CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Measuring Operational Resilience

Key Message: Measures of operational resilience should answer key questions, inform decisions, and affect behavior.

Executive Summary

Fundamentally, measurement is about answering questions, informing decisions, and affecting behavior so that leaders can control current operations and, as best they can, predict the future. The CERT Resilience Measurement and Analysis (RMA) team is conducting research to identify and validate measures that provide maximum value in managing and improving operational resilience practices.

In this podcast, Julia Allen, a principal researcher with the CERT Program discusses the RMA team's work in measuring operational resilience.

PART 1: ANSWER QUESTIONS, INFORM DECISIONS, AND AFFECT BEHAVIOR

Definition of Operational Resilience

The ability of an organization to continue to provide critical services in the presence of operational stress and disruption that does not exceed its limit.

Stress and disruption come from, most often, the four categories of operational risk:

- deliberate or inadvertent actions of people (insider threat is an example)
- systems and technology failures, such as a security incident that might compromise a critical service
- failed internal processes that might result, for example, in customer data being publicly disclosed
- external events: severe weather, fire, earthquake, flood

Operational resilience emerges from the activities the organization performs to manage operational risk. The CERT Resilience Management Model (CERT-RMM) identifies those activities within three domains and the relationships among them: information security, business or service continuity, and aspects of IT operations.

Further foundational content on CERT's resilience work is available in previous podcasts listed in the Resources section below.

Key Questions of This Research

We started this work in 2010 by defining our terminology, foundational principles, and these key research questions:

- How resilient is my organization? How able is it to withstand a punch and to keep on going?
- Am I resilient enough?
- How resilient do I need to be? What's the threshold or what level of resilience am I aspiring to?
- Do I need to spend more money and if so, on what? And what am I getting for what I've already spent?
- What is the business value of being more resilient? There are many things that decision makers need to invest in; does resilience make the cut?

And for measurement:

- Once I've set those thresholds and targets, how do I measure whether I'm achieving them? What should I be

measuring to determine whether I'm meeting my performance objectives for resilience?

Implementation and Effectiveness Measures

This research has categorized and defined different types of measures. The two most noteworthy are *implementation* measures and *effectiveness* measures:

- Implementation measures evaluate whether the process is being performed and to what extent (for example, as evaluated against a process model such as CERT-RMM). They make no judgments about how well the process is being performed or if the process is resulting in improved resilience. Example: the cost or schedule to perform a process.
- Effectiveness measures evaluate the results being achieved. Example: difference in planned versus actual cost and schedule over time. Am I hitting my target or am I improving? And is this allowing me to do more with less?

A more technical example: The cost and schedule to detect and respond to a security incident. What do those measures tell me? What I really care about, on the effectiveness side, is the reduction in impact and consequences due to a security incident. Over time, is it taking less time between detection and response and recovery?

For further information, see our first report [1].

Strategic and Process-Area-Specific Measures

Research performed in early 2011 produced the following results:

- Identified a set of top ten strategic measures.
- Each of the 26 process areas (PAs) in CERT-RMM has an example set of measures. We did a horizontal integration of all measures in all 26 PAs, did a thorough review for consistency and clarity, added new measures, and corrected errors.
- Identified 36 global measures that apply across all 26 process areas, removed them from the individual PAs, and defined them.

This work is described in our second report [2].

Measures in the Context of Defined Processes

Measurement occurs in a context. If you haven't defined a meaningful context, it doesn't make a whole lot of sense to measure.

The activities defined in CERT-RMM describe what to do, not how to do it. So organizations need greater specificity to actually implement a process. This research has produced the following results:

- Examples of processes defined at the implementation level
- Templates for processes and supporting procedures
- Examples and templates for defining measures within the context of these processes

This implementation-level process definition work is available in our third report [3].

PART 2: STRATEGIC RESILIENCE MEASURES COMPLEMENT EXISTING SECURITY MEASURES

Strategic Measures Versus Type "Count" Measures

There are many communities, efforts, documents, standards, guidelines, etc. that describe how to measure information security. Our work is intended to complement these efforts.

Organizations typically collect measures of type count: number of incidents, number of systems with patches installed, number of people trained, number of compliance requirements met. Type count measures, while useful (because you can watch their trends over time), are not as effective in informing decisions; you're often missing the context for how those measures are used.

This research defines an operational resilience management system (ORMS) (or program) as the basis for measurement. The ORMS

- comprises all the elements that need to be in place for an organization to be operationally resilient
- describes at a strategic level how resilience objectives and requirements derive from organizational objectives, including a consideration for risk tolerance
- describes how those resilience objectives and requirements define the controls necessary to protect and sustain high-value services and assets
- describes managing both conditions and consequences. Conditions tend to be more on the information security side, the protect side; consequences tend to be more on the continuity side.

Regarding the community's standards and codes of practice, we've developed a mapping, the CERT-RMM Code of Practice Crosswalk, that maps to many of them, such as ITIL, COBIT, the ISO 27000 series, BS25999, and the Payment Card Industry Data Security Standard, PCI DSS.

Measurement is expensive to perform and sustain. Organizations need to ensure that anything that's being measured has a direct tie to a business strategy, critical success factor, or business objective. These strategic measures explicitly connect more detailed technical, tactical measures to business objectives.

Examples of Strategic Measures

One of the strategic measures relates to *realized risk*—a risk that you're managing and that actually happens, such as a disruption in continuity of a critical service. The measure is:

- In the face of realized risk, the ORMS ensures the continuity of essential operations. An alternative measure is the probability of delivered service in the presence of a security incident.

Business leaders want to know: If I take a hit, how able am I, in some measurable way, to know that I've prepared myself, that I've protected my key services and their supporting assets—the people, information, technology and facilities. Have I made all of those sufficiently robust to provide that service?

One supporting measure is:

- confidence that risks from all sources have been identified and prioritized. Am I confident that I know about and am managing all my risks? Or there may be certain risks that I accept or tolerate, knowing that I'll have to invest in some recovery action if any of those risks is realized.

Other strategic measures relate to demonstrating that

- high-value services and assets satisfy their resilience requirements
- controls that address those requirements are effective and adequate, or if they're deemed to be ineffective and inadequate, they are corrected
- risks to the assets that could adversely affect the organization's ability to deliver services are being effectively managed

Strategic measures are described in more detail in our second report [2].

PART 3: THOROUGHLY DEFINING A MEASURE; GETTING STARTED

Information Required to Define a Measure

A measure is thoroughly defined by the typical six questions Who, What, Where, When, Why, and How.

- Who is the measure for? Who will it be reported to, and how are they going to use it? Who are the stakeholders for the measure? Who is going to collect the data and make it available for analysis?
- What is being measured? And if (as we recommend) the measurement is being done within the context of a process, in what process, or processes, is it being done?
- Where is the data and information stored? You need to develop infrastructure, some type of data repository or a database, that you're going to use to house all of this information. And it too has to be protected and sustained.
- When, and how frequently, are the measures collected? Monthly, quarterly, biannually, annually?
- Why is this measure important versus others?
- How is the data collected? How is the measure analysis reported? What's the visual representation (e.g., histogram, some type of curve, Pareto diagram, Kiviat or spider chart)? The visualization is key for decision makers, and that ties back to who your key stakeholders are. And how will the measure be used? What decisions will it inform?

A template that defines all these fields is available in our first report [1], along with some examples.

Meaningful measurement information is often conveyed by reporting trends over time versus single measures at a particular point in time. So it may take a couple of reporting periods before you can determine the value of the measure.

First Steps for Starting a Resilience Measurement Program

These are some recommendations for getting started:

- Look to integrate resilience measurement into an existing measurement or reporting process, such as financial reporting. This would be optimal because you're then making it part of a normal business process, not something new.
- Identify who the measure is going to be for. Who are the sponsors and the stakeholders for this effort? What questions are you trying to answer or what resilience objectives are you trying to inform progress against?
- What information do you already have and what information do you need to collect and within what processes?
- Start small. Take a couple of key measures. Incident handling (incident response, incident recovery) is typically of interest. Pick a few measures in that particular process. Collect them, analyze, report, and refine.
- Put a bare bones measurement process in place: the role that's going to collect, the role that's going to analyze, how to visualize it, where to store the data.
- As time goes on, quantify the value of each measure. How much is it costing you to collect it? Are you deriving sufficient benefit for the cost that you've invested, both for an individual measure and in comparing measure A with measure B with measure C?
- Refine and retire measures over time. If there is a measure that is not informing any decisions or affecting any behavior, consider retiring it, refining it, updating it, or maybe combining it with another measure.

Resources

[1] 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.

[2] Allen, Julia, & Curtis, Pamela D. *Measures for Managing Operational Resilience* (CMU/SEI-2011-TR-019). Software Engineering Institute, Carnegie Mellon University, September 2011.

[3] Allen, Julia, Curtis, Pamela D., & Gates, Linda Parker. *Using Defined Processes as a Context for Resilience Measures* (CMU/SEI-2011-TN-029). Software Engineering Institute, Carnegie Mellon University, 2011.

Resilience Management website

SEI Measurement and Analysis website

CERT Podcasts on Resilience:

- How Resilient Is My Organization? December 2010
- Train for the Unexpected, March 2010
- Ensuring Continuity of Operations When Business Is Disrupted, November 2009
- Managing Relationships with Business Partners to Achieve Operational Resiliency, October 2009
- Resiliency Engineering: Integrating Security, IT Operations, and Business Continuity, October 2007
- Adapting to Changing Risk Environments: Operational Resilience, May 2007