What Metrics Should a CSIRT Collect to Measure Success?

(Or What Questions Should We Be Asking and How Do We Get the Answers?)

Robin Ruefle, Audrey Dorofee

June 15, 2017

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by Department of Homeland Security 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 sponsored by the United States Department of Defense.

DM-0004640

Agenda

- Background & Motivation
- Project History
- Data Description
- Observations and Challenges
- Next Steps and Future Work

What Metrics Should a CSIRT Collect to Measure Success?

Background & Motivation

Project Motivation

Part of our collaborative work with US-CERT (NCCIC) formalized in our Information Discovery Project.

The project concentrates on finding methods to increase the understanding and use of incident data and organizational process metrics.

Information Discovery Project Objectives

Tasking for the Information Discovery project revolves around three activities:

- Exploratory Analysis
- General Metrics Research
- Collaboration and Support

Our Focus Today - General Metrics Research

This task continues to research what people/organizations are measuring and trying to determine if those measurements are valid, useful, and accurate.

The general metrics research task is focused on two main activities:

- Continued research on new techniques for measuring CSIRT/incident management effectiveness
- Continued development of a recommended set of metrics to be collected by CSIRT/incident management organizations.

As part of this information we will also try to look at emerging domains – what problems are encountered with measurements today, and what is getting traction.

Developing a Recommended Set of Metrics

This will include

- the identification of the questions that should be asked
- the data and metrics needed to answer the questions
- the benefit of collecting and reporting such metrics
- how this can be tied to process improvement

What Metrics Should a CSIRT Collect to Measure Success?

Project History

Project Steps and Where We Are Now -1

1. Collected existing metrics across literature and other sources
   - What was being collected
   - What was recommended
   - What might be useful

2. Developed Internal Reports for US-CERT and Updates:

   State of the Practice: Cybersecurity Incident Management Metrics, Taxonomies, Maturity Frameworks, and Constituency Characterizations CMU/SEI-2015-SR-014

3. Looking to publish this document during next funding period.

Project Steps and Where We Are Now -2

4. Held working session at 2016 FIRST conference Metrics SIG to gather information on what metrics are currently collected and what questions needed to be answered.

5. Brainstormed an initial set of categories, subcategories of questions
   - iterative internal reviews and revisions
   - lots of changing of minds and approaches

6. Created spreadsheet of question categories and subcategories of metrics to see
   - which metrics could answer what questions
   - what questions had no metrics yet identified

Project Steps and Where We Are Now -3

7. Revised spreadsheet multiple times as we reworked categories
   - Found large gaps where many questions had no established corresponding metrics.

8. Brought in a metrics course for interested CERT staff in December: Information Security PRAGMATIC Metrics Boot Camp, Level II
   - Introduced concept of Goal-Question-Metric.
   - Asked the question – How well am I doing?

9. Decided to look at and use SEI Goal-Question-Indicator-Metric (GQIM) methodology.

10. Will apply Goal-Question-Indicator-Metric methodology to categories of questions to achieve a more logical structure

Project Steps and Where We Are Now -4

The intent is to produce a spreadsheet that

- correlates goals and questions to possible metrics
- can answer the questions, verifying the goal has been met (in other words, that the CSIRT is succeeding at its mission)

Will refine cross-references to distinguish between metrics which

- fully answer a question
- partially answer a question
- provide an indication that something needs to be investigated before a conclusion can be drawn

Starter sets of metrics could be created for a CSIRT based on its goals or mission.

What Metrics Should a CSIRT Collect to Measure Success?

A Little More About GQIM

SEI GQIM

- GQIM references
  - Measuring What Matters Workshop Report, CMU/SEI-2015-TN-002
  - Goal-Driven Software Measurement – A Guidebook, CMU/SEI-96-HB-002
- Start with goals of a CSIRT, decompose to major questions to answer that goal, sub-questions, indicators (as needed to help identify metrics) and then match to metrics

GQIM

GQIM process, in general, is a process for identifying metrics to help you determine if you are meeting your goals.

- Identify objectives
- Develop one or more goals for each objective
- Develop one or more questions that, when answered, help determine the extent to which the goal is met
- Identify one or more pieces of information (indicators) that are required to answer each question
- Identify one or more metrics that will use selected indicators to answer the questions

We adapted the process to focus on a hierarchy of goals and questions and tying those to specific metrics.

What Metrics Should a CSIRT Collect to Measure Success?

Data Description

Spreadsheet Status

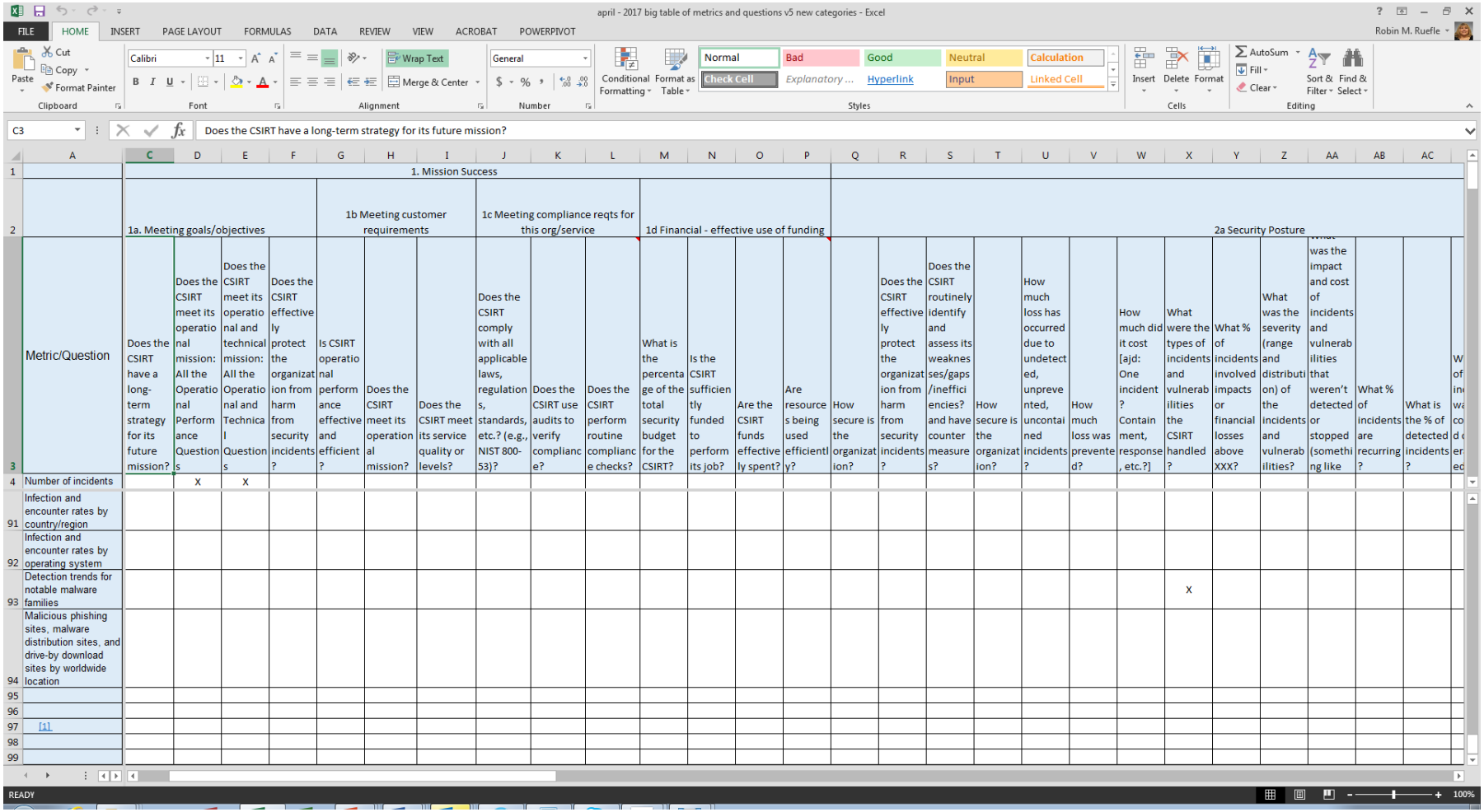
Some data about the current spreadsheet:

- Number of categories and subcategories of questions – 5 categories and 21 subcategories
- Number of questions in those categories and subcategories - 86
- Number of metrics – 90

Spreadsheet sample:

	How efficient and effective is the CSIRT at coordinating and communicating?	How efficient and effective is the CSIRT at sharing information?	How efficient is the CSIRT at communicating? (bi-directional)	How effective has CSIRT communication been? (what difference has it made to constituents?)
Number of security team consultations	X	X	X	X
Percentage of incidents with no measurable costs				
Mean time to know the root cause of an incident				
Mean time to verify and confirm the satisfactory resolution with the parties affected	X	X	X	

Very Large Spreadsheet



What Metrics Should a CSIRT Collect to Measure Success?

Results So Far

Data from Metrics SIG -1

Current Metrics

- Incident statistics
- Vulnerability statistics
- Remediation statistics
- Staff performance
- Compliance

Metrics wanted

- Cost and return-on-investment (ROI)
- Incident statistics
- Response statistics
- Risk management

Data from Metrics Sig -2

Sample questions Metrics Sig members would like to have answered

- How secure is our organization?
- Is our security adequate?
- What security gaps do we have?
- How does our CSIRT compare to peers and others?
- Are we mature or not?
- Is our team effective? Are we adding value to the community?
- Is our team effective at response?
- Is our team presenting information effectively?
- What activity do we improve next year?

Current Set of Question Categories

Overarching set of categories

- Mission success
- Security Performance/Analytics
- Operational Performance
- Constituency Management
- Employee Management

Current Set of Question Categories/Subcategories -1

1. Mission Success
   - Goal /objective measurement – meeting the goals
   - Meeting customer requirements
   - Compliance – meeting all compliance requirements for this org and service
   - Financial – effective use of funding

Current Set of Question Categories/Subcategories -2

2. Security Performance/Analytics – these are all the defensive, preventative, and response activities and results

- Security posture
- Incident management
- Vulnerability management

Current Set of Question Categories/Subcategories -3

3. Operational Performance
   - Benchmarking/maturity (against standards or criteria (like ITIL, F-CND, IMCA, etc.), against peer organizations
   - Right or adequate equipment to perform mission
   - Right or adequate staff to perform mission
   - Business continuity, risk, and resilience
   - Process improvement

Current Set of Question Categories/Subcategories -4

4. Constituency Management
   - Constituent satisfaction
   - Constituent outreach
   - Constituent requirements gathering
   - Capacity building

Current Set of Question Categories/Subcategories -5

5. Employee Management
   - Employee satisfaction
   - Employee retention
   - Employee skill development
   - Employee professional development
   - Employee performance

Category to Question Examples

2. Security Performance/Analytics
   - Security posture (selected questions)
     - How secure is the organization?
     - Does the CSIRT effectively protect the organization from harm from security incidents?
     - How much loss was prevented?
     - What were the types of incidents and vulnerabilities the CSIRT handled?
     - What % of incidents are recurring?

3. Operational Performance
   - Benchmarking/maturity
     - How does this CSIRT compare to others?
     - How does this CSIRT compare to its peers (similar types of CSIRTS, domains, size, etc.)?
     - How does the CSIRT benchmark against standards or criteria (e.g., ITIL, F-CND, IMCA, etc.) or Is this CSIRT mature?

What Metrics Should a CSIRT Collect to Measure Success?

Observations and Challenges

Observations

There are large gaps where questions have no relevant metrics, or at least no simple relationship between metrics and the question

Almost all metrics will answer one or more questions, but it tends to be the same question for many of the metrics

Of the main categories, the matches between metrics and questions is

- Heaviest in Security Performance
- Moderate (but with mostly partial matches) in Mission Success
- Light in Operational Performance
- Almost non-existent in Employee and Constituent Management

Challenges

It’s a big spreadsheet

Still not clear if we have the right set of categories/questions and the possible metrics

- Likely need to investigate more traditional employee and customer management metrics for CSIRT employee and constituent aspects

There are significant gaps that need to be filled either with new metrics or through combinations of other metrics

Many metrics are actually leading indicators of something that may be going wrong but are not direct answers to the question

Theory needing testing: can you group metrics for smaller questions in such a way to reach a reasonable answer to a big question (e.g., How secure is the organization?)

What Metrics Should a CSIRT Collect to Measure Success?

Next Steps and Future Work

What's Next?

Continue using GQIM to refine the goals and questions we are trying to answer with the metrics

- Ensure the questions can be answered
- Decompose questions to smaller questions
- Verify - if I answer these questions will I know if I'm meeting this goal?
- Complete a first draft of the entire spreadsheet
- Seek external review and feedback of both the overall structure and the content of the spreadsheet
- Develop guidance for using the spreadsheet
- Identify and test some sets of starter metrics for different types of CSIRTs based on goals

Related Work

Also working with another group in DHS looking at CSIRT Capability Proficiency Levels.

We are applying GQIM to this work too.

At the capability level it seems more straight forward.

Questions

Contact Information

Presenter / Point of Contact
Robin M. Ruefle

Senior Member of the Technical Staff

Team Lead, CSIRT Development and Training Team

Telephone: +1 412.268.6752

Email: rmr@sei.cmu.edu