  - SP 1.2 Specify Measures
  - SP 1.3 Specify Data Collection and Storage Procedures
  - SP 1.4 Specify Analysis Procedures
- SG 2 Provide Measurement Results
  - SP 2.1 Collect Measurement Data
  - SP 2.2 Analyze Measurement Data
  - SP 2.3 Store Data and Results
  - SP 2.4 Communicate Results

Goal Question Indicator Measure (GQIM) can help you determine what to measure

Goals

Questions

Indicators

Measures

GQ(I)M can be applied to information security

Defects that are vulnerabilities identified in requirements, design, and test reviews

Reduce the number of vulnerabilities

Goal

Measure

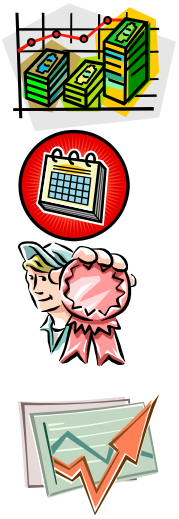
Question

Indicated by a decrease in defects that are vulnerabilities found later in the lifecycle?

How many of our defects contribute to security vulnerabilities?

Start Small

- Apply the basics like Cost, Schedule, Quality, and Growth to your security activities in addition to your project activities
- Start with a manageable, small set of security measures
- Add security measures as the project learns
- Train data collectors to apply their knowledge to security or train security staff to become data collectors (methodology, domain, and behavior)



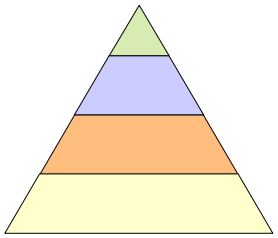
Measure Process Behaviors As Well As Results

- Measurement changes behavior
- Measuring only results produces unintended consequences
- Identify and measure best and worst practice behaviors
- People are in direct control of behavior
- ***Result***: Defect (i.e. Code vulnerabilities) found per unit size goes down
- ***Behavior***: Defect (i.e. Code vulnerabilities) detection effort per unit size is maintained

Get Senior Management Support

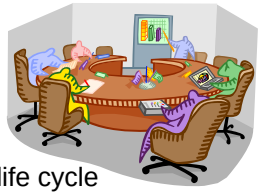
- Obtain tangible support for security measures development and use at every management level
- Maintain support through regular graphs and analysis reporting to management stakeholders (and customers?), tailored to their levels
  - Higher management's measures and analysis must address the goals at their level
  - Reduce detail further up the management chain

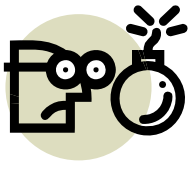
Remember: You don't need to share everything you are collecting!



Integrate security measurement into life cycle just like you already integrated software measurement

- Regular meetings, throughout project life-cycle
- Measure and analyze during each phase
- Measure and analyze functional areas
- Cost and schedule measures should span the entire life cycle
- Incorporate security measures into your existing measurement activities
- Assurance is so much more than counting defects





Use standards and best practices as sources for security goals, questions, and measures

United States

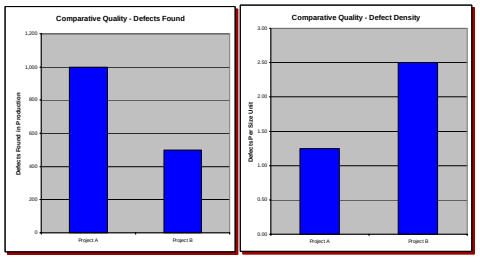
- NIST Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST Special Publication (SP) 800-27**,** *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A*
- NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*
- NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*

Internationally

- ISO/IEC 27001, *Information Security Management System (ISMS) Requirements*
- ISO/IEC 21827, *System Security Engineering Capability Maturity Model (SSE CMM)*
- ISO/IEC 18028, *IT network security*
- WD ISO/IEC 27004, Information Security Management Measurement
- CD ISO/IEC 27005, *Information Security Risk Management*
- ISO/IEC 15408, *Evaluation criteria for IT security* (a.k.a, Common Criteria)
- ISO/IEC 15443, *A framework for IT security assurance*

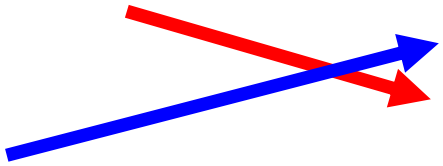
Normalize

- Compare apples to apples by normalizing
- Normalizing often means finding a rate (A per B)
  - Example If Product A has 1000 defects (i.e. Code vulnerabilities) and Product B has 500 defects (i.e. Code vulnerabilities), is A better?
  - What if Product A has a size of 800 while Product B has 200?
  - Product B has a higher concentration of defects, despite a lower, unnormalized count



Triangulate

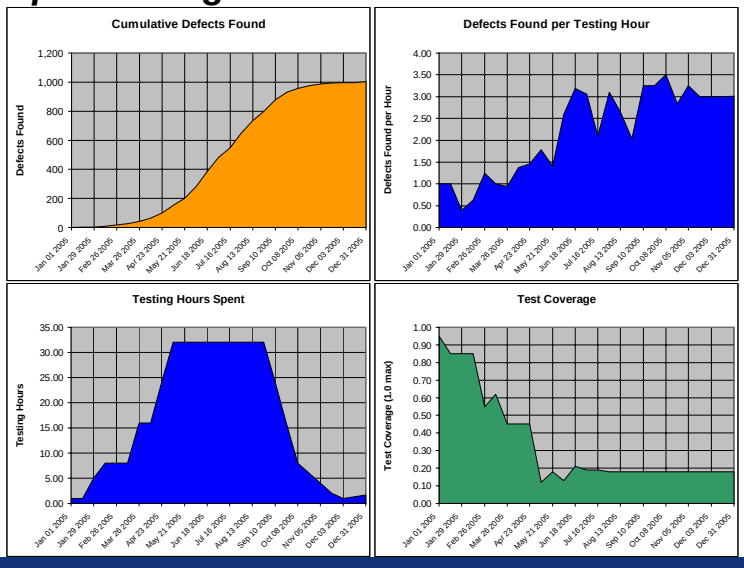
- Triangulation prevents **unintended consequences**
- Target an attribute (e.g., quality, efficiency) using several related measures
- Example: Defect (i.e. Code vulnerabilities) density is going down as scheduled release nears. Does this mean its quality justifies going to release?
  - Measure normalized testing effort
  - Measure test coverage



Booz | Allen | Hamilton

18

Example: Triangulation



Booz | Allen | Hamilton

19

Follow Measurement Best Practices to combat the "Security Stigma"

- Protect Your Sources
  - Measure processes, not people
  - Even the appearance of measuring people kills the measurement program
  - Aggregate individuals' data where necessary
  - Violating this principle will yield fiction as measurements, or no measures at all

- Close the loop
  - Data providers need the results – give feedback that the data is useful
  - Lack of feedback leads to late or missing data
  - Lack of feedback to supporting management leads to loss of funding or resources
  - Infrequent data reporting intervals lead to late reporting
  - The more immediate and actionable is the feedback, the more interested are the participants

There is no magic list of measures…. So now what?

- In the Operations Environment were we must measure things for compliance, we could avoid unintended consequences by ….
  - Reverse engineer compliance measure to the goals that support spirit and intent of legislation
  - What is the business goal we are trying to achieve?
  - Normalize and Triangulate so we know more about our security risk environment
- While we're building or buying the system ….
  - Determine our security assurance goals for our organization and use GQM
  - Derive goals from standards and use GQM
  - Enhance existing measures by asking security related questions (How many of our defects contribute to security vulnerabilities?)

For More Information

CMMs

- ISO/IEC 21827 www.issea.org
- CMMI www.sei.cmu.edu/cmmi/Information

- Information Assurance
  - https://buildsecurityin.us-cert.gov/daisy/bsi/438.html
  - http://www.xisec.com/
  - http://iac.dtic.mil/iatac/
  - http://www.iatf.net
  - http://www.nist.gov
  - http://www.sei.cmu.edu/programs/nss/nss.html

Michele Moss
Associate

Booz | Allen | Hamilton

8283 Greensboro Drive
McLean, VA 22102
Tel (703) 377-1254
moss_michele@bah.com

Riley Rice
Associate

Booz | Allen | Hamilton

8283 Greensboro Drive
McLean, VA 22102
Tel (703) 902-6781
rice_riley@bah.com