RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

SESSION ID: GRC-F03

Developing Useful Metrics

Lisa Young
Vice President, Service Delivery
Axio Global
Lyoung@Axio.com

David Tobar
Senior Cybersecurity Engineer
SEI/CERT Carnegie Mellon University
Dtobar@cert.org

Notices

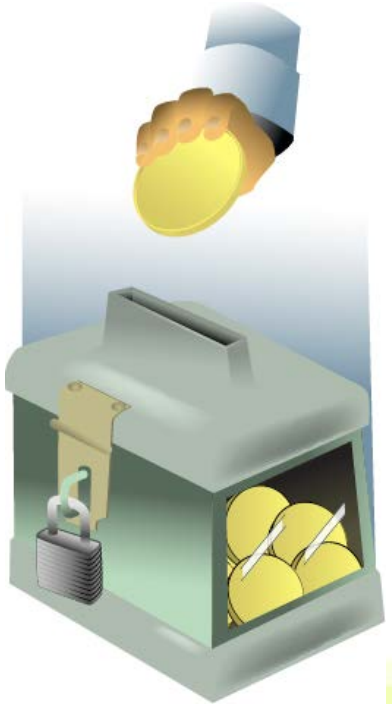
GRC-F03

- 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?

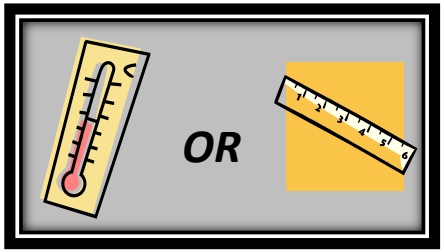
Key questions

- What should I measure 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?



Terminology (*)

- Measure vs. metric
  - I had 2 eggs for breakfast this morning
  - It's 53 degrees in San Francisco, CA
  - This session is 40 minutes 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.

(*) Visualize This! Meaningful Metrics for Managing Risk. Session GRC-F02, RSA Conference 2014.

So what? Why do you care?

- 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?

(*) informed by Douglas Hubbard, *How to Measure Anything*, John Wiley & Sons, 2010

Why measure?

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

RSAConference2017

Deriving Metrics from Objectives - GQIM

Key questions

- Not “What metrics should I use?” but

“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?

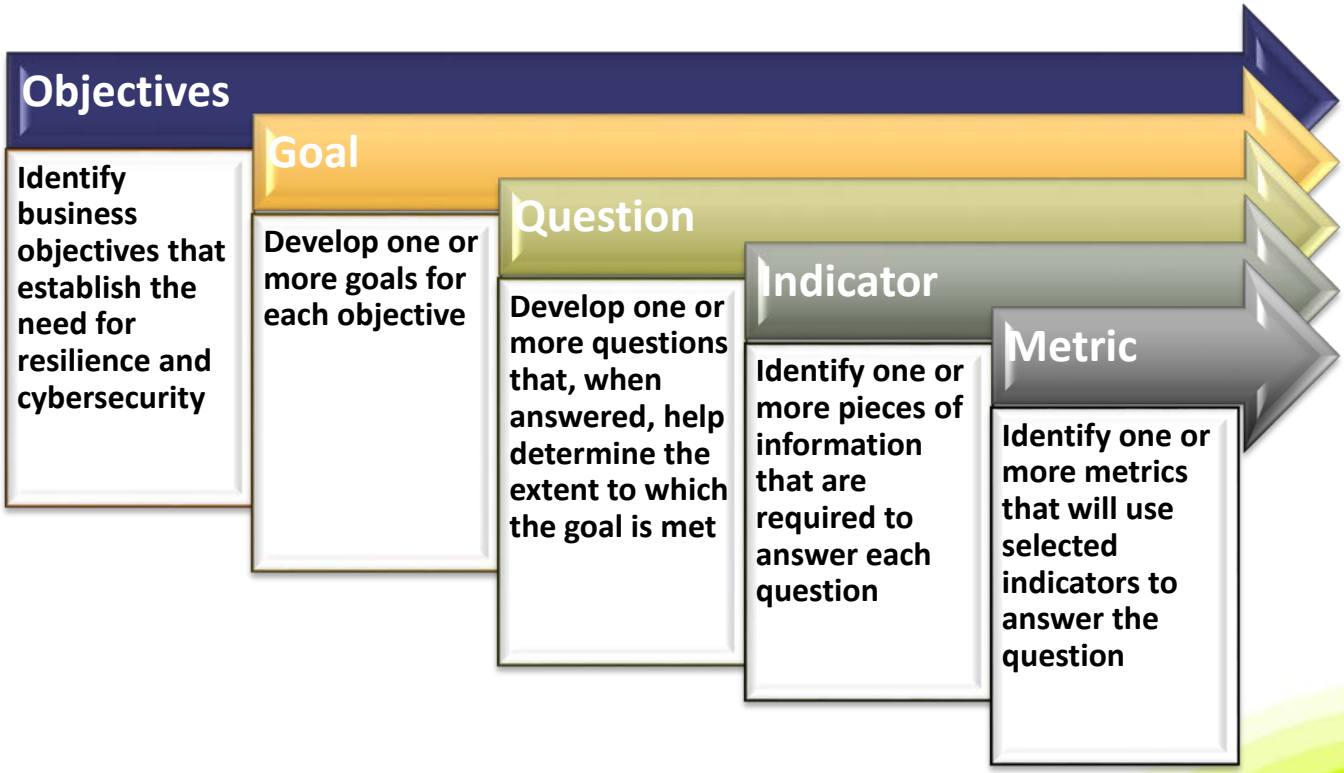
Purpose

- Use a defined, repeatable process to derive meaningful metrics that directly support achievement of business objectives and:
  - demonstrate the business value of each metric (and 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

- Understand a 5-step process for deriving metrics from business or program objectives
- Be able to apply this process to your objectives
- 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



RSAConference2017

Objectives to Goals

Process

- 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 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

Objective	Goal
Mitigate the risks of business disruption and loss resulting from cybersecurity incidents (with impact threshold > [x])	*Operate a cybersecurity incident center that detects, responds to, and reports security incidents in accordance with established standards and guidelines.* • *enterprise and operational unit levels*
	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 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

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

Questions to Indicators

Questions to Indicators

- What data do I need to answer the question?
  - Can add more data granularity than called for in the question
  - In what form should the data be reported?
- Which data is most important?
- Carry forward and 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

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

RSAConference2017

Indicators to Metrics

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?"

RSAConference2017

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

- 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

- **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?
- **Indicators:** Increased efficiencies in the patch management process
- **Metrics:** Actual time between patch release and patch application.

s

What if all I have is a Question? - 1

- **"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

- 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

- **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

- 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?

RSAConference2017

Getting started

Approach

- 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 penalties*

To get started

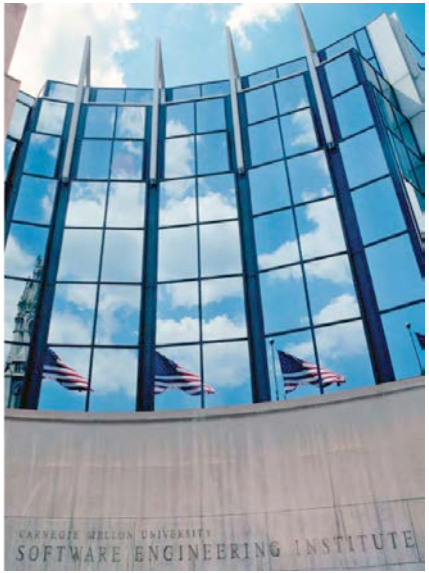
- Identify sponsors and key stakeholders
- Define security objectives and key questions
- Determine information that informs these
  - What information do you already have?
  - What information do you need to collect?
  - What is the value of collecting additional information?
- Define and vet a small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

Questions

Lisa Young
Email: Lyoung@axio.com
Vice President, Service Delivery
Axio Global

David Tobar
Email: DTobar@cert.org
Senior Cybersecurity Engineer
Carnegie Mellon University
SEI/CERT

CERT | Software Engineering Institute | Carnegie Mellon



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