Software Engineering Institute

Measuring What Matters Workshop Report

Katie Stewart
Julia Allen
Michelle Valdez
Lisa Young

January 2015

TECHNICAL NOTE
CMU/SEI-2015-TN-002

CERT Division

http://www.sei.cmu.edu

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.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0002070

Table of Contents

List of Figures

List of Tables

Acknowledgments

The authors would like to thank Jim Cebula and Summer Fowler for their leadership and sponsorship of the development of this workshop.

Abstract

This report describes the inaugural Measuring What Matters Workshop conducted in November 2014, and the team's experiences in planning and executing the workshop and identifying improvements for future offerings. The Measuring What Matters Workshop introduces the Goal-Question-Indicator-Metric (GQIM) approach that enables users to derive meaningful metrics for managing cybersecurity risks from strategic and business objectives. This approach helps ensure that organizational leaders have better information to make decisions, take action, and change behaviors.

1 Introduction

1.1 Purpose

This report describes the inaugural Measuring What Matters Workshop conducted in November 2014, and the experience of the team—staff of the CERT Division of the Carnegie Mellon University Software Engineering Institute (SEI)—in planning and executing the workshop and identifying improvements for future offerings. The Measuring What Matters Workshop introduces a measurement approach that enables users to derive meaningful metrics for managing cybersecurity risks from strategic and business objectives. This approach helps ensure that organizational leaders have better information to make decisions, take action, and change behaviors. It also helps ensure that planning, budgeting, and the allocation of resources are focused on monitoring what matters most to the organization.

1.2 Workshop Approach

The Measuring What Matters Workshop uses a derivative of the Goal-Question-Indicator-Metric (GQIM) approach [Park 1996] to derive example metrics from a stated strategic or business objective. We first demonstrate the approach using a simple objective: teaching a child to properly brush his/her teeth. Next, we demonstrate the approach using a cybersecurity incident management example. We then present a detailed description of a security incident experienced by Forbes in 2014 and demonstrate how metrics are derived from a set of objectives designed to ensure that such incidents do not recur. Last, we ask participants to select a business objective from their own organizations and apply the GQIM process to derive meaningful metrics to take home. After completing the workshop, participants should understand the elements of a measurement program and how to get one started.

As a result of the workshop, participants should be able to

- demonstrate the business value of each metric (and thus justify the cost for collecting and reporting the metric)
- defend meaningful metrics in comparison to others
- add metrics, update metrics, and retire metrics as business objectives change
- use metrics to inform business decisions, take appropriate action, and change behaviors

2 Workshop Overview

This section provides a brief description of the background that motivated our development of the workshop, workshop participants, and the eight topics that composed the workshop.

2.1 Background

One of the common mistakes that organizations make when they embark on a measurement program is to begin collecting whatever data is available and define and report metrics based on that data. Often they are dissatisfied with the results, which may lack information or a clear direction for action. Foundational elements that are typically missing include

- the identification of key stakeholders and audiences—the customers and users of the results generated by the measurement program
- the identification of strategic and business objectives that the measurement program is intended to support
- the development of candidate questions that stakeholders are seeking to answer based on the resulting metrics

It is critical to measure the right things in order to make informed decisions, take the appropriate actions, and change behaviors. But how do senior leaders and managers figure out what those right things are?

Public and private organizations today often base cybersecurity risk management decisions on fear, uncertainty, and doubt; the latest attack reported in the press; compliance mandates such as the Health Insurance Portability and Accountability Act, Federal Information Security Management Act, Sarbanes-Oxley Act, and Payment Card Industry Data Security Standard; and security risk frameworks that typically have little to do with the way the rest of the organization measures risk and prioritizes operational risk management activities.

Chief financial officers, enterprise risk management officers, internal audit directors, and chief information security officers need cybersecurity risk management approaches that align with and support the achievement of business objectives.

A measurement approach tied to strategic and business objectives ensures that planning, budgeting, and allocating operational resources are focused on what matters most to the organization. In addition, a shift to such an approach may help to identify metrics that are expensive to collect and may not be worth the investment.

The report extends and applies the operational resilience measurement concepts described in the work of Allen and colleagues [Allen 2010, 2011a, 2011b].

The workshop was presented as a one-day offering at the ISACA Information Security and Risk Management Conference in Las Vegas, Nevada, on November 18, 2014.

2.2 Participants

Forty-six U.S. and international participants from a range of market sectors registered for the workshop. Of those, 34 completed workshop evaluation forms on which they shared more detailed information on their purpose for attending, market sector, position, and years of experience. In addition, 20 participants responded to our request to provide example strategic and business objectives in advance as part of the workshop pre-work. Those participants provided additional background on their organizational affiliation and roles. This section provides an aggregate description of this information.

The 34 participants who completed workshop evaluation forms stated the following reasons for attending (participants could select multiple reasons):

- Gain awareness: 4
- Improve skills: 18
- Implement concepts: 17
- Teach others: 2

Participants had an average of 15-20 years of experience, with a minimum of 2 years and a maximum of 32 years.

Participants represented the following market sectors:

- Financial services
- Health
- U.S. federal civilian agency
- U.S. Department of Defense
- Telecommunications
- Retail
- IT and security consulting
- (Unspecified) international industry

Participants reported holding the following job titles:

- VP, operational risk
- Director, client services
- Director, technology risk
- Director, risk assurance
- Chief information officer
- Information security officer
- Compliance and security officer; IT compliance
- Manager of (IT/information) governance, security, risk, and compliance
- General manager and program manager
- Security professional, security engineer, security architect, and network engineer

- (Security) risk analyst and IT risk management
- IT audit

The objectives provided by 20 participants in advance greatly influenced our discussions during Topic 2 of the workshop. See Section 3.2 for a description of these objectives and Sections 3.3-3.7 for a description of how they were used during the GQIM process exercises.

2.3 Agenda

The workshop was organized into eight topics as shown in Figure 1.

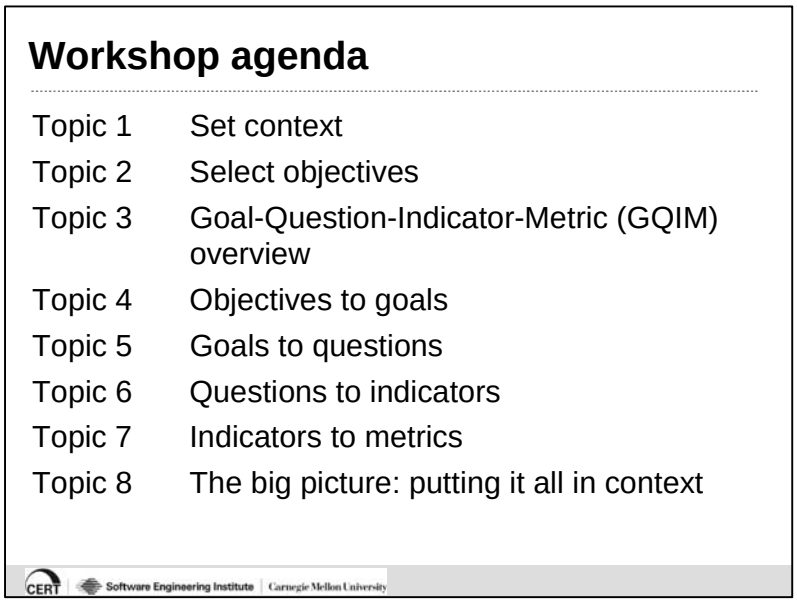

Figure 1: Workshop Agenda

3 Workshop Topics

This section provides a description of each workshop topic, example scenarios, and exercises performed by participants.

3.1 Topic 1: Set Context

3.1.1 Workshop Expectations

The facilitation team began the workshop by establishing a baseline for participant expectations and desired outcomes. The lead facilitator used the workshop abstract and a set of learning objectives to describe the concepts we planned to discuss during the workshop.

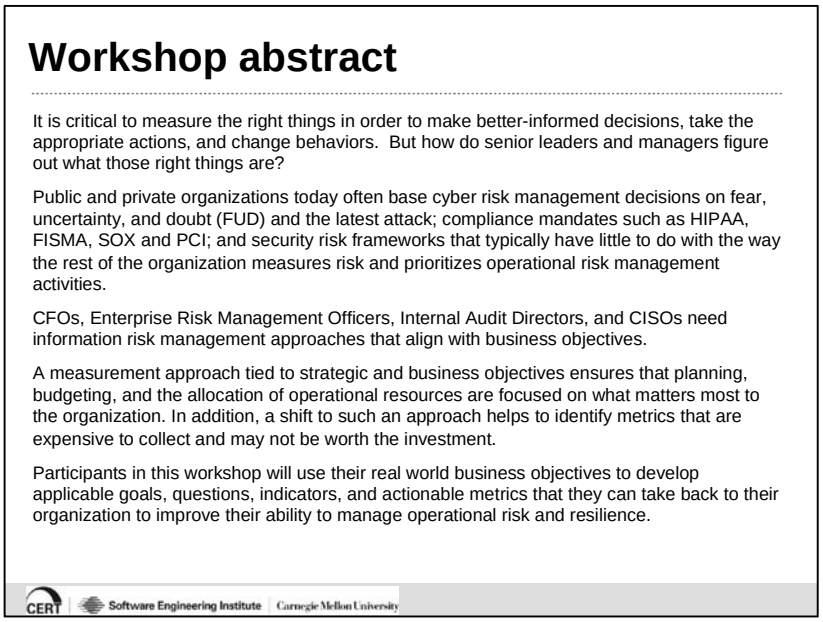

Figure 2: Workshop Abstract

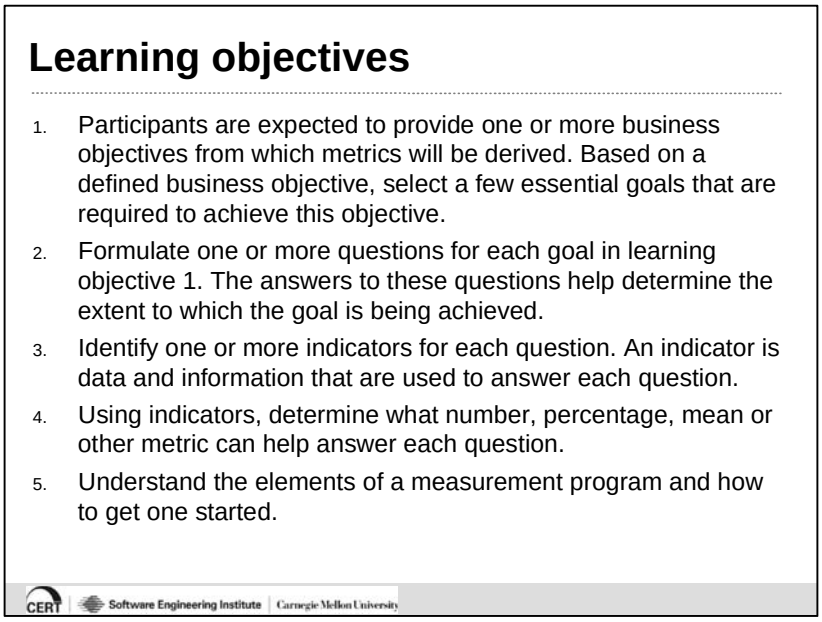

Figure 3: Learning Objectives

The lead facilitator asked participants to provide their personal expectations of the workshop. We received the following inputs:

- Ways to objectively measure
- What to do with all the data—get to the "So what?"
- How to make the value translation
- Ownership and accountability
- CIO to be more transparent to the CEO
- How to present metrics in an effective way
- How to measure things that are disparate/ways to normalize
- Reporting to the board of directors, compliance committee
- Derive from metrics program if current risks are appropriate

3.1.2 Operational Risk Management

Next, the facilitator led a discussion on operational risks and the organizational challenges faced when managing these risks. For the purposes of the workshop, we established the following definition:

> *Operational Risk: A form of risk emanating from day-to-day business operations; the potential failure to achieve mission objectives; typically categorized as inadvertent or deliberate actions of people, systems and technology failures, failed internal processes, or external events.*

We introduced participants to the concept of Operational Risk Management (ORM) and its relationship to security, business continuity, and IT operations. Each of these three activities is essential for managing operational risk. The facilitator discussed our observations of the current state of

risk management: Risk is managed in silos and generally in an ad hoc manner, and risk assumptions are not well understood or effectively communicated across organizations.

The facilitator then introduced the idea that risk management should ultimately drive decision making. When an organization's risk management activities do not drive decisions, the organization's leaders must consider why the organization is performing these activities. The GQIM process helps organizations ensure that their measurement systems are aligned with their strategic business objectives; the process creates a holistic approach for managing operational resilience. An organization's resilience capability increases by managing both sides of the risk equation (condition and consequence) in alignment with business drivers and full knowledge of costs.

The facilitator then asked participants to provide their thoughts on the following questions:

- 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?

The participants identified the following set of challenges:

- Business velocity; need to slow down to identify risks, ownership, and accountability
- Having knowledgeable risk management resources
- Lack of understanding of the need to measure anything—measure it all
- Showing future value of investments if everything is going well
- Complexity of systems, processes, and knowing where to start
- Business units discount metrics
- Measuring ROI, especially with insufficient data
- Have to quantify what you have prevented/avoided
- Decision rights and conflict resolution

Participants were asked what, if anything, they were currently doing to overcome these challenges. They identified the following actions:

- Shifting accountability
- Sponsorship at a leadership level
- Cultural change
- Empowerment at lower levels in the organization
- Helping business units to own and take action

3.1.3 Measurement

Next, the facilitator led a discussion on measurement, explaining that leaders of organizations often ask, "How secure is our organization?" That is,

- How secure are we compared to our competition?
- Are we managing our risks well?

- Do we need to spend more money on security or risk management? If so, on what?
- What are the public relations and legal impacts of a data breach?

To properly answer these questions, leaders must also answer the following questions:

- What should we be measuring to determine if we are meeting our performance objectives for security?
  - Do we know what these performance objectives are?
  - Do our performance objectives reflect today's realities?
- What is the business value of being more secure?
  - Of a specific security investment?
- So what? If we had this metric [Hubbard 2010],
  - What decisions would it inform?
  - What actions would we take based on it?
  - What behaviors would it affect?
  - What would improvement look like?
  - What would its value be in comparison to other metrics?

3.1.4 GQIM Overview

The lead facilitator described the purpose of the GQIM process and provided a brief overview of the process steps.

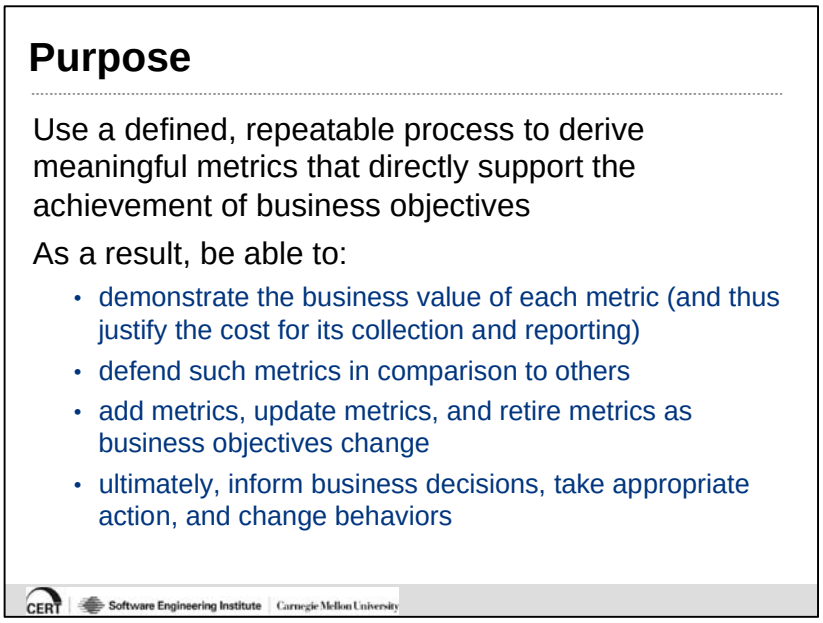

Figure 4: GQIM Process Purpose

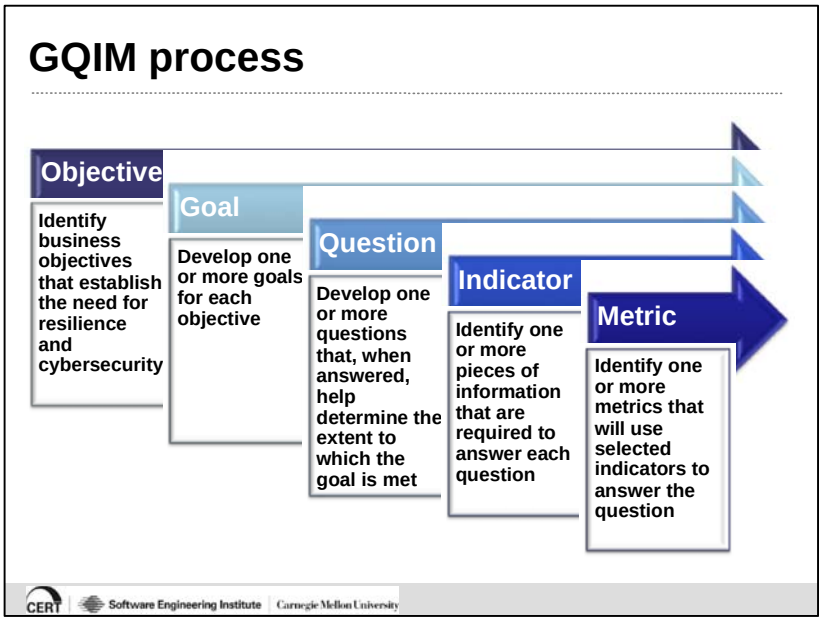

Figure 5: GQIM Process Steps

3.2 Topic 2: Select Objectives

As part of the pre-work for the workshop, we asked participants to identify two or three strategic (enterprise) or business (unit-level) objectives to which they would apply the GQIM process. We encouraged them to use the SMART(ER) criteria shown in Figure 6 in defining their objectives.

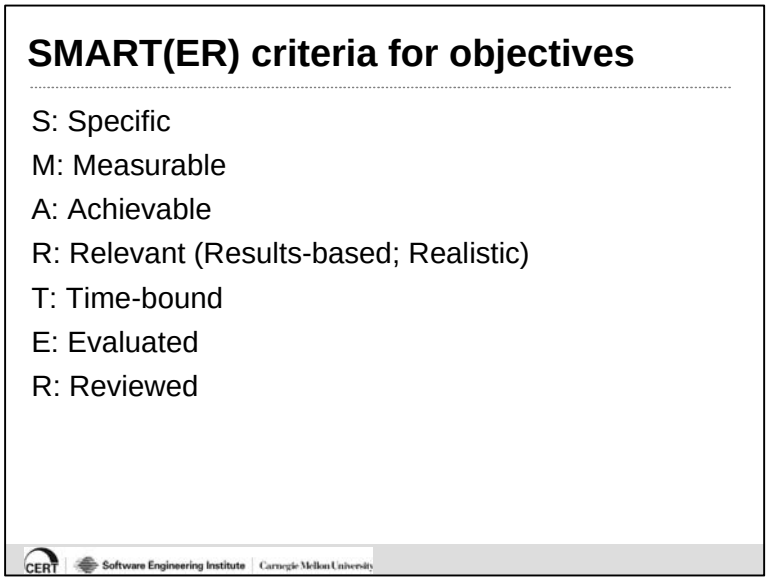

Figure 6: SMART(ER) Criteria for Identifying Objectives

About half of those registered for the workshop provided objectives in advance. The facilitation team integrated the participants' objectives with example objectives the team had developed during workshop preparation. We used the resulting objectives to group participants with similar ob-

jectives at the same table so they could benefit by working with one another on objectives of common interest. Working with a group of peers with similar objectives increases the likelihood of information sharing, shared insights, and focus on the GQIM process (vs. interpretations of any specific objective).

During the Topic 2 discussion, participants were instructed to identify a business objective (if they had not done so in advance) or modify an existing one that they would use to apply the GQIM process.

Based on the facilitation team's objectives and those provided in advance by participants, we identified the candidate objectives in Figure 7 to be used during the workshop.

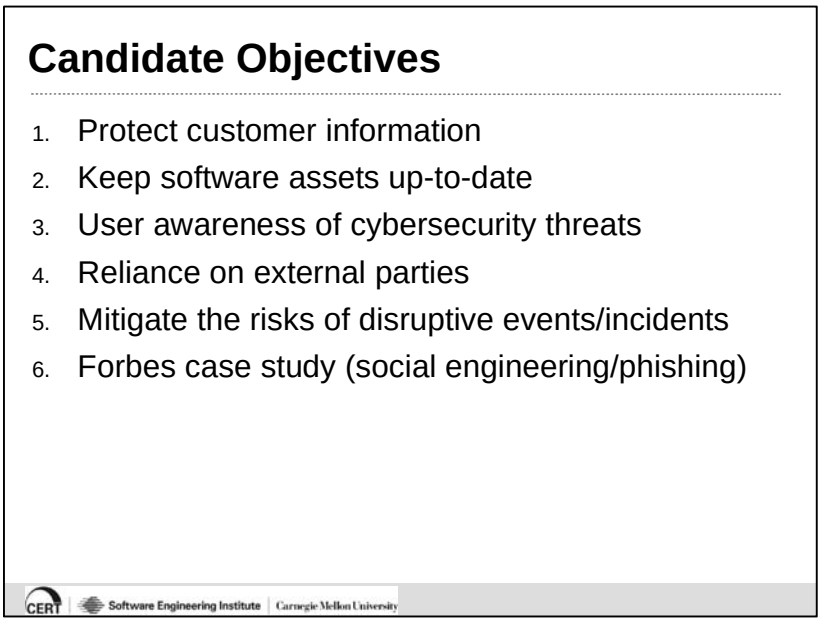

Figure 7: Candidate Objectives for Table Assignments

Each participant selected one of the objectives and we seated participants together according to the objectives they chose. Several of the objectives were so popular that we needed two tables to accommodate the participants who chose them.

A few participants were consultants working with multiple organizations and did not have a specific business objective of their own. We suggested that these participants use the Forbes scenario (provided in the pre-work) as their objective for applying GQIM. The Forbes scenario is described in more detail in Section 3.3.

The facilitation team also completed a detailed GQIM analysis for several of the candidate objectives prior to the workshop. The team used these analyses to facilitate exercises and provided them to participants at the end of the workshop for further study.

3.3 Topic 3: GQIM Overview and Scenarios

The purpose of Topic 3 was to provide an overview of the GQIM process and illustrate it using several scenarios. To introduce the GQIM process, we developed and presented goals, questions, indicators, and metrics based on an easily understood objective: Ensure your child's teeth are healthy.

Next, we used a more relevant cybersecurity risk-related objective to further illustrate the GQIM process: Mitigate the risks of business disruption and loss resulting from cybersecurity incidents (with impact threshold > [x]).

Throughout Topics 4, 5, 6, and 7, we used objectives derived from a real-world incident referred to as the "Forbes scenario." The Syrian Electronic Army used a social engineering phishing attack to access and compromise Forbes.com and its companion publishing application in February 2014. The attack and its impact are summarized as follows and are further detailed in several accounts [Ducklin 2014, DVorkin 2014, Greenberg 2014]:

> *On 13 Feb 2014, a single, successful spear phishing email set in motion a very public compromise of Forbes.com.*
>
> *The Syrian Electronic Army leveraged the variety of social media accounts that the Forbes staffers and contributors have to leap-frog from their email accounts to the publication's blog and social media platforms.*
>
> *All passwords across multiple platforms were forced to be reset as a security measure and Forbes.com and its WordPress platform were taken offline several times over 2 days.*
>
> *Forbes has focused on building unique content and a publishing model for the social media era in an open and secure platform.*

We provided the following objectives as a starting point to apply the GQIM process to this scenario:

- Strategic objective: Provide a content and publishing model for the era of social media that is both open and secure.
- Business objective: Increase user awareness of potential threats and the appropriate responses to social engineering and phishing tactics.
- Business objective: Improve the public's and users' confidence in the ability of Forbes.com to operate securely and to protect user privacy.

The following sections describe questions to ask at each step in the GQIM process and how to apply each step to these three scenarios—ensuring healthy teeth, incident management, and the Forbes scenario—to generate example goals, questions, indicators, and metrics.

Using these examples as references, participants then used their selected objective to walk through the GQIM process. Some of their experiences are described in Section 4.

3.4 Topic 4: Objectives to Goals

To derive goals from objectives, it is useful to answer the following questions:

- What are meaningful actions to take to achieve the objective?
- Which actions are most important (high leverage, high payoff)?
- If I achieve this goal, will I be able to demonstrate substantive progress in achieving the objective?

Table 1, Table 2, and Table 3 provide example goals for selected objectives from the three scenarios described in Section 3.3.

Table 1: Objectives to Goals—Ensuring Healthy Teeth

Objective	Goal
Ensure you child's teeth are healthy.	G1: Ensure your child has everything needed to brush his/her teeth. G2: Ensure your child is brushing his/her teeth at least twice daily.

Table 2: Objectives to Goals—Incident Management

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.

Table 3: Objectives to Goals—Forbes Scenario

Objective	Goal
Increase user awareness on potential threats and the appropriate responses to social engineering and phishing tactics.	Ensure users whose accounts are compromised do not succumb to the same attack(s) again (using random testing for one year following a compromise).

3.5 Topic 5: Goals to Questions

To derive questions from goals, it is useful to answer the following questions:

- What are meaningful questions to answer to determine if the goal is being achieved?
- Which questions are most important?
- If I answer this question, will I be able to demonstrate substantive progress in achieving the goal?

Useful questions are often in the form of

- What is the process for x? (This question provides a more informative answer than "How does the organization do x?")
- How effective is x?

Table 4, Table 5, and Table 6 provide example questions for selected goals by scenario.

Table 4: Goals to Questions—Ensuring Healthy Teeth

Goal	Question
G1: Ensure your child has everything needed to brush his/her teeth.	Q1: Does the child have a good toothbrush? Q2: Does the child know how to brush properly?
G2: Ensure your child is brushing his/her teeth at least twice daily.	Q1: Does your child show you his/her clean teeth?

Table 5: Goals to Questions—Incident Management

Goal	Question
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?

Table 6: Goals to Questions—Forbes Scenario

Goal	Question
G1: Ensure users whose accounts are compromised do not succumb to the same attack(s) again (using random testing for one year following a compromise).	Q1: What is the process for identifying recurring compromised accounts?

3.6 Topic 6: Questions to Indicators

To derive indicators from questions, it is useful to answer the following questions:

- What data (and sometimes in what form) do I need to answer the question?
- Which data is most important?
- If I have this data, will I be able to answer some aspect of this question?

Table 7, Table 8, and Table 9 provide example indicators for selected questions by scenario.

Table 7: Questions to Indicators—Ensuring Healthy Teeth

Question	Indicator
G1.Q2: Does the child know how to brush properly?	Q2.I1: Demonstration of use Q2.I2: Issues found during dental checkups
G2.Q1: Does the child show you his/her clean teeth?	Q1.I1: Evidence that tooth brushing has occurred

Table 8: Questions to Indicators—Incident Management

Question	Indicator
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

Table 9: Questions to Indicators—Forbes Scenario

Question	Indicator
Q1: What is the process for identifying recurring compromised accounts?	Q1.I2: Security incident reports in which the incident is caused by the same user account

3.7 Topic 7: Indicators to Metrics

To derive metrics from indicators, it is useful to answer the following questions:

- Using the indicator data, what number, percentage, mean, or other metric can I collect or calculate to help answer the question?
- Which metrics are most important?
- If I report this metric (over time), will it provide the greatest insight possible to answer the questions from which it derives?

To further define appropriate metrics, it is useful to answer the following questions:

- 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?

Table 10, Table 11, and Table 12 provide example metrics using selected indicators by scenario.

Table 10: Indicators to Metrics—Ensuring Healthy Teeth

Indicator	Metric
Q2.I2: Issues found during dental checkups	I2.M1: Number of cavities I2.M2: Instances of gingivitis
Q1.I1: Evidence that tooth brushing has occurred	I1.M1: Smell of breath I1.M2: Condition of toothbrush (wet vs. dry)

Table 11: Indicators to Metrics—Incident Management

Indicator	Metric
Q1.I1: Process and criteria for detecting and triaging suspicious events	Q1.I1.M1: Mean time to detect suspicious events

Table 12: Indicators to Metrics—Forbes Scenario

Indicator	Metric
Q1.I2: Security incident reports in which the incident is caused by the same user account	I2.M1: Number of user accounts that have been compromised by the same attack I2.M2: Mean time between similar attacks for a given user account

In an effective measurement program, metrics are collected, interpreted, refined, and improved on an ongoing basis. At the completion of the GQIM process, there is an initial set of metrics that can be used to monitor the organization's business objectives. However, metrics need to be routinely revisited (through the GQIM process or another approach) to ensure decision makers are receiving the most useful and actionable metrics to monitor progress against enterprise objectives.

3.8 Topic 8: The Big Picture

The final section of the workshop focused on understanding the "So what?" of the GQIM process. We asked our participants to consider the following questions to determine if they had identified meaningful metrics:

- What decision will the metric inform?

- What actions would I take based on this metric?
- What behaviors would the metric affect?
- What would improvements look like?

Participants were encouraged to refine their metrics as they continue to improve and develop their measurement programs. The GQIM process is not meant to be only executed at program creation; rather, it can and should be used to routinely revisit and improve metrics as part of a risk management approach. Each step in the process and the corresponding questions driving each step are part of a toolkit that should be used to continuously improve an organization's measurement program.

During the closing of the workshop, we revisited participant expectations and challenges. We asked participants to identify approaches to take back to their organizations to address current challenges and barriers they faced in developing a measurement program and identifying meaningful metrics. The following approaches were identified:

- Tie metrics to business objectives and put the outputs in the language of the business.
- Increase awareness of the purpose of measurements and how to tie them to business objectives.
- Make sure you are asking the right questions.
- Focus on the potential impact to show the value of a measurement program instead of trying to prove what was prevented.
- Things are not going to get less complex, so make sure you are asking the right questions and measuring the right things. Also, start with measuring one thing; don't try to boil the ocean.
- Train users and leadership on the GQIM process and encourage them to use it.

4 Workshop Feedback

Participants provided the following information in response to our request for strengths and areas requiring improvement on the workshop evaluation form:

Strengths	Areas for Improvement
Workshop pre-work (objectives, Forbes scenario)	Provide more time for general conversation and knowledge sharing rather than on the table exercises
Having a well-defined, structured approach for deriving metrics from business objectives	Suggest starting out with examples of a set of metrics that have worked in changing behaviors. Then, back up and go through the process of getting there.
Applicability to C-level perspectives; ability to use approach with business stakeholders	Spend more time identifying and describing the right objectives and goals
Instructor engagement during group exercise	Provide more work time during group exercises
Demonstration of how to develop good objectives	Provide more guidance on how to move from questions to metrics
GQIM examples (brushing teeth, incident management, Forbes, several table topics)	Provide examples of metrics that have worked
Hands-on approach	Spend more time on metrics, assessing what is valuable to measure vs. what is not; demonstrate the use of the metrics template
Small group work and discussions; opportunity to collaborate with peers	Provide time during group work for participants to share metrics that they are reporting and how they are doing it
Group exercises and the way they built upon each other; the workshop format was easy to follow	More interaction with instructors during group exercises
Group topics were relevant and real life	Expand this to a 2-day course
Relevant to my job	
Multiple instructors; well prepared; instructor knowledge and experience; team teaching approach; variety of presentation styles; coordination between instructors	

5 Next Steps

Going forward, the SEI will offer the Measuring What Matters Workshop as a one-day public course. We are working to consolidate feedback from all of the participants to improve the preparation, execution, and follow-up activities around the workshop. We have had additional requests for private offerings of the workshop from multiple industry partners. In addition to the release of this report, we will release a podcast on the workshop and its results.

References

URLs are valid as of the publication date of this document.

[Allen 2010]
Allen, Julia & Davis, Noopur. *Measuring Operational Resilience Using the CERT Resilience Management Model* (CMU/SEI-2010-TN-030). Software Engineering Institute, Carnegie Mellon University, September 2010.
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9401

[Allen 2011a]
Allen, Julia & Curtis, Pamela. *Measures for Managing Operational Resilience* (CMU/SEI-2011-TR-019). Software Engineering Institute, Carnegie Mellon University, June 2011.
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=10017

[Allen 2011b]
Allen, Julia; Curtis, Pamela; & Gates, Linda. *Using Defined Processes as a Context for Resilience Measures* (CMU/SEI-2011-TN-029). Software Engineering Institute, Carnegie Mellon University, October 2011.
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9887

[Ducklin 2014]
Ducklin, Paul. *Syrian Electronic Army Hacks Forbes, Spills 1M User Records - Here's What You Need to Know*, February 2014.
http://nakedsecurity.sophos.com/2014/02/16/syrian-electronic-army-hacks-forbes-spills-1000000-user-records/

[DVorkin 2014]
DVorkin, Lewis. *Inside Forbes: After a Digital Attack, a Story of Recovery and What It Means*, February 2014.
http://www.forbes.com/sites/lewisdvorkin/2014/02/18/inside-forbes-after-a-digital-attack-a-story-of-recovery-and-what-it-means/

[Greenberg 2014]
Greenberg, Andy. *How the Syrian Electronic Army Hacked Us: A Detailed Timeline*, February 2014.
http://www.forbes.com/sites/andygreenberg/2014/02/20/how-the-syrian-electronic-army-hacked-us-a-detailed-timeline/

[Hubbard 2010]
Douglas Hubbard. *How to Measure Anything*. John Wiley & Sons, 2010.

[Park 1996]
Park, Robert; Goethert, Wolfhart; Florac, William. *Goal-Driven Software Measurement —A Guidebook* (CMU/SEI-96-HB-002). Software Engineering Institute, Carnegie Mellon University, 1996. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=12453

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	January 2015	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Measuring What Matters Workshop Report	FA8721-05-C-0003

6. AUTHOR(S)

Katie Stewart, Julia Allen, Michelle Valdez, Lisa Young

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2015-TN-002

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This report describes the inaugural Measuring What Matters Workshop conducted in November 2014, and the team's experiences in planning and executing the workshop and identifying improvements for future offerings. The Measuring What Matters Workshop introduces the Goal-Question-Indicator-Metric (GQIM) approach that enables users to derive meaningful metrics for managing cybersecurity risks from strategic and business objectives. This approach helps ensure that organizational leaders have better information to make decisions, take action, and change behaviors.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Goal-Question-Indicator-Metric, GQIM, cybersecurity, incident management, risk	33

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL