Building robust risk management as a method of situational awareness at the local level

Jennifer Schneider, Carol Romanowski, Sumita Mishra, Rajendra K. Raj, and Sarah Dobie
Collaboratory for Resiliency and Recovery
Rochester Institute of Technology
Rochester, New York, USA

[jlwcem, cjrcms, sumita.mishra, rajendra.k.raj, sad6843]@rit.edu

Abstract— Management of risk at the community level continues to be challenging despite the creation of frameworks to support the management of various typologies of risk. As the scope and form of emergent risk evolves, our situational awareness tools and methodologies must also change to identify risks and possible impacts, events, and opportunities for mitigation. This paper examines the major risk frameworks applicable to community systems, and how they may be combined with historical and real-time data to provide a richer awareness of the existing operational environment during potential and actual calamities. The paper concludes with an examination of our opportunities to advance holistic risk management through the application of systems standards.

Keywords— Situational awareness, community resilience, management systems, critical infrastructure, operational resilience, risk management.

I. INTRODUCTION

Community level risk management continues to evolve due to the changing scope and types of risk that must be managed. Risk is the recognition of the effect of uncertainty (positive and negative) on objectives. Functionally, we typically worry about negative consequences. Emergency managers, responding organizations, and critical infrastructure stakeholders find themselves needing to both mitigate risks and respond to incidents that are beyond those they have typically expected to manage under the standard emergency action plans and hierarchies [1]. Climate change has spawned new and greater natural disasters. Technology has given rise to human driven crises that exploit systems we have come to rely upon. Our reliance on experience has been outstripped by the pace of change, and developing situational awareness as a crisis unfolds is not enough; in fact, it may be too late. In contrast, holistic situational awareness begins with an understanding of the range of possible risks and vulnerabilities to inform the actions we may take as we address both those risks and actual impacts [2, 3].

As a society, we have a created a group of frameworks to guide our actions at the infrastructure and community level, such as ISO 31000 (risk management) [4] and then discipline specific standards such as ISO 14001 (environmental) [5], 45001 (health and safety) [6], 37101/120 (community sustainability) [7, 8], 22301 (business continuity) [9], 27031 (information security) [10], and NIST 800 (data security) [11]. These all address the issue of uncertainty in one way or another.

Communities have long relied on emergency action plans that reflect known hazards (based upon past experiences), but those plans are beginning to recognize that future vulnerabilities, triggers and events may not reflect those of the past. For these new emerging risks, experience does not completely inform our preparedness, and typical lookbacks do not provide a holistic vision of our 'new normal'. Further, as risk evolves and includes new vulnerabilities never accounted for, our planning also evolves. For example, Climate Action Plans (CAPs) are predicated on mitigation of climate risks for localities. The design of these plans is often based upon suppositions about vulnerabilities to projected weather patterns. This conjecture can be difficult to accomplish and defend. Similarly, as our critical infrastructure and response organizations face risks arising from advanced data management systems and related cybersecurity vulnerabilities, uncertainty is exacerbated.

Historical data can provide a great deal of information to establish situational awareness in the present [12]. For example, 911 calls provide insight into the types of disruptive events that typically occur in a region, their scope and characteristics, the level of response required to manage and mitigate the disruption, and what resources are needed to deal with the different phases of the event. If emergency managers know that, in the past, events in a particular neighborhood or area lasted for X hours and needed Y emergency vehicles with crew, the process of allocating resources and staging equipment becomes more data-driven and less dependent on experience or hunches.

However, models built on historical data are insufficient when events are extreme or unusual; such events do not occur often enough in the historical record to provide a clear pattern for inference and are usually considered to be outliers. Therefore, historical data always lags the current state. As extreme events become more common, the historical data

978-1-5386-3443-1/18/$31.00 ©2018 IEEE

models will eventually adjust to include the range and scope of these events, but not until there is a critical mass of new data [12, 13]. This reality points out the need for a more integrated, multi-faceted, agile approach to a changing risk landscape than traditional tools can provide.

This paper examines the relationships between emerging risk paradigms, historical data, and extreme event experience for risk management at the local and operational level. The paper proceeds as follows: Section II introduce risk management for the community and critical infrastructure operational level. Section III presents our methodology for analysis and assessment of the scope of possible tools of community based risk management. Section IV discusses relevant issues in our new paradigm and Section V concludes the paper.

II. BACKGROUND

A. General Risk Management

Risk management follows a typical pattern, regardless of the type of risk. This methodology includes risk identification, assessment, analysis, and then mitigation or monitoring and measurement. In previous work, we have shown that community risk assessment actually needs to occur at two key junctures as we pursue community resilience [2]. First, external risks are identified and assessed. These natural or manmade risks are external because they originate from outside a functional community system, even though, for example, a rogue citizen can be part of the community. Then, internal functional risks, such as operational failures, are assessed, typically at the subsystem or critical infrastructure operational level [14]. These risks are considered to be internal because they are always present within the functioning community system.

Risks can assume multiple forms. Environmental heath and safety is typically an internal risk within an operational context, while climate change is typically an external risk. Data and information security can be both internal and external risks. Regardless of type or origin, all risks create potential impacts and present opportunities for mitigations across an event timeline [15]. The quality and robustness of responses depends upon the ability to derive situational awareness of the propagation of impact. However, robust identification systems cannot work alone and management requires proactive mitigation, response and accountability. Integrating our risk knowledge and capabilities within a management systems structure provides a powerful tool to manage and mitigate risks.

B. Operations Security for Critical Infrastructure

Operations Security (OPSEC) is a risk management process that involves assessment of operations from the adversary's point of view, so that appropriate security controls can be put in place. OPSEC is an iterative process that involves five general steps that seek to protect sensitive operational information for Critical Infrastructure (CI) [16].

1. Identification of sensitive information: This information includes organizational information, details on the security measures etc. The information can be both classified and unclassified. Some of these pieces of information can be put together to reveal critical information about the CI assets.
2. Threat analysis: Threat analysis involves a thorough examination of an adversary's technical and operational capabilities to detect and exploit security vulnerabilities. For each information category identified in the previous step, the threats need to be analyzed. Both external and internal threats need to be considered in this analysis.
3. Analysis of vulnerabilities: After the first two steps, we can determine what an adversary needs to know and where that information is available. Next, it is necessary to determine if it is possible for the adversary to acquire and exploit the information. If so, vulnerability exists.
4. Appraisal of risk associated with each vulnerability: The vulnerabilities identified in step three are ranked using knowledge of the opportunity and impacts such as the attack likelihood, the extent of damage that could occur, and the amount of time and effort required in the recovery process. As the risk-impact increases, the mitigation priority also increases.
5. Application of countermeasures: The most effective countermeasures are simple and straightforward procedural adjustments that effectively eliminate the adversary's ability to exploit vulnerabilities. Countermeasures are implemented in priority order to protect vulnerabilities having the most impact on the critical infrastructure, as determined in the previous step of the operational security process.

C. Historical and real-time data

Historical data is often touted as a rich source of hidden information about past events, including daily operational records as well as disruptions to the usual routine and large-scale disasters. However, we often find that organizations lack a comprehensive *analysis-focused* strategy that determines what data actually should be collected in order to generate realistic models, and therefore crucial data fields may be missing. In addition, a full picture of most disruptive events requires metadata such as weather conditions, economic indicators, population demographics, and so on; these fields are rarely included in historical datasets. In the quest to understand and learn from data, *what* to collect is just as important as *how* to collect.

The other major issue with historical data is its inability to predict events that are not present in the dataset. Standard analysis techniques look for patterns that are already there; they cannot predict what has not yet occurred. Nor can they find a pattern from a single instance. Predicting risk in a

978-1-5386-3443-1/18/$31.00 ©2018 IEEE

rapidly changing environment, with ever-greater extreme events, requires expert knowledge and visionary thinking. A possible approach is to adjust data collection strategies to capture a greater measurement range for certain attributes or add new ones, but simple extrapolation from historical models may not be a wise course of action.

Real-time data, similar to historical data, must collect the right information to be truly useful. The "real-time" aspect implies that a more rapid analysis is necessary than is usual with stored historical data. This analysis is, at best, "near real-time"--there's a certain amount of lag between data gathering and data understanding, which requires techniques and skills to deal with quick, accurate analysis. Otherwise, concerns are the same as with stored data.

C. Data security and privacy in Critical Infrastructure

Effective data protection and sharing between CI entities, both private and governmental, is crucial to the safeguarding of CI sectors. We first examine the primary approach used in the healthcare sector, and set it as a canon for other sectors. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) led to the development of national regulations to protect the privacy and security of health information. These regulations include both the HIPAA Security Rule [17] and the HIPAA Privacy Rule [18].

The HIPAA Security Rule [17] requires healthcare providers and plans to have *reasonable* and *appropriate* safeguards for protecting healthcare data. In particular, providers need to ensure the confidentiality, integrity, and availability of all such data that is created, received, maintained or transmitted; identify and protect against anticipated threats to data security or integrity; protect against anticipated, impermissible uses or disclosures; and ensure compliance by their employees and agents. For safeguards, the rule requires ongoing risk analysis processes that evaluate the likelihood and impact of potential risks, implement security measures to address these risks, justify the selected security measures and maintain ongoing security protections. Additional administrative, physical and technical are also mandated.

Building on the Security Rule, the HIPAA Privacy Rule [18] permits the flow of healthcare information to support high-quality healthcare and important uses of this information while ensuring such information is properly protected. Individually identifiable health information includes common identifiers such as name, address, birth date, Social Security Number, demographic data and health conditions. There are no restrictions on the use or disclosure of de-identified health information. Under most situations, individuals have the opportunity to agree, acquiesce, or object to the use of their data, but where the individual is incapacitated or in an emergency situation, other entities generally may make such uses and disclosures if such an action is determined to be in the individual's best interests.

The data security and privacy needs of other CI sectors are similar, but there are others laws that apply in different sectors, for example, the Sarbanes-Oxley Act (SOX) in the financial sector requires information security professionals to understand how internal controls and auditing is ensuring information security [19]. The relative recent strengthening of data privacy in the European Union by the enactment of the General Data Protection Regulation (GDPR) [20] further safeguards individual privacy and provides teeth and uniformity of enforcement of the European Union; an interesting side-effect is that multinational companies operating within and outside the European Union have generally decided to use the GDPR consistently worldwide, thus increasing privacy guarantees to everyone they interact with. This obviously impacts data security in all privately-held CI.

III. METHODOLOGY

As we work to manage risk at the local level, we have many tools to help us do so, including operational standards that seek to manage the impacts of risk systemically. Each of these standards addresses another form of risk (albeit related) that a community faces. Since these standards generally follow similar formats and processes, we examined if a holistic approach would adequately address community risk.

We employ the following methodology: (1) We compare the scope of risk managed across several major frameworks that a community or critical infrastructure stakeholder can implement and assess [8]. [Table 1] Examining those individual views of risk, we then assess the relevant gaps between them, and show areas of potential loss to a community system and to the community's ability to maintain situational awareness across the response and recovery continuum [15]. (2) Even though these gaps exist, we evaluate the interplay between these frameworks, and examine the new avenues of mitigation and management. While new risks--many borne of technologically interconnected systems [21]--are complex, the availability of technology and data also enhances situational awareness of the risk and response environment. Various tools and methodologies, such as sensing and operational data, data mining, data management, provide a richer understanding of the evolving risk and impacts than ever before, and these can be leveraged with the application of management systems to increase overall situational awareness.

A. Gap analysis:

Community-level risk management planning has conventionally focused on emergency preparedness, response and recovery for natural and manmade hazards. More recently, planning has incorporated cyber and other technological hazards. However, limiting the risk management scope to emergency management does not

978-1-5386-3443-1/18/$31.00 ©2018 IEEE

Sections of Risk Based Standards	ISO 31000 Risk Management [4]	ISO 45001 Occupational Health & Safety [6]	ISO 14001 Environmental [5]	ISO 37101:120 Sustainable Development [7, 8]	ISO 22301 Business Continuity [9]	ISO 27031 Information Security [10]	NIST 800 Data Security [11]
General Risk Definition (effect of uncertainty)	Risk sources, potential events, their consequences, & their likelihood"	Combination of likelihood/ exposure & severity of injury or illness	Combination of likelihood/ exposure & severity of consequences	; Combination of likelihood/ exposure & severity of consequences	Combination of likelihood/ exposure & severity of consequences	Readiness for continuity; Likelihood, exposure & severity of consequences	Extent of a threat by circumstance or event based on potential impact & likelihood
Risk Scope	Treatment of organizational risks; Within operations	Prevention of injury and ill-health & compliance; Within operations	Pollution prevention environmental protection & compliance; Within operations	Mitigation of and adaptation to climate change; Other socioeconomic & environmental issues; Within community	Mitigation of business impacts from events; Legal compliance; Within operations	Events and incidents that could have an impact on ICT infrastructure & systems; Within operations and supply chain	Cybersecurity events related to information systems and assets; Within operations and supply chain
Operational Controls & Performance Measurement	Develop plans for risk treatment options to control risks; Including monitoring but does not specify measurements or management system audits	Develop objectives and plan to control risk using Hierarchy of Controls for identified H&S risks; Indicators align with objectives; Audit system	Develop objectives and plan to control aspects/impacts using Pollution Prevention Hierarchy; Indicators align with objectives; Audit system	Develop objectives and plan for addressing risks and opportunities; Indicators align with the 6 purposes and 13 issues; Audit system	Develop objectives and & plan for responding to disturbances; Indicators align with objectives; Perform exercises and tests to evaluate adequacy of plans; Audit system	Develop objectives and plans to control risk, respond to ICT disturbance; Indicators align with objectives; Perform exercises & tests to evaluate adequacy of plans; Audit system	Develop controls, including types of procedures and training; Indicators for monitoring information systems and assets for cybersecurity events and verify control effectiveness

TABLE 1: COMPARISON OF RISK MANAGEMENT SYSTEMS

adequately prepare the community for other types of disturbances [22]. Community risk management must expand its operational scope to incorporate these other areas of risk and longer-term risks to achieve more inclusive risk management. Standards have been developed to manage risks within organizations, including environmental, occupational health and safety, cyber, data quality, and overall business continuity. Additionally, a sustainable development standard was developed for communities to manage longer-term issues, including climate change mitigation and adaptation. These other types of risks and associated vulnerabilities can increase impact and losses during disasters, and incorporating these data informs situational awareness and operational response. The ISO standards allow organizations to set their own boundaries, but may choose to focus merely on their operations or a portion of their operations. The NIST 800 standard appears to bridge multiple scopes of risk in both operations and supply chain. Unlike the ISO standards, NIST defines the types of controls that need to be in place, such as types of policies and trainings. This may work for information security, as it is fairly consistent from organization to organization. However, it may not be practical for other risk scopes. For example, environmental and occupational health and safety management is very context-specific. Different organizations have different hazards based on size, industry, and specific types of equipment and process inputs / outputs. Thus, these standards must be more adaptable.

While the risk management standard, ISO 31000, is meant to be inclusive, its broad structure is focused on risk analysis, requires development, implementation and monitoring of treatment options, however, and there is not great detail about measurement. Measurement is essential to inform an organization's situational awareness - before, during, and after an incident. With little guidance on areas of risk measurement organizations will likely miss key sources of information for situational awareness.

978-1-5386-3443-1/18/$31.00 ©2018 IEEE

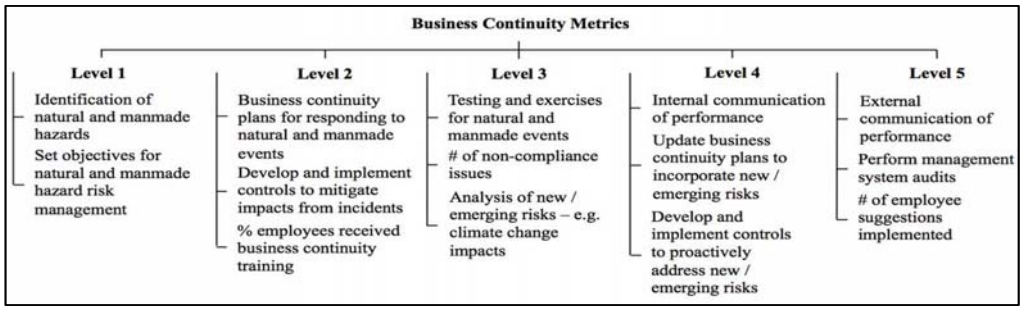

FIGURE 1 – BUSINESS CONTINUITY METRICS

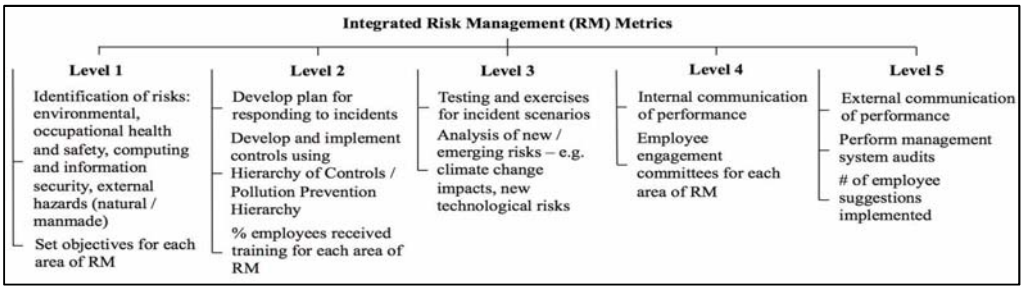

FIGURE 2 – INTEGRATED RISK MANAGEMENT (RM) METRICS

IV. Discussion and Future Work

As a result of this analysis, we then explore these opportunities and challenges as they can be applied at the community level:

A. Using Metrics for Integrated Risk Management

Operational metrics will need to be developed to assess performance and continuous improvement across the various scopes of risk that reflects the integrated implementation of a holistic risk management system across a community by controlling stakeholders. In Figures 1 and 2, we show an example abbreviated framework set of tiered metrics for electricity critical infrastructure at the community-level to demonstrate how community entities can leverage the implementation of risk focused systems, event and historical data on all scales to assess a community's capability to meet real and potential calamities over time. Metrics are both leading and lagging. As the risk management system matures, there is a transition from metrics that are response driven to metrics that are focused on mitigation and control (robustness) and then continuous improvement (Figure 2).

B. Using of operational controls as a form of situational awareness

Each of the risk management methodologies described in this paper applied both mitigative and responsive operational controls, e.g. actions implemented to mitigate risk impacts. If these control actions could be married holistically with informing data, including historical, predictive and near real-time, about the state of the community, then more effective response actions could be employed. Further, the use of metrics of performance not only measure the state of maturity of the risk management system (s) capabilities, they also can illuminate those areas that need further attention during an incident arc. In Figure 3 below we illustrate these impacts and situational awareness opportunities.

978-1-5386-3443-1/18/$31.00 ©2018 IEEE

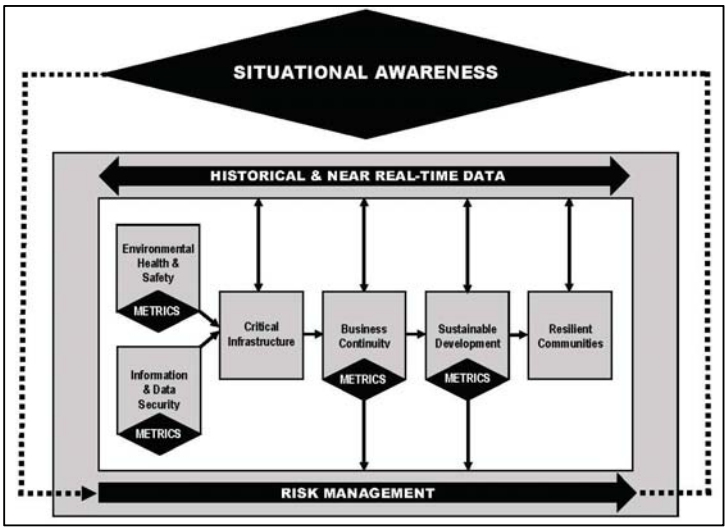

FIGURE 3 – RISK MANAGEMENT THROUGH SITUATIONAL AWARENESS

C. Strategic coordination of community risk management

The integration of climate science, cybersecurity and data security and information security are an integral part of community resilience. Implementation, monitoring and continuous improvement of risk management methodologies across a community will require strategic intent across stakeholders, including the recognition that each risk and vulnerability does not discriminate, and impacts are realized far from the impetus. Improvements in technology, data generation and analysis present unprecedented opportunity, however, this is hampered by the challenges of identifying and preparing critical data and then sharing it. Further, simply because a risk or impact is realized, ownership of management or mitigation is not clear nor straightforward. Typical risk management seeks to mitigate the vulnerability as close to the source as possible, even though impacts may be felt far from that source.

Future events and vulnerabilities are likely more complex and may constitute more of a slow burn. For example, a community struggling with climate change may require critical infrastructure to shoulder more of the burden of risk management. This will force the community and its stakeholders to work together to address the challenges. Single focus operational risk management will no longer be sufficient for long-term community stability.

D. Creating engagement

Advancing this paradigm will not happen overnight, but there are examples and successes including the homeland security focused regional efforts such as urban area working groups, joint terrorism task forces, and even emergency operations centers. The 'next generation' of shared effort will come as we seek to decrease the delineations in risk ownership and management and share knowledge and resources. This responsibility falls upon those professionals in the field now, and especially, future professionals. In one form or another, our highly technological, integrated, and yet brittle society will require us to educate both ourselves and our next generation about our rapidly expanding responsibilities.

V. CONCLUSION

The changing scope of risk impacts our ability to both mitigate risk and maintain situational awareness of the unfolding hazards around us. As surely as climate change exacerbates natural risk, technological change exacerbates manmade risk. In neither case is simple experience enough to bring to bear. The emergence of various risk frameworks can be an informative start in our efforts. Fortunately, that same technological capability can also be used to further elucidate the possible scenarios and support decisions in crisis times. As risks to communities evolve and grow, we must build systems and processes that address these challenges beyond standard approaches. The definition and ownership of risk must be holistically applied. By incorporating process evolution, this work supports the organization and implementation of resilience strategies in a way that operationalizes it within a community and is the next step in the realization of sustainable long-term resilience. This effort thus contributes to the conversation and the actual implementation of resilience initiatives as a community system, employing strategic methods and measures to support the overall growth of resilience.

ACKNOWLEDGMENT

The authors would like to acknowledge the support of the Rochester MSA Urban Area Working Group. The work is partially supported under Award 70NANB16H268 from the National Institute of Standards and Technology, U.S. Department of Commerce, and under Award No. DGE-1433736 from the National Science Foundation. The statements, findings, conclusions, and recommendations are those of the author(s) and do not necessarily reflect the views of the National Institute of Standards and Technology, or the U.S. Department of Commerce, or the National Science Foundation.

978-1-5386-3443-1/18/$31.00 ©2018 IEEE

REFERENCES

[1] J. Schneider, C. J. Romanowski, R. K. Raj, S. Mishra and K. Stein, "Measurement of locality specific resilience: an operational model," 2015 IEEE International Conference on Technologies for Homeland Security (IEEE HST 2015), Waltham, MA. April 2015.

[2] J. Schneider, C. J. Romanowski, R. K. Raj, S. Mishra, J. Aleckna and K. Wang, "Mapping a community resilience management system: building operational knowledge" 2016 IEEE International Conference on Technologies for Homeland Security (IEEE HST 2016), Waltham, MA. May 2016.

[3] J. Schneider, C. J. Romanowski, S. Mishra, R.K. Raj, M. McGuiness and B. Swartz, "Building forward: strategic community resilience" 2017 IEEE International Conference on Technologies for Homeland Security (IEEE HST 2017), Waltham, MA. April 2017.

[4] ISO 31000: 2018 Risk management -- Guidelines. Available at https://www.iso.org/standard/65694.html. (Accessed March 10, 2018).

[5] ISO 14001: 2015 Environmental management systems -- Requirements with guidance for use. Available at https://www.iso.org/standard/60857.html. (Accessed March 10, 2018).

[6] ISO 45001: 2018 Occupational health and safety management systems - Requirements with guidance for use. Available at https://www.iso.org/standard/63787.html. (Accessed March 10, 2018).

[7] ISO 37101: 2016 Sustainable development in communities -- Management system for sustainable development -- Requirements with guidance for use. Available at https://www.iso.org/standard/61885.html. (Accessed March 10, 2018).

[8] ISO 37120: 2014. Sustainable development of communities -- Indicators of city services and quality of life. Available at https://www.iso.org/standard/62436.html. (Accessed March 10, 2018).

[9] ISO 22301: 2012 Societal security -- Business continuity management systems -- Requirements. Available at https://www.iso.org/standard/50038.html. (Accessed March 10, 2018).

[10] ISO/IEC 27031: 2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity. Available at https://www.iso.org/standard/44374.html. (Accessed March 10, 2018).

[11] Special Publication (NIST SP) - 800 53 Rev 4. Available at https://nvd.nist.gov/800-53. (Accessed March 10, 2018).

[12] C. Romanowski, R. K. Raj, J. Schneider, S. Mishra, V. Shivshankar, S. Ayengar and F. Cueva, "Regional Response to Large-scale Emergency Events: Building on Historical Data," International Journal of Critical Infrastructure Protection, Volume 11, December 2015.

[13] C. Romanowski, J. Schneider, S. Mishra, R.K. Raj, R. Rosario, K. Stein and B. Solanki, "Response and recovery: A quantitative approach to emergency management," Proceedings of the 2016 IEEE International Symposium on Technologies for Homeland Security (HST 2016). Ed. Gerald Larocque and Mike French. Boston, MA: IEEE, 2016.

[14] Homeland Security Critical Infrastructure Sectors (2015, October 27). Available at: https://www.dhs.gov/critical-infrastructure-sectors (Accessed March 20, 2016).

[15] Federal Emergency Management Agency, (2011). Recovery Continuum. National Disaster Recovery Framework. Department of Homeland Security. https://www.fema.gov/pdf/recoveryframework/ndrf.pdf (Accessed Sept. 2, 2018).

[16] Operations Security Intelligence Threat Handbook. Available at https://fas.org/irp/nsa/ioss/threat96/part01.htm (Accessed September 13, 2018).

[17] US Department of Health & Human Services – Privacy Rule, "Standards for Privacy of Individually Identifiable Health Information: Final Rule," 2002, https://aspe.hhs.gov/standards-privacy-individually-identifiable-health-information, (Accessed Sep 12, 2018).

[18] US Department of Health & Human Services, "Health Insurance Reform: Security Standards; Final Rule," 2003, http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf (Accessed Sep 12, 2018).

[19] G. Stults, "An Overview of Sarbanes-Oxley for the Information Security Professional," SANS Institute Reading Room, May 2004. https://www.sans.org/reading-room/whitepapers/legal/overview-sarbanes-oxley-information-security-professional-1426 (Accessed Sep 12, 2018).

[20] European Commission, "Data protection in the EU," https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en, (Accessed Sep 12, 2018).

[21] Haraguchi, M., Lall, U., & Watanabe, K. (2015). Building Private Sector Resilience: Directions After the 2015 Sendai Framework: Journal of Disaster Research, 11(3): 535-543.

[22] Martinez-Moyano, I., J. Hummel, and J. Schneider. (2014). Community Resilience & the Role Played By Critical Infrastructure. Disaster Resilience Conference, Denver, CO.

978-1-5386-3443-1/18/$31.00 ©2018 IEEE