Meaningful Metrics & The Board

Katie Stewart, Senior Member of the Technical Staff

CERT Program, Carnegie Mellon University

kcstewart@cert.org

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-1226

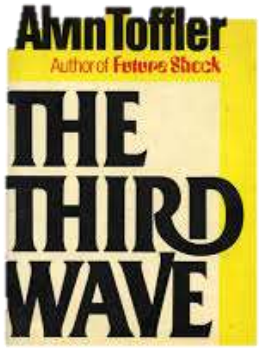
Introduction

NC STATE UNIVERSITY

CISCO SYSTEMS

Wharton
University of Pennsylvania

NORTHROP GRUMMAN



Carnegie Mellon University
Software Engineering Institute

Agenda

Cyber Risks and Operational Resilience

Metrics Overview

Cyber Metrics and the Board

Goal-Question-Indicator-Metric

Testing GQIM

CERT Program

Carnegie Mellon University Software Engineering Institute

Mission: To anticipate and solve the nation's most challenging cybersecurity problems

Cybersecurity Risk and Resilience

Carnegie Mellon University Software Engineering Institute

To protect and sustain assets that are important to the nation's cyber-dependent mission ensuring that they continue to operate during and recover from disruptive events.

Cybersecurity Assurance: Advance the state of the practice of cybersecurity evaluation (technical and process) and support the ability of critical infrastructure providers and government organizations to achieve missions dependent on cyber assets.

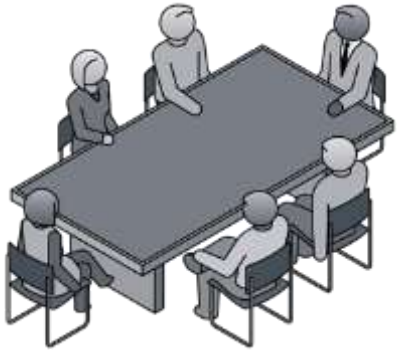
Cybersecurity Risk Management: Research, develop, and deploy processes, tools, and solutions to public and private customers that enable operational surety in times of distress.

Enterprise Threat & Vulnerability Management: Research and develop technical and behavioral policies, processes, and controls to discourage, detect, and contain malicious and non-malicious insider threats

Cyber Risks and Operational Resilience

With Cyber Risk, Who Is The Enemy?

But what about…

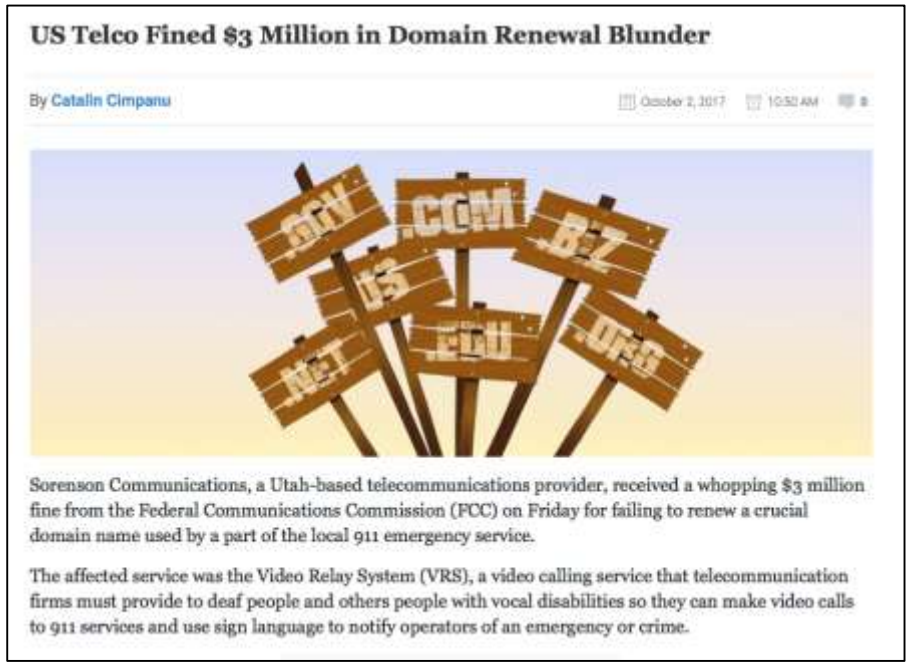


The 2017 U.S. State of Cybercrime Survey found:

- 34% respondents reported an insider incident in 2016.
- 30% of the reported incidents were perpetrated by insiders.
- 61% of insider incidents were unintentional or accidental, as opposed to intentional attacks.
- 43% indicated that insider incidents were more costly or damaging than external attacks.

https://www.csoonline.com/article/3211491/security/state-of-cybercrime-2017-security-events-decline-but-not-the-impact.html /

Failed Internal Processes – A Closer Look



US Telco Fined $3 Million in Domain Renewal Blunder

By Catalin Cimpanu

Sorenson Communications, a Utah-based telecommunications provider, received a whopping $3 million fine from the Federal Communications Commission (FCC) on Friday for failing to renew a crucial domain name used by a part of the local 911 emergency service.

The affected service was the Video Relay System (VRS), a video calling service that telecommunication firms must provide to deaf people and others people with vocal disabilities so they can make video calls to 911 services and use sign language to notify operators of an emergency or crime.

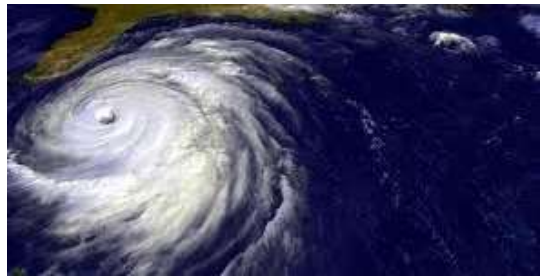
https://www.bleepingcomputer.com/news/technology/us-telco-fined-3-million-in-domain-renewal-blunder/

- On June 6, 2017, Sorenson Communications failed to renew their domain name which ran their Video Relay System that supports 911 services for the deaf and those with vocal disabilities.
- The system was down for 3 days.
- The FCC investigated and found this was preventable and imposed a $2.7M fee, $250K of which was a fine.

Cyber Risks are Both Unique and Not Unique in the Eyes of the Board

- **Cyber *is* unique because the devil is in the architectural and technical details**, and the Board tries to not go down the rabbit holes of "details."
  - Audit Committees or Risk Committees do go deeper.
- **Cyber *is also* unique because most Enterprise Risk Management (ERM) Programs categorize risks into "strategic" and "operational" risks – Cyber risks are both.**
  - Cyber risks can have operational and strategic consequences and those effects could consummate very rapidly--within hours or days.
  - Many Boards are unaware of the laws regarding reporting requirements.
- **Cyber *is not* unique in that it is just a new category of risk that can find unprepared Boards negligent** and cause Companies to lose reputation, shareholder confidence, and market share.
  - Few companies have the organic resources to police themselves.

Why Do Operational Risks Matter?



- Trust and confidence of employees and customers
- Reputation and image
- Regulatory compliance, fines, legal penalties
- Customer retention and growth
- Life, safety, and health of customers and employees
- Productivity and profitability
- Organizational survival
- Internal Process Failures

! …because they have explicit and direct IMPACT

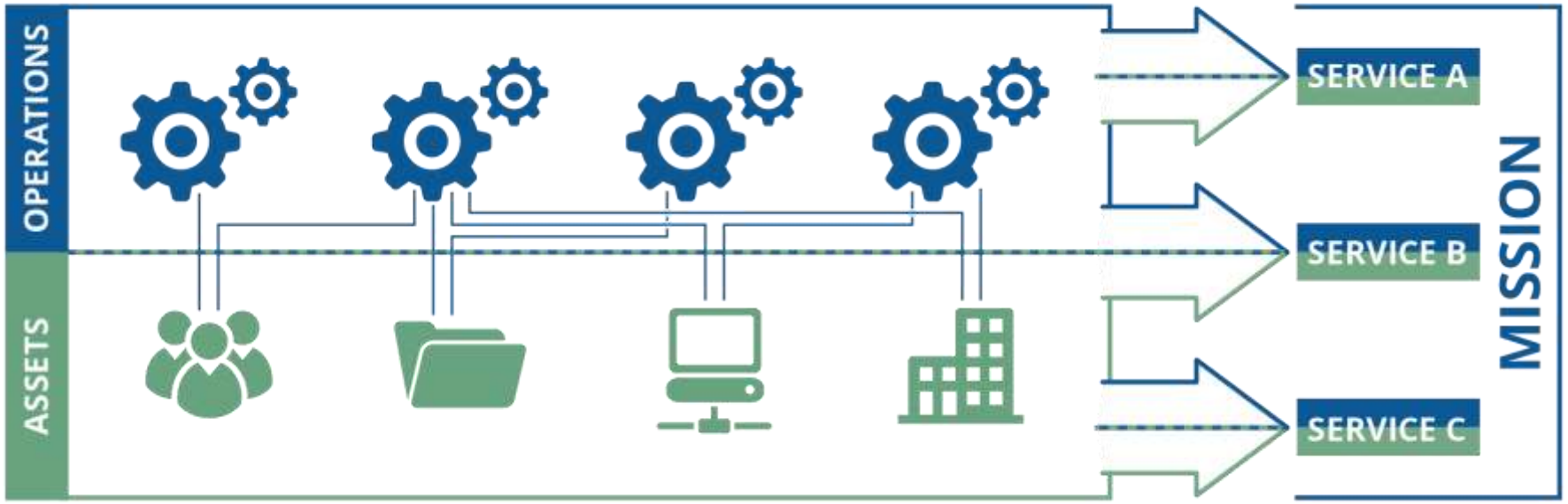
https://www.bleepingcomputer.com/news/technology/us-telco-fined-3-million-in-domain-renewal-blunder/

What Do We Mean By *Operational Resilience*?

- **Operational resilience:** the organization's ability to adapt to risk that affects its core operational capacities; the **emergent property** of an organization that can **continue to carry out its mission** after *disruption* that does not exceed its *operational* limit

"…the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"
–Presidential Policy Directive – PPD 21
Critical Infrastructure Security and Resilience
February 12, 2013

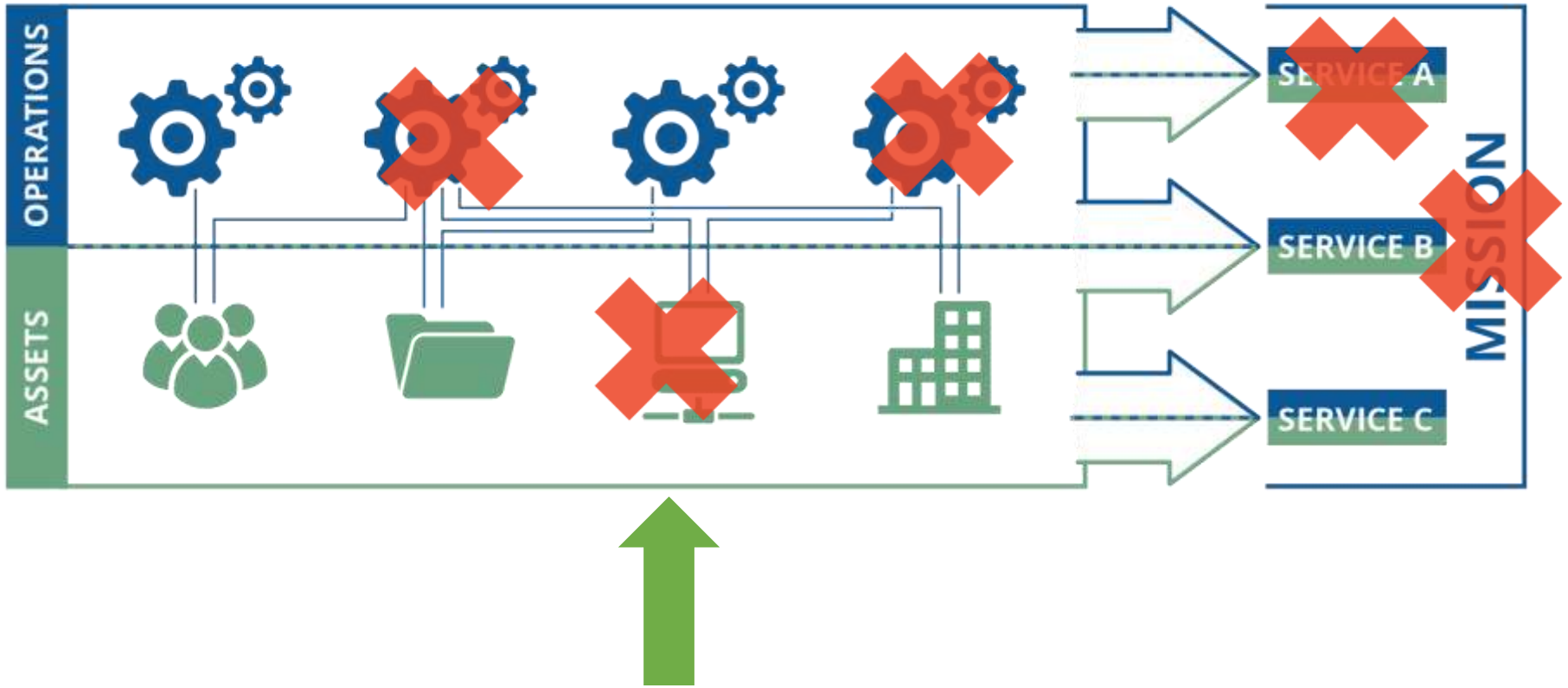
Assets Support Critical Services



- **People**: those who operate and monitor the service
- **Information**: data associated with the service
- **Technology**: tools and equipment that automate and support the service
- **Facilities**: where the service is performed

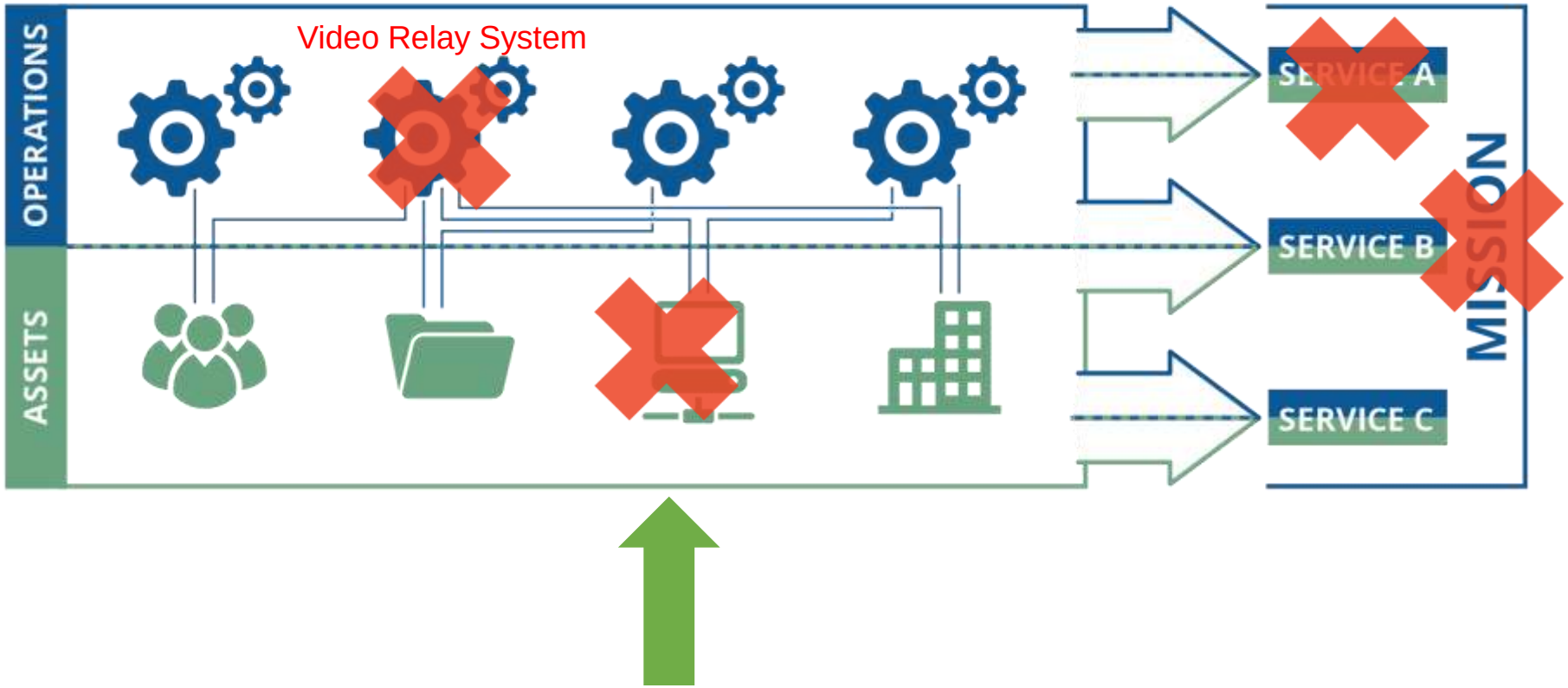
! Assets derive their value from their importance in meeting the critical services that achieve the organization's mission.

Disruption of Assets Can Lead to Mission Failure



Sorenson Communications

Provide 911 capability to deaf and those with vocal disabilities



Domain Name Goes Down

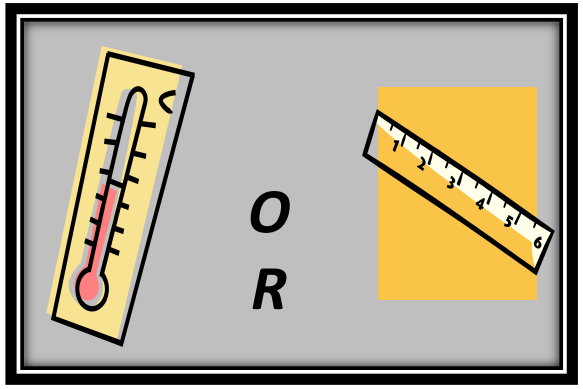
Cyber Resilience Value Proposition

- **Management** – gaining support for simplifying complex cybersecurity challenges
- **Efficiency** – establishing equilibrium by
  - Balancing risk and cost (most bang for your buck)
  - Achieving compliance as a by-product of resilience management
- **Standardization** – identifying what to do by
  - Using an overarching, standardized approach
  - Focusing time and effort on what needs to be protected
- **Ecosystem** – managing
  - Interdependencies
  - Internal and external organizational challenges and silos

Metrics Overview

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.

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

Designing a Meaningful Metric

Who is the metric for?

What is being measured?

Where is the data/information stored?

When/how frequently are the metrics collected?

Why is the metric important?

How is the data collected and used?

Attributes of a Meaningful Metric

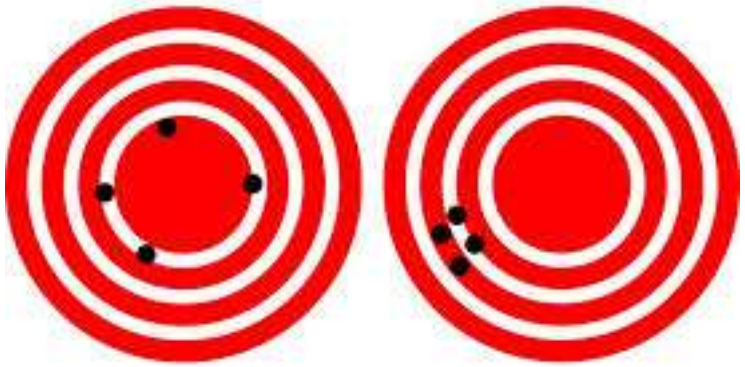
Accurate

Precise (Enough)

Timely

Objective

Cost Effective



Why is Measurement So Hard?

In short, we aren't asking the right questions.

What do I want to know or learn?

What decisions do I want to inform?

What actions do I want to take?

What behaviors do I want to change?

Informed by Douglas Hubbard, How to Measure Anything, John Wiley & Sons, 2010

First Things First

If what you are measuring doesn't drive action, consider if it should be measured at all.

- Provide data for decision making
- Answer key strategic questions
- Demonstrate that your security program has measurable business value
- Demonstrate that your control objectives are (and continue to be) met
- Justify new investments and to show improvement

Cyber Metrics and the Board

How Secure Are We?

When asked:

- How secure are we?
- Are we secure enough?
- How secure do we need to be?

What does this mean?

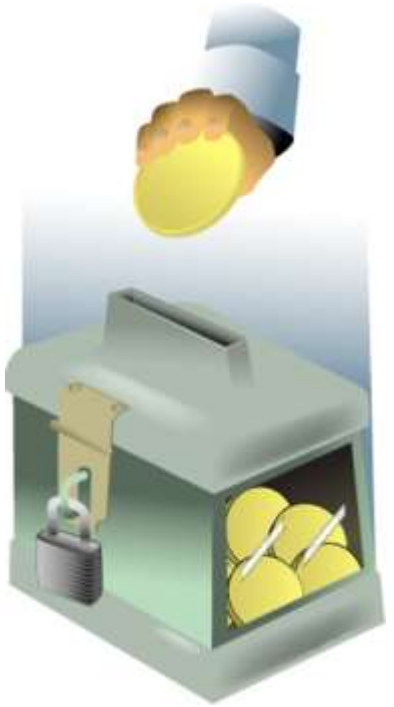
- How secure are we compared to our competition?
- Are we managing risks well?
- Do we need to spend more $$ on security or risk management? If so, on what?
- What are the legal and PR impacts of a data breach?

Key Questions

What should I be measuring to determine if I am meeting my strategic objectives for security?

What is the strategic value of being more secure?

What is the strategic value of a specific security investment?



Examples of Strategic Metrics - There are lots and lots

Strategic Metrics provide assurance that basic structures and policies are in place.

Metrics are often counting and yes-no measures and outcomes, for example:

- % of senior executives who have documented security objectives
- % of security policies that are met (no violations; all exceptions approved)
- number of incidents
- difference in planned vs. actual to perform security activities/actions/investments
- % of staff who have been assessed to determine if training has been effective
- number of exercises completed
- liaison with FBI and State agencies
- development COOP plans

Metrics also address Third Party assurance – acceptance/mitigation of the risk “We don’t know what we don’t know”.

- Often times addressed in the annual plan

But which metrics *should* we be monitoring?

It depends.

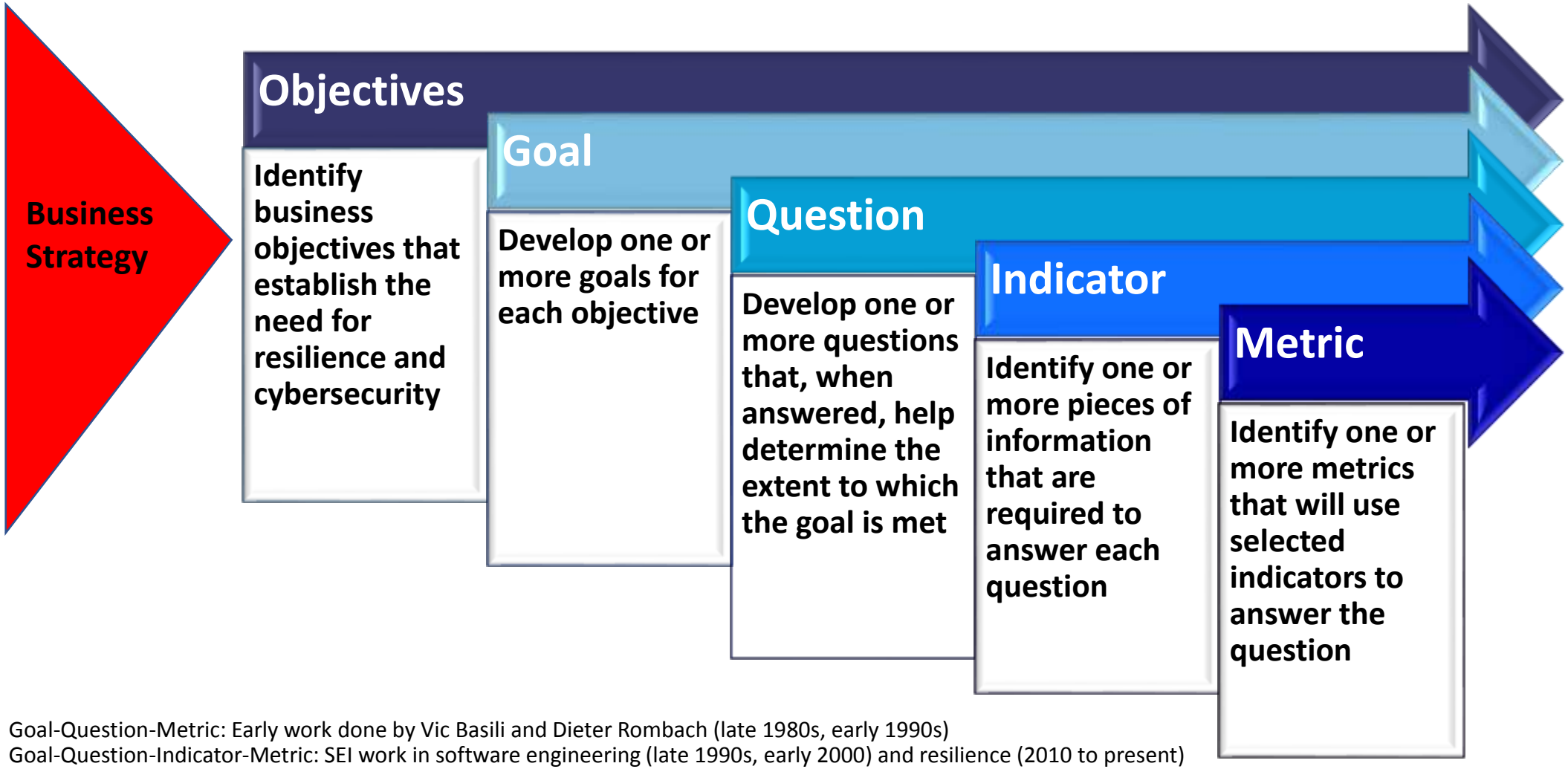
Goal-Question-Indicator-Metric (GQIM)

Purpose

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

GQIM process



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 resilience (2010 to present)

Incident Management GQIM Example

Business Strategy

"Develop and execute a proactive, company-wide security program based on Company's strategic business objectives."[1]

Objectives

Strategic Objective (Example):

"Continually Improve Cybersecurity Posture"

Business Objectives:

IDENTIFY – Enhance organizational capabilities to manage the cybersecurity risk.

PROTECT - Develop and implement enterprise controls to reduce risk and increase resilience; promote enterprise cybersecurity awareness through workforce development and training.

DETECT - Develop tools and processes to accelerate notification of cybersecurity threats.

RESPOND - Rapid analysis of, and response to, anomalies and suspected events.

RECOVER - Develop and implement an incident triage, response, and recovery process to contain and eliminate cybersecurity threats.

[1] https://www.csoonline.com/article/3257230/data-protection/building-a-cybersecurity-strategic-plan.html

Objectives to Goals

Objectives	Goals
RESPOND - Rapid analysis of, and response to, anomalies and suspected events.	Improve the reporting process for events/incidents
	Improve the process for detection of events
	Improve the process of hand-off/escalation of incidents
RECOVER - Develop and implement an incident triage, response, and recovery process to contain and eliminate cybersecurity threats.	Improve the process for investigation of incidents
	Improve the process for remediation of incidents
	Increase automation for incident investigation and remediation

Goals to Questions

Goals	Questions
Improve the process for detection of events	Is there a defined process for the detection of events?
	Is the process for detection of events documented?
	Do we have tools for event detection?
	Are events being detected?
	Are there events not being detected?
	Is there a tool for reporting events?
	Is the information for detected events documented?
	Is staff trained on detecting events?
	Is there a defined process for the detection of events?

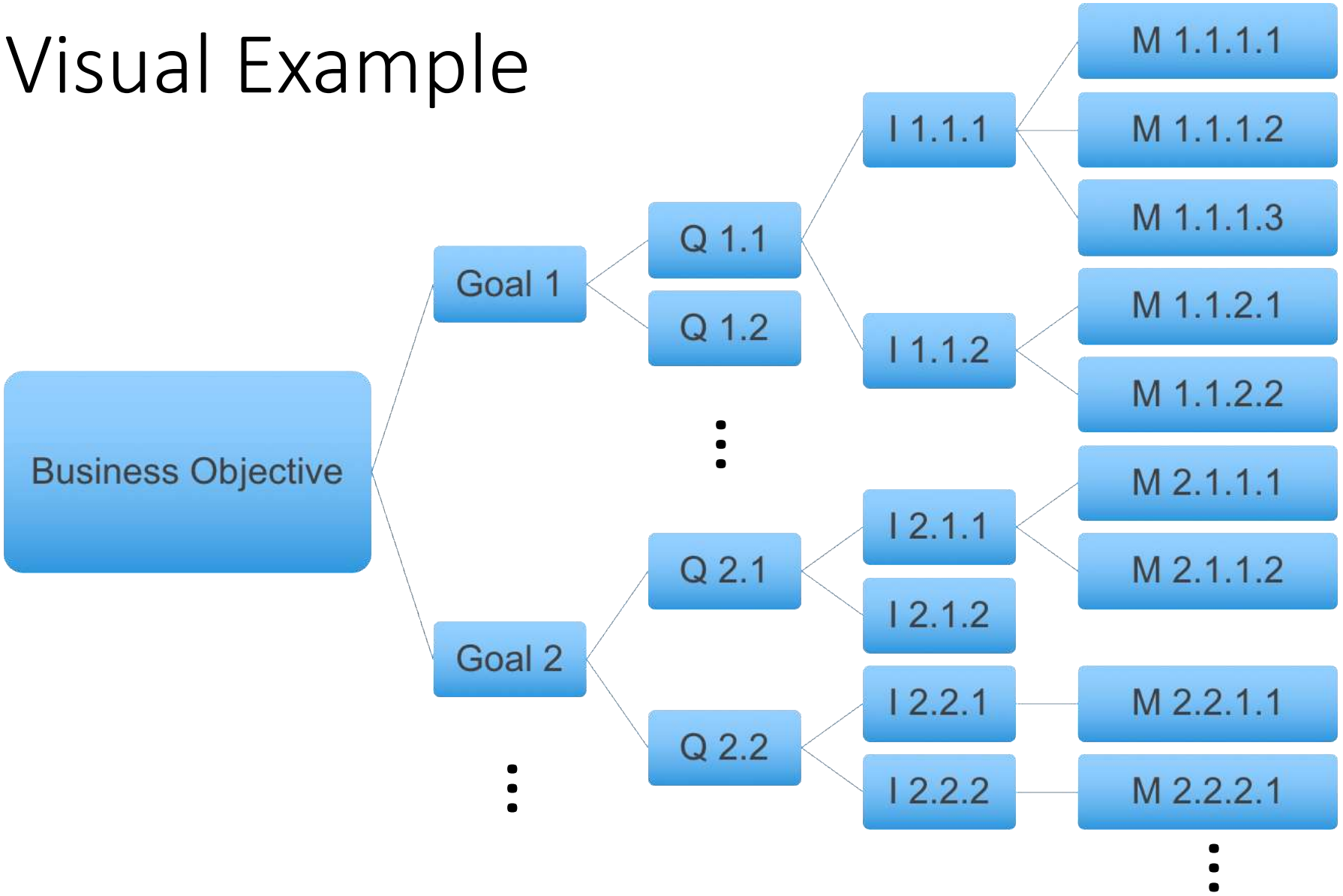
Questions to Indicators

Questions	Indicators
Do we have tools for event detection?	Tools Inventory
	Tool requirements for event detection are documented
Are there events not detected?	Late detection is indicated
	New alerts
	Gaps in investigation capabilities
Is the information for detected events documented?	There is a defined template for event reports
	Tickets are created/reviewed

Indicators to Metrics

Indicators	Metrics
Tools Inventory	Elapsed time since the tools inventory was updated
Tool requirements for event detection are documented	% of unfulfilled requirements for tool detection
	% of tools generating expected reports
	Number of out of date/unauthorized tools in operation
Late detection is indicated	Number of events that are detected “late”
New Alerts	Number of events that were not previously considered suspicious
Tickets are created/reviewed	% of tickets that get flagged in Q/A

GQIM Visual Example



Testing GQIM

Key Takeaways

Understand a 5-step process for deriving metrics from business or program objectives

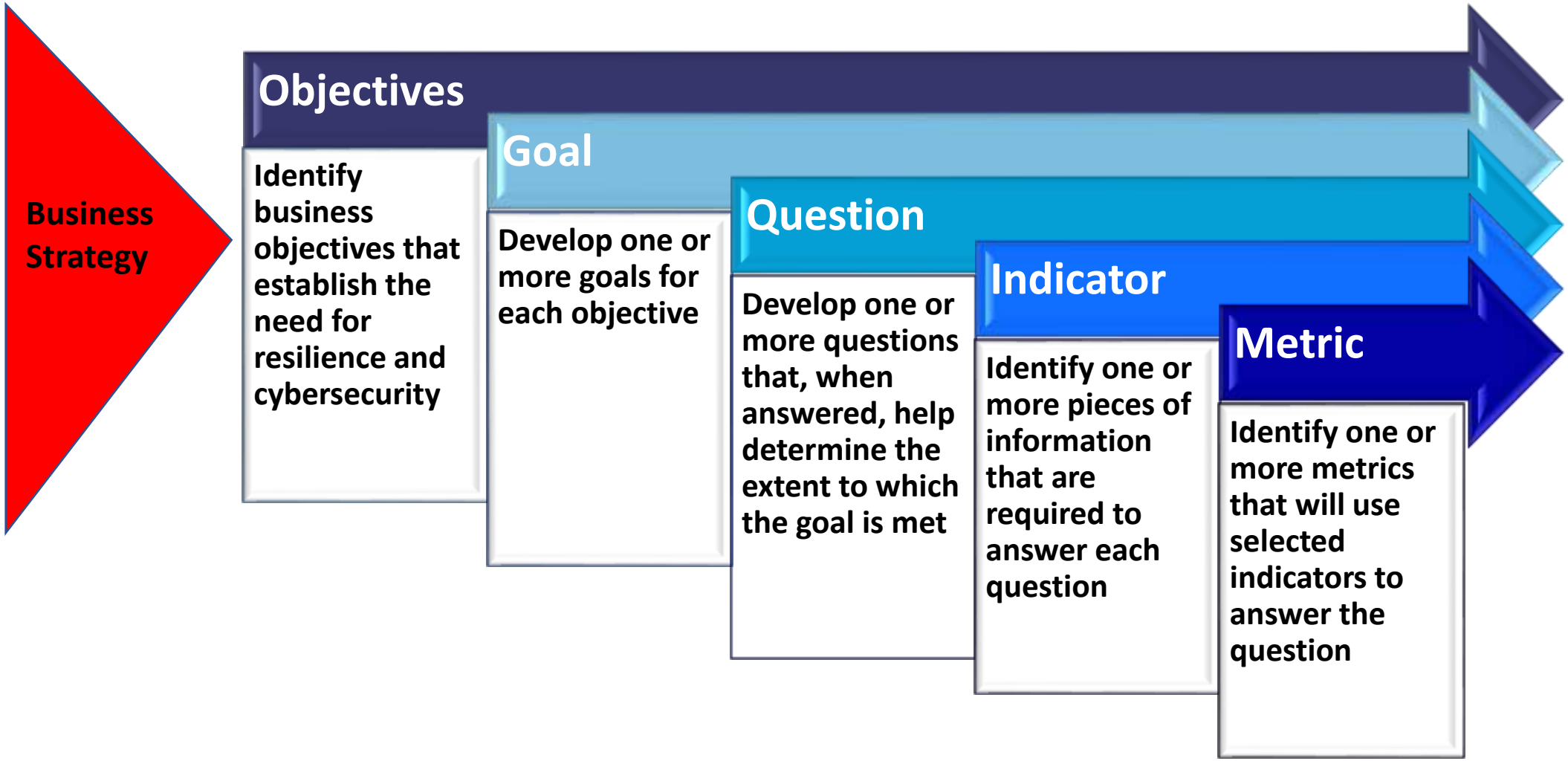
Be able to apply this process to your objective(s)

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



Activity

Choose one strategic objective from your organization – if you don't have one / don't know / don't like it, pick:

Develop and execute a proactive, company-wide security program

Use the Handout

Derive 1 Business Objectives

As a group, use the GQIM approach to develop a handful of possible metrics to address your business Objective

Pick a spokesperson

Measurement Resources

CERT Podcast: Measuring Operational Resilience
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=34512

CERT-RMM Measurement & Analysis website
http://www.cert.org/resilience/research/resilience-measurement-and-analysis.cfm

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

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 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

Hayden, Lance. *IT Security Metrics*. McGraw-Hill Education, 2010.

Hubbard, Douglas. *How to Measure Anything*. John Wiley & Sons, 2007.

Thank you!

Katie Stewart

kcstewart@cert.org