Pre-publication draft. Published version can be found at http://www.igi-global.com/journal/international-journal-secure-software-engineering/1159 .

ADVANCING CYBER RESILIENCE ANALYSIS WITH PERFORMANCE-BASED METRICS FROM INFRASTRUCTURE ASSESSMENTS

For submission to
International Journal of Secure Software Engineering,
Special Edition on Cybersecurity Scientific Validation

July 13, 2012

Eric D. Vugrin (corresponding author)
Sandia National Laboratories
P.O. Box 5800
Mail Stop 1138
Albuquerque, NM 87185-1138
Phone: (505)284-8494
Fax: (505) 284-3850
Email: edvugri@sandia.gov

Jennifer Turgeon
Sandia National Laboratories
P.O. Box 5800
Mail Stop 1138
Albuquerque, NM 87185-1138
Phone: (505) 284-3630
Fax: (505) 284-3850
Email: jturgeo@sandia.gov

ABSTRACT

Cyber resilience is becoming increasingly recognized as a critical component of comprehensive cybersecurity practices. Current cyber resilience assessment approaches are primarily qualitative methods, making validation of their resilience analyses and enhancement recommendations difficult, if not impossible. The evolution of infrastructure resilience assessment methods has paralleled that of their cyber counterparts. However, the development of performance-based assessment methods has shown promise for overcoming the validation challenge. for infrastructure systems. This paper describes a hybrid infrastructure resilience assessment approach that combines both qualitative analysis techniques with performance-based metrics. The qualitative component enables identification of system features that limit resilience, and the quantitative metrics can be used to evaluate and confirm the effectiveness of proposed mitigation options. The authors propose adaptation of this methodology for cyber resilience analysis. A case study is presented to demonstrate how the approach could be applied to a hypothetical system.

Subject headings: resilience, cybersecurity, performance-based metrics, quantitative, validation, assessment

1. INTRODUCTION AND BACKGROUND

Cybersecurity is generally acknowledged as a critical priority within the national, homeland, and business security communities. This sentiment has been echoed at the highest levels of the U.S. government, with President Obama (2009) stating that "cyber threat is one of the most serious economic and national security challenges we face as a nation."

Fortunately, the concept of cybersecurity is not new to the academic and research communities. Cyber security standards and guidelines have been developed (e.g., see Smart Grid Interoperability Panel, 2010; IEEE, 2000, 2010a,b; NERC, 2002; ISO/IEC, 2000). These standards typically list best practices and provide guidance for securing various systems. Existing standards generally focus on mitigating system vulnerabilities to prevent a successful attack from occurring. Some guidelines, such as Guidelines for Smart Grid Cyber Security: Volumes 1-3 (Smart Grid Interoperability Panel, 2010), recommend prioritizing vulnerability mitigations by performing a risk assessment to determine which threats are of most significant concern. Within current standards, the primary focus is on preventing a successful attack. The current cybersecurity philosophy, as represented in these standards, centers on the detection and prevention of an attack.

However, over the past decade, a small but emerging movement within the cybersecurity community has voiced the opinion that cybersecurity strategies must expand beyond the protection-centric focus to incorporate cyber *resilience* principles. Cyber threats are constantly evolving and increasing as the number of cyber assets and system vulnerabilities continues to grow. As Goldman (2010) states, "The notion that we can achieve 100% protection is not only unrealistic but also results in a false sense of security that puts our missions and businesses at serious risk." Franklin D. Kramer (2011), Vice Chair of the Atlantic Council and former Assistant Defense Secretary for International Affairs, affirms that statement and adds that "we cannot assume protection and prevention will be adequate. And so we need resilience. "

Similarly, the private sector has recognized the need for resilience, as evidenced by the launch of the World Economic Forum's Cyber Resilience Initiative. This initiative is aimed at creating partnerships within the public and private sectors to foster cyber resilience (World Economic Forum, 2012). Similar opinions are becoming more common with events such as the STUXNET virus, the Chinese attack on Google, and suspected attacks on power grids. Hence, many have called for cyber resilience to become a primary system objective in cybersecurity activities.

Cyber resilience can be described as a cyber system's ability to function properly and securely despite disruptions to that system. Disruptions can be cyber or physical; they can also be intentional, accidental, or random. Over the past decade, organizations such as the Carnegie Mellon University's Software Engineering Institute and MITRE Corporation led efforts to develop cyber resilience management and design practices. These ground-breaking efforts are significant advances toward the development of resilient cyber systems. However, they have the same limitation that cybersecurity standards have: that is, they are descriptive methods that recommend approaches for increasing resilience, but the emerging cyber resilience standards have yet to be validated.

In parallel to cyber resilience-related efforts, the infrastructure protection community is developing infrastructure resilience assessment methods. Similarities exist between the evolutions of cyber and infrastructure resilience assessment methods. However, a class of infrastructure resilience assessment methods, termed performance-based assessment methods, overcame the validation limitation by evaluating system outputs rather than system structure and design. By measuring the performance of infrastructure systems rather than system structure and attributes, performance-based assessment methods address the central resilience issue: can the infrastructure system continue to deliver critical services in the presence of disruptive events?

This paper presents a particular performance-based infrastructure resilience assessment framework that shows promise for extension to cyber resilience. In the following section, the paper reviews recent resilience assessment methods from the cyber and infrastructure communities and the parallel evolution of their respective assessment methods. The paper then introduces a performance-based infrastructure resilience assessment framework developed at Sandia National Laboratories. An example application is included to demonstrate how the framework could be applied to cyber systems. The paper concludes with recommendations for further development of the framework and its customization to cyber systems.

2. RESILIENCE ASSESSMENT METHODS

Resilience is not a new concept. Holling (1973) is generally credited with giving the first systems-based definition of resilience almost 40 years ago. Since that time, the concept has been explored in a number of different fields, with significant advances being made over the past decade for both cyber and infrastructure security. This section describes the latest cyber resilience assessment methods and their parallel evolution in the field of infrastructure security.

Resilience assessment methods for cyber systems can be separated into two categories. Cyber resilience design methods consider primarily how system architecture and activities enhance the resilience of the system to cyber threats. The second category, operational resilience assessment methods, takes a broader look at how business operations, in addition to system design, can

enhance resilience of the overall system that the cyber system supports. Operational resilience methods consider physical threats and accidents, in addition to cyber threats. For the purposes of this paper, the authors include both categories in a discussion of cyber resilience assessment methods because of the integral role that cyber systems have within the methods.

Cyber Resilience Engineering Framework

Goldman (2010) and Bodeau and Graubart (2011) have described the Cyber Resiliency Engineering Framework (CREF) developed as part of the Resilient Architecture for Mission Assurance and Business Objectives (RAMBO) effort at the MITRE Corporation. The CREF is intended to describe how to engineer cyber-resilient architectures. The ability to anticipate, withstand, recover, and evolve are listed as high-level goals. These goals are achieved by meeting eight cyber-resilience objectives: understand, prepare, prevent, continue, constrain, reconstitute, transform, and re-architect. Objectives can be achieved by performing resilience practices, such as adaptive response to an attack, deception, realignment, etc. Subsequent iterations have expanded the framework. Bodeau et al. (2012) have developed almost 300 metrics for consideration in resilience analyses. Hassell (2012) provides additional metric considerations.

Despite the advancements of the CREF toward quantitative resilience analysis, it still does not provide a practical, tested approach for evaluating and validating the resilience of cyber systems. First, with hundreds of metrics to choose from, the sheer volume is daunting; selection of the appropriate set of metrics could be difficult for even a trained analyst. Second, many of the proposed metrics focus on measuring an aspect of the system architecture. However, Bodeau et al. (2012) do not indicate how that measurement ultimately affects the system's ability to "maintain an acceptable level of service," i.e., cyber resilience as defined within the framework. Third, the authors have been unable to find any documentation of how these metrics have been applied in a quantitative resilience analysis. It is not clear whether the metrics should be aggregated into a single resilience metric or if they need to be considered independently. Bodeau et al. (2012) do not provide mathematical equations or frameworks that indicate how the metrics should ultimately be combined to provide a quantification of resilience. Hence, it is uncertain how simply or practically the metrics can be applied to actual cyber systems and attack scenarios. These framework limitations make it very difficult to validate the expected benefits of using the CREF design principles.

In its initial inception, the framework's primary benefit is that it provides a means for structured discussions on cyber resilience, according to Bodeau and Graubart (2011). Additional work on metric development is required before validation can be considered an additional benefit.

Operational Resilience Assessment Methods

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) approach, a security self-assessment methodology that addresses information risk, was developed by the Carnegie Mellon Software Engineering Institute (Alberts and Dorofee, 2001). The approach attempts to balance the contributions that technology, individuals, and organizational structures make toward resilience of the overall organization.

OCTAVE consists of three high-level phases:

1. **Build asset-based threat profiles**. In the first phase, the organization identifies critical information assets and procedures currently in place to protect those assets.

2. **Identify infrastructure vulnerabilities.** After identification of critical assets, the analysis team evaluates technology vulnerabilities that can result in negative impacts on critical assets.

3. **Develop security strategy and plans.** The final phase consists of evaluating the risks to the critical assets and determining how the organization will respond to and mitigate those risks.

Detailed guides were developed to assist the implementation of the methodology. These guides describe individuals who should be represented on the analysis team; processes associated with each phase; meeting schedules, durations, and objectives; materials (meeting slides and workbooks); and other information necessary for performing an OCTAVE evaluation. The OCTAVE process is highly reliant upon the use of organizational subject matter experts as members of the assessment team. In its formal application, it is a very thorough and time-consuming process.

Alberts et al. published the original OCTAVE approach in 1999, and the OCTAVE criteria were later released in 2001 (Alberts and Dorofee, 2001). Given the level of rigor, time, and information required for implementation, OCTAVE was originally developed for large companies (more than 300 employees). OCTAVE-S was subsequently developed for smaller organizations, and OCTAVE-Allegro was created to provide a stream-lined assessment that required less time, expertise, and subject matter representatives (Woody et al., 2006). All three versions are highly qualitative processes, though OCTAVE-Allegro contains a semi-quantitative component for considering relative risks. Ultimately, each approach provides organizations with a risk-based road map to addressing information security gaps.

The CERT Resilience Management Model (CERT-RMM), Version 1.0, evolved from OCTAVE research and was published in 2010. This CERT-RMM is a maturity model for managing operational resilience, comprising the disciplines of security management, business continuity management, and aspects of information technology operations management. Model outputs identify gaps in processes that could be improved for better operational resilience. CERT-RMM allows for a capability rating to be earned on implementation of each process area implemented within an organization. These capability ratings provide a method for monitoring process improvements over time.

Caralli et al. (2010) define operational resilience as an "organization's ability to adapt to risk that affects its core operational capacities." At a high level, CERT-RMM uses a holistic approach to assess operational resilience. CERT-RMM includes four different categories of organizational process areas. The engineering category includes six process areas such as controls management and service continuity; the enterprise management category has seven process areas such as communications and human resource management; the operations management category

includes access management, knowledge and information management, and 7 other process areas; and the process management category includes monitoring, measurement analysis, and two other related categories. For each process area, the CERT-RMM includes (White, 2012):

1) Specific and generic goals;
2) Specific and generic practices that describe how to achieve those goals; and
3) Sub-practices that describe how to implement the practices.

Using this structure, CERT-RMM provides a semi-quantitative method for assessing the implementation of the process areas. Implementation of each process area can be assessed a Level of 0, 1, 2, or 3 that corresponds to the degree with which the process in institutionalized. Level 0 indicates the lowest degree of institutionalization. Increasing levels indicate greater degrees on institutionalization. Level 3 is the best achievable level since greater institutionalization is an indicator of repeatable and predictable processes (Caralli et al., 2010).

In an attempt to measure and analyze operational resilience, Allen and Davis (2010) established six high-level objectives for managing operational resilience and a template for developing measures that align with the six objectives. The template is based upon a core set of measurement concepts established to provide a clear understanding of the theory behind the measurement template. Allen and Curtis (2011) expanded upon this research by developing a list of ten strategic measures derived from Allen and Davis's objectives. Allen and Curtis also added measures for each of the 26 CERT-RMM process areas. These measures allow an organization to set priorities for its operational resilience and to establish baselines and measure improvements for those priorities. Strategic measures, used collectively, can provide a view of an organization's operational resilience.

The measures established by Allen and Curtis are intended to quantify the current state of an organization's resilience as well as to identify resilience improvements resulting from new or improved processes. Interpretation of these measures is dependent upon the specific environment for which they were developed. These measures are not intended to compare resilience of one organization's activities to another, although one might implicitly make this comparison. Additionally, interpretation of these measures requires domain expertise in each of the CERT-RMM process areas and generic practices.

Two assessment methods were developed to accompany the CERT-RMM model. The Resilient Enterprise Management Team (2011) developed the CERT-RMM Capability Appraisal Method (CAM), which is based upon the Standard Capability Maturity Model Integration (CMMI) Appraisal Method for Process Improvement (SCAMPI). A CAM appraisal provides capability level ratings for organizations implementing CERT-RMM. The Compass tool was developed to provide companies with a quick assessment of their CERT-RMM implementation. Both of these methods require qualitative review of objective evidence to derive characterizations of model practice implementation.

The U.S. Department of Homeland Security (DHS) also developed a Cyber Resilience Review (CRR) method that is derived from CERT-RMM principles. This method was developed through the Cyber Security Evaluation Program within DHS's National Cyber Security Division. CRRs focus on operational resilience and are included as part of DHS recommendations for

cybersecurity activities to protect critical infrastructure and key resources (U.S. Department of Homeland Security, 2012a). The CRR is an evaluation of an organization's overall cybersecurity management policies, practices, and procedures that provides repeatable results (U.S. Department of Homeland Security, 2012b). Its output is a report that highlights strengths and weaknesses within 10 domains similar to CERT-RMM process areas and across four asset types: people, information, technology, and facilities.

These primarily qualitative operational resilience assessment methods, especially OCTAVE and CERT-RMM, have undergone extensive research and have been tested across industry. They require detailed, contextual reviews of organizational assets by both business and technical subject matter experts. The outputs identify gaps in processes that could be improved to better organizational resilience. However, these assessment methods do not provide an overall measure for operational resilience across a system, nor do they provide a measure for determining system impact and recovery efforts when crises do occur.

From a process implementation perspective, OCTAVE, CERT-RMM, and other operational resilience assessment methods work well. They are highly structured and come with an incredible amount of supporting materials that describe how to implement them. Additionally, the methods provide explicit information on how resilience could be improved. The primary implementation drawbacks are the effort and time required to apply the processes, although the evolution of OCTAVE-Allegro, OCTAVE-S, Compass, and CAM Class B and C appraisals do lessen that burden somewhat.

From a risk validation perspective, these methods are less than ideal. The methods rely primarily on qualitative and semi-quantitative assessments from subject matter experts. This reliance can make it difficult to defend and validate risk and resilience assessments. Limited quantification can also hinder attempts to prioritize improvement efforts. Funding to address all security gaps rarely exists, so the ability to prioritize use of scarce resources is an important consideration. The qualitative nature of these assessment methods makes prioritization a highly subjective endeavor. Finally, because these methods do not provide a measure of how organizational performance will improve if certain efforts are undertaken, it is difficult to validate the effect the investments will have on the overall resilience of the organization's operations. The addition of a measure to support improvement prioritization could enhance the results provided from these assessment methods.

Infrastructure Resilience Assessment Methods

Examination of operational and cyber resilience assessment development over the past decade shows a steady trend toward increasingly quantitative analysis. The OCTAVE and CREF frameworks both started as primarily qualitative methods. OCTAVE-Allegro was subsequently developed and includes a semi-quantitative methodology that assigned numerical values to qualitative risk features of the systems under study. The CERT-RMM followed and includes almost 60 pages of suggested metrics and measures. Bodeau et al. (2012) describe a similar advance by the CREF framework toward a more quantitative approach to resilience evaluation.

Over this same time period, infrastructure resilience assessment methods followed a similar trend. For example, the Multidisciplinary Center for Earthquake Engineering and Research's (MCEER's) initial resilience methodology was a primarily qualitative approach. MCEER's TOSE framework described four resilience domains, Technical, Organizational, Social, and Economic (TOSE), and the four fundamental properties of resilience—robustness, redundancy, resourcefulness, and rapidity—that contributed to resilience across these domains (Bruneau et al., 2003).

A number of semi-quantitative indices have followed. Cutter et al. (2010) use 36 socioeconomic variables to calculate baseline resilience indicators for communities to evaluate the resilience of communities to natural disasters. Pettit et al. (2010) used the Supply Chain Resilience Assessment & Management (SCRAM) tool to assess supply chain resilience. The SCRAM tool relies on gathering information using a 152-question survey about a supply chain's vulnerabilities and capabilities. Fisher and Norman (2010) developed a resilience index for the Enhanced Critical Infrastructure Protection Program. DHS and its protective security advisors (PSAs) collect more than 1500 pieces of data for an infrastructure asset using the Infrastructure Survey Tool. These data are used to provide protective measure, vulnerability, and resilience scores.

Although the infrastructure protection and cyber communities both have qualitative and semi-quantitative resilience assessment methods, a third type of assessment approach, not found in the cyber community, was developed for infrastructure resilience assessment. This set of approaches, termed performance-based resilience assessment methodologies, is usually quantitative and estimates resilience by measuring the performance of a system in a particular scenario (i.e., a particular hazard or threat condition). Performance of a system is measured by metrics that vary across methodologies and applications, but the underlying logic of these methods is similar. Most metrics can be distilled to a single metric that describes simply the resilience of a system, and most metrics are used to compare the resilience of different systems. Rose (2007), Chang & Shinozuka (2004), and ASME-ITI (2010) have all proposed metrics for quantitatively measuring the resilience of a particular system. MCEER has further expanded the TOSE framework to include a resilience loss calculation.

In contrast to qualitative and quantitative methodologies, the performance-based methods examine direct observations of the performance of a system (or a simulated system) after a disruption. While qualitative assessment methodologies can be considered "a more holistic approach" (ASME ITI, 2010) to assessing resilience, performance assessment methodologies offer a more precise, validated approach. The qualitative assessment methodologies can be thought of as predictions of how a system may exhibit resilience or explanations of why a system exhibited resilience after the fact, while the performance-based methods provide validation of resilience—a measure of how much resilience a system actually exhibited. This capacity for validation is a significant gap in the set of existing cyber resilience assessment methods. Vugrin et al. (2010a,b; 2011a,b) have introduced a hybrid resilience assessment methodology that combines the strengths of qualitative and quantitative methods to address that gap. The hybrid approach enables both the identification of system weaknesses and resilience enhancement opportunities and a mechanism for measuring and validating the realized benefit of the enhancements. The following section describes Vugrin et al.'s method.

3. A TWO-DIMENSIONAL, HYBRID RESILIENCE ASSESSMENT FRAMEWORK

Vugrin et al. developed an infrastructure resilience assessment framework that expands upon previous performance-based methods. The framework has four primary components:

1. A new definition of resilience that identifies system components required for a resilience assessment;
2. A quantitative methodology that measures system resilience;
3. A qualitative methodology that can be used in place of, or to explain, quantitative results; and
4. A resilience assessment process that formalizes the application of the resilience framework.

Application of the framework to an infrastructure system can provide infrastructure analysts answers to the following questions related to resilience:

1. What are the consequences resulting from decreased infrastructure performance occurring after a disruptive event?
2. What are the costs associated with recovery from that event?
3. What are effective strategies for responding to disruptive events?
4. What preparations and investments should be made prior to the occurrence of a disruption?
5. What balance should be found between investment costs, recovery costs, and damage costs to enhance resilience, especially in a resource constrained environment?

Defining Resilience

Vugrin et al. define resilience as follows:

> Given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events) is the ability to reduce efficiently both the magnitude and duration of the deviation from targeted system performance levels.

As indicated in the definition, system performance is a key factor in evaluating resilience. Given the flexibility of many systems to adjust and reconfigure to a disruptive event, maintaining system structure is not as important as maintaining system performance. Hence, measurement of resilience includes evaluation of how a disruption affects system performance and causes productivity to decrease relative to targeted system performance levels.

The concept of efficiency is a second dimension of resilience that is unique to this resilience definition. Efficiency refers to the resource utilization that occurs during response and recovery activities that initiate after a disruption occurs; depending on the domain, these resources could be measured in dollars, repair man-hours, equipment, time, or similar metrics. In the event of a disruption that affects multiple system components, resources may not be available to repair all impacted components simultaneously. Systems may be competing for scarce resources; hence, the ability to recover efficiently will enhance the overall resilience of the system. All things

being equal, a system that recovers more efficiently than another should be considered more resilient. Thus, Vugrin et al. assert that both system performance and efficiency measures must be considered in resilience assessment and measurement.

Measuring Resilience

Vugrin et al.'s definition of resilience leads to a mathematical calculation for resilience costs: i.e., the comprehensive accounting of consequences resulting from a system disruption. The resilience cost measurement approach requires quantification of two key dimensions: systemic impact (*SI*) and total recovery effort (*TRE*).

SI is the cumulative impact that a disruption has on system productivity and is measured by evaluating the difference between a targeted system performance (*TSP*) level and the actual system performance (*SP*) following the disruption. Figure 1(a) graphically represents systemic impact for a hypothetical system that has been disrupted. In this example, system performance decreases immediately following the disruptive shock that occurs at time *t0*. With the onset of recovery actions, performance levels first stabilize, then eventually increase, and ultimately attain targeted system performance levels. At this point in time (*tf*), recovery is considered complete. *SI* is quantified by calculating the area between the *TSP* and the *SP* curves. Equations (1) and (2) demonstrate how to calculate *SI* if *SP* and *TSP* are represented as continuous or discrete mathematical functions, respectively.
TSP levels represent a performance goal for the system and care should be used when selecting the *TSP* levels since they can significantly affect the calculation of *SI*. Selection of the TSP levels can be a subjective process. Frequently, *TSP* levels are set equal to nominal or pre-disruption performance levels, indicating that the goal of recovery actions is to return the system to its normal operating levels. *TSP* levels for emergency systems may actually exceed nominal performance levels since these systems are needed most during times of crisis. *TSP* levels for systems that are exceeding minimum performance levels at the time of a disruption may be lower than normal operating levels. Hence, the selection of *TSP* levels depends on the system objectives, operating levels at the time of the disruption, and other related factors.

It should be noted that *TSP* levels are intended to represent performance goals, not minimum performance requirements. The *SI* quantity is intended to represent the impact of not performing at a desired level. In some scenarios, individuals may want to assess a system's ability to perform above a minimum requirement. Vugrin et al.'s resilience calculation methodology is not appropriate for that type of analysis. At a minimum, the results would need to be interpreted differently since a small SI value is preferable when defined with Equations (1) and (2). If *SI* is calculated as the difference between *SP* and minimum performance standards, the opposite is true, i.e., increasingly large *SI* quantities indicate increasing levels of resilience.

$$SI = \int_{t0}^{tf} \left[TSP(t) - SP(t) \right] dt. \qquad \textbf{(1)}$$

$$SI = \sum_{i=1}^{f} \left[TSP(t_i) - SP(t_i) \right] (t_i - t_{i-1}) \quad \textbf{(2)}$$

TRE represents the total resource usage from recovery activities that initiate after a disruptive event occurs. This quantity provides a measure of efficiency. After the disruption initiates, the recovery response begins and resources are expended in this effort. The *TRE* is represented by the area under the recovery effort (*RE*) curve in Figure 1(b). Equations (3) and (4) demonstrate how to calculate *TRE* if *RE* is represented as a continuous or discrete mathematical function.

$$TRE = \int_{t0}^{tf} \left[RE(t) \right] dt. \quad \textbf{(3)}$$

$$TRE = \sum_{i=1}^{f} \left[TRE(t_i) \right] (t_i - t_{i-1}) \quad \textbf{(4)}$$

Vugrin et al. calculate the recovery dependent resilience (*RDR*) cost using Equation (5) to measure resilience.

$$RDR(RE) = \frac{SI + \alpha \times TRE}{Norm} \quad \textbf{(5)}$$

Since *SI* represents the performance impacts of the disruption and *TRE* represents the resources and costs expended to recover from the disruption, the numerator in Equation (5) captures the total impacts of the disruption. The parameter α in Equation (5) is a non-negative weighting factor that allows the analyst to assign the relative importance of the systemic impact and total recovery effort terms. Assigning a small positive value to α weighs the systemic impact more heavily; a large positive value for α weighs the cost of recovery more heavily. To equally weight *SI* and *TRE*, α is set to 1.

RDR is a unitless quantity that measures the total impacts of a disruption on a system under a specified recovery effort, *RE*.[i] The *RDR* variable is a linear combination of *SI* and *TRE*. The denominator is a normalization factor that permits the comparison of the resilience of systems whose system performance levels may be of different magnitudes. Vugrin et al. recommend calculating *Norm* with Equation (6) or (7) when TSP can be represented as a continuous or discrete mathematical function. These equations quantify the magnitude of the system by calculating the cumulative targeted system performance during the recovery period.

$$Norm = \int_{t0}^{tf} \left| TSP(t) \right| dt \quad \textbf{(6)}$$

$$Norm = \sum_{i=1}^{f} \left| TSP(t_i) \right| (t_i - t_{i-1}) \quad \textbf{(7)}$$

RDR and resilience are inversely related; that is, larger *RDR* values imply larger impacts from the disruption, and therefore, lesser resilience. Smaller *RDR* values imply higher resilience. Because the *RDR* values are dimensionless quantities, they are most informative when used in a comparative manner. For example, *RDR* values can be used to compare the resilience of a system before and after resilience-enhancing investments. A decrease in the *RDR* value would confirm the benefit of the investment; the magnitude of the decrease would indicate how much of a benefit. *RDR* values can also be used to compare the resilience of the same system to different types of disruptions. Moreover, they can be used to compare the resilience of a system to a disruption under different recovery strategies. Each different recovery strategy will result in different *SI* and *TRE* values. The recovery strategy that results in the smallest *RDR* values will provide maximal resilience for the system.

Analyzing Resilience

Objectively evaluating a system's resilience and verifying the impact changes will have is an important step in resilience analysis. It is equally important to understand the features of the system that are constraining or enhancing resilience. Hence, Vugrin et al.'s assessment framework contains a qualitative analysis component that can be used to explain the results of quantitative measurements. The combination of performance-based quantitative methods and a qualitative systems analysis results in a hybrid framework that can enable comprehensive resilience assessment.

The qualitative analysis is performed through consideration of system structures, characteristics, and features. This portion of the framework uses three fundamental system capacities (absorptive capacity, adaptive capacity, and restorative capacity) to formulate how properties of a system can determine system resilience, specifically by reducing *SI* and *TRE*. These capacities are affected by resilience enhancement features; that is, the features of the system that are in place before a disruption and that affect one or more of the system's capacities. Figure 2 indicates how the resilience capacities contribute to system resilience and differ from each other.

Absorptive capacity is the degree to which a system can automatically absorb the impacts of system perturbations and minimize consequences with little effort. The absorptive capacity is an endogenous feature of the system. Factors such as redundancy, separation, and robustness contribute to a system's absorptive capacity. For example, physical and virtual separation of redundant data centers can enhance resilience to both physical disruptions (e.g., floods, earthquakes) and cyber attacks. Even redundancy in hardware, software, and services, as Goldman (2010) recommends, would contribute to the absorptive capacity of the system and ultimately enhance resilience.

Adaptive capacity is the degree to which the system is capable of self-organization for recovery of system performance levels. It is a set of properties that reflects actions that result from ingenuity or extra effort over time, often in response to a crisis situation. It reflects the ability of the system to change endogenously during the recovery period. Bodeau and Graubart (2011) list "employing applications not previously presented to the adversary, repositioning of critical assets, and changing the configuration of networks, systems, or applications" as examples of adaptive responses that can enhance resilience to cyber threats. Utilization of uninterrupted

power supplies (UPSs) and backup diesel generators is a nonstandard practice during normal business operations. During a power outage, however, this change in operations can enhance resilience to that outage. Using paper forms rather than electronic forms is a form of substitution that is normally more time-consuming and less efficient, but these adaptations could prove useful if electronic systems are unavailable. Adaptive capacity is generally determined by a combination of human and automated activities.

Restorative capacity is the ability of a system to be repaired easily, and these repairs are considered to be dynamic, beginning after the disruption initiates. Similar to adaptive capacity, human and automated actions contribute to restorative capacity. Systems that have the ability to self-segment and isolate compromised components can minimize system-wide damage and lead to faster recovery. Software that enables an automated graceful degradation rather than a hard shutdown can facilitate recovery. Preparedness through development, training, and testing of contingency plans enhance human responses that contribute to restorative capacities. Previous experience with disruptions can also help.

Identifying resilience enhancement features and how they contribute to the resilience capacities provides an understanding of fundamental characteristics that contribute to resilience. The goal of resilience enhancement should not necessarily be maximizing each resilience capacity. Rather, the goal should be finding the right combination of resilience enhancement features for the system under consideration. The right combination of pre-disruption preparatory actions can target the appropriate resilience enhancement features to increase the resilience of the system.

Applying the Process

The final component of the resilience assessment framework is the process in which one applies the framework. The process consists of six primary steps that should be considered when applying the framework (Figure 3). These steps include:

1. **Define System(s):** In the first step, the analyst must choose a system or systems and identify details of that system. Multiple systems may be identified if the analyst is interested in comparing systems. The analyst may answer questions such as "What system is being considered?" and "What are the boundaries of the system?" Examples of factors to consider in the context of cyber systems include relationships between databases, limitations on data sharing within an information technology (IT) system, access controls, and system architectures.

2. **Define Scenario(s):** The analyst should define a disruption scenario or multiple scenarios if interested in comparing resilience across different events. Historical scenarios may be based on actual events, while hypothetical scenarios should be plausible, although not necessarily high-probability events. The analyst should consider how events in a scenario disrupt systems and what recovery processes might occur; that is, the analyst should qualitatively identify system performance and recovery efforts. Examples of scenario considerations for cyber systems could include evaluation of specific cyber and/or physically disruptive events; whether these events actually damage system components or simply render them non-functional; cascading impacts resulting from system or data

dependencies; and activities necessary to stabilize the system and ultimately get the system back online.

3. **Define Metrics:** The previous step qualitatively identifies system performance and recovery efforts. Step 3 requires metrics that measure these processes be identified. Metrics must be identified for system performance, targeted system performance, and recovery efforts. In general, any number of metrics can be found, but in practice there is usually a single metric for system performance and corresponding targeted system performance, and multiple metrics for recovery effort. As noted by the CREF and CERT-RMM, hundreds of possible metrics exist for cyber systems. Application response time for queries, mean and actual time to repair, mean and actual time between failures, and mean and actual down time are possible metrics for consideration. However, when attempting to identify the appropriate metric, it is important to recognize what functionality the cyber system is intended to support. This caution is consistent with Bishop et al.'s (2011) argument that metrics for resilience need to be developed on a site-by-site basis. Hence, in some cases, performance metrics may be more physical in nature. For example, power delivery might be a suitable performance metric for SCADA (Supervisory Control and Data Acquisition) systems supporting the power grid.

4. **Obtain Data:** The fourth step is the collection of system performance and recovery data for the *RDR* calculations. Data can be obtained from:

   a. Modeling and simulation. If a numerical model exists that can be used to simulate disruption and recovery of the system, analysts can use the model to generate the necessary data.

   b. Historical data. Disruption and recovery data from previous events may be recorded and stored. Analysts can use these data to assess the resilience of the system to that previous event or to extrapolate system performance and recovery estimates for a similar event.

   c. Expert judgment. If modeling or historical data are not available, analysts can apply expert judgment to estimate the *SI* and *TRE* quantities.

   The flexibility to use any of these data sources for quantitative analysis is a strength of the assessment framework. However, the results of the analysis are only as good as the data being used. Hence, if expert judgment is the data source, data should be provided by an individual who is knowledgeable and qualified to provide those estimates.

5. **Calculate Resilience Costs:** The fifth step calculates resilience costs according to the Equations (1) – (7). Resilience costs are measures of relative resilience to a disruption; a system/scenario with a higher resilience cost has lower resilience than a system/scenario with a lower resilience cost.

6. **Perform Qualitative Assessment:** The final step identifies resilience enhancement features that affect the resilience of a system and lead to the quantitative results. Identification of these features provides guidance on how a system can be improved to become more resilient. This step may also identify behaviors of a system that were not

considered previously (especially identification of recovery efforts) in the resilience analysis and may lead back to previous steps.

In some events, it may not be possible to acquire quantitative data for the resilience calculations. These instances should not prevent an analyst from attempting resilience assessment of the system. Rather, proceed with the qualitative aspects of the analyses (all steps but 4 and 5) and gain important understanding of the system.

Vugrin et al. demonstrated how the resilience assessment framework can provide better understanding of infrastructure resilience through application to numerous infrastructure systems. For example, Vugrin et al. used the framework to assess resilience of the national petrochemical sector to various hurricane scenarios (2011a); to evaluate contingency strategies for military munitions production chains (Vugrin et al., 2010b); and to identify optimal recovery strategies for resource-constrained rail carriers in response to flooding events (Vugrin et al., 2011b). Vugrin et al. were able to identify a restoration approach that simultaneously decreased recovery time by 20 percent and decreased disruption costs by almost 40 percent. Most recently, the framework was used to inform the development of a resilience certification program for buildings. The general applicability of Vugrin et al.'s framework indicates that it could be leveraged effectively in the context of cyber systems. The following section describes such an application.

4. A CASE STUDY

Human resources (HR) systems are a cyber system that is often taken for granted. This oversight can result in serious security or functionality issues. Depending upon the organization, this system may include a number of different databases that contain sensitive data about employees and potential employees. Typical assets within this type of system include payroll, employee personally identifiable information, and recruiting records. This information is frequently shared with other systems and people within the company, such as security, management, medical, IT groups, and training groups. This frequent sharing increases the opportunities for unintended loss or theft. If this information is compromised, it affects not just the organization that houses that information, but the individuals whose information is affected. For these reasons, this resilience case study focuses on an HR database system.

Consider the following hypothetical scenario in which all numerical values are notional:

- A relatively small company has a single HR database. This database includes personally identifiable information such as names, addresses, birth dates, and other sensitive information. Other groups within the organization such as security, training and education, IT, management, and payroll access information from this database. Access to this information is on a need-to-know basis, so a limited number of people can view the data. Software systems that access this information must go through verification and validation activities to ensure they are secure and have established limited access controls. The database went through extensive testing to ensure that access to data was controlled and that risk of potential data leaks was within an acceptable level.

- To save money on start-up and maintenance costs, the company chose not to purchase a backup server or a vendor support contract for server hardware or software. The company has not developed emergency procedures to be performed if the server is compromised or non-functional for an extended period of time. These assumptions are somewhat extreme but, unfortunately, not unrealistic.

- A new, untrained employee is assigned the task of ensuring that periods are inserted after middle initials of customer names stored in the database. As a result of poor training, the employee ends up deleting records for a quarter of the customers. The employee stores the information for the remaining customers in a personal folder on a company repository accessible to all employees.

- The following morning (approximately 24 hours later), an employee notices the deleted records and that sensitive information is stored in a generally accessible location. Fearing that the database has been hacked, the company takes the server offline to assess the cause of the problems.

- Due to the lack of vendor support and limited IT employees at the company, the company is not able to determine the cause of the problem for 48 additional hours. The company realizes the issues were caused by human error and were not due to a malicious attack. The server is placed back online after sensitive information is removed from the generally accessible folder. The company goes through a staged approach for restoring access to groups within the organization, so complete accessibility is not restored for another 48 hours. Adding the deleted customer files was completed within an additional 24 hours. At this point, the system is considered completely restored.

Losing server functionality had an adverse impact on business operations, and the company incurred significant business interruption costs. This section describes how the company might perform a cyber resilience assessment using Vugrin et al.'s assessment approach to enhance resilience to a similar event.

The fundamental questions to be addressed in this analysis are:

- What were the impacts and costs of the business interruption?
- How resilient was the company to the interruption?
- How could the company become more resilient to this type of interruption?

These questions are addressed by going through the six-step resilience assessment process.

1. **Define System(s):** The system under consideration includes the HR server, the company functions (sales, security, management, etc.) that depend on the server, the computer networks relied upon by those company functions, and the HR staff who populate the server.

2. **Define Scenario(s):** This scenario includes an accidental disruption caused by an untrained employee. Improvement of cybersecurity would not have prevented the disruption. Human error resulted in loss of data and sensitive data being made accessible to individuals who did not have a need to know. Business functions requiring access to the deleted customer records were halted for 24 hours. Although server access was entirely prevented for another 24 hours, some dependent company functions were able to recover prior to access restoration through the use of paper records. Business functions requiring server access were brought back in a staged process, with complete access restored within another 48 hours. Total functionality was restored 24 hours later when the deleted records were replaced. Figure 4 shows how server functionality evolved during the recovery process. Loss of functionality resulted in business interruption costs. System restoration required a number of activities to occur that were not normally performed. In-house IT staff worked overtime to identify the cause of the interruption and to restore the server. External IT consulting was brought in to assist, and because a support contract was not in place, this assistance came at a premium price. The overtime and external consulting costs were above and beyond regularly budgeted IT costs.

3. **Define Metrics:** To measure system impacts, the company selected company revenue (Table 1). The targeted system performance was equated to the daily company revenue, and system performance is the actual daily company revenue. Systemic impact is the cumulative difference between the two quantities and can be considered the business interruption costs: i.e., costs associated with lost revenue and decreased productivity resulting from the disruption. Other costs, such as opportunity costs and damage to reputation, are possible metrics for systemic impacts, but as these are generally more difficult to estimate. It is assumed the company chose not to use these additional metrics. To measure the total recovery effort, the company uses the external IT consultant costs and internal IT staff overtime labor charges.

4. **Obtain Data:** The company was able to use the invoice for the IT consultant and labor charging records to calculate the total recovery effort. The company inspects sales records to obtain daily revenue amounts. Table 2 lists the IT consultant costs, overtime charges, and daily revenue amounts.

5. **Calculate Resilience Costs:** *SI* is calculated according to Equation (2) and determined to be $2,760. *TRE* is calculated by summing the recovery costs (Equation 4), so *TRE* is determined to be $1,500. The variable α is set equal to 1 because business interruption costs and recovery costs are considered equally important. Consequently, *RDR* costs are calculated to be 0.36, as shown in Equation (8).

$$RDR(RE) = \frac{SI + \alpha \times TRE}{Norm} = \frac{2760 + 1 \times 1500}{12000} = 0.36 \quad \textbf{(8)}$$

6. **Perform Qualitative Assessment:** The company performed an assessment of resilience enhancement features that contributed to the interruption and delayed the recovery process. Table 3 summarizes the results of that assessment.

The lack of training is a key factor contributing to the disruption, so the company decided to perform additional training to address this incident. The training ought to decrease the likelihood this incident would occur again, but the training cannot guarantee the incident or a similar one would never occur again. Hence, the following process improvement options were put forth to supplement the training:

- Option 1 - Purchase a backup server: upon detection of the initial problem, the company could take the primary server offline and use the backup server. Because the backup server would contain static data and not allow updates, complete functionality could not be restored through the presence of a backup server. Expert judgment predicts that 90 percent functionality could occur through the use of a backup server. This option would not affect external consulting costs, overtime charges, and the length of time required to restore access to the initial server.

- Option 2 - Purchase a vendor support contract: upon initial detection of the problem, the vendor could be contacted. Expert judgment predicts that the vendor could identify the cause of the problem within a day of the initial detection (as opposed to two days for the base case). Vendor support would negate the need for an external consultant, and restoration of server access would begin one day after detection of the problem rather than two days. The shorter overall recovery period would decrease overtime charges by $400.

- Option 3 - Develop a contingency plan: the primary benefit of the contingency plan is that it would facilitate the recovery process by decreasing the access and data restoration process once the cause of the issue is identified. Expert judgment was used to estimate that access and data restoration could be completed in one day rather than three days. An external consultant would still be required to identify the source of the interruption, but overtime charges would decrease by $400.

- Option 4 - Combine Options 1, 2, and 3. No consultant is required and overtime charges are decreased by $600.

Figure 5 illustrates the expected server functionality for each of the four options in the event that the incident occurs again. To determine the expected benefit from each of these options, the company can recalculate the *RDR* values. Historical data are not available for these calculations, but for the observed interruption, each percent loss in functionality of the server resulted in an $8 loss in revenue on average (Table 4). This relationship can be used to estimate revenue loss and *SI* for each of the four options. Recovery costs and *TRE* values are shown in Table 5.

Not surprisingly, implementation of Option 4 results in the most resilient system (Table 6). *RDR* costs are a sixth of what they were in the initial scenario. *SI* and *TRE* values are decreased by almost 90 and 60 percent, respectively, and the length of the recovery period decreases from six to three days, a 50 percent reduction. Option 1, use of the backup server, is the next most resilient option because it results in the second smallest business interruption costs. The drawback of this option is that the total recovery still takes six days. Options 2 and 3 result in nearly identical *RDR* values. The Option 3 *SI* value is slightly smaller than the respective Option

2 value, and complete recovery is achieved in one day less. However, Option 3's higher recovery costs essentially offset the savings in business interruption costs.

Having gone through the resilience assessment process, the company now has a comprehensive understanding of what caused the interruption, what delayed recovery, the costs of the business interruption, recovery costs, options for enhancing the resilience of the company, and an analysis of how effective those options would be. The company can now make informed decisions on how to prevent future interruptions and how to respond to the next one.

5. CONCLUSIONS AND SUMMARY

Cyber resilience is increasingly recognized as an important component of comprehensive cybersecurity practices. Cyber system managers should still strive to protect their systems against malicious attacks, but they must also be prepared for situations in which their systems are compromised and disrupted. Current cyber resilience frameworks such as MITRE's CREF and the Software Engineering Institute's OCTAVE and CERT-RMM methods are effective at identifying system weaknesses and recommending improvements; however, these highly qualitative approaches do not have the capacity to validate the effectiveness of the proposed improvements.

The evolution of infrastructure resilience assessment methods paralleled the development of the cyber resilience assessment methods. However, the additional development of performance-based infrastructure resilience methods addressed the resilience validation issue. By focusing on the performance of a disrupted system, performance-based assessment methods address the central infrastructure resilience question: how well does the system perform in the context of a disruption and how much better will it perform if recommended resilience enhancements are implemented?

This paper describes a hybrid infrastructure resilience assessment methodology. It uses performance-based metrics to assess the impacts of a disruption. A qualitative analysis approach can then be used to evaluate system weaknesses and identify options for enhancing the system's resilience. The performance-based metrics can then be used again to validate the effectiveness of the options and to prioritize them. The paper discusses how this infrastructure resilience assessment approach could be extended to cyber systems. Further, the assessment approach is applied to a hypothetical cyber system to demonstrate the utility of the assessment approach. In this resilience analysis case study, an HR system is disrupted due to human error by an employee of the company. (The resilience assessment framework is generic and can also consider malicious attacks.) The infrastructure resilience assessment framework is used to identify and evaluate options for improving the resilience of the system.

The challenge with applying the infrastructure resilience assessment framework to cyber systems is that it has not been customized for cyber systems. Future development could create a cyber-centric resilience assessment framework. The authors recommend the fusion of current cyber resilience methods and infrastructure resilience assessment methods to incorporate the best of both approaches. For example, this new framework could combine OCTAVE's structured cyber-specific approach to identifying system weaknesses and system improvements with the resilience

metrics of Vugrin et al. The resulting methodology would enhance cyber resilience assessment and validation.

6. ACKNOWLEDGMENTS

The authors thank Sharon O'Connor for her editorial assistance. This work was funded by the Sandia National Laboratories Laboratory Directed Research and Development program. Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

REFERENCES

Alberts, C., Behrens, S., Pethia, R., and Wilson, W. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0*. (CMU/SEI-99-TR-017) Retrieved on July 5, 2012, from http://www.sei.cmu.edu/library/abstracts/reports/99tr017.cfm.

Alberts, C., and Dorofee, A. (2001). *OCTAVE^{SM} Implementation Guide Version 2.0*. Retrieved July 4, 2012, from the CERT OCTAVE website: http://www.cert.org/octave/download/intro.html.

Allen, J., and Curtis, P. (2011). *Measures for Managing Operational Resilience* (CMU/SEI-2011-TR-019). Retrieved July 03, 2012, from the CERT Resilience Management website: http://www.cert.org/archive/pdf/11tr019.pdf.

Allen, J., and Davis, N. (2010). *Measuring Operational Resilience Using the CERT Resilience Management Model* (CMU/SEI-2010-TN-030). Retrieved July 03, 2012, from the Software Engineering Institute, Carnegie Mellon University website: http://www.sei.cmu.edu/library/abstracts/reports/10tn030.cfm.

ASME-ITI (American Society of Mechanical Engineers Innovative Technologies Institute). (2010). *Risk Analysis and Management for Critical Asset Protection (RAMCAP®) Standard for Risk and Resilience Management of Water and Wastewater Systems Using the ASME-ITI RAMCAP Plus® Methodology*. Washington, D.C.: ASME ITI, LLC.

Bishop, M., Carvalho, M., Ford, R., and Mayron, L. (2011). Resilience Is More Than Availability. *Proceeding of New Security Paradigms Workshop*, pp. 95–104.

Bodeau, D., and Graubart, R. (2011). *Cyber Resiliency Engineering Framework* (MITRE Technical Report MTR1-10237). Bedford, MA: MITRE Corporation.

Bodeau, D., Graubart, R., LaPadula, L., Kertzner, P., Rosenthal, A., and Brennan, J. (2012). *Cyber Resiliency Metrics, Version 1.0, Rev. 1* (MITRE Technical Report MP12-0053). Bedford, MA: MITRE Corporation.

Bruneau, M., Chang, S., Eguchi, R., Lee, G., O'Rourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W., and von Winterfeldt, D. (2003). A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra,* 19(4), pp. 737-738.

Caralli, R., Allen, J., Curtis, P., White, D., and Young, L. (2010). *CERT Resilience Management Model, Version 1.0* (CMU/SEI-2010-TR-012). Retrieved July 03, 2012, from the Software Engineering Institute, Carnegie Mellon University website: http://www.sei.cmu.edu/library/abstracts/reports/10tr012.cfm.

Chang, S., and Shinozuka, M. 2004. Measuring improvements in the disaster resilience of communities. *Earthquake Spectra*, 20, pp.739-755.

Cutter, S. L., Burton, C. G., and Emrich, C. T. (2010). Disaster resilience indicators for benchmarking baseline conditions. *Journal of Homeland Security and Emergency Management*, 7(1), Article 51.

Fisher, R. E., and Norman, M. (2010). Developing measurement indices to enhance protection and resilience of critical infrastructures and key resources. *Journal of Business Continuity and Emergency Planning*, 4(3), pp. 191-206.

Goldman, H. (2010). *Building Secure, Resilient Architectures for Cyber Mission Assurance* (MITRE Technical Report 10-3301). Bedford, MA: MITRE Corporation.

Hassell, S. (2012). Cyber Resiliency and Agility—A Call to Action. *2nd Annual Secure and Resilient Cyber Architectures Workshop*, accessed on June 22, 2012, at https://register.mitre.org/sr/files/hassell.pdf.

Holling, C. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, 4, pp. 1-23.

IEEE (Institute of Electrical and Electronics Engineers) (2000). *IEEE Standard 1402-2000, IEEE Guide for Electric Power Substation Physical and Electronic Security*. New York, NY: IEEE, Inc.

IEEE (Institute of Electrical and Electronics Engineers) (2010a). *IEEE Standard Criteria for Security Systems for Nuclear Power Generating Stations*. Institute of Electrical and Electronics Engineers, New York, NY: IEEE, Inc.

IEEE (Institute of Electrical and Electronics Engineers) (2010b). *IEEE Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links*. Institute of Electrical and Electronics Engineers, New York, NY: IEEE, Inc.

ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) (2000). *ISO/IEC 17799:2000, "Information Technology -- Code of Practice for*

Information Security Management." International Organization for Standardization/ International Electrotechnical Commission: Geneva.

Kramer, F. D. (2011). Cyber Conflict: Challenging The Future. *Black Hat Federal Briefings, Arlington, VA.* Retrieved on April 19, 2012, from http://www.acus.org/news/franklin-kramer-us-should-aim-cyber-resilience.

NERC (North American Electric Reliability Corporation) (2002). *NERC Security Guidelines for the Electrical Sector*. Washington, D. C.: North American Electric Reliability Corporation.

Obama, B. H. (2009). *Remarks by the President on Securing Our Nation's Cyber Infrastructure*. Washington, D. C.: The White House.

Pettit, T. J., Fiksel, J., and Croxton., K. (2010). Ensuring Supply Chain Resilience: Development of a Conceptual Framework. *Journal of Business Logistics*, 31(1): pp. 1-21.

Resilient Enterprise Management Team. (2011) . *CERT® Resilience Management Model Capability Appraisal Method (CAM) Version 1.1* (CMU/SEI-2011-TR-020). Retrieved July 03, 2012, from the Software Engineering Institute, Carnegie Mellon University website: http://www.sei.cmu.edu/library/abstracts/reports/11tr020.cfm.

Rose, A. (2007). Economic resilience to natural and man-made disasters; multidisciplinary origins and contextual dimensions. *Environmental Hazards*, 7(4), pp. 383-398.

Smart Grid Interoperability Panel (2010*). Guidelines for Smart Grid Cyber Security: Volumes 1-3*. Gaithersburg,MD: National Institute of Standards and Technology.

U.S. Department of Homeland Security (2012a). Fiscal Year 2012 Homeland Security Grant Program Supplemental Resource: Cyber Security Guidance. Retrieved July 5, 2012, from http://www.fema.gov/pdf/government/grant/2012/fy12_hsgp_cyber.pdf.

U.S. Department of Homeland Security (2012b). Cyber Resilience Review. Retrieved July 5, 2012, from http://www.ahrmm.org/ahrmm/news_and_issues/issues_and_initiatives/files/ahrmm_cyber_resilience_review_032712.pdf.

Vugrin, E.D., and Camphouse, R. C. (2011). Infrastructure resilience assessment through control design. *International Journal of Critical Infrastructures*, 7(3): pp. 243-260.

Vugrin, E. D., Warren, D. E., Ehlen, M. A., & Camphouse, R. C. (2010a). A framework for assessing the resilience of infrastructure and economic systems. In K. Gopalakrishnan and S. Peeta, eds., *Sustainable and resilient critical infrastructure systems: simulation, modeling, and intelligent engineering* (pp. 77-116). Berlin: Springer-Verlag, Inc.

Vugrin, E. D., Turnquist, M. A., & Brown, N. J. K. (2010b). *Optimal Recovery Sequencing for Critical Infrastructure Resilience Assessment*. Technical Report SAND2010-6237. Albuquerque, NM: Sandia National Laboratories.

Vugrin, E. D., Warren, D. E., and Ehlen, M. A. (2011a). A resilience assessment framework for infrastructure and economic systems: quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. *Process Safety Progress*, 30: pp. 280–290.

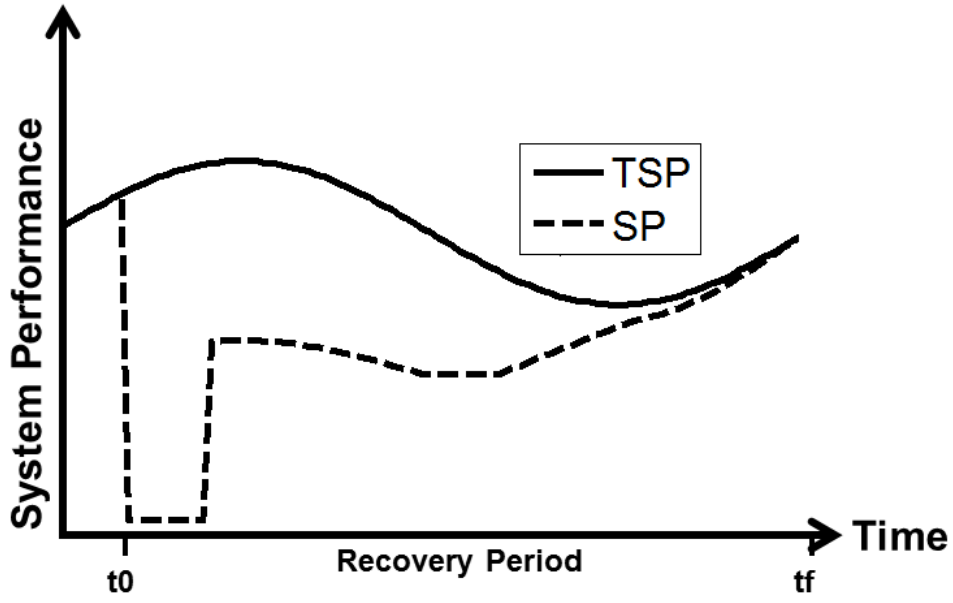
Vugrin, E. D., Turnquist, M. A., & Brown, N. J. K. (2011b). *Optimal Recovery Sequencing for Resilience Assessment of Transportation Networks*. Technical Report SAND2011-8980J. Albuquerque, NM: Sandia National Laboratories.

White, D. (2012). CERT-RMM Overview. Retrieved July 13, 2012, from http://osgug.ucaiug.org.

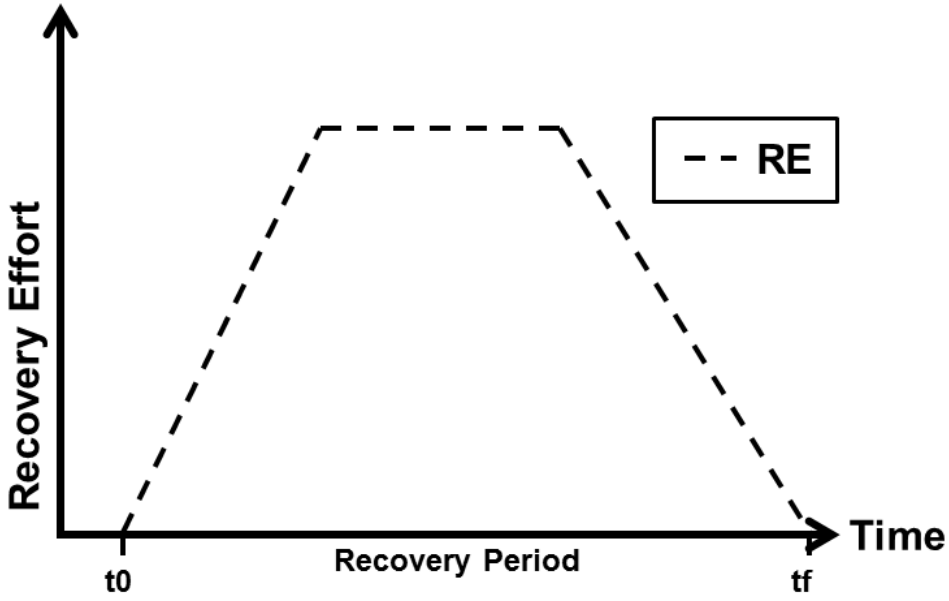
World Economic Forum (2012). Partnering for Cyber Resilience. Retrieved June 23, 2012, from http://www.weforum.org/issues/partnering-cyber-resilience-pcr.

Woody, C., Coleman, J., Fancher, M., Myers, C., and Young, L. (2006). *Applying OCTAVE: Practitioners Report* (CMU-SEI-20060TN-010). Retrieved on July 5, 2012 from http://www.cert.org/archive/pdf/06tn010.pdf.

Figures



(a)



(b)

Figure 1. Systemic Impact (a) and Total Recovery Effort (b) Are Measured by Calculating the Shaded Areas Under the Curves During the Recovery Periods. (Adapted from Vugrin et al., 2010a).

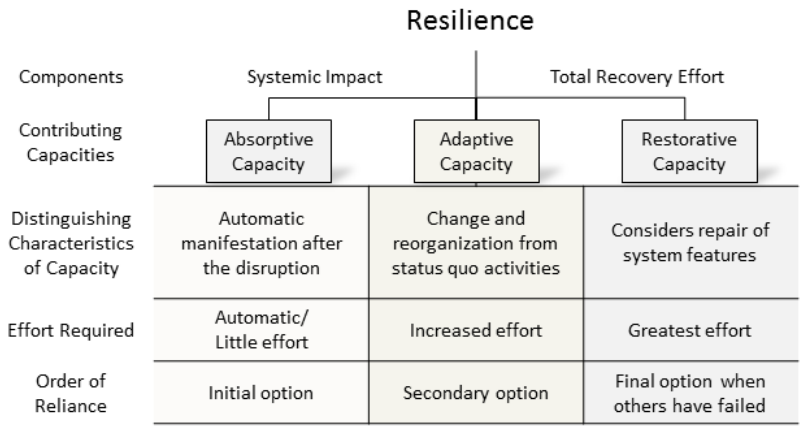


Figure 2. Resilience Capacities. (adapted from Vugrin et al. 2010a)

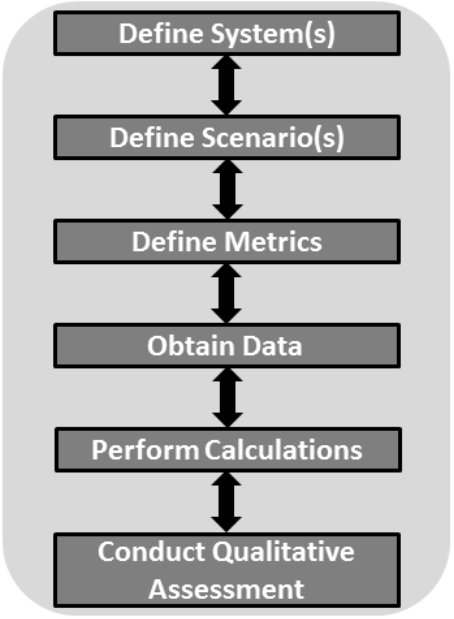


Figure 3. Resilience Analysis Process.

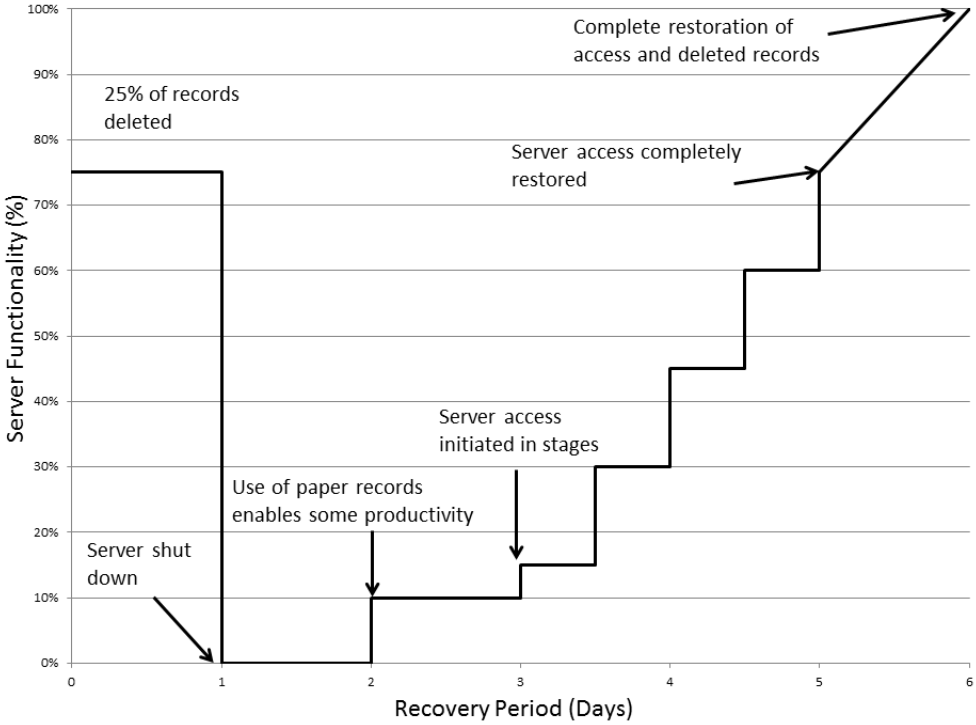


Figure 4. Server Functionality During Recovery Activities.

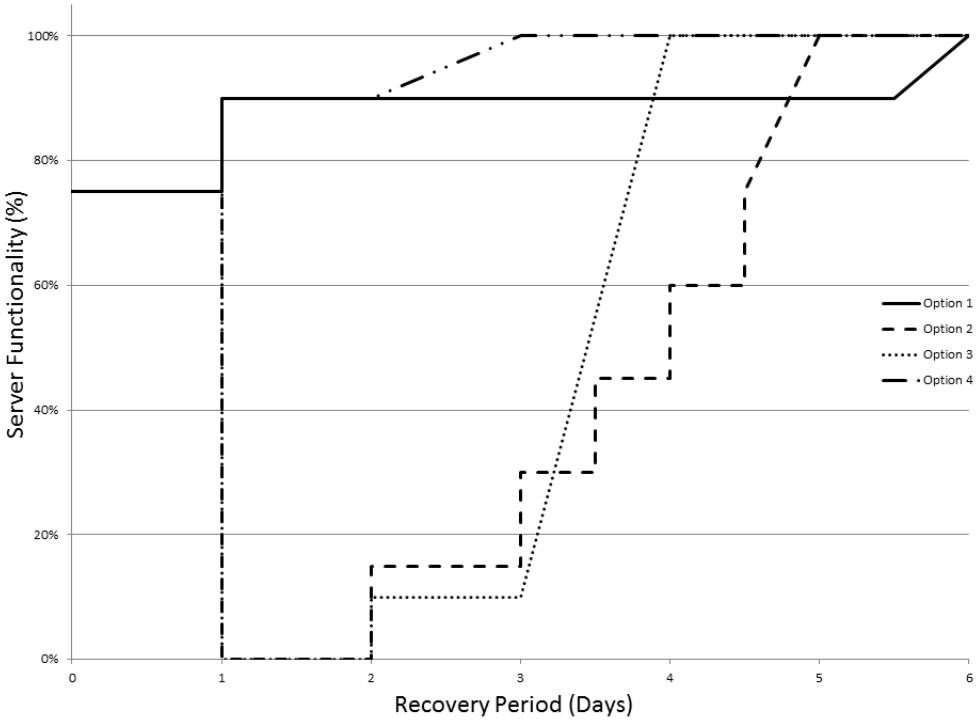


Figure 5. Server Functionality During Recovery Activities, Options 1-4.

Tables

Table 1: Case Study Metrics

Targeted System Performance (TSP)	Systemic Impact (SI)	Total Recovery Effort (TRE)
Average daily revenue, measured in $	Daily revenue, measured in $	Overtime labor charges, measured in $
		External consulting fee, measured in $

Table 2: System Performance and Recovery Cost Data

Days	*TSP*	*SP*	*TSP-SP*	Recovery Cost Categories	Amount
1	$2,000	$1,800	$200	Overtime Labor Charges	$1,000
2	$2,000	$1,200	$800		
3	$2,000	$1,280	$720		
4	$2,000	$1,380	$620	External Consultant	$500
5	$2,000	$1,680	$320		
6	$2,000	$1,900	$100		
NORM	$12,000	***SI***	$2,760	***TRE***	$1,500

Table 3: Analysis of Resilience Enhancement Features

Resilience Capacity	Enhancement Feature	Possible Change
Absorptive	Lack of training for HR employee	At a minimum, increased training could decrease the frequency of these disruptions, if not prevent them altogether.

Resilience Capacity	Enhancement Feature	Possible Change
Absorptive	No backup server	Acquisition of backup server could enable company functions that depend on the primary server to continue operations by using static data on the backup server.
Adaptive	Use of paper records	Use of paper records enabled the continuation of some company functions that depend on the affected server, although these functions were limited and they proceeded at a slower pace than usual.
Restorative	Lack of vendor support contract	Addition of a vendor support contract would have identified the problem more quickly and enabled a faster recovery. It could also decrease future costs because the external consultant charged a premium rate.
Restorative	Lack of a contingency plan	Developing contingency plans for dealing with future interruptions could expedite the recovery process. The plan might include a list of end users to inform if the server goes down so they can adapt more quickly. It could also include a set of well-developed test cases that could be performed to ensure server access and connectivity is more quickly restored.

Table 4: Revenue Loss, Options 1-4

	Average Daily Server Functionality					Revenue Loss (TSP-SP)				
Day	Base	Opt.1	Opt.2	Opt.3	Opt.4	Base	Opt.1	Opt.2	Opt.3	Opt.4
1	75%	75%	75%	75%	75%	$200	$200	$200	$200	$200
2	0%	90%	0%	0%	90%	$800	$80	$800	$800	$80
3	10%	90%	15%	10%	95%	$720	$80	$680	$720	$40
4	23%	90%	38%	55%	100%	$620	$80	$500	$360	$0
5	60%	90%	75%	100%	100%	$320	$80	$200	$0	$0
6	88%	95%	95%	100%	100%	$100	$40	$40	$0	$0

SI	$2,760	$560	$2,420	$2,080	$320

Table 5: Recovery Costs, Options 1-4

	Recovery Costs				
	Base	Opt.1	Opt.2	Opt.3	Opt.4
Overtime Labor charges	$1,000	$1,000	$600	$600	$400
External Consultant	$500	$500	$0	$500	$0
TRE	$1,500	$1,500	$600	$1,100	$400

Table 6: *RDR* Costs, Options 1-4

	***RDR* Costs**				
	Base	Opt.1	Opt.2	Opt.3	Opt.4
SI	$2,760	$560	$2,420	$2,080	$320
TRE	$1,500	$1,500	$600	$1,100	$400
Norm	$12,000	$12,000	$12,000	$12,000	$12,000
RDR	0.36	0.17	0.25	0.27	0.06

[i] Vugrin et al. have also defined optimal resilience (OR) costs, the resilience costs for a system when the optimal recovery strategy, minimizing the combined SI and TRE costs, is employed. See Vugrin and Camphouse (2011) for a detailed discussion on optimal resilience costs.