
Information Security Metrics - an Overview

Presentation to ISACA, Edmonton Chapter
Edmonton, Canada

By Matunda Nyanchama, PhD, CISSP
Agano Consulting Inc.

© Copyright 2009 Agano Consulting Inc.

This material is intended ONLY for participants at ISACA, Edmonton Chapter. Any copying, transmission and circulation in any form need express permission from Agano Consulting Inc. contact: info@aganoconsulting.com

Matunda Nyanchama – Short Bio

- Principal Consultant/Director, Agano Consulting Inc. - www.aganoconsulting.com; publisher Nsemia Inc. Publishers – www.nsemia.com); technical author and commentator
- Experience:
 - 12+ years in consulting – IT & IT Security with focus on financial services and security product development
 - 7+ years in telecommunications engineering
- Previous positions held
 - Delivery Project Executive/Senior Delivery Program Manager: Managed IT Services, Global Technology services, IBM Canada; sessional faculty (Msc Security Program) University of Ontario Institute of Technology UOIT; Senior Manager of Information Security, Moneris Solutions Inc.; Senior Manager, Bank of Montreal Financial Group; Director, Security Architecture, Intellitactics Inc.; Senior Consultant, Ernst & Young LLP & Executive Engineer, Kenya Posts & Telecommunications Corporation (Kenya)
- Certified Information Systems Security Professional (CISSP)
- Msc. & PhD, Computer Science (UWO), Bsc. Electrical Engineering (UoN, Kenya)
- Contact: mnyanchama@aganoconsulting.com

Agano Consulting Inc. – A profile

- IT Consulting Company
 - Based Canada
 - With “tentacles” in East African Region
- Key focus areas
 - IT (specifically Info Sec) Training
 - IT consulting – Strategy, Architecture, Information Security & Risk Management
 - Strategic Planning for SMB, NGOs
 - Market Research – IT Market Trends
 - Strategic Advice & Strategic Planning
- Sectors
 - Government/Public, Non-Government & Private

Agenda

1. Quick Introduction
2. Recent Research Findings
3. Some Working Definitions
4. The Need for Security Metrics
5. Examples of what to measure
6. Metrics Development Process
7. Some Caveats
8. Summary
9. Discussions

Recent Research Findings

- **Security breaches at Canadian firms**
 - account for an average annual loss of \$834,149 per firm
 - a 97% increase from the \$423,469 average cost in 2008.
 - Average # of breaches rose from 3.0 in 2008 to 11.3 in 2009
- **Government organizations**
 - average annual cost of breaches was \$1 million in 2009, up from \$321,000 in 2008.
- **Private companies**
 - average annual cost of breaches was \$807,000 in 2009, up from \$294,000 in 2008
- Publicly traded companies
 - 6% year-over-year increase
- The average cost per breach
 - was to \$75,014 in 2009, down from \$213,926 in 2008 for publicly traded companies

Source: Telus-Rotman School of Business report of October 2009

The Need for Measurements

“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 ...” - Lord Kelvin (circa 1870)

Definitions – I

- **Metric**
 - “relating to measurement; involving, or proceeding by, measurement” (*Webster’s Revised Unabridged Dictionary*)
- **Information Security**
 - pertains to integrity, confidentiality & availability; auditability and accountability
- **Information Security Metric**
 - “A measurable attribute of the result of a [information] security engineering process that could [be] evidence its effectiveness.”
- **Effectiveness**
 - having an intended/expected effect; operative; in effect; efficacy, force, punch, power, strength, success, validity, vigor, weight (*The American Heritage Dictionary*)

“If you cannot measure it, you cannot improve it.” – Lord Kelvin

Definitions – II

- **Efficiency**

- production of desired effect/results with minimum waste of time, effort, or skill ;
- a measure of effectiveness; specifically, useful output/input;
- proficiency, capability, adeptness, adequacy, suitability (*The American Heritage Dictionary*)

- **Benchmark**

- reference, a standard by which something is measured; criterion, gauge, goal, measure, standard, touchstone, yardstick

- **Return on Investment (ROI)**

- a measure of profitability; it measures how effective a company uses its capital to generate profit; income that an investment provides in a specified time (e.g. one year)

- **Return on Security Investment (ROSI)**

- A measure of how effective investment in security benefits the company

The Need for Security Metrics – Summary - I

- **Strategic support**

- Security assessments can aid different kinds of decision making, e.g. program planning, resource allocation, & product and service selection.

- **Quality assurance**

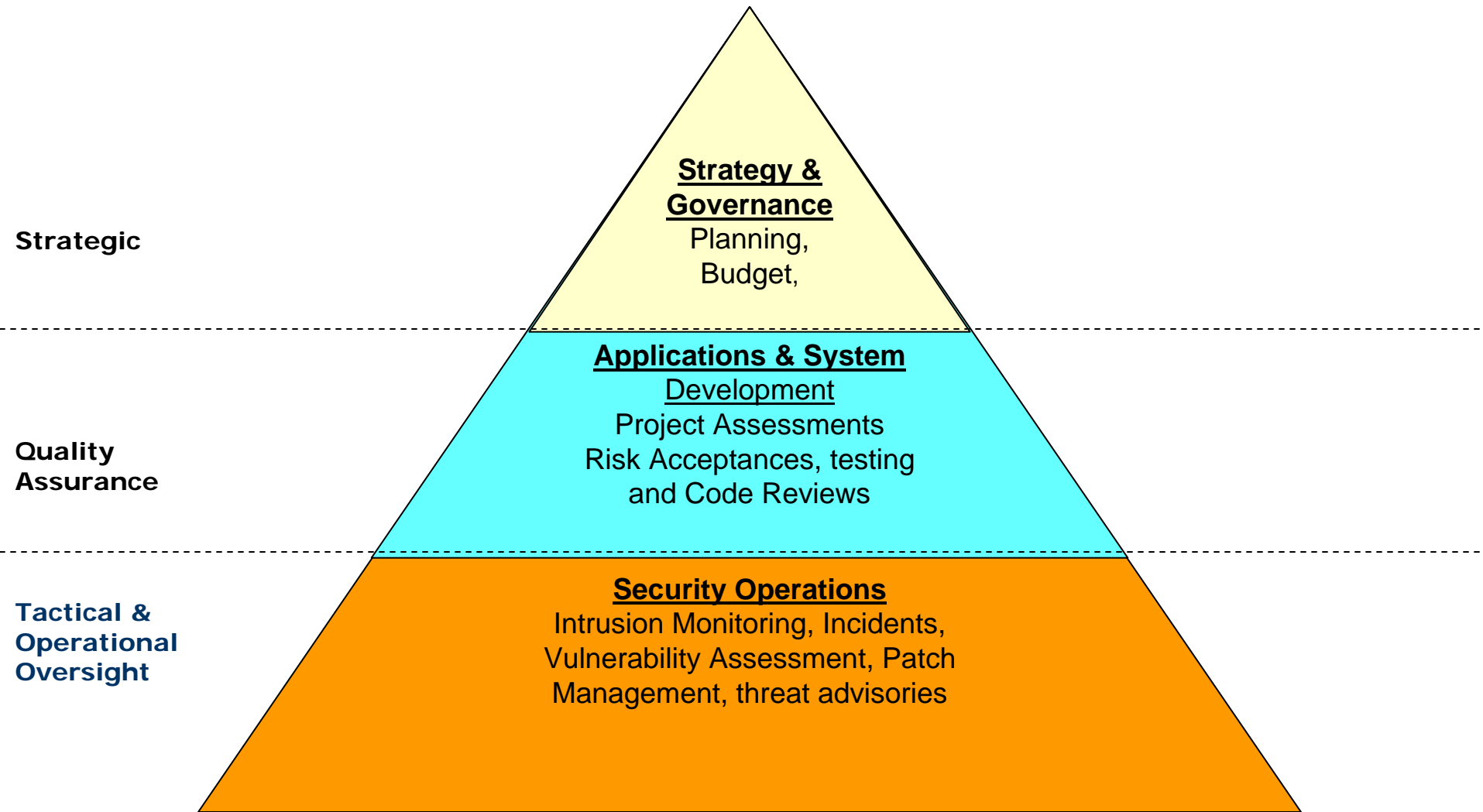
- Applied to SDLC to eliminate vulnerabilities; measuring adherence to secure coding standards, identifying likely vulnerabilities that may exist, and tracking and analyzing security flaws that are eventually discovered.

- **Tactical [& Operational] oversight**

- Monitoring & reporting of the security posture can determine compliance with security requirements (e.g., policy, procedures, and regulations), gauge the effectiveness of security controls and manage risk, provide a basis for trend analysis, and identify specific areas for improvement.

Source: Wayne Jensen - NIST

The Need for Security Metrics – Summary - II



The Need for Security Metrics - I

- **Establish a baseline for monitoring & improvement.**
 - An organization that understands its security posture, likely understands its level of security risk.
- **Assess the effectiveness of controls & gaps thereof**
 - How well are implemented controls working? What are the gaps? What're risks associated with gaps?
- Help with **decision making:**
 - What are the shortcomings? How closely are objectives met? What gaps if any? Need change of direction?
- **Risk Identification**
 - What assets need protection? What is their value?
 - What threats and vulnerabilities exist to the assets?
 - What chances for exploitation exist?
 - What's the likely impact?

What gets measured, [is likely to] gets done.

The Need for Security Metrics - II

- **Risk Management**
 - Risk assessment - extent of exposure to threats + potential business impacts should attacks happen
 - Controls - What countermeasures/controls to identified risks
 - Controls assessment - How effective are those controls
- **Identify priorities**
 - resource deployment based on risk levels to assets
- **Facilitate corrective action**
 - What are the weak controls that need to be fixed
- **Demonstrate performance & accountability**
 - How well is security investment used? To what extent are performance measures realized? Who is accountable?

"Metrics are tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data." – Swanson - NIST

The Need for Security Metrics - III

- **Compliance**
 - Legislative compliance (e.g. SOX); internal and external audits
- **Aggregate detailed technical data for management's consumption:**
 - Averages, trends, impact, summaries, etc. is more useful to management than detailed technical data.
- **Budgets & influence decision makers**
 - Budget justification & support for new initiatives
 - Efficiency & effectiveness of previous expenditures for ongoing programs
 - How new expenditures would be used based on cost-benefit analysis;
- **Demonstrate the value of information:**
 - Return on Security Investment (ROSI)

Repeatable and consistent metrics can be extremely valuable -- even if they're "inaccurate". - Wes Sonnenreich, SAGE LLC

The Need for Security Metrics - IV

- **Benchmark against industry**
 - How does an organization compare with peers?
- **Track security posture trends**
 - Is the “state of security” improving, staying the same or getting worse?

“If you don’t know where you are going, any road will take you there!”

– Lewis Carroll

“If you don’t know where you are going, you might end up in some place!”

– Yogi Berra

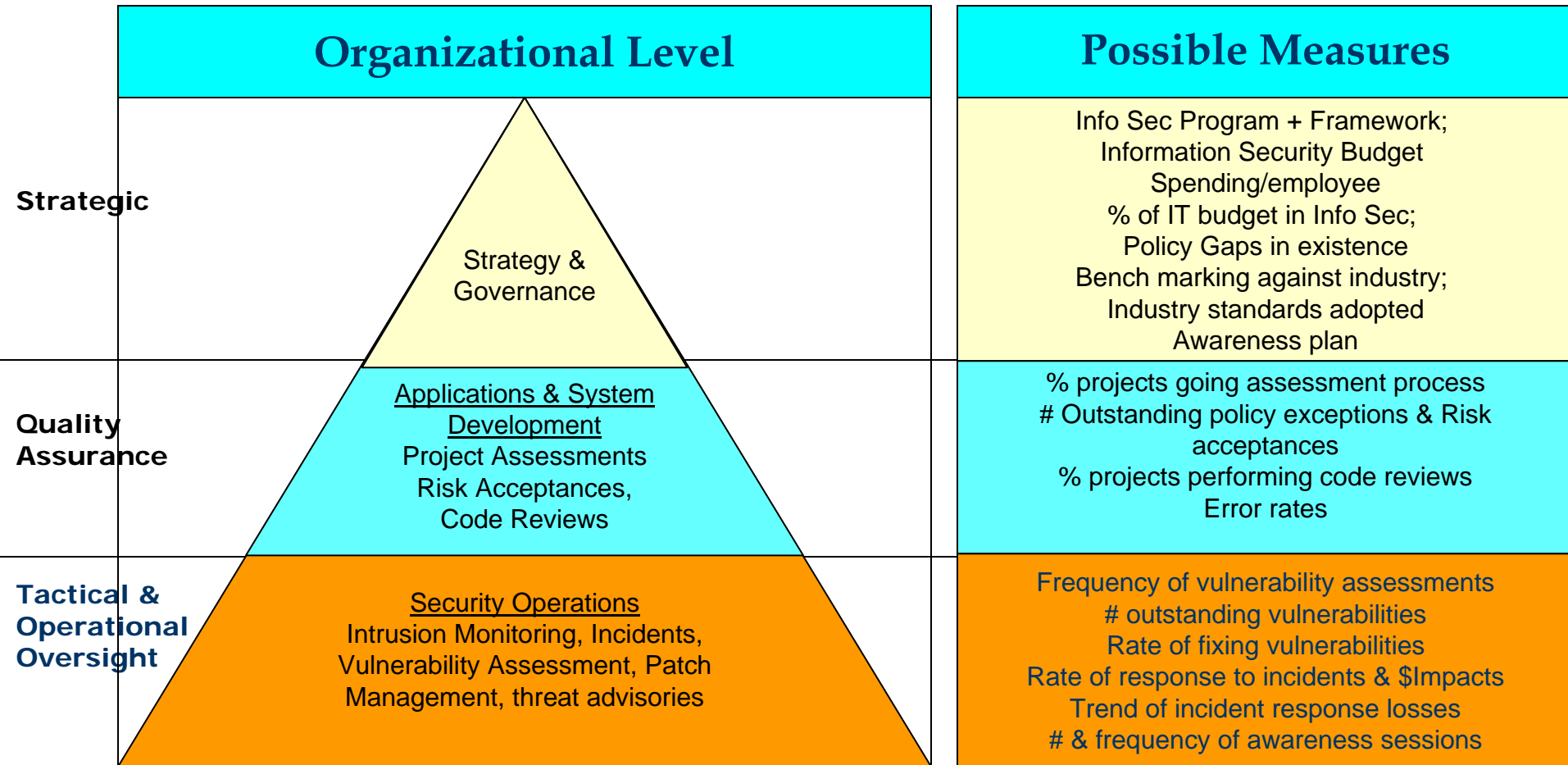
Attributes of Security Metrics

- Metrics capture **measurable attributes** in support effectiveness & efficiency
- Metrics can be **objective** or **subjective**; they can be **quantitative** or **qualitative**.
- Should be **SMART**: **S**pecific, **M**easurable, **A**ttainable, **R**epeatable & **T**ime-independent

“IT security metrics must be based on IT security performance goals and objective.” – Swanson - NIST

What Do You Measure?

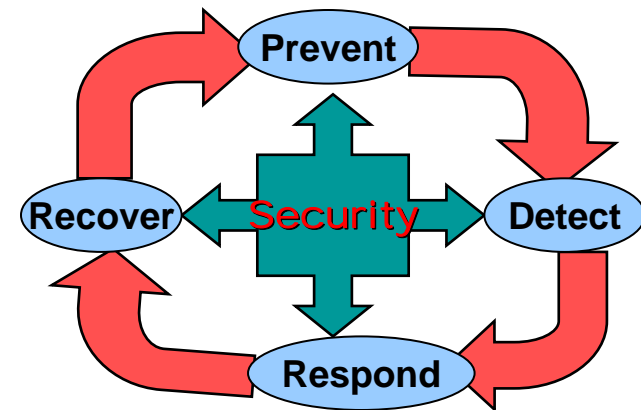
What to Measure?



What to Measure?

Objectives/Goals of Security	
Prevention	Prevent attackers from violating security policy; Prevent attack from taking place
Detection	Detect violation of a security policy, e.g. detect an attack
Response	Respond to stop an attack (or violation of security policy) and hence prevent damage
Recovery	Assess and repair damage; continue to function correctly even if attack succeeds; recover from an attack, including root cause analysis

For of the elements of the security "life cycle" develop metrics that meaningfully measure effectiveness of controls.

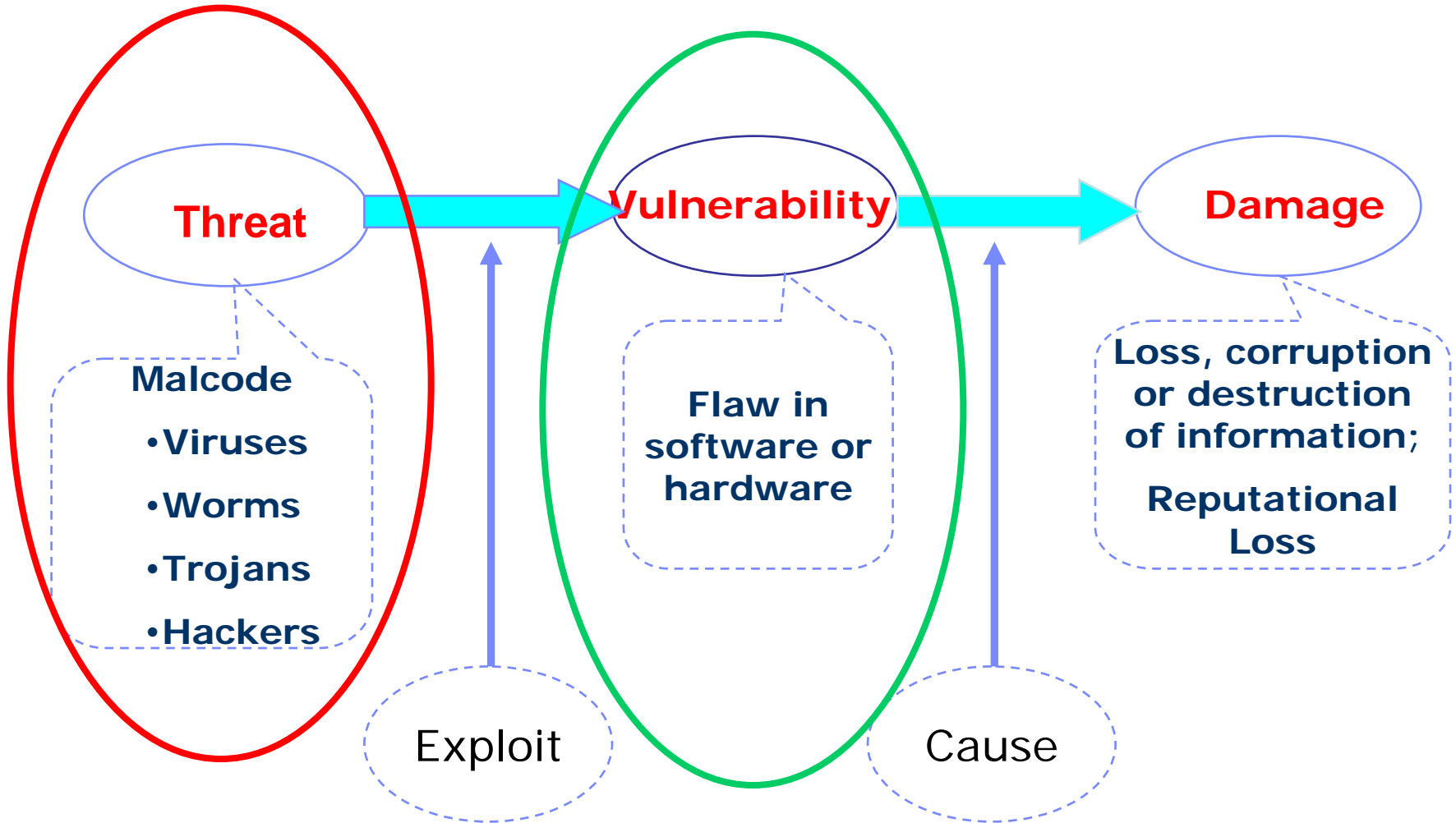


What to Measure? – ISO 17799 View

ISO Area	Sample Measurements
Security Policy	Gaps in policies; Potential impacts of policy gaps; # security violations per period of time.
Security Organization	% staff with certification; formal roles and responsibilities; staff turnover; security spending/employee; IS spending as % IT budget
Asset Classification & Control	% assets in inventory; % assets with classification; % assets with valuation; % assets with protection plan
Personnel Security	# security training sessions; level of security awareness; # of personnel security-related incidents
Physical & Environmental Security	Frequency of review of physical access; # access anomalies or violations
Communications & Operations Management	# incidents; incident impacts; frequency of assessment; % systems with exposures; incident response metrics; how quickly threats are communicated; frequency of awareness activities; change control issues
Access Control	Access activation/termination turnaround; % of expired accounts; % accounts with expired pwds; % of accounts with weak passwords
Systems Development & Maintenance	% projects that use IS; # policy exceptions/risk acceptances; % projects that perform code reviews; freq. of VAs; % systems with vulnerabilities
Business Continuity Management	% systems with BCP/DRP; frequency of BCP/DRP testing; % systems that pass BCP/DRP testing; System availability
Compliance	# & trend of exemptions; cumulative penalties and trends

Some Examples

The Threat-Vulnerability-Damage Chain



Example - Quantitative Risk Analysis

- **The result of the quantitative Risk analysis:**
 - Assign monetary values for each asset
 - Develop a comprehensive list of significant threats
 - Estimate the probability of each threat occurring
 - Compute the loss potential for the company on a per-threat and per threat basis over 12 months; and per .
 - Add per threat potential loss to obtain cumulative loss potential for the company for all threats on all assets
 - Recommend safeguards, control, actions, and costs thereof; develop cost/budget-justification based on the risk
 - Track these year after year for trending purposes

Example – Return on Security Investment (ROSI)

- **Annual Loss Expectancy:**

- $ALE = SLE \times ARO$

- **Return on security Investment:**

- $ROSI = (ALE^* \text{ before control}) - (ALE \text{ after control}) - \text{annual cost of controls.}$

- Track and trend this from year to year

A simple equation for calculating the Return on Investment for a security investment (ROSI) is as follows:

$$ROSI = \frac{(\text{Risk Exposure} \bullet \% \text{ Risk Mitigated}) - \text{Solution Cost}}{\text{Solution Cost}} \quad (2)$$

Source: Wes Sonnenreich

ALE = Annual Loss Expectancy

SLE = Single Loss Expectancy

ARO = Annual Rate of Occurrence

Example – Effectiveness of ID Admin

- Security admins given instructions on add/change/move for IDs
- Quality assurance checks and tracks errors
- Calculates error rates and trends this
- Uses these trends for root cause analysis
 - Unclear instructions
 - Poor system admin “workmanship”
 - Failure to understand/follow instructions
- Use error rates to calculate productivity
- Track this on a regular basis to determine whether there are improvements; if not, seek root cause

Metrics – Breadth, Depth & Meaning

- *"What you measure is what you get, ... the results of measurement are as good as the data collected"*
 - R. S. Kaplan & D. P. Norton in *"Putting the Balanced Scorecard to Work"*
- *"Not everything that can be counted counts, and not everything that counts, can be counted."*
 - Albert Einstein
- You can have **too many or too few** measures?
- Measures can be **too specific or too general**
- Usefulness of information **depends of meaning** derived from the metrics

Metrics – Breadth, Depth & Meaning (Cont'd)

- Top-down
 - E.g. based on management objectives
- Bottom up
 - E.g. incident/intrusion data that is then aggregated
- Metrics useful at one level in the organization may not mean much at another level; ensure that generated reports make sense for the purpose for which they were meant
 - Detailed intrusion data may be good for technical people
 - Trends, summaries and aggregates suit management
- Metrics selected should serve a purpose; this should lead to required data.
- Measurements in any specific area of Information Security can be onerous

Metrics Development Process

Follow ISO17799's "plan-do-check-act" cycle

- **Plan**

- Establish key objectives for the metrics required
- Identify the required metrics and hence required data
- Design & implement strategy for data collection & metrics generation
- Establish targets/benchmarks; where possible compare with industry
- Determine the process for collecting and analyzing data, and reporting
- Establish metrics review program, and the refinement process/cycle

- **DO**

- Communicate with stakeholders and ensure buy-in
- Implement the metrics program – people, process and technology

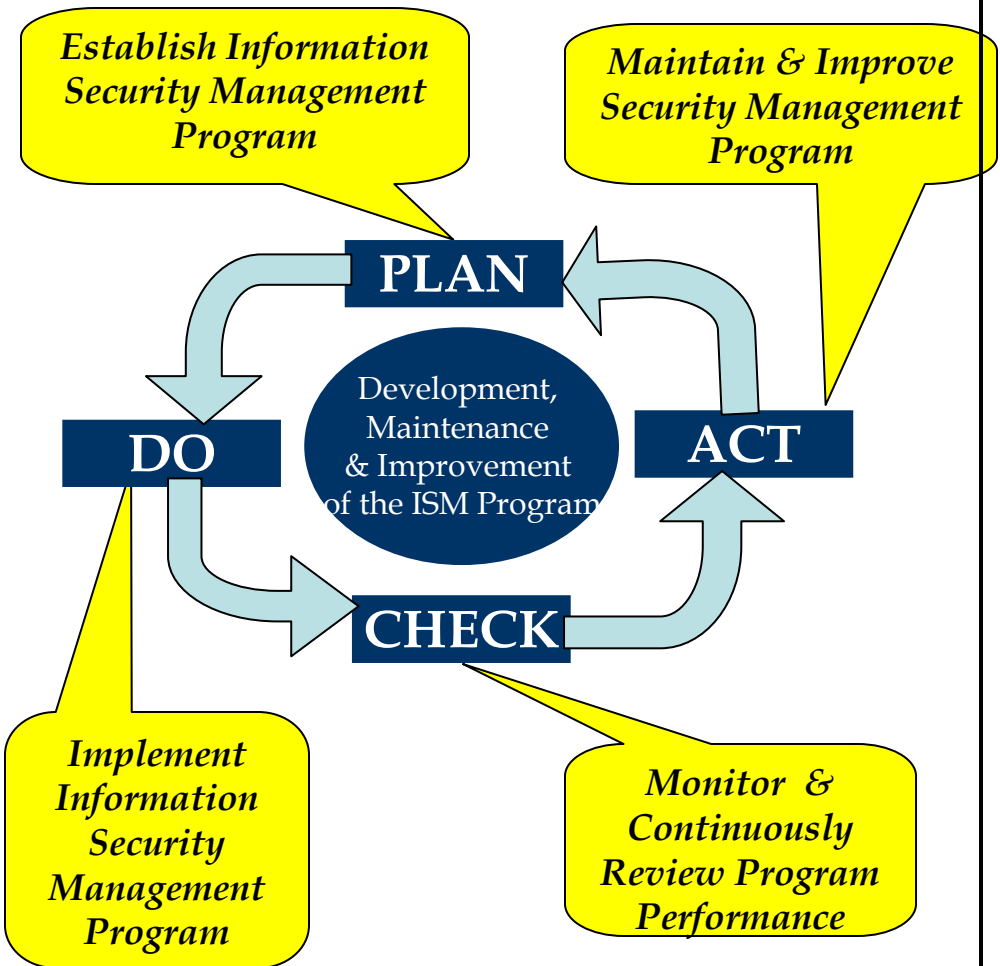
- **CHECK/Monitor**

- Continuously review metrics report against objectives and benchmarks
- Monitor program performance against objectives and benchmarks
- Identify gaps, if any, in the program

- **ACT**

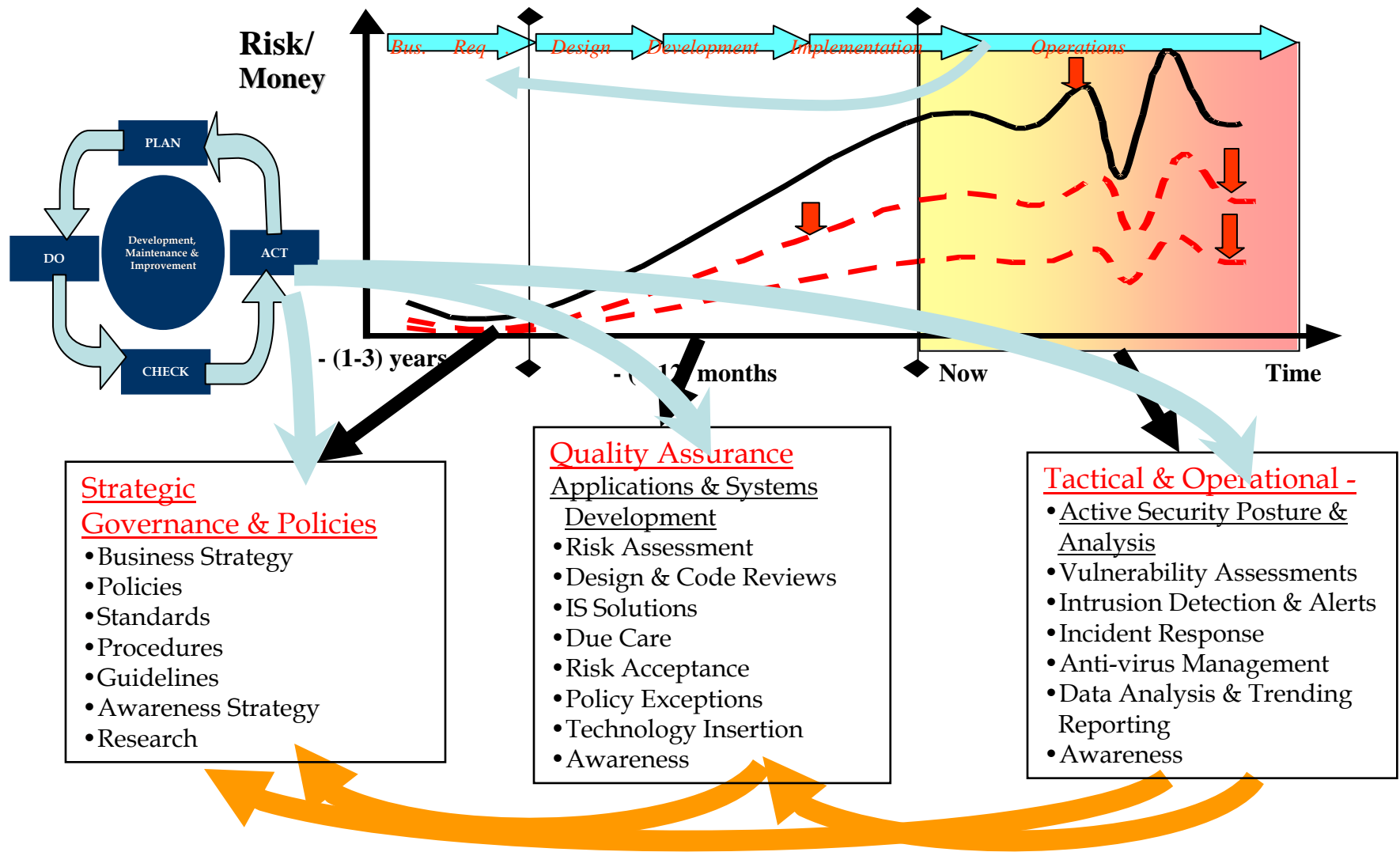
- Address gaps in program
- Refine specific metrics, where necessary
- Refine metrics program, where necessary

Elements of an IS Program –IS Management Life Cycle



- Key Security Program Elements
- Strategic**
- Governance, Policies & Business Strategy
 - Strategy, Policy, Procedures, Standards, Awareness Plan
- Quality Assurance**
- Risk Assessment, Design Reviews, Due Care, New Technology Insertion, Risk Acceptance, Policy Exceptions, Code reviews
- Tactical & Operational**
- Active Security: Intrusion Detection & Alerts, Incident Management, Vulnerability Assessments, Data Aggregation & Analysis, Trending, Root Cause Analysis; what takes place daily captures the robustness or weakness of controls, e.g. incidents, external events

Information Security - Another View



Sources of Data for Metrics

Information Security

Vulnerability Assessments
Incident data
Intrusion detection statistics
Antivirus statistics
Project assessment reports
Policy exceptions & risk acceptances
Education & Awareness data
Risk control self-assessment
Access management reports

Organization Units

Log analysis exceptions
Corporate security reports
Risk control self-assessments

Risk Management Groups

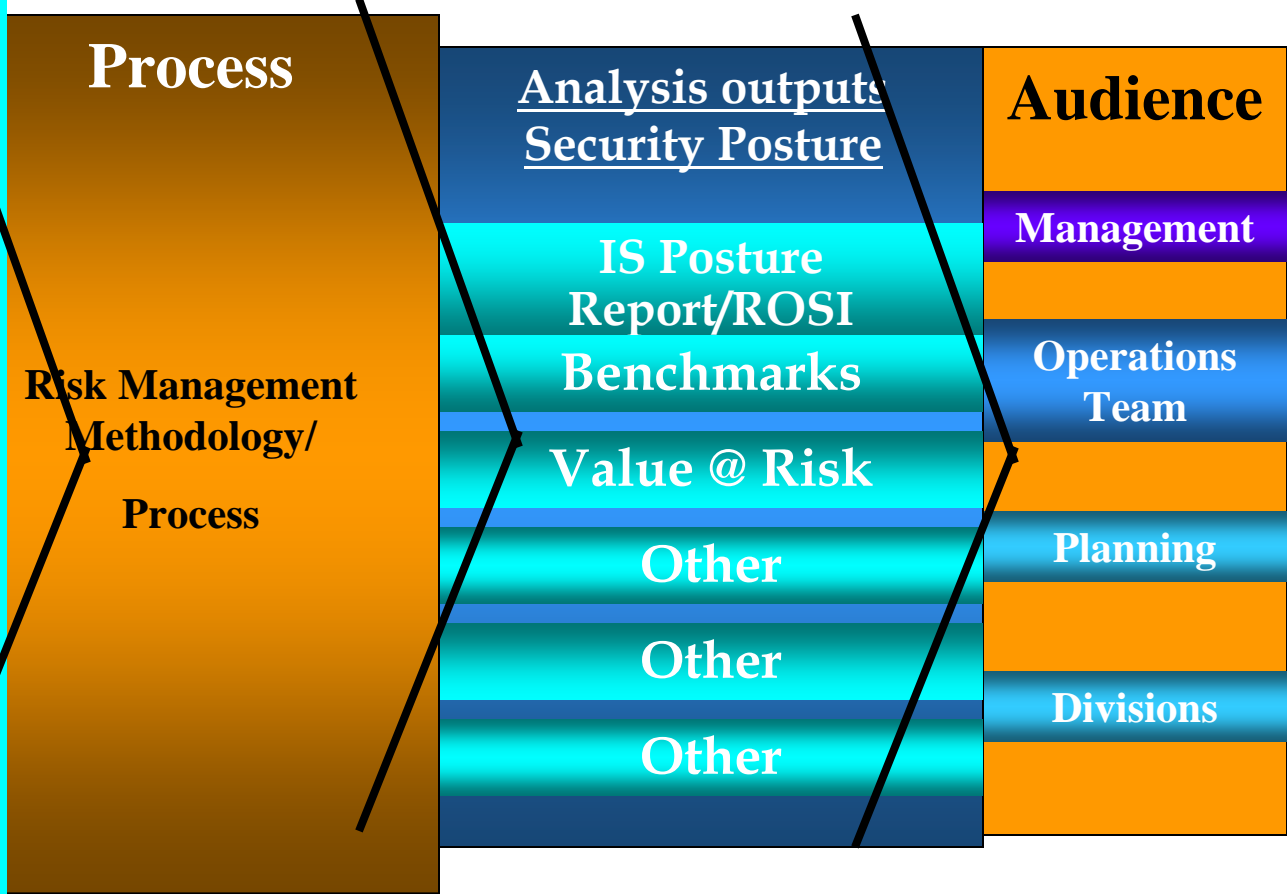
Audit - external & internal
Configuration management

IS Reporting

Risk Assessment Reports
IS Posture

IS Metrics Process & Reporting

- Information Sources**
- Assessments – projects, systems, infrastructure
 - Policy reviews
 - Vulnerability Assessments
 - Intrusion detection statistics
 - Incident Response Data
 - Anti-virus statistics
 - Access Management
 - Systems (physical & logical) Logs
 - Audit reports – ext/Int.
 - Security Investigations
 - Self Assessments
 - Corporate Security Reports



Adopted from Marc Stefaniu – see references

Example – Incident Data

- Incidents that took place within a reporting period? E.g. total number of incidents; number of incidents of high, medium & low impact;
- Percentage of total incidents with high material (high, medium) impact;
- Associated business impacts (monetary and otherwise);
- Losses (tangible & intangible) were incurred as a result of the incidents;
- Incident losses comparison with industry for similar types of businesses and size;
- Failures in security controls that led to the incidents:
- Whether or not the failures have been fixed; outstanding gaps;

Incident Data (Cont'd)

- Improvement plans/processes are underway to prevent future recurrence of similar incidents?
- The trend to date:
 - Is the situation getting better or worse?
- An incident dashboard would have the following:
 - Current incident posture (#incidents, monetary impacts, etc.)
 - Trend from last reporting period (are things getting better or worse?)
 - Overall trend to date
 - Comparison with industry benchmarks
 - Impact of past improvement plans
 - Existing gaps between desirable risk levels and current posture

Sample Incident Management Dashboard

	Total #	High Impact	Medium Impact	Low Impact	Monetary Costs (\$)
Incident Posture	12	2	6	4	\$100K
Trend from last report					
Trend to date					
Comparison with Bench Marks					
Net Impact of Past Improvements					
Existing (known) Gap Trends					

Cumulative Incident costs to date = \$500K

Metrics Development – Some Suggestions

- Identify the **key areas** of risk to your business and ensure appropriate focus
- Select a **few IS metrics** that make sense to your organization based on risk assessment; think of the 80:20 rule
- **Start small** collecting required data & refine with time
- Implement a program for **continuous improvement**; seek feedback on the value of the measures selected
- **Focus on outcomes**, i.e. what the analysis points to; metrics should not be ends in themselves.
- Keep abreast with **industry practices** and incorporate best practices

The State of Security Metrics

- There exists **intense interest** in IS metrics – *just search google to see # of hits*
- Most literature talks about **how to define** Info Sec metrics i.e. *qualities/properties of good metrics*; **few specifics are suggested**
- IS metrics remain **ill-defined**; industry practices may in future lead to specific IS metrics
- Most suggested measurements tend to be qualitative; quantitative measures are slowly emerging;
- Quality & effectiveness of IS program is **dependent on individual opinion and judgment**
- Debate on Return on Security Investment (ROSI) will continue for a while to come

Metrics – Some Caveats

- Ultimately IS metrics are intended to improve understanding or support decision making wrt IS posture. However,
 - They are often ill-defined and require context and process for their generation;
 - There is a risk that IS measurement can become an end in itself, i.e. the consumer of the metric may lost in the definition of the metric.
- Context is key –
 - ensure that metrics are used with intended purpose.
- Metrics should be performance indicators, assess the value of IS and offer pointers to performance improvement.
- The heterogeneous nature of infrastructures make measurements difficult
- Issues pertaining to IS change rapidly and hence measures should evolve with the changes
- The nature of threat can change with circumstances & time

Information Security Metrics Benefits Summary

- Productivity indicators:
 - Effectiveness & efficiency of a security program
 - Security return on investment (ROI) (where possible to measure)
 - Information security program maturity
- Information Security posture:
 - Collected data can be used as baseline for measurements & trending
 - Risks are identified and a business case made to address the risks
- Help define a baseline and hence deviations:
 - Apply risk management methodology for deviations from baseline
 - Quantify risk and hence plan for better risk management strategy

Used appropriately:

- Metrics can engender process improvement.
- Demonstrate value of Information Security investment, e.g. ROI
- Facilitate risk management
- Allow benchmarking with industry peers

Questions

References - I

- Ron Knode. *Security Value Metrics* – 2002. CSC Global Information Security Services.
- http://www.csc.com/aboutus/lef/mds69_off/uploads/Enterprise_Info_Risk_Management.pdf
- Paul W. Lowans *Implementing a Network Security Metrics Program*. GIAC Administrivia. www.giac.org/practical/Paul_Lowans_GSEC.doc.
- Dr. Stuart Katzke. *Security Metrics*. Computer System Security & Privacy Advisory Board. June 13-14, 2000.
- James P. Craft. *Metrics and the USAID Model Information Systems Security Program (MISSP)*.
- Christina Kormos, Natalie Givens, Lisa A. Gallagher and Nadya Bartol. *Using Security Metrics to Assess Risk Management Capabilities*.
- *Proceedings - Workshop on Information Security System Scoring and Ranking*
- Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash, and Laurie Graffo *Security Metrics Guide for Information Technology Systems*. NIST Special Publication 800-55. July 2003.
- Shirley C. Payne. *A Guide to Security Metrics, SANS Security Essentials GSEC Practical Assignment Version 1.2e*. July 11, 2001
- Workshop on Information-Security-System Rating and Ranking (WISSRR) - <http://www.acsac.org/measurement/>
- Information Security Metrics. Using Foundstone's FoundScore™ to Assign Metrics and Measure Enterprise Risk. www.foundstone.com. April 2003.

References - II

- *Proceedings*. Workshop on Information Security System Scoring and Ranking Information System Security Attribute Quantification or Ordering. May 21-23, 2001
- C. Kormos, L. A. Gallagher, N. Givans & N. Bartol. *Using Security Metrics to Assess Risk Management Capabilities*
- Wes Sonnenreich. *Return On Security Investment (ROSI): A Practical Quantitative Model*. SageSecure, LLC. NY.
- Wayne Jansen. *Directions in Security Metrics Research*, NIST. www.nist.org., NISTIR 7564.
- George Jelen. "SSE-CMM Security Metrics." NIST & CSSPAB Workshop, Washington, D.C., 13-14 June 2000; <http://csrc.nist.gov/csspab/june13-15/jelen.pdf> July 2001.
- Shirley Payne. A Guide to Security Metrics. Shirley C. Payne. *SANS Security Essentials GSEC Practical Assignment*. July 11, 2001
- Eddie Schwartz, NetForensics Inc. Measuring Security. In Computerworld July 15, 2004. <http://www.computerworld.com/securitytopics/security/story/0,10801,94524,00.html>
- Steve Foster and Bob Pacl. Analysis of Return on Investment for Information Security. www.getronics.com
- R. S. Kaplan and D. P. Norton in "Putting the Balanced Scorecard to Work"
- Marc Stefaniu – *Metrics & Executive Reporting*. CFI-CIRT Presentation; March 2004
- Rotman School of Management at the University of Toronto and Telus Corp study. 2009