

RSA[®]Conference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: GRC-R05

Measuring What Matters



Connect **to**
Protect

Lisa Young

Senior Engineer
CERT-Software Engineering
Institute-Carnegie Mellon
University



#RSAC

Notices

Copyright 2016 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM-0003301



**Carnegie
Mellon
University**

Software Engineering Institute (SEI)

- Federally funded research and development center based at Carnegie Mellon University
- Basic and applied research in partnership with government and private organizations

CERT – Anticipating and solving our nation's cybersecurity challenges

- Largest technical program at SEI
- Focused on information security, digital investigation and forensics, insider threat, operational risk, vulnerability analysis, network situational awareness, metrics, and governance



- This session
 - does not cover specific technical security metrics
 - does cover the importance of metrics tied to things that matter to the business
- Why you might want to stay for this session - if you are interested in
 - determining what to measure in support of business objectives
 - identifying risks and gaps in your current measurement processes
 - a process for developing metrics that will help you do these things

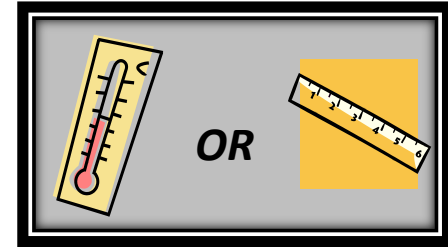
Why do you want to measure?



Terminology (*)



- Measure vs. metric
 - I had 2 eggs for breakfast this morning
 - It's 90 degrees in Las Vegas, NV
 - This workshop is 8 hours long
- A measure (or measurement) is the value of a specific characteristic of a given entity (collected data).
- A metric is the aggregation of one or more measures to create a piece of business intelligence, in context.



How secure am I?



#RSAC

- When asked:
 - How secure am I?
 - Am I secure enough?
 - How secure do I need to be?
- What does this mean?
 - How secure am I compared to my competition?
 - Am I managing my risks well?
 - Do I need to spend more \$\$ on security or risk management? If so, on what?
 - What are the PR and legal impacts of a data breach?

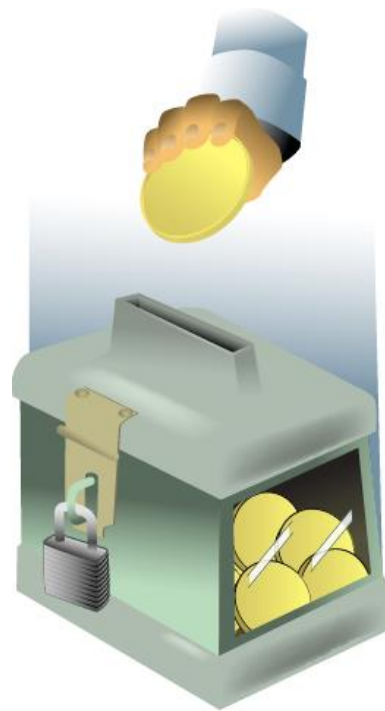


Key questions



#RSAC

- What should I be measuring to determine if I am meeting my performance objectives for security?
- What is the business value of being more secure?
 - Of a specific security investment?



So what? Why do you care?



#RSAC



- If I had this metric: (*)
 - What decisions would it inform?
 - What actions would I take based on it?
 - What behaviors would it affect?
 - What would improvement look like?
 - What would its value be in comparison to other metrics?

Barriers and challenges



#RSAC

- What current barriers do you face in establishing, managing, and/or executing a measurement program?
- What challenges do you face in identifying meaningful metrics within your organization?

Some typical technical metrics



- % of assets (systems, devices) patched
 - min/mean/max time from patch release to patch implementation
- % of scanned assets not found in the CMDB
 - Goal: 100% of assets inventoried in CMDB and reflect standard configurations
- % of devices/assets regularly scanned by anti-virus software
- number of incidents reported/closed
 - number of incidents with a known solution (patch) that was not applied
- % of assets subject to ingress/egress filtering

Some typical strategic/business metrics



#RSAC

- % of senior executives who have documented security objectives that are reviewed as part of the performance management review process
- % of security policies that are met (no violations; all exceptions approved)
- difference in planned vs. actual to perform security activities/actions/investments
 - schedule
 - resources
 - cost
- % of staff who have been assessed to determine if training has been effective commensurate with their job responsibilities



Why measure?



- Demonstrate that the security program has measurable business value
- Speak to decision makers in their language
- Answer key questions
- Demonstrate that control objectives are (and continue to be) met
- Justify new investments; improve
- Use trends to help predict future events

Who, what, where, when, why, how?



- **Who** is the metric for? Who are the stakeholders?
Who collects the measurement data?
- **What** is being measured?
- **Where** is the data/information stored?
- **When/how** frequently are the metrics collected?
- **Why** is the metric important (vs. others)?
- **How** is the data collected? How is the metric presented? How is the metric used?



Deriving metrics from objectives - GQIM





- Goal-Question-Metric (*)
 - Early work done by Vic Basili and Dieter Rombach (late 1980s, early 1990s)
- Goal-Question-Indicator-Metric (*)
 - SEI work in software engineering (late 1990s, early 2000) and operational resilience (2010 to present)

(*) [Allen 2010]

Key questions



#RSAC

- Not “What metrics should I use?”
- “What do I want to know or learn?”
- Alternatives:
 - What decisions do I want to inform?
 - What actions do I want to take?
 - What behaviors do I want to change?





- Use a defined, repeatable process to derive meaningful metrics that directly support the achievement of business objectives to:
 - demonstrate the business value of each metric (and thus justify the cost for its collection and reporting)
 - defend such metrics in comparison to others
 - add metrics, update metrics, and retire metrics as business objectives change
 - ultimately, inform business decisions, take appropriate action, and change behaviors

Key takeaways



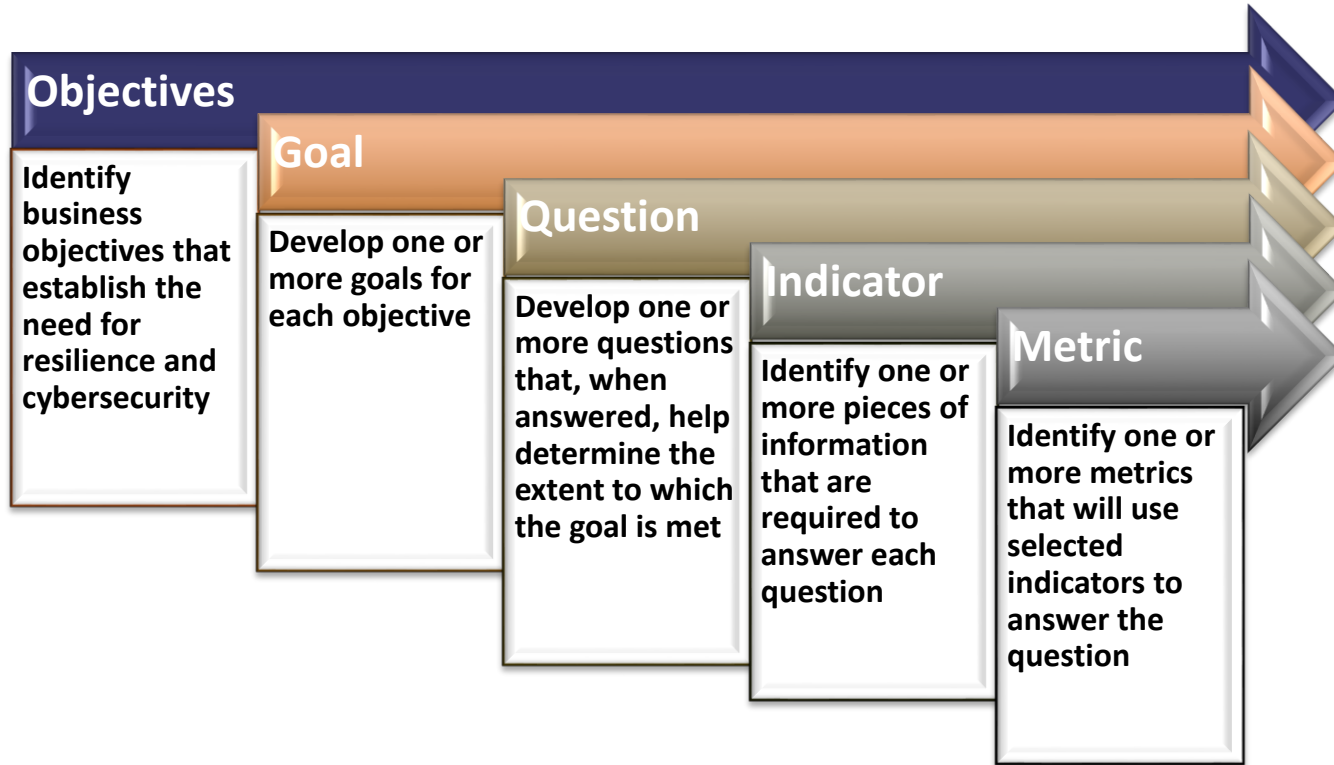
#RSAC

- Understand a 5-step process for deriving metrics from business or program objectives
- Be able to apply this process to your objective(s)
- Identify at least one metric that you can use immediately
- Be able to better communicate with business leaders in their language
- Assess the utility of current metrics

GQIM process



#RSAC





Objectives to goals





- State a business or program objective
- Define one or more goals that are required to achieve the stated objective
- Goal: the end toward which effort is directed
 - Fewer are better
 - Essential (high leverage/high payoff) vs. complete coverage
 - Judgment informed by stakeholder review

Objectives to goals



- What are meaningful actions to take to achieve the objective?
- Which actions are most important?
 - 2-3 that are essential, high leverage, high payoff
- Carry forward and further refine key terms from the objective in the goals

Ask “If I achieve this goal, will I be able to demonstrate substantive progress in achieving the objective?”

Objective to goals – incident management example



#RSAC

Objective	Goal
Mitigate the risks of business disruption and loss resulting from cybersecurity incidents (with impact threshold > [x])	<i>Operate a cybersecurity incident center that detects, responds to, and reports security incidents in accordance with established standards and guidelines.</i> <ul style="list-style-type: none"><i>enterprise and operational unit levels</i>
	Others?



Goals to questions



Goals to questions -1



- What are meaningful questions to answer to determine if the goal is being achieved?
 - Requires subject matter expertise
- Which questions are most important?
- Carry forward and further refine key terms from the goal in the question

Ask “If I answer this question, will I be able to demonstrate substantive progress in achieving the goal?”

Goals to questions -2



- Useful questions are in the form of:
 - *What is the process for . . . (better than “How does the organization . . .”)*
 - leads to implementation metrics
 - *How effective is . . .*
 - leads to effectiveness metrics
 - most desirable but need implementation metrics first

Goal to questions – IM example



#RSAC

Goal	Questions
G1: Operate a cybersecurity incident center that detects, responds to, and reports security incidents in accordance with established standards and guidelines.	Q1: <i>What is the process by which suspicious events are detected and declared as incidents?</i>
	Q2: What is the criteria for escalating high-impact incidents? To whom?
	Others?

Questions to indicators



Questions to indicators



- What data (and sometimes in what form) do I need to answer the question?
 - Can add more data granularity than called for in the question
- Which data is most important?
- Carry forward and further refine key terms from the question in the indicators

Ask “If I have this data, will I be able to answer some aspect of the question?”

Question to indicators – IM example



#RSAC

Goal	Question	Indicators
G1	Q1: What is the process by which suspicious events are detected and declared as incidents?	Q1.I1: <i>process and criteria for detecting and triaging suspicious events</i>
		Q1.I2: process and criteria for declaring incidents
		Others?

Indicators to metrics



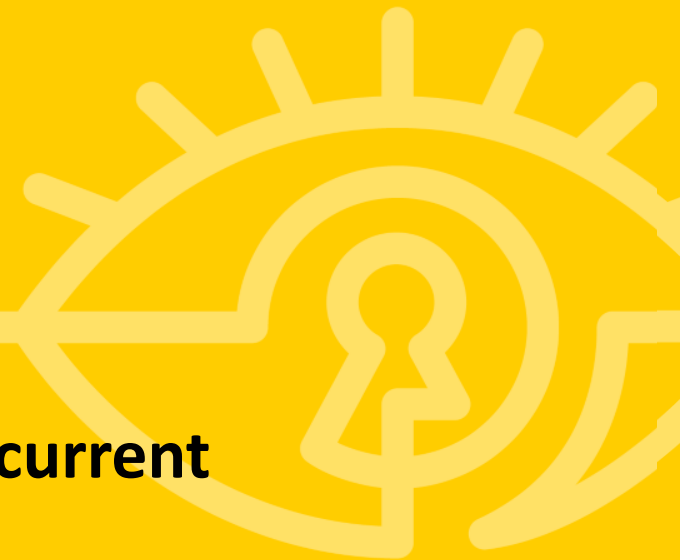


- Using the indicator data, what number, percentage, mean, or other metric can I collect/calculate to help answer the question?
 - a percentage presumes 2 numbers are available so you don't need to list the numbers as a metric if the percentage is based on it
- Which metrics are most important?
- Ask “Do I need additional data (more indicators)?”

Ask “If I report this metric (over time), will it provide the greatest insight possible to answer the questions from which it derives?”



Using this method to validate your current questions or metrics



What if I only have a metric? - 1



- **“We’ve always reported the number of machines with patches out of date.”**

- **How are you using this metric today?**

“What question will this metric answer?”

- This metric answers the following question: “How many machines are currently out of date?”

What if I only have a metric? - 2



#RSAC

“Answering this question will demonstrate substantive progress in achieving what goal?”

- The goal answered by this question is “Keep machines up to date through patching.”
- Will this goal demonstrate progress against **an existing strategic business or program objective?**

By measuring the actual time between patch release and patch application, you are able to measure your organization’s ability to improve patch capability.



Using GQIM to Restate



#RSAC

- **Strategic Business Objective:** Mitigate the risk of successful software exploits by minimizing out-of-date software systems.
- **Goal:** Improve my organization's process for patch management
- **Question:** How effective is my patch management process?
- **Indicator:** Increased efficiencies in the patch management process
- **Metric:** Actual time between patch release and patch application.

What if all I have is a question? - 1



#RSAC

- **“I’m always asked if my users have the proper level of system access.”**
- **How are you answering this question today?**
- If the answer to this question is yes, what is the goal I am trying to achieve?
 - **Goal: Ensure all users have the proper level of system access for their job responsibilities.**

What if all I have is a question? - 2



#RSAC

- What is the strategic business objective tied to this goal?
 - Strategic business objective: Mitigate insider threats by ensuring appropriate levels of system access for all users.
- What data would I need to answer the question: “Do all users have appropriate system access?”
 - Inventory of IT systems with required security and access attributes
 - Current list of users with approved security attributes
 - An ability to compare IT systems access and users list

Using GQIM to Restate



#RSAC

- **Strategic Business Objective:** Mitigate insider threats by ensuring appropriate levels of system access for all users.
- **Goal:** Ensure all users have the proper level of system access for their job responsibilities.
- **Question:** Do all users have appropriate system access?
- **Indicators:**
 - Inventory of IT systems with security and access attributes
 - Current list of users with approved security attributes
 - An ability to compare IT systems access and users list
- **Metrics:** (more user centric)
 - Time (min, max, med) to add a new system to inventory
 - Time (min, max, med) to remove access when violation is discovered
 - “Age” Time (min, max, med) of security and access attributes

Barriers and challenges revisited



#RSAC

- What current barriers do you face in establishing, managing, and/or executing a measurement program?
- What challenges do you face in identifying meaningful metrics within your organization?
- Have you identified some new/updated approaches for tackling these?



Getting started





- State a business objective
 - Ideally your business objective supports a stated strategic objective
 - **Ensure that** *[business unit, service, product, supply chain, technology, data center]* **is ...**
 - *available to meet a specified customer or revenue growth objective*
 - *unavailable for no more than some stated period of time, number of transactions, other units of measure*
 - *fully compliant with [law, regulation, standard] so as not to incur [z] penalties*

To get started



#RSAC

- Identify sponsors and key stakeholders
- Define security objectives and key questions
- Determine information that informs these
 - What information do you already have?
 - What information do you need to collect?
 - What is the value of collecting additional information?
- Define and vet a small number of key metrics
- Collect, analyze, report, refine
- Leverage an existing measurement program



Questions



#RSAC

