TRUSYS

R-SEC™

A Recommended Management Methodology for Organizational Resilience

John B. Gargett, Director, TRUSYS Institute.

Head Office : **TRUSYS** | 1916 Eastlake Avenue East | Seattle, Washington 98102 | (360) 656-5700
UNITED STATES | CANADA | GUYANA | INDIA | NETHERLANDS

ABSTRACT

R-SEC is a risk based management methodology for implementing the ANSI/ASIS SPC.1:2009 Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use Standard. This paper explores how R-SEC supports Organizational Resilience and its relationship to the proposed ASIS International Organizational Resilience Maturity Model.

TABLE OF CONTENTS

Introduction 4

Overview of Organizational Resilience 4

Risk, Safety & Security, Emergency & Crisis Management (R-SEC) 4

R-SEC Defined 5

Methodology 5

The Role of the Individual 7

T4 NetCentric Operational Excellence 7

Teams 7

Techniques 8

Technologies 8

Training 9

NET CENTRIC Systems 9

Achieving Operational Excellence 10

R-SEC Process Execution 10

Establish An Organizational Resilience Management Policy 10

Risk Assessment and Impact Analysis (RAIA) 10

Example: RAIA For Property Loss (Copper Theft) 10

Applying R-SEC Results For Maturity Modeling 14

Conclusion 16

About... 16

TRUSYS 16

The **TRUSYS** Institute 16

John B. Gargett 16

INTRODUCTION

OVERVIEW OF ORGANIZATIONAL RESILIENCE

In March of 2009, ASIS International (ASIS) released the ANSI/ASIS SPC.1:2009 Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use Standard[1], in conjunction with the American National Standards Institute, Inc. (ANSI). In June of 2010, Department of Homeland Security (DHS) Secretary Janet Napolitano announced the adoption of the final standards for the Voluntary Private Sector Preparedness Accreditation and Certification Program, for which a Private Sector organization can be considered fully compliant if they meet the ANSI/ASIS SPC.1:2009 Organizational Resilience Standard.

ASIS International, the British Standards Institution and the National Fire Protection Association developed the ANSI/ASIS SPC.1:2009 Standard. They were published in a Federal Register following a series of regional public meetings and the incorporation of public comments. It also has been adopted in the Netherlands, along with Organizational Resilience Standards in Australia. The ANSI/ASIS Organizational Resilience Standard offers a business-friendly, globally tested and proven method, based on the ISO management system standard model, for organizations to improve their resilience and preparedness performance. Implementing the ANSI/ASIS Organizational Resilience Standard positions an organization for the upcoming ISO standards for Organizational Resilience, as well as the ISO Business Continuity Management standard.

It is the only preparedness standard that takes an enterprise-wide view of risk management, enabling an organization to develop a comprehensive strategy to prevent when possible, prepare for, mitigate, respond to, and recover from a disruptive incident. This allows seamless integration with the new ISO 31000 Risk Management standard for a comprehensive risk management program and is 100% compatible with existing ISO management system standards (such as ISO 9001, ISO 14001, ISO 27001 and ISO 28000), thus enabling a cost-saving integrated application. By implementing the ASIS Standard, organizations can satisfy both ISO 28000 and BS 25999 requirements.

The ANSI/ASIS SPC.1:2009 Organizational Resilience Standard is a management framework and implementation of the Standard requires a Management Methodology. This document puts forth a risk based management methodology that draws from over thirty years of experiences in the planning, implementation, and decision making needed to anticipate, prevent, prepare, respond to, and recover from events that occur frequently such as daily Safety and Security incidents, to less frequent, but larger impact Emergencies and Crisis events.

RISK, SAFETY & SECURITY, EMERGENCY & CRISIS MANAGEMENT (R-SEC)

R-SEC is a risk- based management methodology used to implement the ANSI/ASIS SPC.1:2009 Standard. Traditional safety & security, emergency and crisis management planning efforts have been proven insufficient in today's world. The "silos" of safety & security, emergency and crisis management, as well as "silos" of response do not provide organizational resilience. R-SEC views risks, threats and the potential for harm an enterprise faces as the responsibility of every individual with a stake in the enterprise. Every person has a role, has responsibilities, and must make a commitment to achieve Organizational Resilience. Building on the individual is what makes an enterprise resilient.

The name R-SEC is derived from the risk management approach that is undertaken. The "R" stands for Risk. Risk is ever present and comes in a vast multitude of forms – from a minor slip and fall in the workplace to terrorism and everything in between. However to attempt to try to identify, plan for and mitigate every potential risk is simply not feasible for any organization. Risk assessment must reflect the actual risks to the greatest degree possible.

[1] American National Standards Institute, Inc. & ASIS International. "Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use Standard." March, 2009.

The remaining letters "S", "E" and "C" each represent levels of risk within an organizations impact continuum. The "S" risks are those that are the most common and occur on a nearly daily basis. These daily incidents are almost always Safety and Security related. The "E" risks, Emergencies, occur less frequently, perhaps only once a year, but do result in moderate to significant impact. The "C" risks, Crises, occur with even less frequency but result in significant to catastrophic impact.

Steps must be taken to implement actions that result in outcomes that reduce risks through Organizational Resilience. T4 NetCentric Operational Excellence is this implementation process.

R-SEC, implemented with T4 NetCentric Operational Excellence, is an integral part of daily business operations and is:

- Developed, sustained and run effectively and efficiently;
- Designed to meet employee, corporate, stakeholders' and the public needs
- Has an explicit mission and a vision;
- Long-term and near-term with respect to goals and objectives that are defined and pursued;
- Ongoing;
- A Corporate Vision and Master Plan
- Cross-silo (e.g. Operations, Risk Management, Business Continuity, Operations Resilience, Security, Safety, Environmental, Management, as well as Internal and External Stakeholders);
- Complimentary with management models such as LEAN, Bolger, Six Sigma and others.

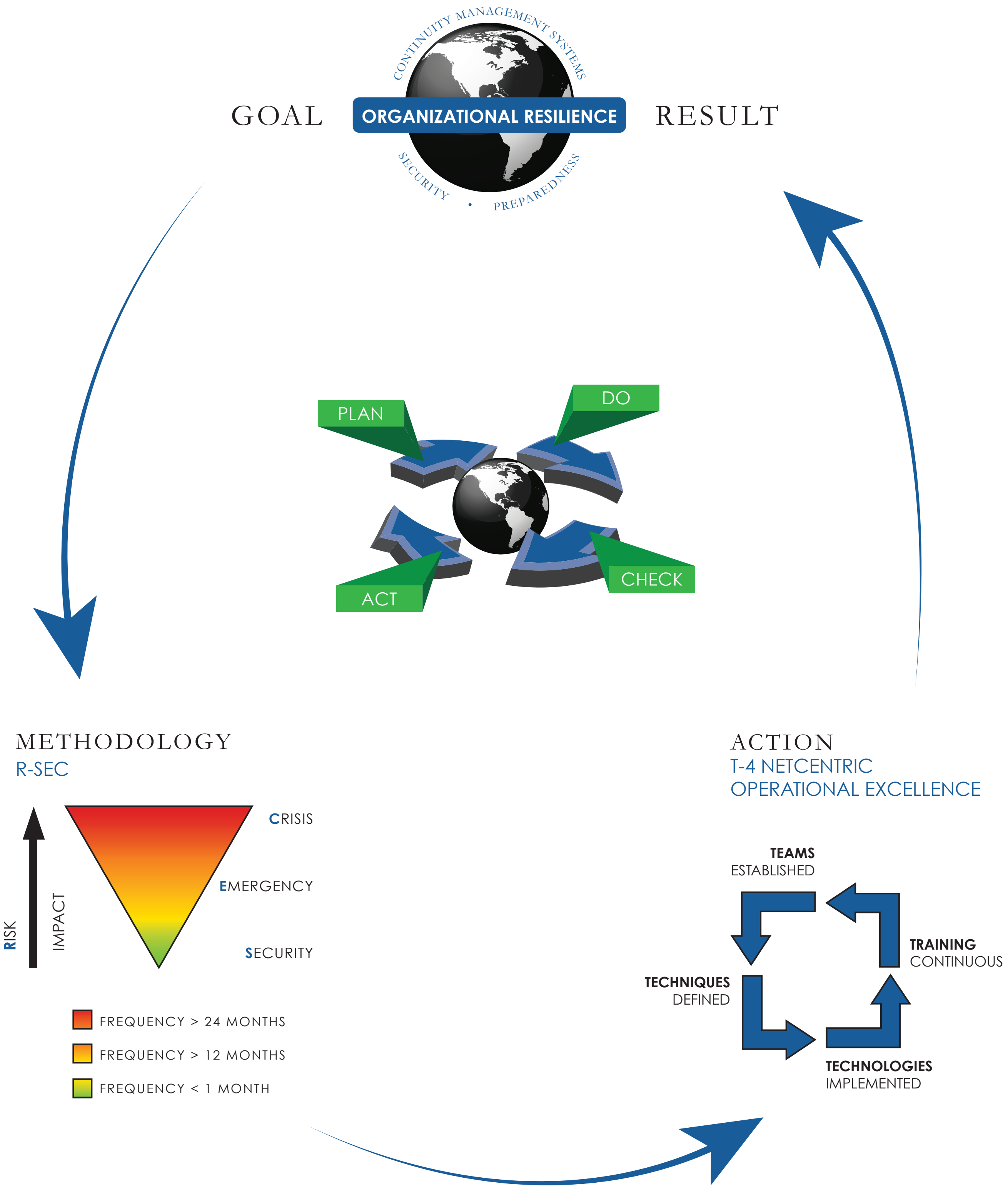
R-SEC DEFINED

METHODOLOGY

R-SEC is a management methodology that recognizes the risks, threats and the impacts of events that can harm any business, community, or organization, but that are not departmental or corporate responsibilities. Instead, they are the responsibility of every individual, department, and internal/external stakeholder. R-SEC requires teams of people, using the best techniques, correct technologies, and regular training to ensure continual safety from risks at all levels.

R-SEC represents over 30 years of work and experience in over 40 countries by multiple practitioners who have worked in all areas of R-SEC. This work and experience has covered nearly every discipline involved in risks, ranging from small companies to large multi-national firms, from local governments to national governments and from multi-lateral responses to major international responses. It is these lessons, these observations, studies and research that have led to the R-SEC methodology.

Recognizing that R-SEC threats happen, with events from small to large, requires an ongoing and consistent program. In R-SEC this is T4 NetCentric Operational Excellence. This addresses these threats so that dealing with them provides the greatest protection and assurance that when faced with the risks, threats and potential for harm that the best that can be done, is done.



CONTINUITY MANAGEMENT SYSTEMS

GOAL

ORGANIZATIONAL RESILIENCE

RESULT

SECURITY • PREPAREDNESS

PLAN

DO

CHECK

ACT

METHODOLOGY

R-SEC

RISK

IMPACT

CRISIS

EMERGENCY

SECURITY

🟥 FREQUENCY > 24 MONTHS

🟧 FREQUENCY > 12 MONTHS

🟩 FREQUENCY < 1 MONTH

ACTION

T-4 NETCENTRIC
OPERATIONAL EXCELLENCE

TEAMS
ESTABLISHED

TRAINING
CONTINUOUS

TECHNOLOGIES
IMPLEMENTED

TECHNIQUES
DEFINED

THE ROLE OF THE INDIVIDUAL

Recognizing that the individual forms the cornerstone of responding to the impacts of risk events, regardless of where the R-SEC threat is (workplace, home, or community) is key to addressing these threats and implementing T4 Net Centric Operational Excellence. Each individual has a role that must be understood and accepted. Once a person recognizes that they face threats in a variety of locations within their world, they can be ready to undertake a strategy to address the R-SEC threats they face by building their own personal resiliency and sustainability which in turn adds to the resilience, and sustainability, of the community based on the collective strength of the individuals that comprise it.

T4 NETCENTRIC OPERATIONAL EXCELLENCE

Initial action designed to implement R-SEC is T4 Net Centric Operational Excellence:

- 4 “T’s” : Teams, Techniques; Technology; and Training;
- NetCentric: Technical, Social and Human Networks; and;
- Operational Excellence: Leadership, teamwork and problem solving in continuous improvement cycle.

TEAMS

Teams are made up of individuals, and therefore, as previously stated, the strength of R-SEC. Individuals are, in fact, the adaptive capacity of an organization to deal with the impact continuum of its R-SEC assessment. The ability to remain resilient and sustainable is based on the collective strength of its employees, staff and stakeholders.

Teams take the form of the following:

- Functional Teams consist of individuals from different departments, agencies or external stakeholders who are brought together to study, plan and recommend procedures or guidelines in response to a need. Examples of Functional Teams include workplace violence planning teams; developing a baseline R-SEC assessment; or an Organizational Resilience Audit Team.
- Tactical Teams are comprised of those individuals within an organization who have the background, character and training to respond when an event occurs. Examples of Tactical Teams include facility Emergency Response Teams, Fire Brigades and Environmental Response Teams.
- Strategic Teams are those individuals who set the direction and policy for an organization. These individuals generally have experience on both the Functional and Tactical Team level as well as the ability to work with senior leaders of the organization. Examples of Strategic Teams include facility the Communications Team, the Risk Management Team and the Strategic Business Development Team.

TECHNIQUES

Teams must have techniques based upon the task at hand, as well as on the structure of the organization, legislation and stakeholder involvement. There can, of course, be a number of different Techniques employed for different R-SEC Threats, however at a minimum there are Assessment, Operational, and Compliance Techniques.

- Assessment Techniques are techniques that are employed in order to better understand the potential impact for an R-SEC event. Examples would include a Workplace Violence Risk Assessment, Security Systems Engineering Assessment and Business Continuity and Resiliency Assessment.
- Operational Techniques include how the Tactical Teams, and the organization, will respond to R-SEC Events. Within the United States, as well as much of the world, the Incident Command System (ICS) is used as an operational technique. Some organizations use their corporate structure to define how Tactical Teams will respond, while the military uses a Command and Control technique where a commanding officer overseas forces.
- Compliance Techniques are techniques employed to ensure that the organization is meeting the direction of the Strategic Teams. Examples would include Technical and Physical Security Audits, Audited Drills & Exercises, and Emergency or Environmental Compliance Inspections.

TECHNOLOGIES

In order to support the teams and their techniques, technologies must be introduced based on strategies, how they are employed, and the tasks that need to be accomplished. Technologies must not drive the process; they must support the teams and the techniques that are employed to accomplish their mission.

- R-SEC Assessment Technologies are technologies that are employed in order to better support Assessments. Examples would include a Risk Assessment and Impact Analysis Model, Customs-Trade Partnership Against Terrorism (C-TPAT) Assessment Software, and Chemical Release Modeling. These tools provide the assessment team with the ability to assess, model and determine where individual strengths and weaknesses lay.
- R-SEC Operational Technologies include direct support to Tactical Teams, situational awareness and as well as daily security and fire/life safety technologies.
- R-SEC Compliance Technologies include systems that help insure compliance. Examples would include Near-Miss Compliance Systems, Environmental Management systems and Security Compliance Software. These tools validate, document and report on specific compliance regulations. Also included in Compliance Technologies are process level technologies that monitor specific processes.

TRAINING

Training is critical for implementing R-SEC and achieving Organizational Resilience. Training must be continuous for all teams, in all areas in which they are working. It is critical in order to ensure Operational Excellence. Without training, the teams will not be current in the techniques or the technologies they are using, or as new techniques and technologies emerge. Training includes:

- R-SEC Positional Training is focused on the individual within an organization and is targeted to help ensure that they are prepared for any situation with which they may be faced. In the United States for example, the Incident Command System is the system for managing a response to any event. Every person in an organization should have ICS 100 level training, supervisors and managers should have ICS 200, and ICS 300 if they are managing events, and executives should have ICS for Executives. In addition to operational training, this is where regular Workplace Safety & Security training and Personal Safety & Security training occurs.
- Systems Training includes the specific training on those technologies that are being employed by the teams, using the techniques that meet their requirements. Included in this training are daily operational systems such as Fire/Life Safety Systems, Security Systems, Command & Control and Situational Awareness systems.
- Exercises are the way that validation of the teams, techniques and technologies occurs. In R-SEC exercises are not viewed in the traditional context, they are viewed as baseline and ongoing audit and assessment tools. An exercise program includes Discussion Based exercises (Games, Models & Simulations, Seminars, Table-Tops, and Workshops) as well as Operations Based exercises (Drills, Functional and Full-Scale exercise).

NET CENTRIC SYSTEMS

Traditional Risk Management has departmental functions operating in silos, often completely different, non-communicating groups. The Operational Excellence model requires that Teams work together in a true NetCentric environment that includes computer networks, social networks, and human networks.

- Technical Networks include the systems, networks, fire/life safety systems, computers, operations centers, process management systems, SCADA systems and a host of other equipment and software that enables us to communicate across the world at the speed of light, delivering emails, documents, presentations, all of which enable individuals to communicate across boundaries and cultures;
- Social Networks technically are defined as a social structure made up of individuals (nodes) which are connected by one of more types of interdependencies such as friendship, kinship, common interest or other relationships. Today common examples are Facebook, Twitter, and Linked-In which represent a fraction of the Social Networks available across technical networks.
- Human Networks are personal relationships established between two or more individuals. Human Networks are perhaps the strongest and most important of the three types of networks that are part of R-SEC. It is these networks that have trust, faith and can only be passed via another person through an introduction. Human Networks are the hardest to build, but when a disruptive event occurs, many times it is these networks that are the strongest.

ACHIEVING OPERATIONAL EXCELLENCE

Operational Excellence is achieved when the individuals, Teams, Techniques, appropriate Technologies, and Training, are working together in networked environments, preventing, preparing, responding, recovering and mitigating disruptive events in a continuous improvement cycle that is part of the business management process of the organization.

R-SEC PROCESS EXECUTION

ESTABLISH AN ORGANIZATIONAL RESILIENCE MANAGEMENT POLICY

The first requirement for Organizational Resilience is to establish an Organizational Resilience Management Policy. Without it Organizational Resilience will not succeed. According to the ANSI/ASIS SPC.1:2009 Standard,

> *"Top management shall define, document and provide resources for the organizations OR management policy reflecting a commitment to the protection of human, environmental, and physical assets; anticipating and preparing for potential adverse events; and business and operational continuity."*

Failure to have an organizational resilience management policy will result in a negative audit finding. Once the policy is in place, then the R-SEC Risk Assessment and Impact Analysis is undertaken.

RISK ASSESSMENT AND IMPACT ANALYSIS (RAIA)

R-SEC begins with the RAIA. When assessing risks and their associated impacts, the RAIA Assessment Team, a Functional Team comprised of representatives of key internal and external stakeholders, begins by agreeing on the Techniques to be used for the assessment. The RAIA Assessment Team establishes, implements and maintains a formal and documented evaluation process as well as ensures that it is using appropriate Technologies to support their work, and that the team is fully trained on the process.

EXAMPLE: RAIA FOR PROPERTY LOSS (COPPER THEFT)

For the purposes of an example of a RAIA we will consider an "S" type of risk, which occur frequently and have generally a low to moderate impact. For example, the theft of a company asset, in this case Copper Theft.

There are four stages in conducting the RAIA:

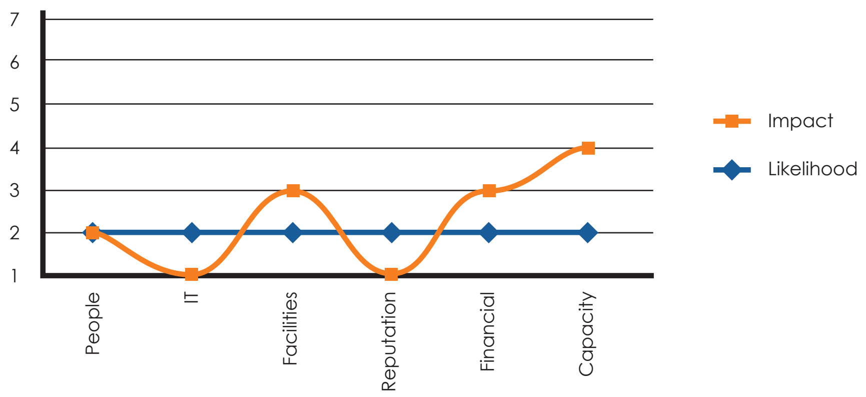
ASSESSMENT

The assessment stage begins with creation of a disruptive risk scenario that outlines the theft of a company asset. For this example we will use the theft of copper, an asset that is used in the manufacturing process. In the scenario, the theft of the copper is not significant, but is an internal threat that can have an impact on production if quantities fall below supply levels.

CONSEQUENCE EVALUATION

Based on the Assessment scenario, a consequence evaluation is made. The R-SEC RAIA Template evaluates the scenario on six criteria – People, IT, Facilities, Reputation, Financial and Capacity. Each is ranked on a scale for Likelihood and Consequence. A sample-ranking sheet is shown in Figure 1 on Page 11:

SITE:	FAIRHAVEN MARINE	RISK:	COPPER THEFT

	People	IT	Facilities	Reputation	Financial	Capacity
Likelihood	2	2	2	2	2	2
Impact	2	1	3	1	3	4
RANKING						

Regulatory	No	Citation:	None
Standard	Yes	Citation:	Organizational Resilience (4.3.1)
Policy	Yes	Citation:	Theft Policy
Plan:	Yes	Citation:	Security Plan (3.1)

	Likelihood Key	Impact Key	RAIA Scoring	
SCORING AND ACTIONS			Likelihood	2.0
	1 - Daily	1 - No Impact	Impact	2.3
	2 - Weekly	2 - Minor	Recommended Action	
	3 - Monthly	3 - Moderate	Update Plan	
	4 - Quarterly	4 - Significant	Review Security Technologies	
	5 - Annually	5 - Major	Worker Bulletin	
	6 - Multi-Year	6 - Severe	Exercise	
	7 - Unknown	7 - Catastrophic		

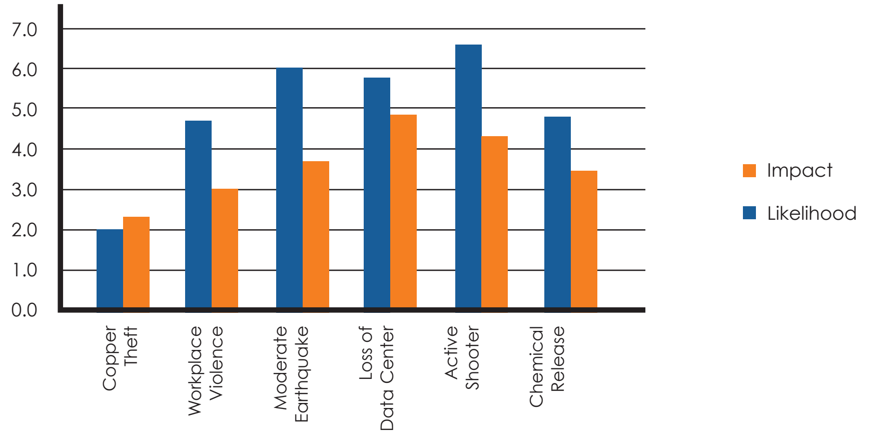
Figure 1 - Sample Consequence Evaluation for Copper Theft

The results of this consequence evaluation are that the greatest consequence of copper theft are on the capacity criteria where the impact may be significant and may result in reduced production. The reduced production as a result, while it should not harm the organization overall, could affect profitability and delivery to customers. The plot also shows that for both criteria Facilities and Financial that there may be a moderate consequence.

When each of the risks an organization faces is completed using the RAIA, they are plotted so that they can be compared against each other. A sample plot for all risks is shown in Figure 2 on Page 12:

	Copper Theft	Workplace Violence	Moderate Earthquake	Loss of Data Center	Active Shooter	Chemical Release
Likelihood	2.0	4.7	6.0	5.8	6.5	4.8
Impact	2.3	3.0	3.7	4.8	4.3	3.5

RANKING



RISK SCORE AND PRIORITIES	Likelihood Key	Impact Key	RAIA Risk Score	
			Likelihood	5.0
	1 - Daily	1 - No Impact	Impact	3.6
	2 - Weekly	2 - Minor	Current Year Priorities	
	3 - Monthly	3 - Moderate	Copper Theft	
	4 - Quarterly	4 - Significant	Loss of Data Center	
	5 - Annually	5 - Major	Workplace Violence	
	6 - Multi-Year	6 - Severe	Chemical Release	
	7 - Unknown	7 - Catastrophic		

Figure 2 - Consequence Plot All Risks

RECOMMENDATIONS

Based upon the RAIA consequence plot for all risks, because of the likelihood of copper theft being frequent, and that the impact can affect production and delivery, then when it is measured against the other risks in the RAIA, then it is recommended that Copper Theft be the highest priority for the current years efforts in R-SEC risk reduction.

IMPLEMENTATION

When implementing a plan for Copper Theft, there are 4 key recommendations that were identified during the RAIA Consequence Analysis – Updating the existing Security Plan, Reviewing the use of security technologies, training and education of the workforce, and conducting an exercise to validate the implementation actions. This implementation plan should be both measurable and auditable. A sample is shown in Figure 3 on Page 13:

Task	Recommendations	Improvement Action	Responsible Party	Completion Date
Worker Bulletin and Training	The theft of copper can cause production delays and it is possible that workers may be let go early if there is not enough copper to keep the production line running. It is recommended that a worker bulletin be issued and training be undertaken to ensure the workforce is fully aware of the problem and their role in helping solve it.	The Human Resources Department shall work with Security to develop both a bulletin and a training update. The bulletin will be posted in the Lunchroom and the training will occur at the weekly safety meeting.	Human Resources	Feb-11
Update Security Plan	The last update to the Security Plan for Copper Theft was done in 2005 and the production process has changed so that copper is now stored in a different area and there are larger quantities. The Security Plan should reflect this and Post Orders should be updated for the Security Force.	The Director of Security shall interview key stakeholders and issue an updated copper theft plan.	Security	Mar-11
Review Security Technologies	Because production has increased the quantity of copper and it is now staged in two areas as well as being used in production, it is recommended that a review be made of appropriate security technologies that can be used for access control and monitoring.	The Facilities Department shall evaluate the existing security technologies and determine if they can be augmented so that access control to the area can be implemented and video surveillance can be increased.	Facilities	Jun-11
Exercise	Following the update to the plan, review of security technologies and worker training, it is recommended that a Functional exercise be conducted to audit the results of the recommendations and if appropriate make changes.	The Security Department shall conduct a Functional Exercise to audit the results of the Improvement Actions for reducing Copper Theft.	Security	Aug-11

Figure 3 - Sample Implementation Plan for Copper Theft

APPLYING R-SEC TO THE ORGANIZATIONAL RESILIENCE MATURITY MODEL

The goal of the Organizational Resilience Maturity Model (ORMM)[2] is to *"establish a resilience management and preparedness culture throughout the organization"* and to *"achieve total integration of resilience management in all the organizations everyday activities and functions."* The ORMM, which correctly states the goal, continues by breaking implementation of Organizational Resilience into six phases beginning with no process in place to a Holistic Organizational Resilience Management Program which goes well beyond the ANSI/ASIS SPC.1:2009 Standard:

- *Phase One – Ad Hoc Approach* – For all intents and purposes nothing is in place and the organization is reacting, not planning and does not recognize the value of resilience and preparedness;
- *Phase Two – Project Approach* - The management of the organization has decided there may be value in resilience and preparedness and in order to determine its applicability they establish a pilot project to validate Organizational Resilience;
- *Phase Three – Program Approach* – The program approach could be an expansion of Phase Two, or management could understand the value of Organizational Resilience and move directly to a programmatic approach to implementation. Also in Phase Three is where the emergence of proactive plans and processes is either introduced or enhanced;
- *Phase Four – Systems Approach* – Management has committed to Organizational Resilience and it is part of the business management process of continual improvement. Detailed work on Risk, Vulnerability and Consequence management is occurring, root causes are being identified, and strategies for success are being put in place;
- *Phase Five – Management System* – In Phase Five the organization is fully committed and Organizational Resilience is being implemented to the point where independent auditing can demonstrate compliance with the Standard;
- *Phase Six – Holistic Management* – Phase Six goes beyond the Standard and Organizational Resilience is now a culture where it is embedded in all aspects of the business.

The R-SEC Management Methodology applies to all six Phases of the ORMM. R-SEC also builds on key milestones of the ANSI/ASIS SPC.1:2009 Standard:

- R-SEC requires a Management Policy;
- R-SEC is cross-functional and does not operate in silos;
- R-SEC involves every individual within an organization as well as external stakeholders;
- R-SEC builds resilient teams, using applicable techniques, appropriate technologies and regular training as part of a Plan - Do - Check - Act model;
- R-SEC has a comprehensive and flexible Risk Assessment and Impact Analysis approach that is part of the business continual improvement process;
- R-SEC benchmarks and audits itself through exercises.

[2] Dr. Marc Siegel, ASIS International & Maya Siegel, Brandeis University. A Maturity Model for the Phased Implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard; ASIS International 2010.

When R-SEC is overlaid on the Phases of the ORMM, because of the management methodology of R-SEC, an organization will begin at least at Phase Three (Program Approach) and will also meet a number of the ANSI/ASIS.SPC1:2009 Standard Clauses in Phase Five. This does not mean that R-SEC will either speed the implementation of the Standard or that an organization can consider itself Organizationally resilient if they are using R-SEC. R-SEC is simply a management methodology that when applied to the Organizational Resilience Standard enables success in an efficient way.

In the proposed Organizational Resilience Maturity Model Recognition Program an Organization using R-SEC would be recognized at a Phase Four (Gold) Achievement Level.

CONCLUSION

R-SEC is a risk-based management methodology used to implement the ANSI/ASIS SPC.1:2009 Standard and associated Organizational Resilience Maturity Model. R-SEC views risks, threats and the potential for harm an enterprise faces as the responsibility of every individual with a stake in the enterprise. Operational Excellence is achieved within R-SEC when the individuals, Teams, Techniques, Technologies, and Training, are working together in networked environments, preventing, preparing, responding, recovering and mitigating disruptive events in a continuous improvement cycle that is part of the business management process of the organization. Organizational Resilience is achieved when R-SEC is used as the management methodology.

ABOUT...

TRUSYS

TRUSYS is an employee owned corporation that delivers Organizational Resilience – the adaptive capacity of an organization to protect value to its stakeholders when faced with internal and external events that disrupt operations. **TRUSYS** delivers Organizational Resilience through it's R-SEC methodology that minimizes the Risks facing the firm by building strategies and tactics to mitigate the effects of disruption. **TRUSYS** only sells knowledge. It does not sell product nor endorse any supplier, product or service. **TRUSYS** is headquartered in Seattle, Washington in the United States with resident professionals in 8 locations, in five countries on four continents.

THE TRUSYS INSTITUTE

The **TRUSYS** Institute was established by **TRUSYS** a place to research, learn and teach Organizational Resilience, R-SEC and best practices required to ensure a fully resilient organization. Courses cover a range of topics, from personnel specific job related training to implementing the ANSI/ASIS Organizational Resilience Standard, to technical systems design for security and fire/life safety systems.

JOHN B. GARGETT

Mr. Gargett is the developer of the Risk, Security, Emergency & Crisis Management (R-SEC) management system that is implemented using his T4 NetCentric Operational Excellence methodology. His depth of experience includes planning, exercising, response, communications and spatial information system (SIM) work around the world. Mr. Gargett has provided expert lectures to Japanese private sector companies on the threats facing, and working in, hostile and overseas environments. He has designed multiple Operations Centers. From the early 1980's to the present, Mr. Gargett has written and audited numerous security and safety programs for a variety of organizations ranging from public to private, including development of plans for the that have streamlined and created effective strategies for Organizational Resilience.