View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by NSU Works

Nova Southeastern University
NSUWorks

CEC Theses and Dissertations

College of Engineering and Computing

2012

Constructing a Community Response Grid (CRG): The Dublin, Ohio Case Study

John Freund
Nova Southeastern University, jfreund@gmail.com

This document is a product of extensive research conducted at the Nova Southeastern University College of Engineering and Computing. For more information on research and degree programs at the NSU College of Engineering and Computing, please click here.

Follow this and additional works at: http://nsuworks.nova.edu/gscis_etd


Part of the Computer Sciences Commons

Share Feedback About This Item

NSUWorks Citation

John Freund. 2012. *Constructing a Community Response Grid (CRG): The Dublin, Ohio Case Study.* Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (156) http://nsuworks.nova.edu/gscis_etd/156.

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

Constructing a Community Response Grid (CRG): The Dublin, Ohio Case Study

by

John F. Freund, III

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

Graduate School of Computer and Information Sciences
Nova Southeastern University

2012

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Constructing a Community Response Grid (CRG): The Dublin, Ohio Case Study

by
John F. Freund, III
March 2012

During an emergency, information availability is critical to preserving life and minimizing damages. During the emergency response, however, information may not be available to those who need it. A community response grid (CRG) can help ameliorate this lack of availability by allowing people to document and distribute emergency information to professional emergency responders (PERs). A CRG combines mobile communications services, Internet technologies, e-government applications, and social network concepts with traditional emergency response systems.

The problem that this case study investigated was how to construct a CRG for the City of Dublin, Ohio, Division of Police that works in conjunction with an in-place emergency management system (EMS). The goal was to create a process that is replicable by similarly sized cities that wished to implement a CRG. In this investigation, the author examined CRG design and implementation issues such as message origin, training needs, policy design, security issues, and funding.

The results of this investigation were organized in terms of Systems Development Lifecycle (SDLC) phases. Throughout these phases, the author identified information that can aid PERs in to better implement a CRG. Based on the results, the author developed a paradigm for constructing a CRG that meets the requirements of residents of the City of Dublin, Ohio, Division of Police and of similarly sized municipalities.

Acknowledgments

I want to thank Dr. Marlyn Kemper Littman, my committee chair, for her support during this process. Dr. Littman, Dr. Ling Wang, and Dr. Steven Zink, members of my Dissertation Committee, have been a source of constant professional support in enabling me to complete this work.

Of course, my true source of inspiration has been my loving wife, Angela, and beautiful daughter, Lorelei; without you, none of this would have been possible.

Table of Contents

List of Tables

Table

List of Figures

Figures

Chapter 1

Introduction

In the past decade, there have been numerous man-made and natural disasters that have demonstrated the need, locally, regionally, nationally, and internationally, for effective utilization of emergency management technologies, resources, and services (Van de Walle & Turoff, 2007). According to Jaeger et al. (2007), the development of Community Response Grids (CRGs), in conjunction with emergency management systems (EMSs), is an effective way to improve disaster response at the local level. B. Shneiderman (personal communication, May 12, 2010) explained that the characteristics of CRGs as a type of EMS are still evolving. What is known, however, is that CRGs are utilized informally in a number of emergencies (Jaeger et al., 2007). In addition, the need to enhance the performance of professional emergency responders (PERs), such as firefighters and police, in handling disasters underscores the importance of evaluating CRGs in conjunction with in-place EMSs as a means to preserve human life and minimize the impact of a disaster (B. Shneiderman, personal communication, May 12, 2010).

Van de Walle and Turoff (2007) noted that first responders are adversely affected by an inability to communicate effectively during large-scale emergencies. The integration of communications processes with information and communications technology (ICT) increases efficiency and aids in removing barriers to effective response efforts (Van de Walle & Turoff, 2007). Jaeger et al. (2007) noted that the implementation of CRGs in conjunction with EMSs facilitates life-saving efforts in emergencies. A CRG can

supplement conventional EMSs with mobile communications, Internet technologies, e-government services, and social networks (Jaeger et al., 2007). Implementing a CRG in conjunction with an EMS facilitates dissemination of information during an emergency. According to Jaeger et al. (2007), "Web-based systems that integrate Internet and mobile technologies . . . facilitate response in large-scale emergency situations by enabling individuals to report information, PERs to disseminate instructions, and residents to assist one another" (p. 594).

In this investigation, the author examined security issues as well as adoption and deployment challenges associated with implementing CRG services. Currently, the City of Dublin, Ohio, operates an EMS that follows guidelines specified in the *National Incident Management System* (NIMS; United States Department of Homeland Security [USDHS], 2008a) standard. In the NIMS document, the USDHS describes overarching operational strategies for design, implementation, and integration of EMSs locally and nationally. Implementing a CRG in Dublin, Ohio, is a departure from this city's current EMS deployment (Participant K, personal communication, September 16, 2010). Therefore, the author, in conjunction with the City of Dublin, Ohio, Division of Police (Dublin Division of Police), evaluated the impact, merits, and limitations associated with establishing a CRG that works in cooperation with the police department's EMS. The author used a case study, guided by systems development life cycle (SDLC) methodology, described by the United States Department of Justice (USDOJ), to develop a paradigm for CRG deployment (Butler & Fitzgerald, 2001; USDOJ, 2003; Yin, 2003).

Statement of the Problem Investigated and Goals Achieved

Problem Statement

The problem this author examined was how to construct a CRG for the Dublin Division of Police that operates in conjunction with the municipality's in-place EMS applications, operations, and services. Jaeger et al. (2007) investigated the capabilities of "how technologies—such as mobile communication technologies, the Internet, and e-government—and social networks can be better employed to more effectively coordinate community response to major disasters" (p. 594). The author built on the approach developed by Jaeger et al. to establish guidelines for effectively implementing a CRG for the Dublin Division of Police. To achieve this objective, the author employed a case study approach in conjunction with the SDLC methodology. The findings from this investigation facilitated the development of a paradigm for CRG deployment for the Dublin Division of Police (Butler & Fitzgerald, 2001; USDOJ, 2003). In conducting the investigation, the author also documented functions enabled by the EMS operated by the Dublin Division of Police as well as described how the CRG can be integrated into neighboring EMSs and the State of Ohio EMS.

This study fills a research gap identified by Schafer, Carroll, Haynes, and Abrams (2008) as well as Horan, Marich, and Schooley (2006). Schafer et al. indicated the importance of defining the emergency preparedness needs of communities. This understanding is critical because local communities may respond informally during extreme duress. According to Horan et al., EMS frameworks generally lack the specificity needed for practical implementation. Therefore, Horan et al. determined that "case studies were crucial to providing insight and grounding to the concepts" (p. 121).

Horan et al. concluded that case studies, such as this investigation, must examine local EMS implementations to better understand the needs of these communities.

Goals

The primary goal of this investigation was to provide a model of the USDOJ (2003) SDLC paradigm that police departments can use to implement a CRG in conjunction with an existing EMS. Additionally, the author investigated approaches to incorporating data about an emergency from Dublin, Ohio, residents who use mobile devices during emergencies into a CRG. These data facilitate the provision of fast and effective disaster services by local government agencies to municipal residents in the event of emergencies (Jaeger et al., 2007). Such community feedback to PERs could support new strategies for managing large-scale catastrophes. Further, incorporating networks such as the Internet, as well as third generation (3G) and beyond 3G (B3G) devices such as cellular phones, into the CRG configuration should enhance vital decision-making efforts that support safety and survival (Jaeger et al., 2007).

Characteristics of the City of Dublin Division of Police

The focus of this investigation is the Dublin Division of Police, which is administratively a part of the City of Dublin. Horan et al. (2006) recommended that a community's emergency management needs should be documented in the research on information systems and emergency management. In response to this recommendation, the author chose the City of Dublin. In the following section, the author provides background information on the city and how its police force operates.

The City of Dublin, Ohio

In the 1970s, Dublin was a rural village and suburban business center (Franklin, Kehoe, & The City of Dublin, 2004). At that time, the U.S. Interstate 270 roadway project and the Muirfield Village Golf Club (now the present home of the Memorial Tournament of the Professional Golfers' Association) had just been completed. Dublin officially became a city in August 1987 (City of Dublin, 2010b). The latest U.S. Census Bureau (2011) estimate of the city's population is 39,310, significantly higher than the 5,000 residents required to qualify as a city in Ohio (Ohio Revised Code § 703.01). There are 11,209 households in the city, with approximately 2.8 people per household (City of Dublin, 2011a; U.S. Census Bureau, 2011). Dublin, Ohio, occupies approximately 21 square miles and has approximately 5,360 businesses within the city boundaries (City of Dublin, 2011a; U.S. Census Bureau, 2011).

Dublin, Ohio, is home to several well-known corporations, including Wendy's International, Inc.; Ashland, Inc.; Cardinal Health, Inc.; and the Online Computer Library Center, Inc. Other large corporations that operate in this region include Nationwide Insurance, Inc., *Bayerische Motoren Werke* (BMW) Financial Services, and Verizon Wireless, Inc.

Dublin, Ohio, has a council-manager form of government (City of Dublin, 2010a). The city council acts as the representative of the residents of Dublin for all government matters. A mayor, whose role is administrative, heads the council. Council members elect the mayor from their own ranks and appoint a city manager to run the city. In Dublin, the city manager is the chief administrative and law enforcement officer (City of Dublin, 2010a). In a typical council-manager city, the council makes laws (legislative

function) and the city manager oversees city operations (Svara, 2005). Council-manager operations are like a corporation with a board (the city council), run by a chairperson (the mayor), who appoints a chief executive officer (the city manager) to run the day-to-day tasks.

Dublin Division of Police

The Dublin Division of Police has been in operation since 1957. As of September 2011, there were 65 sworn officers and 25 civilians in service. The breakdown of these employees is presented in Figures 1 and 2.

STAFFING TABLE	SWORN Authorized 65				
	Chief	Lt	Sgt	Cpl	Police Officer
Number Authorized	1	2	6	6	50
Number Actual	1	2	6	6	50
Office of the Chief	1				
Operations Bureau					
Commander		1			
Patrol Sergeant			3		
Corporal				6	
Patrol Officer					34
Canine Officer					1
Officer(s) in Training					3
Services Bureau					
Commander		1			
Detective Sergeant			1		
Detective					3
Juvenile Officer					1
CEU Sgt			1		
CEU Officer					8
Staff Assistant					
Technical Services Bureau					
Commander					
Training/Accreditation Sgt			1		
Comm Supervisor					
Comm Technician					
Property Technician					
Office Assistant					

Figure 1. Dublin Division of Police sworn staffing table. From City of Dublin (2011b, p. 4). Reprinted from the public domain for educational purposes only.

STAFFING TABLE	CIVILIAN Authorized 25							
	Tech Svcs Comm	Law Enf Planner	Comm Supvsr	Comm Tech	Admin Spec	Staff Asst	Property Tech	Office Asst II
Number Authorized	1	1	2	14	1	1	1	4
Number Actual	1	1	2	13*	1	1	1	3*
Office of the Chief		1			1			
Operations Bureau								
Commander								
Patrol Sergeant								
Corporal								
Patrol Officer								
Canine Officer								
Officer(s) in Training								
Services Bureau								
Commander								
Detective Sergeant								
Detective								
Juvenile Officer								
CEU Sgt								
CEU Officer								
Staff Assistant						1		
Technical Services Bureau								
Commander	1							
Training/Accreditation Sgt								
Comm Supervisor			2					
Comm Technician				13*				
Property Technician							1	
Office Assistant								3*

*below authorized staffing level

Figure 2. Dublin Division of Police civilian staffing table. From City of Dublin (2011b, p. 4). Reprinted from the public domain for educational purposes only.

Figures 1 and 2 show the distribution of the police force across leadership roles, officers, and civilian roles. These charts show a relatively lean management structure, with the majority of employees in sworn police officer roles and a small number of leadership roles (15 or ~23%; City of Dublin, 2011b). The division of police leadership is represented in the organizational chart below (Figure 3). This chart shows the distribution of responsibilities within the Dublin Division of Police, including the relationship between the emergency management coordinator who reports to the chief of police. The emergency management coordinator's role is central to the success of a CRG implementation.

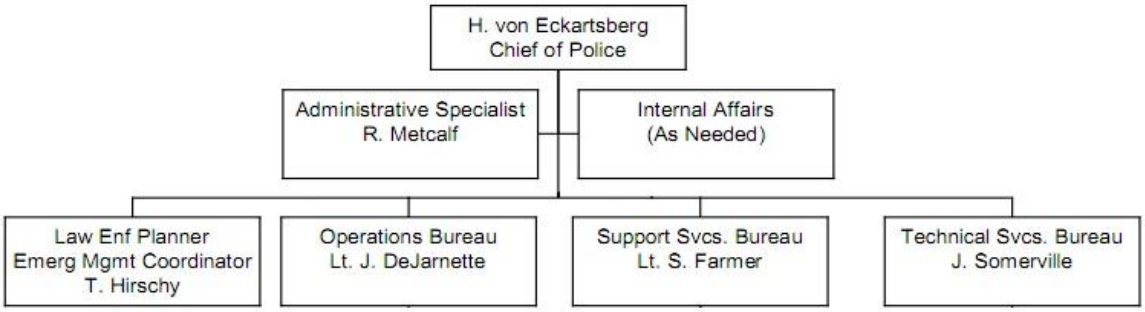

Figure 3. Dublin Division of Police organizational chart. From City of Dublin, (2011b, p. 5). Reprinted from the public domain for educational purposes only.

Administratively, the City of Dublin consists of five districts, as illustrated in Figure 4. District 1 is bound by I-270 to the north and west as well as by the Scioto River to the east. District 2 is bound by the Delaware County line to the north, Martin Road to the south, the Scioto River to the west, and Sawmill Road to the east. District 3 includes all City of Dublin areas north of Brand Road and west of the Scioto River. District 4 is bound by Brand Road to the north, U.S. 33 on the south, and I-270 on the west. District 5 is represented by U.S. 33 to the north, and I-270 on the west. For the July-through-September 2011 reporting period, the Division of Police received 15,238 calls for service (City of Dublin, 2011b). Excluding traffic stops, foot patrols, and courtesy calls, the number of calls for service was 6,822. There were 702 traffic citations, 216 adult arrests, 89 juvenile arrests, 147 property damage reports, and 60 injury reports.

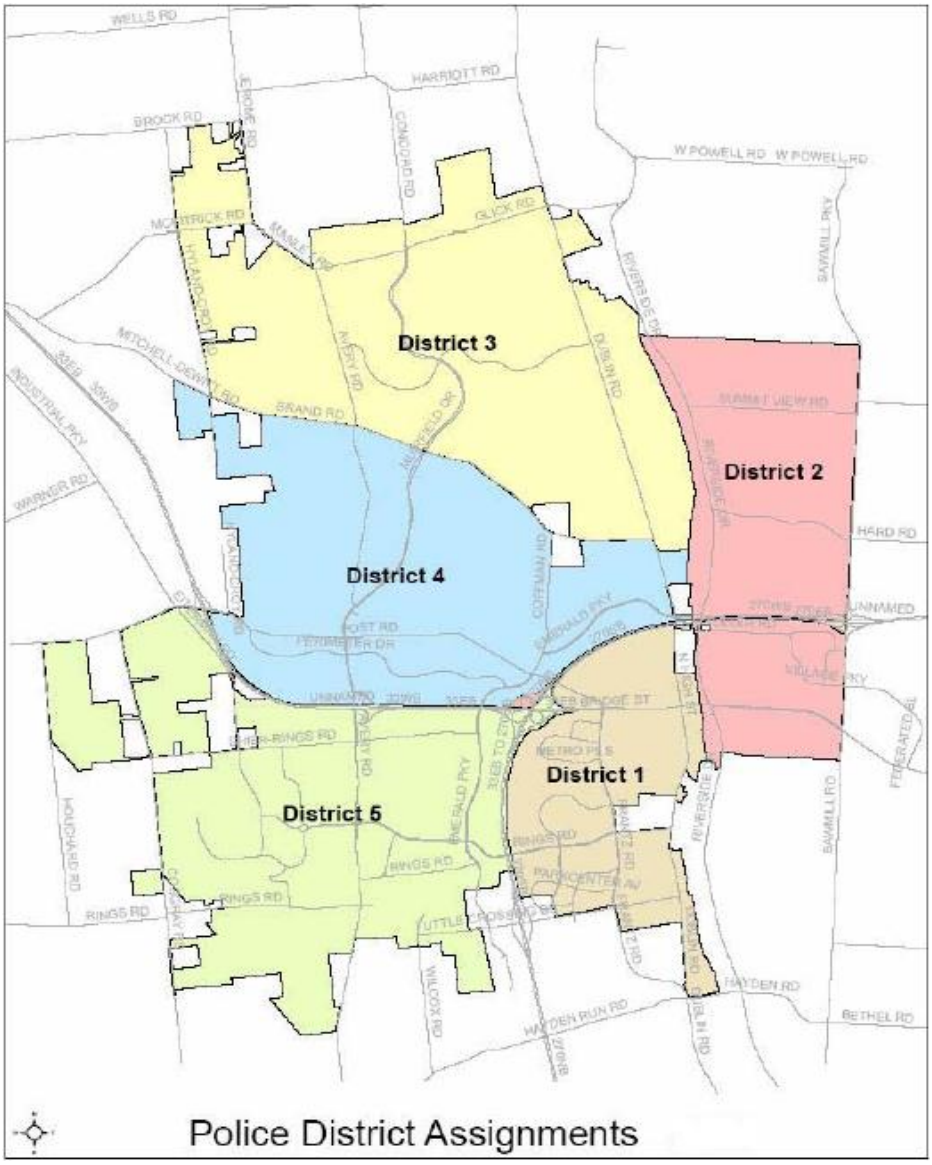

Figure 4. Dublin Ohio Police district assignments. From City of Dublin (2011b, p. 6). Reprinted from the public domain for educational purposes only.

The Dublin Division of Police maintains a Twitter account to provide another channel of communication with its citizens outside of television and radio (City of Dublin, 2010d). Twitter is a microblogging site, or online journal, that allows users to post messages of less than 140 characters (Kwak, Lee, Park, & Moon, 2010). The same message limit applies to text messaging or short message service (SMS). Twitter is used

for personal, professional, and governmental purposes. As of December 2011, 3,433 individuals followed police activity on Twitter, and the Dublin Division of Police made 1,267 posts. Any response sent to the Dublin Division of Police Twitter account concerning an emergency is referred to the traditional 911 system. Examples of Twitter posts made by the Dublin Division of Police in December 2011 include the following (City of Dublin, 2012b):

> North bound Emerald is closed at Shier Rings Rd due to an auto accident. Use West bound Shier Rings to North bound Avery as an alternate.
> 17 Dec
>
> use caution in area of Glick/Carnoustie-Police and Fire on scene for auto accident West bound Glick shut down at Carnoustie
> 6 Dec
>
> Police and Fire are clearing the gas leak at Frantz/Corbins Mill roads are being re-opened
> 2 Dec

Latonero and Shklovski (2010) documented the use of Twitter for emergency purposes, as follows:

1. Citizens' posting information about the emergency
2. Citizens' reposting information about the emergency
3. PERs' posting information about the emergency
4. PERs' collecting information about the emergency

In particular, they have documented the use of Twitter by the Los Angeles Fire Department (LAFD) as an example of the last two categories. The LAFD posts emergency information but also collects Twitter information that is relevant to emergencies. Sometimes the LAFD instructs individuals to call 911, and, at other times,

they will take the initiative and contact the affected individuals, either by telephone or with in-person support, when they are able to verify locations and identities.

Relevance and Significance

According to Schafer et al. (2008) and Pelfrey (2005), frameworks and taxonomies for managing disasters and emergencies generally lack a real-world perspective of community needs. Pelfrey underscored the importance of conducting case studies in communities to determine the feasibility of emergency classification schemas. In this inquiry, the author conducted a case study in conjunction with the SDLC methodology to develop a paradigm for CRG implementation.

The use of case studies in EMS analysis is well established. Yates and Paquette (2011) support such use of case studies in their research on the 2010 Haitian earthquake. The authors volunteered with an Air Force group responsible for responding to the Haitian earthquake and documented the results of their consultations and observations while responding to the aftermath of the earthquake. Likewise, in the current investigation the author volunteered to work in conjunction with the City of Dublin and to document observations. The results of the present case study can facilitate the creation of a CRG that works in conjunction with an EMS for cities similar in size to Dublin, Ohio. As noted above, CRGs are expected to enable the provisioning of time-critical information services in emergency management and the achievement of EMS objectives and goals.

Schooley, Marich, and Horan (2007) used a case study methodology that involved an analysis of systems technologies and the social constructs associated with these

technologies. Their approach was to study the organizational changes necessary to implement new technologies. In keeping with this, the current investigation documented the organizational changes that would be necessary for a successful CRG implementation.

The author used an investigative approach similar to that of Schooley et al. (2007). Specifically, the author investigated the implementation of CRGs at the Dublin Division of Police by determining the technologies and the institutional processes necessary for success (Qu, Wu, & Mahindrakar, 2009; Wu et al., 2008). The author focused primarily on the information technology (IT), organizational network (people and processes), and policies that govern EMS operations and service provisioning and, by extension, CRG implementations (Schooley et al., 2007). Similarly sized organizations can repeat this approach to implement CRGs in their communities.

Horan and Schooley (2005) also examined EMS technologies, people, and policies. Specifically, they examined emergency services and methods for optimizing their use and requirements, such as the support of system interoperability between vendors and jurisdictions. Horan and Schooley described the critical need for, as well as detailed the importance of, intra-agency and inter-agency cooperation. According to these authors, such cooperation includes working with both formal and informal responders. This cooperation is particularly important because CRGs specifically rely on community input as well as formal and informal agreements between communities. Horan et al. (2006) stated:

> Extreme events, such as storms, natural disasters, or terrorist attacks provide obvious examples of situations that could cause a range of system failures including overload

> or even collapse [in the absence of a collaborative community response]. Dealing with crises or extreme events can be a pivotal test of the overall system management capability. (p. 118)

Horan et al. (2006) provided specific recommendations for future research, including the need for case studies and CRGs, and Schooley et al. (2007) came to the same conclusion. According to Schooley et al., conceptual models of EMSs are abstract, and there is a need for case studies to provide a foundation and framework for EMSs. Further, Horan et al. identified the need for an IT solution, such as a CRG, that is functional at the end-user level and that will work with in-place EMS systems. These authors defined end-users as employees of the EMS (formal responders, or PERs). This definition of end-users also applies to citizens (or informal responders) participating in a CRG (Horan et al. 2006).

Barriers and Issues

Enabling the seamless interoperability of a CRG with the in-place EMS in the Dublin Division of Police is difficult to accomplish. Numerous issues pose barriers to success. For instance, using the Internet can allow an individual to be nearly anonymous. According to Jaeger et al. (2007), identification of message origin is critical to CRG adoption success because it reduces false requests for assistance (Abrahamsson, Hassel, & Tehler, 2010; Dilmaghani & Rao, 2007). The ability of the CRG to ensure non-repudiation of these requests is a major barrier to message security (Jaeger et al., 2007). At the same time, these messages may contain sensitive information that citizens may wish to have limited distribution. This privacy consideration is an important component of an overall CRG implementation (Jaeger et al., 2007).

In implementing a CRG, practical issues, ranging from maintenance costs to training sessions, must be addressed. A budget indicating allocations for expenditures for hardware and software, software development services, and personnel costs must be determined (T. Hirschy, personal communication, January 6, 2009). In this investigation, the author worked jointly with the Dublin Division of Police to identify the total cost of ownership of the CRG and to resolve implementation issues associated with the interoperation of the CRG implementation.

Approaches for implementing CRGs in local communities and cities have not been fully investigated. According to Schafer et al. (2008) and Schooley et al. (2007), the absence of research reflects difficulties in coordinating operations among local agencies. Schafer et al. noted that these difficulties reflect a research focus on abstract and superficial models that do not necessarily involve the participation of local communities. As a consequence, there is an absence of approaches for establishing guidelines for CRG implementation, maintenance, and security (Yates & Paquette, 2011).

Research Questions Investigated

The goal of this investigation was to provide a replicable model of how a city police department can utilize the SDLC paradigm, as defined by the USDOJ (2003), to implement a CRG in conjunction with an existing EMS. According to He and King (2008), Markus and Mao (2004), and Butler and Fitzgerald (2001), key challenges include resolving implementation issues to ensure that prior mistakes are addressed and employing effective methodologies to support seamless operations. The author used the following research questions to guide the current investigation.

1. To what extent will the "type, degree, content, extent, and formality of user participation" affect the Dublin Division of Police's design for incorporating a CRG in conjunction with their EMS? (Butler & Fitzgerald, 2001, p. 14).
2. To what extent will the organizational context of the Dublin Division of Police affect the implementation of a CRG? (Qu et al., 2009; Wu et al., 2008). Organizational context refers to the Dublin Division of Police's policies and management necessary to facilitate the implementation of a CRG.
3. Can a CRG address communication issues during emergencies in cities similar in size and demographics to Dublin, Ohio? (Jaeger et al., 2007; Qu et al., 2009; Wu et al., 2008).

The author employed the methods described by Butler and Fitzgerald (2001) and by Hunter (2004). These methods include the use of a single case study and the analysis of user participation and inputs into the SDLC process. Specifically, the author utilized the case study methodology to establish and evaluate the CRG in the context of the Dublin Division of Police's EMS. In addition to conducting the case study analysis, the author used findings from the Dublin, Ohio, case study in conjunction with the SDLC, to establish a paradigm that can be used by police departments in other similarly sized cities to implement a CRG in conjunction with their in-place EMS (Chen, Sharman, Rao, & Upadhyaya, 2008; USDOJ, 2003). Moreover, the author explained the processes that the Dublin Division of Police should use to implement a CRG in conjunction with its EMS. The author described the Dublin Division of Police's EMS, identified factors contributing to CRG implementation, and reviewed strategies necessary to implement a CRG cost effectively. As Project Director of the Dublin CRG Project, the author conducted the

case study and facilitated implementation of the CRG in conjunction with the Dublin Division of Police's EMS.

Critical to the investigation is the concurrent use of the case study methodology with the SDLC. According to Chen et al. (2008), "A life cycle approach provides a broad and systematic view of the activities relating to emergency response management" (p. 68). The SDLC phases for this investigation included the following (USDOJ, 2003):

1. Phase 1 or the Initiation Phase: Identification of the project, development of the business case, and assignment of Dublin Division of Police resources.
2. Phase 2 or the System Concept Development Phase: Establishment of the feasibility, appropriateness, and scope of the proposed solution.
3. Phase 3 or the Planning Phase: Identification of the success criteria and planning elements of the system.
4. Phase 4 or the Requirements Analysis Phase: Identification of functional user requirements to identify data, system performance, security, and maintainability.

Utilization of the SDLC, as defined by the USDOJ, ensures a structured approach to implementing CRGs in cities such as Dublin, Ohio (Chen et al., 2008). The SDLC enabled the development of a replicable paradigm for implementing CRGs that function in tandem with EMSs. This paradigm can be useful for similarly sized cities that plan to implement CRGs.

Limitations and Delimitations of the Study

The author employed a case study methodology and gathered data based on observations, workshops, and documents. When using this approach, several inherent

limitations must be addressed (Creswell, 2003). The presence of the author in the process had the potential to bias the behavior and responses of participants or be viewed by respondents as intrusive to the process (Yin, 2003). Information obtained through direct interviews was filtered through the biases and opinions of the interviewees (Creswell, 2003). When the author reviewed documentation, he considered that the documents may not represent current practices, may be incomplete, or may not contain critical processes (Yin, 2003). Overcoming these limitations was accomplished by ensuring the validity of the process, as detailed in Chapter 3.

This research was delimited in that it is representative of the city studied, namely, Dublin, Ohio. This city may have greater or fewer resources, personnel, or physical space to support its emerging infrastructure than do other cities (Jaeger et al., 2007). These differences may limit the generalizability of this study to cities with comparable demographics seeking a similar endeavor (Jaeger et al., 2007).

Definition of Terms

Catastrophe. An emergency initiated by one of a number of sources (e.g., humans or nature) that renders a community unable to conduct day-to-day activities. The damages and losses associated with a catastrophe are significant and are generally a worst-case scenario. Processes, economies, and supply chains for items such as food, clothing, and shelter are lost and difficult to rebuild. A community's immediate actions are focused on self-preservation, containment, and recovery from the event (Barnshaw, Letukas, & Quarantelli, 2008).

CRG. A Web-based system utilizing mobile communications, Internet technologies, e-government services, and social networks to support emergency communications. According to Jaeger et al. (2007):

> CRGs are Web-based systems that integrate Internet and mobile technologies to facilitate response in large-scale emergency situations by enabling individuals to report information, PERs to disseminate instructions, and residents to assist one another. In short, CRGs use technology to enable residents and responders to work together in community response to emergencies. (p. 594)

CRGs provide a platform to formalize the community response to an emergency.

Disaster. An emergency that is somewhat less devastating than a catastrophe. Generally, the damage and impact are localized to a single area. The affected area can expect help from the surrounding areas, as the surrounding areas are largely unaffected (Barnshaw et al., 2008).

EMS. A system of preparation, response, and management for resolving emergencies (Barnshaw et al., 2008). EMSs, as with CRGs, include the people, processes, and technologies necessary to manage an emergency effectively (Barnshaw et al., 2008). Usually, a government entity, such as the police department, creates and maintains an EMS.

Formal responder. A synonym for a professional emergency responder (PER; Jaeger et al., 2007).

Informal responder. An individual who is not a formal responder. Such a responder is typically an individual who contributes resources to recovery efforts. This phrase also

refers to ad hoc groups of individuals who coordinate their efforts in responding to emergencies (Jaeger et al., 2007).

NIMS. A standard for creating, implementing, and maintaining an EMS (USDHS, 2008a). The U.S. Federal Emergency Management Agency (FEMA) developed NIMS to foster the alignment of resources across multiple jurisdictions. NIMS provides a framework for a uniform response system that aids in quickly acclimating PERs that are not indigenous to the emergency area (USDHS, 2008a).

Non-governmental organizations (NGOs). NGOs do not act directly under the auspices of a government or government agency (Davies, 2008). Emergency response NGOs, such as the Red Cross, typically work across borders in bringing resources and personnel from unaffected areas into the emergency area to provide support and assistance.

PER. Refers to official emergency personnel who respond during an emergency, specifically police, fire, medical, and other personnel whose primary role is to prepare for and respond to emergencies. PER also describes volunteers who perform professional services in the affected areas (Barnshaw et al., 2008).

Social network. A social network is a sociological term for the connections that people make with each other due to a relationship they have built with one another (Freeman, 2004). An online representation of these real-world social linkages includes models and visual representations as seen in popular social networking sites that include Facebook, LinkedIn, and MySpace (Kumar, Novak, & Tomkins, 2010).

Summary

The author conducted a case study documenting how the Dublin Division of Police can implement a CRG in conjunction with their in-place EMSs. With the implementation of a CRG, citizens should be able to provide specific information about an emergency that augments the traditional concepts of community notification that requires a citizen to call 911 and to request a specific emergency resource (Jaeger et al., 2007). CRGs also enable citizens to help each other resolve emergency problems, such as a need for resources, without necessarily involving a formal emergency response (Jaeger et al., 2007). The author discussed the need to identify key issues associated with establishing a CRG for the Dublin Division of Police prior to implementation.

Chapter 2

Review of the Literature

In this chapter, the author presents literature on the advancements and problems in the field of disaster and emergency management generally as well as CRGs, social networks, and EMSs. The review serves as the foundation for this case study and provides a framework for understanding how CRGs can resolve current issues. In this chapter, the author also demonstrates the existence of a gap in the case study research conducted on local police departments that develop CRGs.

EMS Features and Functions

The terrorist attacks on the World Trade Center in New York on September 11, 2001, changed the nature of emergency management in the United States by combining domestic emergency management with border defense against foreign attack (Sylves & Cumming, 2004). September 11 was the catalyst for Bush (2003, 2010) to promulgate Homeland Security Presidential Directive 5, which facilitated the establishment of NIMS. As noted by the USDHS (2008a), NIMS provides:

> a consistent nationwide template to enable Federal, State, tribal, and local governments, NGOs, and the private sector to work together to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity. (p. i)

A NIMS-supported EMS consists of six modules (USDHS, 2008a): (a) command and management, (b) preparedness, (c) resource management, (d) communications and

information management, and (e) ongoing management and maintenance. In the following sections, the intent of each module in enabling emergency management functions for a local governmental unit, such as the Dublin Division of Police, is described.

The scope of the original 2003 NIMS document was expanded in 2008 by the National Response Framework (NRF) to include incident response (USDHS, 2008b). USDHS defined incident response as the "immediate actions to save lives, protect property and the environment, and meet basic human needs" (p. 1). NRF is intended to be a guide for federal, state, and local governments to interact, cooperate, and coordinate during the response to various disasters. NRF was originally based on the 1992 Federal Response Plan that focused solely on the role of the federal government in emergency response (USDHS, 2008b).

Command and Management

A critical element for success in an emergency is to quell confusion by establishing order. In the NIMS standard, maintaining order is referred to as the command and management of an emergency (USDHS, 2008a). Command and management of an emergency and its recovery efforts are critical in responding to natural or artificial disasters. Effective execution of containment and recovery efforts can happen only when local residents know who is in control of the responding governmental organizations. Command and management defines how communication works during an emergency and throughout the recovery cycles (USDHS, 2008a). Specific methodologies must be in place to ensure that response efforts are coordinated between all responding groups, such as NGOs and local government entities (USDHS, 2008a).

The command-and-management function was used in emergencies before being formalized in NIMS (USDHS, 2008a). Jenson (2011) and Jenson and Yoon (2011) noted the reluctance of firefighters to adopt NIMS command and management due to their desire not to have outside management be in control of their actions. Jenson and Yoon indicated that a lack of NIMS command and management training and experience might have contributed to these perception problems. Because command and management is a critical component of a successful NIMS emergency response, it is important that all responding PERs have a clear understanding of which agency has authority at the scene of an emergency.

Preparedness

The NIMS standard details the procedures that government agencies can take to prepare for emergencies. This planning includes developing strategies for allocating personnel, equipment, and resources in emergencies (USDHS, 2008a). NIMS also supports the use of standardized courses and exercise routines (USDHS, 2008a). Various types of training activities are defined for PERs. These activities inform first responders about new developments and training sessions.

The preparedness guidelines also include the building of reciprocity agreements with neighboring communities (USDHS, 2008a). During an emergency, local government agencies typically rely on neighboring communities to assist by offering resources. Reciprocal support agreements need to be in place before an emergency occurs. The NIMS standard provides a framework for mutual aid agreements in this pre-emergency preparedness planning (USDHS, 2008a).

A critical requirement of preparedness is the need for uniform documentation (USDHS, 2008a). This gives PERs a standard set of documentation for use during an emergency. Such documentation can include operations manuals, report forms, and reciprocity agreements.

Communications and Information Management

Managing information in an emergency is the most critical aspect of emergency management (USDHS, 2008a). Incident management functions, such as directing resources, support a variety of communications solutions and technologies. During an emergency incident, communication services must be supported across various jurisdictions, government agencies, and NGOs. Computer and communication technologies facilitate dissemination of information across localities and regions (USDHS, 2008a). The NIMS standard also requires a plan for overall information management, including collection, analysis, and dissemination, to support decision making during the emergency and to inform first responders, affected communities, and the media of the status of the emergency (USDHS, 2008a).

Resource Management, Ongoing Maintenance, and Support

NIMS identifies the following needs for resource management: (a) a systematic process for handling the resources for emergency management, (b) the ability to describe, inventory, mobilize, dispatch, track, and recover resources over the life cycle of an incident, and (c) efficient resource allocation in response to an emergency (USDHS, 2008a). Walsh et al. (2012) stated that IT can assist in resource management by (a) identifying resource requirements, (b) ordering and acquiring resources, (c) mobilizing resources, (d) tracking and reporting on resources, (e) recovering and demobilizing

resources, (f) reimbursing others for resources, and (g) inventorying resources. Walsh et al. noted that IT can assist in these areas by providing general communication tools, online resource acquisition and payment, and inventorying and accounting.

USDHS (2008a) indicated the need for continuous and ongoing reviews of emergency response plans. Regular plan reviews should be conducted to ensure the currency of the network infrastructure as well as of the wireless and wireline components, communications devices, and policies and procedures. Ongoing periodic reviews and plan testing ensures that first responders are familiar with the procedures and can carry out the required tasks (USDHS, 2008a).

Shortcomings of NIMS

Crowe (2010) and Buck, Trainor, and Aguirre (2006) described the following deficiencies in the NIMS standard: (a) the lack of accommodation for social media in communication strategies and (b) unorganized and volunteer group emergency response. Emergency communications problems have emerged with the introduction of social media technologies such as Facebook and Twitter. According to USDHS (2008a), public information should only be released after the review and approval of the incident commander. However, the victims of the emergency will rely on social media as well as traditional media to stay informed of the incident (Crowe, 2010). As a result, the use of social media during an emergency is problematic to the controlled release of public information.

In studying the records of the Federal Emergency Management Agency's Urban Search and Rescue System, Buck et al. (2006) noted an overemphasis on federal response to disasters. Buck et al. found that local communities in the study tended to rely on

FEMA for immediate relief, instead of developing their own capabilities. Despite the PERs reliance upon Federal resources, generally, the victims of an emergency rely on family and friends for immediate relief during their recovery (Crowe, 2010). Buck et al. stated that this "presence of unorganized volunteers and emergent groups" in the response is largely unaccounted for in the NIMS standard and that, even if the standard took such groups into account, NIMS could not effectively control these groups (p. 3). According to Jaeger et al. (2007), the ability to incorporate these volunteers and emergent groups can be accomplished through the use of systems such as CRGs.

Other EMS Frameworks

While the NIMS standard is an important component of establishing emergency services in the U.S., it is not the only EMS standard. According to Saleem et al. (2008), recent EMS research also focuses on the exchange of information among PERs, government agencies, and NGOs. Saleem et al. described a model for business continuity and rapid disaster recovery. The model involves a central repository for collecting data on communication services, local damage reports, and recovery plan execution that can be shared with governments and NGOs. According to Saleem et al., the model operates in real time and within traditional communication channels (telephones, two-way radios, and television) as well as through the Internet, mobile devices, and SMS.

Another EMS framework is the Canadian Emergency Management Framework (Public Safety Canada, 2011). This framework solidified the decision of the Council of the Federation to support federal, provincial, and territorial (FPT) Premiers of Canada. This framework includes principles similar to those of NIMS, namely, prevention and mitigation, preparedness, response, and recovery. Partnerships among the FPT groups

are a critical component of a successful EMS. These partnerships enable PERs to share information in accordance with action plans that are part of the Canadian standard. The Canadian standard also provides for periodic self-reviews that enable systematic improvements.

Emergency Incident Categorization

USDHS (2008a) originally released NIMS in March 2004. A NIMS system facilitates emergency and incident management for federal, state, and local agencies. NIMS defines standards for command and management of systems and resources during an incident, including the need to coordinate with multiple agencies. The document also indicates strategies, such as training and personnel qualifications, for preparing for emergencies. Additionally, the document outlines the need for information management between internal elements of the system and external entities such as other organizations, agencies, and the public.

USDHS (2008a) categorizes incidents and emergencies according to their seriousness and complexity from least complex (Type 5) to very complex (Type 1).

- Type 5 incidents are resolved and contained in a few hours and typically involve from one to six PERs. Higher-level management resources or incident commanders are not required. An example of a Type 5 incident is a truck crash during rush hour.
- Type 4 incidents are resolved in one 8- to 12-hour shift, thereby eliminating the need for shift changes. Personnel handling a Type 4 incident are typically

categorized as strike and/or task forces. An example of a Type 4 incident is a fuel spill on a major highway.

- Type 3 incidents involve the participation of several units or groups. These incidents require coordination and information sharing among participants. An example of a Type 4 incident is that same fuel spill but one that occurs near an airport, school, or water supply, necessitating coordination with other groups.
- Type 1 and 2 incidents involve regional and/or national resources available from entities such as the U.S. FEMA. In these incidents, the number of responding personnel can range from 200 to 500 individuals. Type 1 and 2 incidents are of national significance and typically involve federal response. Hurricanes and terrorist attacks are Type 1 or 2 incidents.

CRGs

Features of CRGs

A CRG is a tool that PERs can use to assist in formalizing the informal response to an emergency (Jaeger et al., 2007). Qu et al. (2009) described three features of CRGs:

1. Web-based infrastructure. A CRG can be accessed via a Web portal using normal Internet protocols such as Hypertext Transfer Protocol (HTTP). The Web portal will contain information that is pulled from various sources and displayed in a unified view. The Web, application, and database systems necessary to support the CRG are hosted by a police department, university, or outsourced to a datacenter anywhere in the world.

2. Internet accessibility. Individuals can use any fixed or mobile device with Internet access (e.g., computers, 3G or B3G smartphones, netbooks, iPads) to connect to and utilize the CRG. These modes of access are important because, in the aftermath of an emergency, the communications infrastructure is often disrupted.
3. Dissemination of information. Residents can use a CRG to report information about an emergency and to view others' requests for assistance and offer help as they are able. PERs also can use CRGs to acquire and disseminate information about the emergency.

The use of the Internet and mobile technologies during an emergency engenders what Crowe (2010) identified as a shortcoming in the NIMS standard. PERs and residents use these technologies during an emergency to communicate outside of the chain of command. In fact, designers of CRGs implicitly assume that certain types of information cannot be extracted by traditional means such as 911 emergency telephone calls (Jaeger, et al., 2007). Instead, emergency details that were once available only by placing PERs on the ground can now be collected and disseminated by any citizen with an Internet-enabled cell phone (Jaeger et al., 2007). Other communications patterns also are supported. For instance, instead of reporting information only up the chain of command, information can be reported in a CRG portal that can allow citizens to see instantly the state of the emergency at their local level. These portals also serve as a platform to enable citizens to request assistance and fulfill their neighbors' needs (Jaeger et al., 2007).

According to Wang, Hämäläinen, and Lin (2008), the creation of two-way channels of communication between PERs and residents of the community is critical to the success of

managing a disaster. In their discussion of the Sichuan earthquake, Wang et al. described how cell phones, satellite phones, fixed-line phones, computers, and personal digital assistants (PDAs) can be used to access a CRG. Wang et al. also discussed residents' providing emergency information to PERs through online portals, smart phones, and mash-ups. Palen, Hiltz, and Liu (2007) explain that mash-ups consist of a combination of Google Maps and a third-party set of geographic datasets that aid in identifying problem areas. Wang et al. have described a communications pattern that communities can build into their EMS by the use of a CRG.

Effective emergency response requires the combination of human and computer components, which Stair and Reynolds (2011) refer to as information systems (IS). According to Schafer et al. (2008) and Carver and Turoff (2007), the design of emergency computer systems should take into account human needs and limitations. One example of these limitations is an emergency response not progressing in a way commensurate with how the PERs were trained (Carver & Turoff, 2007).

Whenever there are unexpected situations in an emergency, first responders are often unable to make an appropriate adaptation (Carver & Turoff, 2007). These unexpected situations require ad-hoc decision making as the situation unfolds. To make appropriate decisions, responders are required to rely on whatever information is available to them, some of which may not be current (Carver & Turoff, 2007). This is where a CRG can help keep PERs and the community up-to-date (Jaeger et al., 2007).

CRG Portal and Implementations

An example of a CRG portal is presented in Figure 5. As seen in this figure, several tasks can be completed, depending on portal design. For instance, a reporting function

enables residents to submit information about emergencies to their PERs. Individuals can also view requests that neighbors make for assistance as well as offer assistance. A major feature of a CRG portal is the registration function (Shneiderman & Preece, 2007). Following registration with a municipal EMS, citizens can identify the location of their residence to emergency organizations and associate with other groups such as homeowners associations and neighborhood watch groups. Registration also enables individuals to monitor group-specific messaging and requests (Shneiderman & Preece, 2007). Registration also enables police departments to determine the origin of requests, thus helping to ensure responsible use of the system and verifying the assistance types requested (Jaeger et al., 2007).

Figure 5. Example of a CRG portal. From Shneiderman and Preece (2007, p. 944). Reprinted with permission from American Association for the Advancement of Science (AAAS; Appendix A).

Qu et al. (2009) described their design and prototyping of a CRG implementation for the University of Maryland. Qu et al. surveyed students in the College of Information Studies to determine levels of interest in various communications options during emergencies. The authors indicated that the students wanted the CRG to be integrated with the 911 system. The students felt that having two separate, non-integrated emergency alert systems would be confusing. Qu et al. noted that their prototype has the following requirements: (a) information collection and dissemination, including workflow, filtering, and distribution, (b) peer-to-peer assistance that enables users to request and offer assistance, and (c) social functions that support user interactions before, during, and after an incident.

Catarci et al. (2008) described the software platforms for PERs in Italy that have the capacity to support a CRG implementation. They discussed front- and back-end systems that enable PERs to gather information from the field using PDAs and then to relay observations, notes, and pictures from the disaster area back to a central system for analysis and storage. Catarci et al. stated that the system was resilient during outages because the PDAs communicate with peers to forward information. What is absent from the Catarci et al. system that would make it a full CRG, is support for public access via wired and wireless Internet (Jaeger et al., 2007).

Marchese et al. (2009) described the role that the OpenKnowledge system could play in emergency scenarios. The OpenKnowledge system is an open source, peer-to-peer networking framework that includes communications protocols and markup languages to facilitate a decentralized-file and message-sharing architecture (Besana, 2011). Marchese et al. presented scenarios of how PERs could benefit from using the OpenKnowledge

system in the technology they carry with them, including communicating the impact of flooding or the debris from a crashed cargo plane in an urban area or communicating evacuation messages. If the OpenKnowledge peer-to-peer system is utilized in a CRG environment, however, then citizens as well as PERs can collect information about the emergency on their smart phones and notebook computers and share the information with each other (Jaeger et al., 2007).

According to Wu (2009), who conducted research with students at the University of Maryland, there is little community involvement in CRGs during the preparedness phase. Wu found a number of factors that affect user participation: (a) culture, (b) confusion about emergency message sources, and (c) the special-purpose nature of emergency systems. Wu also identified student biases against email and most Web-based communications, noting that students generally viewed these as antiquated and favored SMS alerts. The university already maintained an emergency alerting system, and the introduction of a CRG system caused some confusion for the community as to the authoritative source of information during an emergency. Wu noted that people, unless they used a CRG daily, were unlikely to use it during an emergency. This reinforces that social networking sites are used during emergencies because the community used them regularly before the emergency.

Starbird and Palen (2010) investigated the use of Twitter for emergencies. Specifically, they reviewed the forwarding ("retweets") of Twitter messages ("tweets") during the 2009 Red River Flooding in North Dakota and Minnesota and the 2009 Oklahoma grass fires. Starbird and Palen concluded that retweets made by people in North Dakota, Minnesota, and Oklahoma during those emergency events were far more

likely to be about the emergencies than about anything else. In other words, people affected by a widespread emergency are more likely to tweet about that emergency than about anything else. Additionally, the individuals who were more likely to retweet were associated with mainstream media sources and emergency organizations and used Twitter accounts specifically for reporting information about emergencies. According to Starbird and Palen, many local communities are using Twitter for emergency communications; however, many do not have the knowledge to use it as a full-fledged two-way emergency response tool.

Disaster Recovery and CRGs

A community can use social media as a part of response and recovery in the aftermath of a natural disaster, and, according to Draheim and Pirinen (2011), social media is an important part of a community's continuity-planning efforts. Draheim and Pirinen discuss the use of wikis to communicate planning efforts prior to a disaster. A wiki is a Web site-publishing tool that allows for quick updating and publishing of information such as in disaster response activities (Shirky, 2009). In the context of the Dublin Division of Police, utilizing a CRG can help local community groups, such as HOAs and youth groups, plan for and communicate how to weather and recover from disasters (Qu et al., 2009; Wu et al., 2008). To provide for community awareness and training, a CRG should include the capability to share documentation on evacuation routes and procedures in a wiki format or as a document repository (Qu et al., 2009; Wu et al., 2008).

Saleem et al. (2008) discuss the creation of a Web portal that resembles a CRG, with a focus on area businesses affected by a disaster. The portal enables the businesses to advertise their availability during the aftermath of a disaster. They can communicate to

the local community when they plan to close their doors prior to a hurricane evacuation as well as the availability of supplies (Saleem et al., 2008). This capability can be added to the Dublin Division of Police CRG to integrate individuals and community groups with businesses in the same portal (Qu et al., 2009; Wu et al., 2008). Adding business information to the CRG will increase the situational awareness of the PERs who respond to the disasters in the Dublin community.

In this present study, the Dublin Division of Police indicated they would utilize off-site Web hosting at Verio, Incorporated. However, other organizations that implement a CRG and choose to host it internally will need to implement business continuity and disaster recovery planning (Draheim & Pirinen, 2011). Bala, Venkatesh, Venkatraman, Bates, and Brown (2009) discuss the need to build redundancy into database operations for the Veterans Health Administration after Hurricane Katrina caused some databases to become unavailable. Bala et al. indicated that the use of an enterprise data warehouse would provide the recovery capability necessary to maintain service levels during the aftermath of a disaster. The authors indicated that, because an enterprise data warehouse copies data from its data sources, it can effectively provide disaster recovery services during outages (Bala et al., 2009). The CRG database will eventually reach a state similar to that described by Bala et al. in regard to the Veterans Health Administration and, as such, will become susceptible to the same regional outages that effected many during Hurricane Katrina.

One area not addressed in the current research was integration of the CRG with the 911 system in use by the Dublin Division of Police, which warrants further investigation. Truong, Manzoor, and Dustdar (2009) describe a system for sharing disaster response

information using extensible markup language (XML), a formatting standard for creating machine-readable documents (World Wide Web Consortium, 2008). Using XML to encode the event data can allow transmission from the CRG system to the 911 system. There are many design decisions that would need to be considered in integrating these two systems; however, using a common language format such as XML will allow for interoperability among various services and applications necessary for emergency reporting and dispatching (Juszczyk & Dustdar, 2008; Truong et al., 2009).

It is also valuable to conduct research to determine which CRGs can best be integrated with state and federal emergency management organizations. USDHS (2008b) stated that the value of emergency response planning for local communities lies in the predetermination of the processes and procedures for disaster response and in the provision of a common blueprint for coordinating organizations. Although it was determined that the CRG in Dublin would not have technical interfaces to the 911 system at this time, the 911 operators would use information gathered by the CRG in the dispatch of PERs. Because the Dublin Division of Police maintains relationships with state and federal emergency management organizations, they can share information collected from the CRG with them. Creating a CRG environment in which the information gathered by a multitude of communities is aggregated and made available at the state and federal levels would provide a valuable area of research.

Residents as First Responders in CRG Initiatives

Palen et al. (2007) described the role of community residents as first responders in emergencies. Residents often are the first on site in the event of disasters and initially

respond by helping neighbors. After the initial disaster, they may continue their support by providing food, shelter, childcare assistance, employment, and transportation (Bartlett, 2006; Palen et al., 2007; Shklovski, Palen, & Sutton, 2008). Because individuals self-organize to resolve the problems that they and their neighbors are experiencing, this is a largely uncoordinated effort.

The Internet is a uniquely capable tool for generating informal community responses to situations (Shklovski et al., 2008). For example, the use of the Internet eliminates jurisdictional and geographical boundaries by enabling individuals who share a common interest, regardless of their physical location, to collaborate in the event of emergencies. Thus, those who are not geographically peripheral to the disaster have at their disposal resources, such as time, money, electricity, working computers, and telephone equipment, which are in need during disasters (Palen et al., 2007).

For example, during Hurricane Katrina in 2005, a virtual community of first responders self-organized (Palen et al., 2007; Shklovski et al. 2008). Originally privately owned, the www.katrina.com Web site owner subsequently converted it to a public Web site that served as a tool for locating food, shelter, jobs, childcare, and other resource needs as well as a message board to help locate victims of the hurricane (Palen et al., 2007). Another Web site, Hurricane Information Maps at www.scipionus.com, used Google's mapping technology to create a mash-up (Palen et al., 2007). Hurricane Information Maps combined Google's map technology with the contributed information of those affected by Hurricane Katrina. Postings on the Hurricane Information Maps Web site included the status of buildings (e.g., open, flooded) and bridges (e.g., out of

service, completely flooded) as well as anything else that could help the victims and responders (Palen et al., 2007).

Another example of a community Web site that was developed in response to a disaster is the 2003 Southern California Wildfire Web site. One resident (who came to be known as Ranger Al) refused to evacuate and subsequently kept evacuated neighbors up to date on the status of their homes on this Web site (Palen et al., 2007; Taylor, Gillette, Hodgson, & Downing, 2005). Residents would regularly call Ranger Al to get updates on the status of their neighbors and then update the Web site.

Local government and family preparedness plans are indispensable in the response to a disaster. A group of grassroots volunteers maintains www.fluwikie.com to provide information on how to prepare for an avian influenza pandemic (Mattson, 2009; Palen et al., 2007). This Web site also provides access to documents from organizations such as the World Health Organization and information on the science of influenza and personal and family preparedness as well as access to a forum on rumors. The information is presented in a wiki format.

Cellular phones also support emergency efforts (Scholl, 2009). During the 2001 Severe Acute Respiratory Syndrome (SARS) epidemic in China, citizens used the SMS features of their cell phones to share information not available from government sources (Palen et al., 2007). During the 2005 London subway bombings, eyewitnesses documented their experiences through the use of multimedia messaging service (MMS) that subsequently helped in the recovery effort (Palen et al., 2007). With the popularity of present-day global positioning systems (GPS) applications and the ubiquity of mobile services, the coordinate data available further support the capabilities of first responders

in enabling recovery efforts and rescue missions. With the increased use of GPS for mobile applications, additional data will be available for use in emergencies by first responders. Utilization of 3G and B3G mobile devices are also expected to enhance first responder activities in provisioning critical services.

Palen et al. (2007) noted issues in regard to incorporating user feedback into the emergency management processes. Misinformation can limit the successful integration of community feedback in the EMS, and spurious data may place the local community in danger. Technological solutions to these issues can include an approval system for posting to forums or message boards as well as user rating systems that enable participants to rate the trustworthiness of the person posting and the accuracy of his or her statements. Social mechanisms for information vetting include social contracts, such as usage agreements between the community forum and the users, as well as requiring users to be registered and verified with a physical address. The social mechanisms for information vetting have certain consequences, however. Negatively perceived responses may force an individual off the Web site, and misleading postings may subject individuals to legal proceedings (Shneiderman & Preece, 2007).

According to Zittrain (2009), in Wikipedia, inaccurate and malicious updates are generally resolved through social feedback (via the discussion page) and revision history (Wikipedia saves all changes, and, in case of vandalism or inaccuracy, the live page can be reverted to an earlier version). These tools enable Wikipedia authors to build a reputation that gives them authority in their online activities. Zittrain (2009) indicated that the use of Wikipedia reputational tools could assist police departments in sifting through large amounts of data. As an example, Zittrain (2009) indicated that the City of

Oakland police department used reputational feedback when implementing the ShotSpotter gunshot detection system by SST, Inc. Interested citizens could review City of Oakland camera recordings of areas near reported gunshots and request police resources, as needed. The City of Oakland police department used citizens to verify that an event warranted police response, which had the benefit of reducing false alarms (Zittrain, 2009).

According to Palen et al. (2007), unofficial CRG deployments are already being implemented. During emergencies, individuals and first responders use mobile devices to communicate with each other and to disseminate information about the emergency outside of the chain of command. As a consequence of the NIMS command-and-management policy and USDHS's (2008a) preference for top-down crisis management, the utilization of mobile devices by first responders and PERs is sometimes undervalued.

University campus violence, such as the shooting at Virginia Polytechnic Institute and State University in 2007, has caused educational institutions to institute or improve their emergency alerting systems. Of interest to universities is the use of SMS text messaging to alert students to dangerous conditions. According to Sullivan (2011), SMS emergency notification is available at over 81% of the nation's universities. Other communications methods in use by universities include email, Web pages, and social networking sites such as Facebook (Sullivan, 2011).

Additionally, the use of mobile phones has been documented in the SARS outbreak in China in 2003, the earthquake and tsunami in the Indian Ocean in 2004, the subway bombings in London in 2005, and the earthquake in Haiti in 2010 (Gordon, 2007; Satyanarayanan, 2010). In each emergency, mobile phone use was a critical success

factor. Individuals also make use of SMS, MMS, and Internet and social networking services such as email, Internet browsing, Facebook, and Twitter (Gordon, 2007). Gunawan (2008) describes a service for using mobile phones to aid in the evacuation of the injured during disasters. Using these services enables people to access remote resources as well as to report events to a worldwide audience.

CRGs as Social Networks

According to de Nooy, Mrvar, and Batagelj (2005), social networks are representations of real-world social links between individuals, organizations, government agencies, and NGOs. Social networking sites, such as Facebook, MySpace, and LinkedIn, utilize several types of communications features. These features include personal Web pages, messaging, photo sharing, and the ability to view one's own as well as others' social networks (Ellison, Lampe, & Steinfield, 2009). Ellison et al. indicated that social network sites allow people to maintain social connections at low cost, to provide information to which other individuals might not otherwise have access, and to mobilize people for social actions, such as disaster recovery. Humanitarian relief efforts of government agencies and NGOs, such as the United Nations and the Red Cross, depend on these linkages to achieve their goals, include fundraising and volunteering.

Due to difficulties in determining facts in crisis events, PERs may not be fully aware of recovery process requirements (Jaeger et al., 2007). According to Jaeger et al., CRGs as well as social networks are viable options in provisioning information on the status of the emergency and enabling coordination of the distribution of scarce resources. This use of social networks can assist PERs in providing effective services to those in need.

Stephenson (2005, 2009) determined that the current state of cooperation among NGOs during an emergency is indicative of a weak bureaucratic social network and a lack of top-down coordination.

Social networks are used to support a variety of objectives relevant to EMSs. For example, mash-ups, such as Hurricane Information Maps (Palen et al., 2007), have been utilized in a number of emergency management situations. The Ushahidi (Swahili for testimony or witness) application allows citizens to submit crisis data via SMS, email, or a Web form (Okolloh, 2011). Using the Ushahidi application, a user can assemble information about abuses of power and voting irregularities and displays them on a map or a timeline. This system is being used to track violence and voting irregularities in the Democratic Republic of the Congo (Okolloh, 2011).

Summary of What is Known and Unknown about CRGs

According to Jaeger et al. (2007), CRGs can overcome deficiencies in traditional EMS initiatives by enabling residents in a disaster area to help each other resolve their needs. Additionally, they give the residents the ability to communicate to PERs information that may be relevant to the ongoing management of the disaster (Crowe, 2010). People are more likely to communicate to PERs during an emergency because of their experience in the daily use of social media. CRGs are an attempt to formalize these informal responder activities (Jaeger et al., 2007). Crowe noted that the current NIMS standard for managing emergencies with PERs cannot easily support social media use because NIMS is too dependent upon command and management for success. Finding ways to bridge this gap is an important area of research.

According to Schafer et al. (2008), emergency preparedness and management often are missing real-world community perspectives. Schafer et al. underscored the importance of case studies to measure the feasibility of these emergency research classification schemas. In this inquiry, the author conducted a case study, using the SDLC methodology, to develop a paradigm for CRG implementation.

Schooley et al. (2007) support the use of case studies to facilitate EMS analysis and an inquiry approach to study the provision of time-critical information services in emergency management. Schooley et al. use a case study methodology that involves an analysis of systems technologies and the social constructs that surround these technologies. According to Schooley et al., this focus on technologies and social constructs provides a holistic research approach.

Schooley et al. (2007) also looked at EMS technologies, people, and policies, focusing on time-critical emergency services and how best to optimize their use. The researchers noted that interoperability among emergency agencies was critical to success. Interoperability is particularly important because CRGs rely on community input and agreements between communities.

The Contribution this Study Makes to the Field

Based on findings from this investigation, the author provided guidelines for effectively planning and implementing a paradigm for CRG implementations that optimizes the provision of first responder services (Crowe, 2010; Schooley et al., 2007). Outcomes from this Dublin, Ohio, case study also can contribute to the development of a model for integrating CRG functions with EMS operations in municipalities that are

similar in size to Dublin, Ohio. The results of this study should enable PERs to better optimize emergency resources and to receive more feedback from citizens.

Chapter 3

Methodology

This chapter presents the methodology used in the study. The chapter describes the research methods employed, followed by a presentation of the system development life cycle, the exploratory case study methodology, unit of analysis, instrumentation, reliability and validity, formats for presenting results, criteria used to interpret findings, and resource requirements.

Research Methods Employed

The author employed the Butler and Fitzgerald (2001) case study methodology. Butler and Fitzgerald analyzed the role that user participation played in the management of change in the systems development process. The use of this approach was critical to this author's investigation. To ensure a successful CRG implementation, it was critical to examine the role of user participation in its construction, as the users of the system would be central to its eventual success.

Exploratory Case Study

This research was an exploratory case study of the adoption of CRGs using an SDLC. An exploratory case study was utilized due to the experimental nature of CRGs at the time of this research (Jaeger et al., 2007). Formalizing CRGs with an existing in-place EMS has not been attempted outside of an academic environment (Wu, 2009). Thus, conducting this research as an exploratory case study was appropriate to better understand the implications of this novel technology for existing emergency management operations. According to Yin (2003), exploratory studies should identify their purpose

and criteria for success. The study's purpose was to develop a replicable process based on the SDLC to develop a paradigm for implementation of a CRG. The success criteria were the documentation and analysis of this process.

Unit of Analysis

Yin (2003) identified two attributes to describe case studies: the number of cases in the case study and units of analysis (or the scenario for analysis). As an example, a case study of primary schools could cover a single case (one school) or multiple cases (multiple schools). The units of analyses in these examples could range from a single scenario (such as faculty use of technology) to multiple scenarios (faculty use of technology and student adoption of technology). Yin (2003) classified these attributes into four types of case studies: (a) Type 1 single-case holistic design, (b) Type 2 single-case embedded design, (c) Type 3 multiple-case holistic design, and (d) Type 4 multiple-case embedded design.

The present study was a Type 1 case study, as the author examined a single case (Dublin Division of Police) in conjunction with a single unit of analysis (the entire organization). Yin defined Type 1 as a single-case, holistic case study design. Yin presented five criteria for using a Type 1 case study: (a) a critical case, (b) an extreme or a unique case, (c) a representative or typical case, (d) a revelatory case, or (e) a longitudinal case. The use of a Type 1 case study is justified in the present study because the Dublin Division of Police represents a typical case due to its adherence to the two standards detailed next.

Since 1990, the Dublin Division of Police has certified its department's operations in accordance with the Commission of Accreditation for Law Enforcement Agencies, Inc.

(CALEA; 2010; City of Dublin, 2010c) standard. The CALEA's Standards for Law Enforcement Agencies provide the following imperatives for law enforcement: (a) written directives for administration and operations, (b) standards for management decisions, (c) preparedness programs for incident management, and (d) fostering a relationship with the community. Additionally, the Dublin Division of Police has standardized its EMS using the NIMS standard. NIMS describes overarching operational strategies for design, implementation, and integration of EMSs, locally and nationally (USDHS, 2008a). The CALEA and NIMS standards generally identify specific methods and techniques for technologies and operations that enabled the Dublin Division of Police to be identified as a typical case study.

System Development Life Cycle

The USDOJ (2003) SDLC was utilized in this investigation as the framework for developing a paradigm for implementing CRGs. The Dublin Division of Police indicated that they did not have funding or approval to make any changes to their EMS, and, as a result, this investigation was limited to the first four phases, specifically the Initiation, Systems Concept Development, Planning, and Requirements Analysis Phases. The fifth phase, Design, could potentially have affected the current operations of the Dublin Division of Police EMS, as it involved deconstructing the current environment and spending funds that have not been allocated. The Dublin Division of Police was not yet ready to commit to phases that could affect current operations (T. Hirschy, personal communication, January 6, 2009). The complete list of USDOJ SDLC phases is as follows:

1. Initiation Phase
2. System Concept Development Phase
3. Planning Phase
4. Requirements Analysis Phase
5. Design Phase
6. Development Phase
7. Integration and Test Phase
8. Implementation Phase
9. Operations and Maintenance Phase
10. Disposition Phase

In the following section, the four phases that form the framework for this investigation are discussed in detail.

Phase 1 or Initiation Phase

This phase begins when management identifies that it is necessary to improve or to implement a business process through the use of information technology (USDOJ, 2003). The purpose of this phase is threefold (USDOJ, 2003):

1. Identify and validate the need and opportunity
2. Identify assumptions and constraints
3. Identify alternate options to satisfy the need.

Specific tasks include the identification of the opportunity, appointment of a project sponsor, formation of the project committee, documentation of the efforts, and the formal approval of the appropriate ranked level of management in the organization (e.g., chief

information officer). The deliverable for this phase is the concept proposal. Items for inclusion in this document are presented below (USDOJ, 2003):

1. Mission/Goals that this Project Supported. This ties the project to the strategic plans of the organization.
2. Existing Structure. Comparison of the current state of infrastructure versus the future state after this project is completed. This deliverable ensures that the project leadership ties the project to the strategic plans of the organization.
3. Benefits and Warranted Investment. Identification of organizational needs that this project will address and how this project will support the priorities of the organization.
4. Funding. Estimate the project costs.

Phase 2 or System Concept Development Phase

This phase commences when the concept proposal document is formally accepted. Activities in this phase include further study and analysis of the business need; project planning, including schedule, cost, and performance measures; development of a project acquisition strategy; development of the risk management plan; and obtaining project resources (USDOJ, 2003). These activities were documented in the following deliverables: system boundary document, cost benefit analysis, feasibility study, and a risk management plan (USDOJ, 2003).

The system boundary document lists the following elements of the project: critical success factors, performance metrics, existing methods and procedures, users' information and functional requirements, data sensitivity, network and interface requirements, business organizational structure, legal considerations, security

considerations, system assumptions and constraints, and program and project management (USDOJ, 2003). The cost benefit analysis includes an enumeration of assumptions, constraints, alternatives, cost analysis, benefit analysis, and comparison of costs and benefits (USDOJ, 2003). The feasibility study includes evaluation criteria, alternative descriptions, and alternative evaluation (USDOJ, 2003). The risk management plan includes risk identification list, risk assessment, and risk action plan (USDOJ, 2003).

Phase 3 or Planning Phase

The planning phase proceeds after the formal approval of the documents created in the System Concept Development Phase. Tasks and activities in this phase include the review of the project schedule, review of internal processes, establishment of agreements with stakeholders, development of the project management plan, review the feasibility of alternative solutions, and review of security implications (USDOJ, 2003). These activities were documented in the following deliverables: acquisition plan, configuration management plan, quality assurance plan, concept of operations, system security plan, project management plan, and validation and verification plan (USDOJ, 2003).

The acquisition plan should include performance requirements, sourcing processes, make or buy decisions, distinctions between government and contractor functions, and the acquisitions cycle (USDOJ, 2003). The configuration management plan should contain details about configuration management activities, responsibilities, identification, and subcontractor control (USDOJ, 2003). The quality assurance plan should provide the quality management processes, problem reporting, and quality tools, techniques, and methodologies (USDOJ, 2003). The concept of operations plan should address the goals

of the new system, functional and operational requirements, and any impact considerations (USDOJ, 2003). The security management plan should include data sensitivity analysis, security management controls, security operational controls, and security technical controls (USDOJ, 2003). The project management plan covers a work breakdown structure, resource estimates, schedules, and responsibilities (USDOJ, 2003). The validation and verification plan should detail criteria to measure and test for validation and verification at each phase of the project (USDOJ, 2003).

Phase 4 or Requirements Analysis Phase

The activities in this phase begin after the completion and approval of the deliverables from the planning phase (USDOJ, 2003). Tasks in this phase include analyzing requirements, developing test criteria, completing a functional review of the system, and reviewing the privacy impact of the system (USDOJ, 2003). These activities were documented in the functional requirements section and the privacy impact assessment (USDOJ, 2003). The functional requirements should identify system requirements such as processes, security, audit, data currency, reliability, recoverability, availability, fault tolerance, performance, capacity, and data retention (USDOJ, 2003). The privacy impact assessment should identify the management framework (policies and accountabilities), data discovery, risk assessment, data lifecycle management, and ongoing privacy management (USDOJ, 2003).

Instrumentation

Triangulation of data contributes to the development of logical conclusions in a case study (Yin, 2003). Data triangulation is the use of various sources of data in the case

study analysis to develop better conclusions. These conclusions are better developed because they have multiple sources of data corroborating the results. Yin (2003) indicated that, if several sources of data point to the same findings in a case study, then there is a stronger indication that the results are valid. In this study, the author used the following sources of data:

1. Dublin Division of Police documentation.
2. Direct and participant observations of the author during his interactions with Dublin Division of Police.
3. Facilitated workshops with the Dublin Division of Police. These workshops were conducted with stakeholders from the Dublin Division of Police to determine the requirements for implementation of the CRG, according to the processes defined in the SDLC (USDOJ, 2003).

The triangulation of these three sources of data provided the foundation for evaluating the principal unit of analysis in this research.

The format for the facilitated workshops was based on guidelines created by Hubbard (2010). Hubbard detailed procedures for soliciting estimates of minimum, maximum, and most likely values for single metric estimates, such as the frequency of events, percentages, and cost from groups of individuals. The procedures utilized include soliciting input from all participants, building consensus, and avoiding leading the participants toward specific answers.

Reliability and Validity

Yin (2003) identified four requirements to ensure validity in case study design: (a) construct validity, (b) internal validity, (c) external validity, and (d) reliability. Yin stated that construct validity refers to the operational measures of the study. In this research, the author utilized multiple sources of data, maintained appropriate chains of evidence, and asked key informants to review the drafts of the case study report.

Internal validity is a threat to establishing causal relationships in a case study (Yin, 2003). According to Yin, however, internal validity is not a threat to exploratory case studies such as the present research. External validity concerns generalizability of the findings (Yin, 2003). In this research, the author established the unit of analysis as the Dublin Division of Police. Findings from this investigation may be generalized to similarly sized cities as a means to facilitate innovations in city disaster response and EMSs.

Reliability in a case study refers to the ability of the study to be replicated by other researchers (Yin, 2003). In this investigation, the author used the case study approach in conjunction with SDLC to guide the investigation. The use of SDLC supports the reliability that Yin recommends.

Formats for Presenting Results

This author conducted data analysis for this study by categorizing results as well as providing details of facilitated workshops and of observations as described in the instrumentation section above (Yin, 2003). The author included the deliverables from

each of the completed SDLC phases in this study. The data were organized in conjunction with the research question.

Criteria for Interpreting Findings

Yin (2003) indicated that a case study should include details on how to interpret the results of the findings. In this study, the author created a replicable process based on the SDLC to develop a paradigm for implementation of a CRG. The criterion for interpreting the findings in this study is the extent to which the replicable process that the author creates meets this goal. The research questions served as a guide for interpreting the results (Yin, 2003).

Resource Requirements

This case study was conducted with the Dublin Division of Police. The author received a letter granting permission to conduct research with them (Appendix B). This letter was signed by the Dublin Division of Police Emergency Management Coordinator, Tom Hirschy. Due to the involvement of human subjects in this research, the author obtained from the Nova Southeastern University (NSU) Institutional Review Board (IRB) the approval letter included in Appendix D.

The Dublin Division of Police agreed to have the author complete the first four phases of the SDLC (USDOJ, 2003; T. Hirschy, personal communication, January 6, 2009). Tom Hirschy agreed to allow the author access to documentation and the division's sworn and civilian staff members (personal communication, January 6, 2009). To complete the first four phases of the SDLC, the author reviewed documents on the emergency operations plan maintained by the Dublin Division of Police, which were not

approved for public release or publication (T. Hirschy, personal communication, February 10, 2011). The documentation detailed the processes for responding to emergencies, including (a) activating the plan, (b) mobilizing emergency personnel, (c) obtaining support from other agencies, (d) communicating with the public, (e) documenting the incident after it is over, and (f) responding to specific emergency types. Reviewing these documents enabled the author to design practical approaches for the implementation of a CRG in conjunction with the Dublin Division of Police EMS.

The author did not hold any paid or volunteer positions or roles with either the City of Dublin, Ohio, or the Dublin Division of Police. For the duration of this case study, the author served as the Project Director. In this role, the author conducted workshops, reviewed Dublin Division of Police EMS documentation, recorded observations made during the research, and completed a final research report.

Summary

In this chapter, the author described the methodology that was used to conduct this case study. A detailed description of the four USDOJ SDLC processes employed was provided. The author also defined the unit of analysis and described the instrumentation that was used. Tactics for ensuring the reliability and validity of this investigation and formats for presenting results were described. Additionally, criteria for interpreting findings, and identifying resource requirements for this inquiry were delineated.

Chapter 4

Results

This chapter presents the results of the data analysis, discussed in terms of the requirements documented during the execution of the four phases of the investigation: Phase 1 or Initiation Phase Deliverables, Phase 2 or System Concept Development Phase Deliverables, Phase 3 or Planning Phase Deliverables, Phase 4 or Requirements Analysis Phase Deliverables. This chapter ends with a summary of the findings.

In the section below, the author presents the findings from the four SDLC phases. The findings are in the form of detailed assessments of what is required for success in the implementation of a CRG. The author presented the impact and benefits of CRGs to the participants in workshops, during which the author noted participant comments. Below is a presentation of the results for each phase, its respective deliverables, a summary of each deliverable, and participants' feedback.

Phase 1 or Initiation Phase

Phase 1 or the Initiation Phase is the first step in the implementation of a CRG. The only deliverable in Phase 1 is the Concept Proposal, which serves as the foundational document for documenting the requirements of the Dublin Division of Police.

Concept Proposal: Mission/Goals that this Project Supported

This project will support the following strategy developed by the Dublin City Council (City of Dublin, 2012a):

> The City provides appropriately designed, well-maintained and robust public infrastructure systems. Additionally, the City provides exemplary public services delivered in a manner to ensure an extraordinary quality of life. Infrastructure and services are provided in a cost-effective manner to meet the needs and expectations of residents, businesses, visitors and other stakeholders. These systems and services are created and implemented through a process of thoughtful prioritization with broad community input. (p. 1)

According to Participant A (personal communication, October 5, 2010), a CRG implementation can support the ongoing needs for developing robust public infrastructure for emergency management that meets the needs and expectations of residents and others.

Concept Proposal: Existing Structure

The existing IT infrastructure consists of an internal network for daily business processing, a separate emergency management system network, and an externally hosted Web site (Participant A, personal communication, October 5, 2010). Initial discussions with the Dublin Division of Police indicated that they are open to and familiar with the use of private companies to provide technological solutions (Participant A, personal communication, October 5, 2010). Communications with the IT staff indicated that their current Web hosting company could offer robust solutions that can scale to the levels needed to respond to demands during emergencies (Participant D, personal communication, October 14, 2010).

The Dublin Division of Police also uses the Nixle Web site as a tool to communicate with the community. Nixle enables PERs to communicate information about specific communities to those who elect to receive that information (Nixle, LLC, 2011). Finally,

the Dublin Division of Police does not maintain a full-time software development team (Participant A, personal communication, October 5, 2010). Thus, any software development efforts needed to be commissioned by the City or the Dublin Division of Police from a private sector business.

The author conducted several workshops with the Dublin Division of Police to document the current state of its IT infrastructure. According to Participant A (personal communication, October 5, 2010), the Dublin Division of Police, along with the City of Dublin, maintained two internal networks: (a) an internal network for regular daily police functions and (b) a dedicated network for connecting to the Ohio Law Enforcement Automated Data System (LEADS) network. The LEADS network provides operational tools for submitting and viewing criminal information such as the Federal Bureau of Investigation (FBI) Automated Fingerprint Identification System (AFIS), computerized criminal history (CCH), and the criminal justice information services (CJIS). The Ohio Administrative Code in § 4501:2-10-10 (H) mandates that, to attach to and utilize the LEADS tools, a police department must provide a dedicated network and workstations that are not connected to the Internet. The internal network provided access to the Internet, as well as allowed Mobile Data Terminals (MDTs), specialty laptops that reside in each police vehicle to provide access to police resources and criminal records searches (Participant A, personal communication, October 5, 2010), to connect using mobile Code Division Multiple Access (CDMA) connections of less than 384 kilobits per second (Lawton, 2011). The results of these workshops are presented in Figure 6.

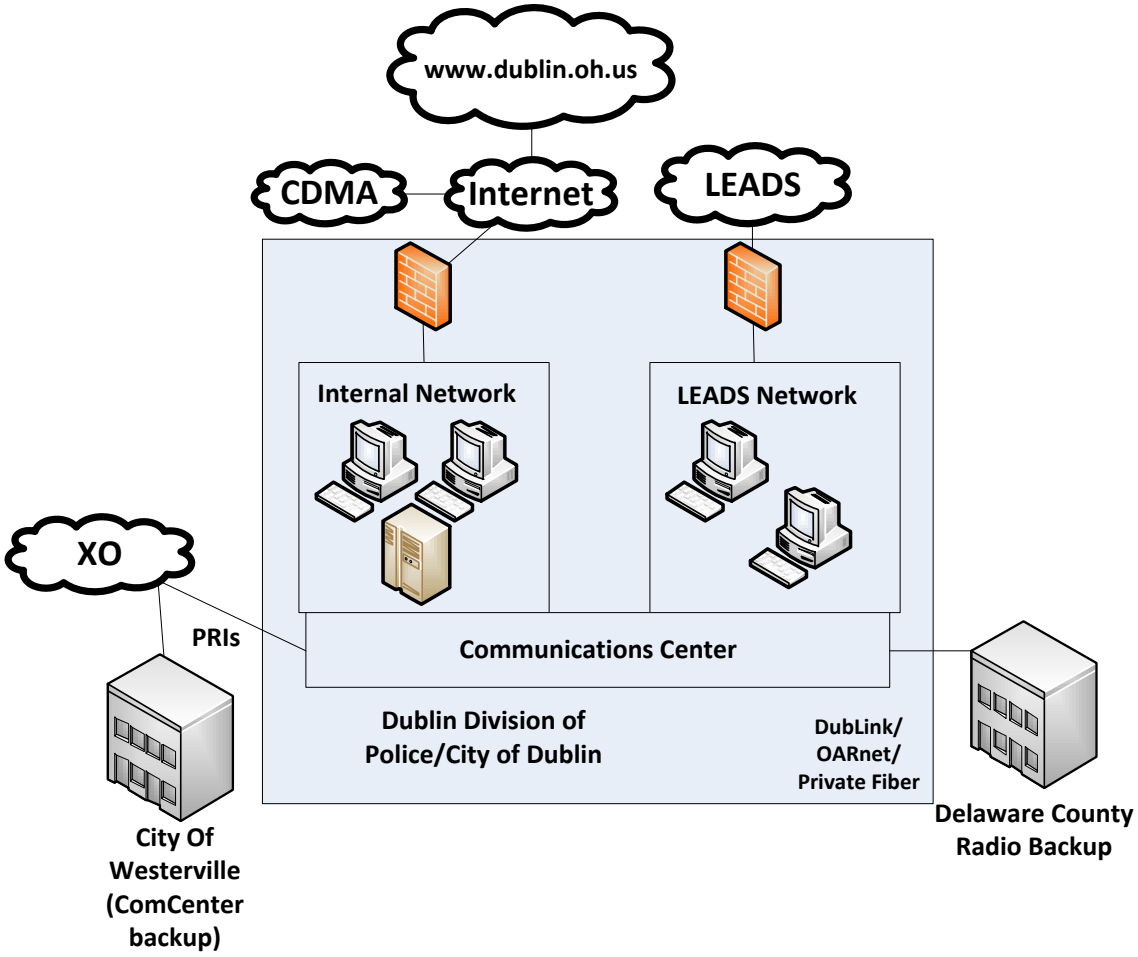

Figure 6. Dublin Division of Police network diagram.

The communications center houses equipment that allows employees to access resources on both the internal and LEADS networks (although no single computer attaches to both networks), and the phone lines that support 911 are monitored here. These lines are capable of failing over to a backup site owned by the City of Westerville by utilizing primary rate interfaces (PRIs) telecommunications connections procured from a competitive local exchange carrier (CLEC), XO Holdings, Inc. The Dublin Division of Police also maintains a radio backup site in Delaware County that is connected via a combination of a City of Dublin private fiber (DubLink) and fiber

connections from Ohio Academic Resources Network (OARnet), which provides infrastructure services for the Ohio Board of Regents.

The Web site for the City of Dublin (inclusive of the Dublin Division of Police) is hosted externally in a non-city-owned facility. No Web hosting is available at the Dublin Division of Police or the City of Dublin facilities. According to Participant A (personal communication, October 5, 2010), the CRG implementation mainly augments the external Web hosting arrangements. Thus, new services would need to be provisioned at the Web hosting provider and connections enabled for the communications center. Utilizing external Web hosting seemed to be the best course of action to satisfy the availability requirements to operate a CRG (Jaeger et al., 2007). Further, it was determined that collocating the CRG in Dublin, Ohio, would subject the hardware and software that support it to the same emergencies that it was meant to help ameliorate. As a result, it was concluded that off-site hosting was the best solution.

Concept Proposal: Benefits and Warranted Investment

This section concerns how this project will support the priorities of the organization. The benefits that the Dublin Division of police will realize after the implementation of a CRG include a simplified strategy for emergency communication using the Internet, the ability to support emergency reporting and response over the Internet, and a reduction in duplicate incident reporting via landline or mobile phones.

The first benefit is the development of a simplified strategy for emergency communication using the Internet. The Dublin Division of Police utilizes three Internet-enabled emergency communication tools: Twitter, Nixle, and the Dublin Division of Police Web site. The use of these tools causes confusion, as indicated by residents'

explaining that they do not know how to communicate with the Dublin Division of Police (Participant C, personal communication, October 12, 2010). Participant B (personal communication, October 7, 2010), however, stated that some residents felt there were too many ways to communicate and that they were often confused when trying to decide how to contact the Dublin Division of Police. Throughout this investigation, the Dublin Division of Police made clear their preferred method of communication.

The key triage decision to call 911 or to go online concerns whether there is an immediate, life-threatening emergency. For example, if one's life were in immediate danger or if someone were witnessing a break-in at a neighbor's residence, the Dublin Division of Police would like them to call 911 (Participant K, personal communication, September 16, 2010). However, for other types of incidents, the Dublin Division of Police indicated that it is appropriate to log onto the CRG portal or to call the non-emergency number (Participant K, personal communication, September 16, 2010; Figure 7).

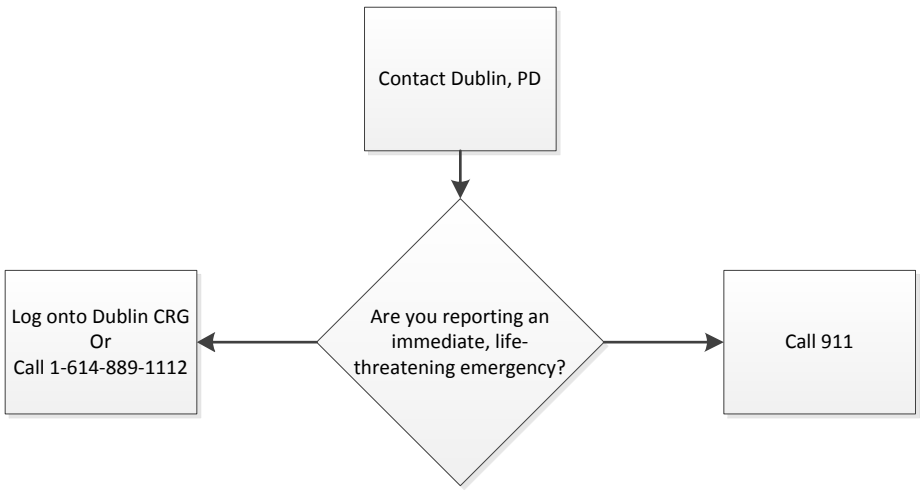

Figure 7. Preferred communications methods flowchart.

The second benefit is the ability to support emergency reporting and response over the Internet. According to Participant K (personal communication, September 16, 2010), people assumed that the Dublin Division of Police monitored and responded to their Twitter account in real time and that communicating with them via Twitter was the same as calling 911. The Dublin Division of Police does not maintain a vigil on their Twitter account and, as such, may not be able to provide assistance or even advise people who send messages that way. Implementing a CRG would give the police the ability to utilize volunteer resources (as discussed in the *System Boundary Document: Business Organizational Structure* section) to monitor and respond to requests for assistance or to advise people to call 911 for immediate assistance.

The last benefit for the Dublin Division of Police is a reduction in duplicate incident reporting and decreased phone usage. According to Participant B (personal communication, October 7, 2010), the Dublin Division of Police experienced increased use of operational resources due to repeat reporting of automobile accidents. Implementing a CRG will provide the residents of Dublin with information about current incidents and citizen reports about emergencies in their neighborhoods. Because they will be able to see events unfolding in real time, residents will not repeatedly report incidents. Additionally, residents will have a viable method for communicating with the Dublin Division of Police that will reduce communication by phone, as residents will triage their own issues and determine whether they should be reported via 911 or can be communicated via the CRG.

Concept Proposal: Funding

During the early stages of any project, costs are less well articulated, in general, due to the project management concept of progressive elaboration, which means that there is more detailed information about a project's plans as they become available over time (Project Management Institute [PMI], 2008). The author utilized two tools to provide cost estimates: the program evaluation and review technique (PERT) for estimating minimum, maximum, and mode values and Monte Carlo methods (Hubbard, 2010; PMI, 2008).

For this project, Participant J (personal communication, April 21, 2011) estimated that Web site design costs would be no less than $10,000 and that requisite platform development and hosting, as well as the specialized collaborative software and database development, would make the minimum costs $150,000. If the Dublin Division of Police utilizes more advanced business intelligence and data warehousing technologies, then the costs could be as high as $500,000 (Participant J, personal communication, April 21, 2011). Given that the mode value could be dependent on a number of factors, it was placed in the middle of this range, at $325,000, with low confidence as an input into the Monte Carlo function. The results of this estimation are presented in Figure 8.

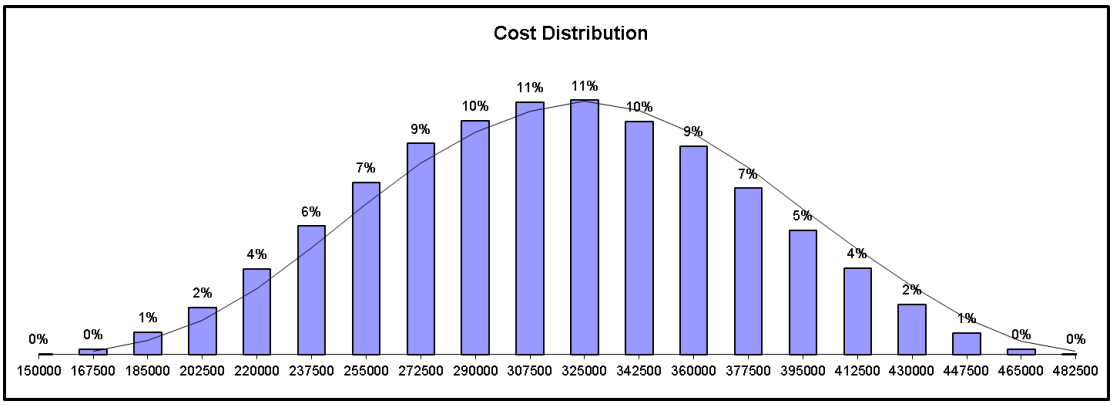

Figure 8. Development cost estimate distribution.

The author used the cost estimates above as inputs into a Monte Carlo Excel function provided by RiskAMP (Structured Data, LLC, 2008), which displays the values using a beta-PERT distribution and 30,000 random samples. This provided a most likely (mode) project cost of $319,702 with a minimum value of $160,995 and a maximum value of $495,114.

Phase 2 or System Concept Development Phase

The next step in the investigation was Phase 2 or the System Concept Development Phase, which included the following deliverables: (a) System Boundary Document, (b) Cost Benefit Analysis, (c) Feasibility Study, and (d) Risk Management Plan. In this phase, the author provides detailed success factors for the proposed CRG implementation project.

System Boundary Document: Critical Success Factors

This section presents the factors that contribute to success in reaching the business-related goals of implementing a CRG. According to Participant K (personal

communication, September 16, 2010), successful completion of the CRG implementation will encompass the following high-level activities:

1. Procure and install the hardware and software to operate a robust CRG portal.
2. Develop and implement the processes necessary to successfully operate the CRG.
3. Communicate and educate the residents of Dublin, Ohio, on how to conduct their emergency communications using the CRG system.

According to the Dublin Division of Police, the successful completion of the above three items would represent successful completion of the CRG implementation project.

System Boundary Document: Performance Measures

To provide the best project execution, the author determined that this project should be conducted utilizing the best practices outlined in the Project Management Body of Knowledge (PMI, 2008). Based on this body of knowledge, regular communications from the project leadership regarding the status of items identified for implementation in the work breakdown structure (WBS) should occur. The WBS includes measures that indicate the projected versus actual schedule and cost performance. According to Participant K (personal communication, September 16, 2010), post-implementation performance measures should include the amount of emergency communication that occur on the CRG as well as the number of residents who are able to find successful resolutions to their issues by using the system.

System Boundary Document: Existing Methods and Procedures

This section concerns the current means in place to meet the emergency communication needs of the residents of Dublin, Ohio. According to Participant A (personal communication, October 5, 2010), Participant C (personal communication,

October 12, 2010), and Participant K (personal communication, September 16, 2010), the residents' communication needs during emergencies were being serviced by the following technologies: traditional telephony, cellular telephony, and Web sites not operated by Dublin, Ohio (such as Twitter), as well as by traditional print, radio, and television media. Most residents who needed to alert the Dublin Division of Police did so by calling 911 from their mobile and landline phones (Participant B, personal communication, October 7, 2010). Communications from PERs to the residents were typically accomplished by direct communication to them via official channels (the Dublin Division of Police Web site or reverse 911 calls) to alert individuals in affected areas. Other intermediated communication methods included traditional print, radio, and television journalism. According to Participant B (personal communication, October 7, 2010), the residents seek out Web sites that allow them to contribute content, as their natural inclination is to communicate with each other about the state of the emergency and how it affects them. Participant K (personal communication, April 21, 2010) indicated that these existing methods do not allow for an official mechanism for citizens to report, respond to, and request aid from PERs during an emergency solely in a Web-based environment, regardless of client platform.

System Boundary Document: Users' Information and Functional Requirements

This section contains the user's information and functional requirements for CRG implementation. These functional requirements were determined through the workshops held with the Dublin Division of Police. The requirements are as follows:

1. Residents can register and authenticate with the CRG portal to gain access to its resources.

2. Residents can report emergencies.
3. Residents can request assistance.
4. Residents can view and respond to requests for assistance from other residents.
5. Residents can view information about their registered communities (overview map, news, and general information about how to report emergencies as well as offline contact information).
6. Residents can view information about volunteer opportunities, training events, and other activities of interest.

System Boundary Document: Data Sensitivity

This section focuses on data protection requirements. According to Participant F (personal communication, October 29, 2010), the data classification scheme for the CRG Portal should be as follows:

1. Public data: All records kept by the Dublin Division of Police are public records unless they are exempt from disclosure. "Public" is the default initial classification for all records.
2. Exempt data: Records that are exempt from disclosure under § 149.43 of the Ohio Revised Code. Examples include confidential law enforcement investigatory records, suspects not yet charged with offenses, and most information about persons under the age of 18.

The author determined that data that are subject to exemption from public disclosure should be protected with strong information security controls. These controls should include the use of data encryption, user access controls, confidentiality and non-disclosure agreements, secure disposal methods, and appropriate logging and monitoring.

Residents should be informed as to the public nature of the CRG (Participant F, personal communication, October 29, 2010). This can be accomplished via a notice during the registration process that all information disclosed to the CRG may be subject to public disclosure, as required by law.

System Boundary Document: Network and Interface Requirements

The CRG network support requirements and their relationship with other systems are presented in this section. According to Participant E (personal communication, October 29, 2010), CRG bandwidth needs will vary based on what emergencies are occurring in the community. Because emergencies are infrequent, most daily bandwidth requirements will be minimal. However, when an event occurs that generates a lot of interest, there will be a significant spike in traffic (Participant E, personal communication, October 29, 2010). Participant E determined that the network bandwidth requirement should be between 1,500 and 3,000 kbps (personal communication, October 29, 2010). Participant E estimated that, after the CRG portal is publicly available, there will be approximately 50,000 page views a week (personal communication, October 29, 2010).

According to Participant A (personal communication, October 5, 2010), the interfaces to other systems will be limited. This was a deliberate design requirement prescribed by the Dublin Division of Police, as they believe that the best way to provide emergency services to the City of Dublin is by utilizing the existing 911 system (Participant C, personal communication, October 12, 2010). This means, in practice, that either the person who reports the incident or a moderator will determine that the situation requires PERs to assist. The person will then stop communicating in regard to the incident through the CRG and will switch to the 911 system. Technologically, this means that

there will not be any interfaces between the CRG and other emergency management systems. While it may be the case that moderators of the CRG forum will also be 911 operators working on Web-enabled computers in the communications center, there will still be a bifurcation of the systems (Participant A, personal communication, October 5, 2010). However, future upgrades and modification to the CRG portal may consolidate and integrate the 911 and CRG systems.

System Boundary Document: Business Organizational Structure

This section focuses on the impact of the introduction of this system on the organizational structure. Participant C (personal communication, October 12, 2011) did not anticipate that the introduction of this system would have a significant impact on the organizational structure of the Dublin Division of Police. Because the CRG Portal will result in additional data feeds, however, there will be a need for personnel to process the data. Due to this additional workload, the author discussed the following two approaches with the Dublin Division of Police participants during the workshops: (a) have the current 911 operators triage and moderate all the submissions on the CRG site, or (b) incorporate volunteer labor to conduct the initial triage and moderate the site while escalating important submissions and data to the 911 operators so that they can respond (Participant H, personal communication, January 20, 2011; Participant I, personal communication, January 20, 2011). The volunteers will need to undergo training on how to provide an initial triage and the factors for which they should look. Given the financial obligation that would be required to operate this system with several new full-time people, it was the preference of the Dublin Division of Police leadership to pursue implementing CRGs with volunteer resources. Indeed, Participant G (personal communication, November 2,

2010) has indicated that a CRG would likely attract many volunteers. Participant D (personal communication, October 10, 2010) indicated that serving in this capacity might be of interest to the local Boy Scout troops. If there are large numbers of volunteers, additional people may be needed to assist the Dublin Volunteer Services office in vetting and coordinating the volunteers (Participant G, personal communication, November 2, 2010).

System Boundary Document: Legal Considerations

Legal implications that would result from the development of a CRG in Dublin, Ohio, are presented in this section. Operation of the CRG portal would fall under the legal auspices of the City of Dublin (Participant F, personal communication, October 29, 2010). As indicated by Participant F (personal communication, October 29, 2010), all governments in Ohio have immunity against civil action as defined in Ohio Revised Code § 2744.01. Based on this code, Participant F (personal communication, October 29, 2010) had no reservations about putting the system into operation. Other minor legal issues include executing any contracts for procuring computing hardware, software, and services.

System Boundary Document: Security Considerations

This section concerns the high-level security requirements of a CRG. During the workshops, the participants stated that the CRG portal should ensure: (a) identity of the users, (b) authenticity of the user, (c) confidentiality of public and exempt data, (d) integrity of the data, and (e) availability of the system and the data (Participant A, personal communication, October 5, 2011). To provide a secure approach to operating the CRG portal, the author recommended the following access levels be instituted:

1. General access level: A user with this level of access has self-registered with a valid email address. This level of usage is available for all users who request access to the site from any source. These users are limited to viewing only general announcements. Information accessible at this access level may include traffic alerts, safety alerts, or other special messages issued by the Dublin Division of Police. A user with this level of access would not have privileges to post messages in the CRG portal.
2. Member access level: A user with this level of access has verified his or her membership in a community group within the City of Dublin. A community group can be a homeowners association (HOA), neighborhood group, religious organization, school, or other organization. Businesses also are allowed to establish communities (for those people who do not reside, but who work, in Dublin). The owner of the group would need to validate the individual's application for inclusion in his or her group before the individual would have access to messages and data specific to that group. After authentication with the group's owner, the individual would be able to post messages to the community.
3. Moderator access level: A user with this level of access assists the Dublin Division of Police in triaging and prioritizing communications in the CRG portal. This level of access is predicated on membership in one or more of the community groups (all communities need at least one moderator). A moderator will have special access that allows him or her to forward or escalate messages to the attention of the 911 operators. This level of access should be granted only to those individuals who have appeared in person to vet their identity, who submit to

criminal background investigations, and who participate in the volunteer application process.

4. Administrators access level: A user with this level of access has responsibilities for the technical operation of the CRG portal. This person will necessarily have access to many of the underlying platforms that enable the system to work and, therefore, may be able to view data and messages on the system. This role should be restricted to employees and contractors for whom the City of Dublin has vetted through an employment or vendor selection process.

Authenticators for all groups should engage in security best practices such as using complex passwords, password expirations, and password histories (International Organization for Standardization, 2005).

Participant K (personal communication, September 16, 2010) indicated that CRG system availability should be prioritized alongside the other critical systems in the Dublin Division of Police. Participant E (personal communication, October 29, 2010) indicated that, to make the CRG available not only during everyday activities but also during large-scale emergencies, it is important that the system be hosted in an environment that is highly resilient to outages. Building a data center to house the system was out of scope for this project (and was in excess of what is needed); however, procuring hosting services at a geographically dispersed Tier 3 or Tier 4 data center would well serve the needs of the system (ADC Telecommunications, Inc., 2006; Participant K, personal communication, September 16, 2010).

System Boundary Document: System Assumptions and Constraints

This section focuses on the preferred technological approach and alternatives for successful completion of the CRG implementation. Through consultation with the Dublin Division of Police, the author determined that the preferred technological approach was to use a Web-based portal hosted at an offsite data center. This determination was driven by several factors: (a) there are no Web hosting resources at the Dublin Division of Police, (b) the current Web site is hosted offsite, and (c) there is no requirement to integrate the portal with the CRIMES Records Management System, which was the primary application used to track police and fire units, calls for service, geolocation services, and response recommendations (Participant A, personal communication, October 5, 2010).

The Dublin Division of Police did not request that the CRG be integrated with the CRIMES Records Management System. The technology that is required to accomplish this would have required a great deal of custom coding by the vendor. According to Participant A (personal communication, October 5, 2010), the Dublin Division of Police decided not to attach critical 911 systems to the Internet because any interruptions to the 911 system cannot be tolerated.

System Boundary Document: Program and Project Management

In this section, the program and project management needs for the CRG implementation project are presented. Based on discussions with the Dublin Division of Police, the author determined that managing the elements required to deliver a CRG portal on time, on budget, and to specification would require a disciplined project management approach, as outlined by the PMI (2008). When the Dublin Division of

Police wishes to pursue the implementation as a formal project, the foundational documents developed as a result of the current investigation could be used to help estimate requirements, effort, duration, and cost.

Cost Benefit Analysis

The methodologies for cost estimations, one-time and recurring costs, and elements of cost estimate uncertainty are discussed in this section. The cost estimates presented above in Phase 1 or Initiation Phase show an estimated CRG project cost of between $160,995 and $495,114. There is inherent uncertainty in the estimates because the project is still in its early stages, and bids for this work have not been solicited. One-time costs for the CRG portal include project management, system architecture planning, disaster recovery (recovery locations and services, backup, and restoration), software development, initial Web hosting arrangements, process development, volunteer recruitment, employee and volunteer training, and communications with the residents of Dublin, Ohio. The recurring costs included Web site operation costs (including Web hosting contracts), ongoing volunteer recruitment, and training.

Feasibility Study

This section concerns the feasibility of alternate technological approaches to implementing a CRG. USDOJ (2003) mandates that a feasibility study be conducted as a means to compare the business and technology requirements with an alternative that offers better results. As noted above, the author established that there was only a single feasible alternative for implementation, namely utilizing an external hosting provider.

Risk Management Plan

This section presents the potential threats to the successful implementation of the CRG portal and ways that these threats can be ameliorated. During the workshops, the author developed a list of threats to successful CRG implementation:

1. Lack of project funding. Without appropriate funding, the project will not be successful. The Dublin Division of Police has not approved CRG implementation at this time, and, as a result, there is no funding available (Participant K, personal communication, September 16, 2010).
2. Cultural friction. Changing the emergency reporting pattern will have an impact on the culture of PERs and the residents. Further, PERs may consider information submitted through online sources less than reputable and, as such, discount them in their investigation and response (Participant H, personal communication, January 20, 2010; Participant I, personal communication, January 20, 2010).
3. Lack of volunteers or enthusiasm. Because the operation of this system will rely heavily on volunteer involvement, it is important that the city have volunteers to fill this role (Participant G, personal communication, November 2, 2010). Participant G (November 2, 2010) indicated that it is critical that there be recruitment of volunteers from community organizations (e.g., HOAs, religious organizations, schools, businesses, Boy and Girl Scouts).

The author reviewed and rated each risk above with the Dublin Division of Police and determined that each item has the potential to make a large impact on the success of the project. Items 1 and 2 have medium to high probability of occurrence, while number 3

has a low probability. This low rating was based on the remarks of Participant G (personal communication, November 2, 2010), who stated that there would be great interest in volunteering among community members.

Phase 3 or Planning Phase

The next step in the investigation was Phase 3 or the Planning Phase, which includes the following deliverables: (a) Acquisition Plan, (b) Configuration Management Plan, (c) Quality Assurance Plan, (d) Concept of Operations, (e) System Security Plan, (f) Project Management Plan, and (g) Verification and Validation Plan (USDOJ, 2003). In this phase, a description of additional technological details critical to the success of the CRG implementation project is generated.

Acquisition Plan

This section concerns the plan for acquiring resources during the course of the project. In consultation with the Dublin Division of Police, the author determined that there needs to be two procurement efforts for this project: (a) selecting a hosting provider and (b) choosing the software development contractor. Participant K (personal communication, September 16, 2010) indicated that, as a government agency in the State of Ohio, the Dublin Division of Police is eligible to purchase from suppliers on State Term Schedule (STS). Vendors registered to sell on STS have already been vetted and have their rate schedules posted and available for review (State of Ohio, 2011). However, according to Participant K (personal communication, September 16, 2010), the Dublin Division of Police is not obligated to purchase on STS and can make a selection from any vendor in the marketplace. Participant K (personal communication, September

16, 2010) and the author, in conjunction, developed the following guidelines for the two main procurement efforts:

1. Hosting Provider

   The CRG portal will need to operate in a data center that is highly available. The data center should have less than one hour of outage a year (99.99% availability). According to ADC Telecommunications, Inc. (2006), this equates to the specifications of a Tier 4 data center.

2. Software Development

   Software development efforts will comprise the majority of the project. A firm skilled in developing highly robust social media applications is needed. According to Participant J (personal communication, April 21, 2011), the coding for the CRG portal should be done in Java™, Ruby on Rails™, and PHP™. Java™ is an object-oriented programming language designed to allow the same code to run on multiple platforms. Ruby on Rails™ is an open-source Web application framework designed for rapid development of Web applications. PHP™ is a server-side scripting language for dynamic Web pages. The firm selected should employ project management staff committed to this project. Finally, the firm should carry enough insurance to cover any potential claims. Inasmuch as the CRG will be a custom application, it is important that the selected firm must have the financial strength to remain in business to support the application throughout its lifecycle. Regular maintenance should be included in the contract to enable periodic defect and security fixes as well as minor feature changes.

Other procurement guidelines discussed include using performance incentives in the contract to ensure that the vendor meets the stated requirements (Guth, 2009). For example, tying user acceptance testing (UAT) to invoice payments will incentivize contractors to meet performance specifications. Participant D (personal communication, October 14, 2010) indicated that the City of Dublin already has a relationship with Verio, Incorporated to host the city Web site, and, as such they may be able to meet the hosting needs for the CRG portal. Another procurement guideline discussed with the Dublin Division of Police was the need to have regular in-person communications with the city such that there is a forum for communicating the city's needs with the vendors (Guth, 2009).

Configuration Management Plan

The plan for managing the configuration of the CRG portal is presented in this section. Participant A (personal communication, October 5, 2010) indicated that the CRG portal configurations will need to be developed by the contracted party. The author determined that the types of configurations that should be identified during the development of the CRG portal include (a) server configurations, (b) platform software configurations, and (c) portal software configurations (administrative items and user management as well as other modules that need configuration items).

Participant A (personal communication, October 5, 2010) also indicated that change management will be an important component of the maintenance of the configurations identified above. Participant A (personal communication, October 5, 2010) and the author discussed two main types of changes that should be addressed in this policy: maintenance and emergency. Maintenance changes occur routinely and allow for

changes to be implemented on a predictable basis. According to Akkiraju, Bhattacharjya, Plaskon, and Jennings (2011), the activities that occur during regular maintenance include upgrading the site, maintaining log files, checking for dead links, reviewing site statistics, checking security settings, and performing test restores of backed-up data. Prior to implementing the maintenance changes, there should be a review of the activities that need to be conducted (Akkiraju et al., 2011). Impact analysis and testing must occur before any changes go into production. These preparatory steps are necessary to ensure that there are no unintended consequences in the proposed changes. The second category of changes, emergency, should proceed through the same steps as a regular change, except on an unscheduled and expedited timeline. Finally, all changes should be logged so that they can be reviewed and audited at a later date (Akkiraju et al., 2011).

Quality Assurance Plan

This section concerns the plan for managing the quality of the CRG portal. The quality plan discussed with the Dublin Division of Police included two major activities: (a) the initial development of the portal application and (b) the managing of data input into the system after it goes into production (Qu et al., 2009). Because this application will be developed by a third party, quality assurance will be the primary focus during the UAT and during the final review before the closeout of the project (Jiang, Avritzer, Shihab, Hassan, & Flora, 2010). To ensure the quality of the final product from the vendor, the contract must be structured in a way that allows for testable modules of code to be released prior to the final version (Jiang et al., 2010). In consultation with Participant A (personal communication, October 5, 2010), the author determined that the Dublin Division of Police should elect several people who are the end users to test the

application and to ensure that it meets with their approval. Any discrepancies should be resolved before work commences on the next module. The UAT team should be comprised of individuals from the following groups: Information Technology, Emergency Management, 911 operators, volunteers, and some representatives of the public (Jiang et al., 2010).

Once the system is in production, it will be supported by ongoing data management. The extent to which these data are accurate depends on the individuals who submit the data. Their reputation for submitting quality information will be measured by an online reputation system, similar to those found on eBay and Wikipedia (Shirky, 2009). Specifically, the CRG should provide a rating for the system users that can be in the form of a percentage, a number of stars, or a thumbs-up-like feature like the one seen on Facebook (Shirky, 2009). Volunteer moderators will be selected from among those who have expressed interest in this role, completed training, and passed the necessary background checks. These moderators will be responsible for reviewing posts and information submitted to the CRG and selecting those that need the attention of the PERs, in accordance with the specifications outlined in the training course and at their own discretion. Information that is clearly spurious will be rejected by the volunteer moderators and removed from visibility in the system (Shirky, 2009).

Errors in the operation of the system must be logged and forwarded to the individual who will have responsibility for the relationship with whomever is chosen as the CRG software vendor (Akkiraju et al., 2011). This person must be empowered, in the maintenance contract, to request fixes in the CRG portal from the vendor (Akkiraju et al.,

2011). If the vendor refuses to provide a fix, then the issue should be brought to the attention of the city's attorneys.

Concept of Operations

The high-level operational requirements of the CRG are presented in this section. In conjunction with participants, the author determined that the high-level requirements of the CRG should include the following:

1. An online Web portal that enables the rest of the requirements.
2. Functionality that supports the ability of a user to register with the site. Registration should allow for four types of users (detailed in the Systems Boundary Document): (a) general, (b) member, (c) moderator, and (d) administrator.
3. Functionality that supports the ability of a user to submit information about a situation that is occurring in the community. This information should include geolocation information (or it should be allowed to be appended).
4. Functionality that supports the ability of a user to make a request of the community.
5. Functionality that supports the ability of a user to offer to assist someone who has made a request.
6. Functionality that supports the ability of a user to view information about the state of affairs in the community. This includes any open requests for assistance, weather (forecasts, watches, warnings), and community news and events. All of this information can be presented on an overview map that has markers that represent incidents, events, and other items of interest.

7. Functionality that supports the ability of a user to view information about how to request emergency assistance (e.g., call 911 for any immediate threats).
8. Functionality that supports the ability of a user to connect with his or her mobile device (i.e., a mobile version of the site and/or a smartphone application; Participant A, personal communication, October 5, 2010; Participant D, personal communication, October 14, 2010; Participant E, personal communication, October 29, 2010; Participant K, personal communication, September 16, 2010).

In addition to the above high-level requirements, the following non-functional requirements should be included in the final design:

1. Performance. Although the majority of the time, the CRG will have a low level of usage, during community incidents (from relatively common events such as fires and burglaries to more intense events such as terrorists attacks, tornados, and floods), the system must be able to endure the load placed upon it. This may necessitate the need to overprovision bandwidth or have the ability to scale throughput to very high levels.
2. Accessibility. The CRG's Web interface should be designed to allow access by those with disabilities, according to guidelines set forth by the State of Ohio.
3. Portability. The CRG should be accessible from mobile devices.
4. Security. The CRG should maintain user access levels as spelled out in the System Boundary Document. It should provide confidentiality of the data, as related to their classification level.

5. System survivability. The CRG must be capable of surviving the destruction of the hosting environment. The CRG does not need real-time failover capability, but a recovery environment should be available to allow the system to recover within four hours (one-half a shift of an emergency responder). (Participant A, personal communication, October 5, 2010; Participant D, personal communication, October 14, 2010; Participant E, personal communication, October 29, 2010; Participant K, personal communication, September 16, 2010)

System Security Plan

In this section, the author identified the security requirements for the system. According to Participant F (personal communication, October 29, 2010), the CRG system will maintain the data classifications as defined in the System Boundary Document. Thus, all data initially will be considered public data and will be compliant with the legal requirements to which State of Ohio are subject (Ghosh, 2011). Thus, the CRG should allow access to the data when requested by those in the media and other interested parties (Jaeger et al., 2007). Occasionally, there will be information in the system that will need to be flagged as exempt data and removed from view of all those except PERs and others whom the City of Dublin's legal counsel deems necessary (Participant F, personal communication, October 29, 2010). In addition to these confidentiality requirements, the CRG software should have the ability to detect unauthorized, unanticipated, or unintentional modification (USDOJ, 2003). Finally, the data should have the appropriate backup controls to enable the data to be available in a timely fashion to the community (Tipton & Nozaki, 2012).

The author recommends that, during the construction of the CRG portal, a security review be conducted (Tipton & Nozaki, 2012). During this process, the assessor will determine risk levels associated with the design and operational choices (Tipton & Nozaki, 2012). Notably, the security controls listed in Appendix A of the ISO/IEC 27001:2005 security standard should be a template for system security requirements at the outset of the project (International Organization for Standardization, 2005).

According to Tipton and Nozaki (2012), certain security practices also should be incorporated into the implementation of the CRG. A third party should be used to conduct an application security penetration test prior to the project closeout and final vendor payments' being made (Tipton & Nozaki, 2012). This will allow any discovered vulnerabilities to be remediated prior to the end of the contract and the initiation of support and maintenance by the vendor (Andersson, 2010). The system should maintain log files and audit trails for high-risk activities to ensure that there is appropriate monitoring of site activities (Tipton & Nozaki, 2012). Finally, all users of the site should undergo regular security awareness and training sessions to ensure that they are familiar with the security options available (Tipton & Nozaki, 2012).

Project Management Plan

The preliminary project management plan for this project is presented in this section. As a result of the workshops held with the Dublin Division of Police in 2010 and 2011, the author developed a WBS table (Table 1) that presents the tasks, predecessors, and durations of the CRG implementation project.

Table 1. Work Breakdown Structure

Task	Predecessor	Duration
CRG Project		402 days
Select team members		10 days
Project kickoff meeting	2	1 day
Create Web Portal	3	274 days
Vendor Selection	3	85 days
Develop Request for Proposal (RFP)	3	10 days
Advertise RFP	6	60 days
Select vendor	7	15 days
Software Development	8	189 days
Requirements analysis	8	30 days
Identify Development Phases	10	1 day
Phase 1	11	150 days
Develop story cards	11	30 days
Develop wireframes	13	30 days
Develop test cases	14	10 days
Code story cards	15	60 days
Unit testing	16	10 days
User acceptance testing	17	10 days
Phase 2	11	150 days
Develop story cards	11	30 days
Develop wireframes	20	30 days
Develop test cases	21	10 days
Code story cards	22	60 days
Unit testing	23	10 days
User acceptance testing	24	10 days
Integration Testing	17, 24	10 days
Final User Acceptance Testing	26	5 days
Configure Web site on host systems	27, 32	3 days
Procure Hosting Arrangement	3	85 days
Develop hosting RFP	3	10 days
Advertise RFP	30	60 days
Select vendor	31	15 days
Make Community Aware of CRG	3	391 days
Develop communications plan	3	5 days
Recruit volunteer moderators	3	90 days
Advertise the CRG portal	28, 32	120 days
Closeout Project	28, 32, 36	0 days

Verification and Validation Plan

This section focuses on how verification and validation will occur during the testing phase of the CRG implementation project. The author, in consultation with the Dublin Division of Police, determined that verification and validation would be accomplished using iterative feedback during the development of the CRG (O'hEocha & Conboy, 2010). Any deviation from the intended function and purpose of the CRG should be rectified in these early development stages. According to Participant J (personal communication, April 21, 2011), verification and validation of the CRG should test whether the Web portal (a) is a recognizable extension of the Dublin Division of Police, (b) provides the functionality for residents to report incidents to PERs and each other, and (c) provides the functionality for residents to respond to each other's requests for assistance. Measuring the extent to which the vendor has correctly met these requirements can be accomplished during the UAT to be performed after the wireframes and story cards are coded into production-ready code and validated in the integration testing (O'hEocha & Conboy, 2010). In the Agile software development method, the wireframe is a mock-up of what the Web page will look like after coding, and the story card is a story written in short bullets about how the Web site should function (O'hEocha & Conboy, 2010).

Phase 4 or Requirements Analysis Phase

The last step in the investigation was Phase 4 or the Requirements Analysis Phase. This included developing the Functional Requirements and the Privacy Impact

Assessment. The development of these final documents completes the planning stages necessary for successful implementation of the CRG at the Dublin Division of Police.

Functional Requirements

The functional requirements for the database for the CRG Portal are presented in this section. The author developed the entity relationship diagram below after consultation with Participant J (personal communication, April 21, 2011; Figure 9). The entity relationship diagram presents the three major database tables that are required to make the CRG Portal functional.

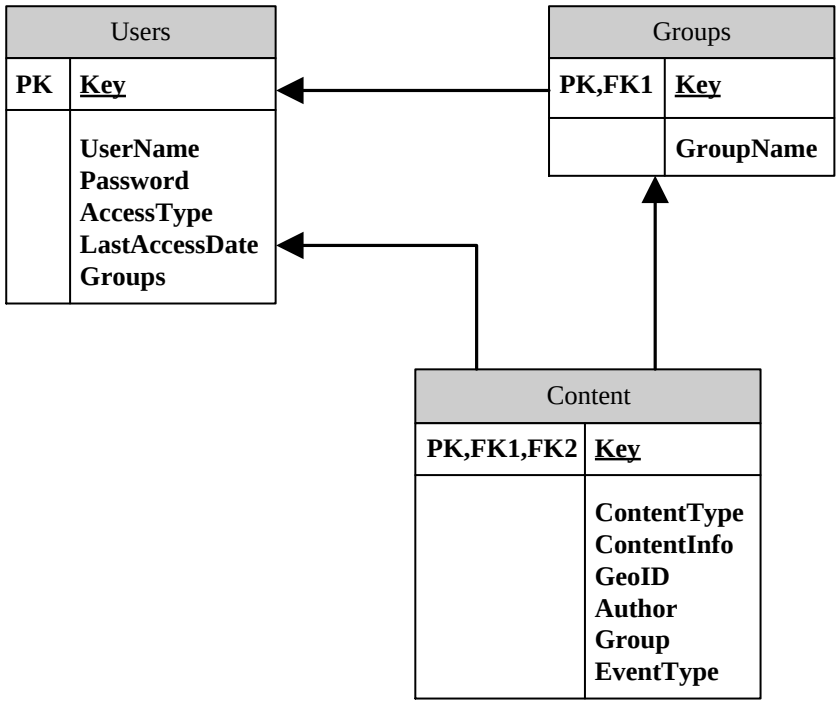

Figure 9. CRG entity relationship diagram.

The database tables for the CRG should be comprised of three tables: (a) Users, (b) Groups, and (c) Content. Each of these tables will have a unique, automatically generated primary key (PK) to identify each row of data. The Groups and Content tables

also will contain the PK from the Users table (called Foreign Key 1 or FK1), and the Content table will contain the PK from the Groups table (called Foreign Key 2 or FK2). The Users table contains the authorized users of the system, their encrypted credentials, authorized access levels, and groups. The Groups table contains a list of the user communities that will be participating in the CRG. Finally, content generated by the users will be in the Content table. This content is classified by its format (e.g., blog post, incident), information about the event, a geolocation field, author, groups that are allowed to view the content, and the type of event (e.g., hurricane, flood, or physical assault).

Privacy Impact Assessment

This section presents a discussion of the privacy concerns associated with the operation of the CRG, identified during the workshops held with the Dublin Division of Police. This discussion will include the types of data collected, how that data will be used, and the risks of misuse. Resident data collected by the Dublin Division of Police will include names, addresses, phone numbers, emails, emergency contacts, and other personal details (Participant B, personal communication, October 7, 2010). Further, when a registered user submits an incident or a request for assistance, the Dublin Division of Police collects the following information: emergency type, location, and image/video/audio (Participant B, personal communication, October 7, 2010). The Dublin Division of Police will collect this data to enable PERs to log and to respond to emergencies. Based on the data classification requirements identified in the Data Sensitivity section of the System Boundary Document, all of the data collected will be public and, thus, fully disclosable to members of the public who request it (Participant F, personal communication, October 29, 2010). According to Participant C (personal

communication, October 12, 2010), the privacy risk associated with the use of the data indicated above is marginal. Most of this information is publicly available through other venues, such as a telephone directory. The information about the emergency is also available through other means, such as the media's obtaining copies of 911 phone calls or the public's listening to police band radio. According to Participant F (personal communication, October 29, 2010), however, certain information could be classified as exempt if it is a part of a police investigation.

Summary of Results

In this chapter, the author detailed the findings that were the result of the investigation. In regard to each of the four phases, the author explained what was needed to produce an effective CRG portal application for the Dublin Division of Police. Critical findings include the following:

1. The CRG supported the Dublin City Council goals for 2010-2011 to develop a strategy to provide for a robust public safety and emergency management infrastructure (City of Dublin, 2012a).
2. The residents of Dublin, Ohio, expected that the Dublin Division of Police would post and respond to social media messages (Participant A, personal communication, October 5, 2010), even though this was not the official channel for communicating emergency information to the Dublin Division of Police.
3. The cost to implement a CRG for the Dublin Division of Police was estimated to cost between $160,000 and $495,000, with a mode value of approximately

$319,000. Rough estimates placed the total completion time of the project at approximately 400 days.

4. Data classification for this system will be comprised of two categories: public data and exempt data. According to Participant F (personal communication, October 29, 2010), all data should initially be classified as public data, with data being placed in the exempt category as needed (e.g., during an investigation).
5. Participant F (personal interview, October 29, 2010) expected minimal legal exposure in the operation of the CRG because, according to Ohio Revised Code § 2744.01, all governments in Ohio have immunity against civil action. Thus, when the CRG becomes a part of the normal operation of the City of Dublin, its operation would be immune to lawsuits.
6. The CRG should support the following user types: general, member, moderator, and administrator (Participant A, personal communication, October 5, 2011), with member users having more privileges than general users and so on down the list.
7. Because the City of Dublin and the Dublin Division of Police did not own or lease a suitable web hosting environment, it is necessary to procure a hosting arrangement for the Web portal operations and software development (Participant D, personal communication, October 14, 2010).
8. Potential risks to the successful completion of the project include a lack of project funding, cultural friction that limits adoption, and a lack of volunteers to serve as forum moderators (Participant K, personal communication, September 16, 2010; Participant A, personal communication, October 5, 2010; Participant G, personal communication, November 2, 2010).

9. The Dublin Division of Police plans to contract out the software development to a third party (Participant D, personal communication, October 14, 2010) to ensure that the needed functionality is delivered. In this case, quality assurance would be accomplished during UAT (Jiang et al., 2010).
10. The database tables for the CRG should be comprised of three tables: (a) Users, (b) Groups, and (c) Content. Each of these tables will have a unique, automatically generated PK to identify each row of data. The Groups and Content tables will also contain the PK from the Users table (FK1), and the Content table will contain the PK from the Groups table (FK2).
11. According to Participant C (personal information, October 12, 2010), the information submitted to the CRG will be public data by default, and the privacy risk to a user of the system will be marginal. This is because most of the data collected in the system were already available in other formats, e.g., the phone book, public 911 call records.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

In this chapter, the author presents a discussion of the results, presented in the previous chapter, as related to all four phases of the investigation: Phase 1 or Initiation Phase, Phase 2 or System Concept Development Phase, Phase 3 or Planning Phase, and Phase 4 or Requirements Analysis Phase. The chapter begins with the conclusions, which are presented by each research question. This is followed by implications for other organizations and for future research and then by recommendations. The chapter concludes with a summary of the findings.

Conclusions

This study was guided by three research questions:

1. To what extent will the "type, degree, content, extent, and formality of user participation" affect the Dublin Division of Police's design for incorporating a CRG in conjunction with their EMS? (Butler & Fitzgerald, 2001, p. 14).
2. To what extent will the organizational context of the Dublin Division of Police affect the implementation of a CRG? (Qu et al., 2009; Wu et al., 2008). Organizational context refers to the Dublin Division of Police's policies and management necessary to facilitate the implementation of a CRG.
3. Can a CRG address communication issues during emergencies in cities similar in size and demographics to Dublin, Ohio? (Jaeger et al., 2007; Qu et al., 2009; Wu et al., 2008).

In the sections that follow, each of the research questions is addressed.

Research Question 1

The author determined that user participation was central to the development and overall success of the implementation of the CRG portal application and supporting processes in the Dublin Division of Police. User participation was found in the following areas: (a) the UAT to ensure that what was delivered was what was requested, (b) the users who will serve as volunteers in operating the CRG portal, and (c) the residents who will communicate on the CRG.

As a result of consultation with the Dublin Division of Police, the author determined a third party will conduct the development efforts for the CRG portal. The input of the users, obtained through the UAT process, will help ensure that the final product suits their needs. Volunteers will be needed to serve as moderators on the CRG. The author determined that the additional information that will be generated by operating the CRG would be too much for the current 911 operators to integrate into their daily work. As a result, for the CRG to be successful, the Dublin Division of Police needs to supplement the current workforce with volunteers (Participant H, personal communication, January 20, 2010; Participant I, personal communication, January 20, 2010). The Dublin Division of Police's limited budget for hiring new personnel also contributes to the need for volunteers. Nevertheless, Dublin, Ohio, has a volunteer community of over 3,000 people, and it was expected that the introduction of this system would attract volunteers to assist in the filtering, triage, and escalation of issues to PERs (City of Dublin, 2012c). Finally, the CRG will be successful only if the residents of the City of Dublin use the system. The residents need to be made aware of the system as a part of an overall

communication strategy for how to communicate with each other and the Dublin Division of Police during emergencies.

Research Question 2

The results indicated that two factors in the organizational context of the Dublin Division of Police are significant in the success of the CRG implementation. The first factor was Dublin's commitment to conforming to the NIMS standard for emergency management. This commitment, which pre-dated this investigation, has created a foundation on which to build this CRG portal for the residents of Dublin, Ohio. Specifically, the use of the NIMS standard has helped the Dublin Division of Police to create communications plans and information management processes to facilitate the resolution of emergencies. Also important was the Dublin Division of Police's creation of the role of Emergency Management Coordinator. The coordinator's capacity to communicate with the Dublin Division of Police and the City of Dublin to solicit the information necessary to launch the CRG is vital to its success.

Also noteworthy was that, due to the relatively small size of the Dublin Division of Police, the level of detail required by the USDOJ (2003) was far greater than was necessary for execution in their environment. Smaller organizations require less structure in their development projects and often are overwhelmed or even intimidated by the full battery of documentation and processes required to complete a very detailed and mature SDLC such as the one in place by the USDOJ. As a result, the use of the USDOJ SDLC often caused consternation among the Dublin Division of Police. The author assisted in interpreting the phases and requirements of the SDLC so that they were comprehensible for the Dublin Division of Police.

Research Question 3

The author identified emergency communications issues that can be resolved using a CRG. In this regard, the Dublin Division of police lacked (a) a unified strategy for emergency communication using the Internet, (b) the ability to support emergency reporting and response over the Internet, and (c) a way to reduce duplicate incident reporting via landline or mobile phones. To resolve these issues, the Dublin Division of Police will need to implement a social media emergency response tool, such as a CRG, along with a program to educate the residents on its use. The Dublin Division of Police needs to make sure that residents are conditioned to utilize a CRG during an emergency. The author believes that one way to help ensure this is to make the CRG available for daily use. In this way, the CRG will enable residents and community groups to communicate issues and organize events as well as to report incidents in their neighborhoods, outside of an emergency, such as a suspicious vehicle, that they think have relevance to law enforcement.

Implications

This investigation supported the use of CRGs as a mechanism to improve communications during an emergency. The author determined the requirements for a police department to adopt a CRG portal to facilitate emergency communications. The author also has contributed to the IS body of knowledge by developing a repeatable approach to implementing CRGs in police departments similar to that of the Dublin Division of Police.

For organizations that are interested in implementing a CRG solution, the results of this investigation provide a basis for the development and implementation process. Future CRG researchers should consider the role that CRGs can play in disaster recovery and response (Crowe, 2011). For IS researchers, the results present a starting point for conducting a requirements analysis for more large-scale police departments and for studying actual CRG deployment, including implementation, volunteer experiences, and resident adoption and response.

Recommendations

The author developed the following high-level recommendations for organizations that intend to implement a CRG.

1. Use a SDLC that is appropriate for the organization. The use of the USDOJ (2003) SDLC allowed for a comprehensive review of the Dublin Division of Police's requirements for their CRG and for the determination that they were more robust than was needed. To use the USDOJ (2003) SDLC properly, one must seek requirements and approvals regarding the project specifications from a number of different stakeholders. However, many small- to medium-sized organizations will not have the various stakeholders identified in the SDLC. For instance, the USDOJ (2003) SDLC calls for the gathering of requirements and approvals from the Chief Information Officer (CIO) and the Executive Review Board (ERB), which were not defined roles at the Dublin Division of Police. In many cases, the primary stakeholders of the CRG are persons responsible for developing the requirements and, ultimately, doing much of the work needed for

implementation. However, not having the roles indicated in the USDOJ (2003) SDLC is common in smaller organizations and, thus, was not indicative of irresponsible behavior by the Dublin Division of Police. Based on this finding, the author determined that small- to medium-sized police departments that plan to implement a CRG should utilize a SDLC designed for smaller groups.

2. If possible, procure the CRG from a third party. The Dublin Division of Police expressed interest in procuring a CRG as a package from an outside vendor. For example, a vendor could offer the service as a hosted, software-as-a-service (SaaS), or cloud-based solution. In this arrangement, the vendor would own and be responsible for the software and infrastructure. The police department would then be responsible only for the administration of their instance of the software and for conducting tasks such as user additions, modifications, and deletes.
3. Develop community and volunteer involvement as soon as possible. The Dublin Division of Police was fortunate to have dedicated staff available to manage the volunteers needed to conduct their business. Police departments without an existing strategy for utilizing volunteers will need to develop a program for engaging the community groups that they intend as users of their CRG and will need to recruit volunteers to serve as moderators.

At the conclusion of this investigation, the author developed a list of requirements for the Dublin Division of Police to implement a CRG in their environment. Thus, an area that is open for future research is to study how a police department operates with a CRG in place. Case study research on the adoption and development of the CRG would be beneficial. Further, the present investigation is focused on a suburban city near the

capital city of Ohio in the US. Other case studies that duplicate this effort or that concern organizations that are geographically distinct from the Dublin Division of Police (urban and rural locales across the US as well as internationally) can provide an understanding of the requirements for a successful CRG implementation.

Wu et al. (2008) identified several areas for future research that still need work. The first is how the information collected by police departments through their CRGs will be organized and filtered. This issue is not addressed in the current investigation. It would be beneficial to conduct research on how 911 operators and CRG moderators are able to use the system to manage incidents in the City of Dublin or in other cities. Wu et al. also identified the need for research on the efficacy of volunteers versus paid professionals in operating a CRG. Although this investigation revealed that the City of Dublin was obligated to classify all information submitted via the CRG as public data, a determination needs to be made as to whether the residents will be comfortable contributing to a system that offers them little in the way of privacy. Again, geography may be relevant because data classification and legal obligations for data protection may vary by region. A final area of future research is the need to identify key factors and technologies necessary for integrating a CRG with a 911 system.

Summary

This investigation used a case-study approach, guided by the USDOJ (2003) SDLC, to develop a CRG for the Dublin Division of Police. A CRG is a Web-based system that utilizes mobile communications, Internet technologies, e-government services, and social networks to support emergency communications. CRGs have three primary features: (a)

the use of a Web-based infrastructure, (b) the ability to support interaction with multiple client platforms (smartphones, traditional PCs, and tablets), and (c) the ability to support multi-directional communication (Jaeger et al., 2007). Through the use of an appropriate triage methodology, a CRG can enable PERs to focus on the most critical situations by allowing residents to assist in resolving the less-critical requests through the CRG.

The focus of this investigation was the Dublin Division of Police in Dublin, Ohio. Dublin is located just outside of Columbus, Ohio, the state capital. Dublin began as a rural village and suburban business center in the 1970s (Franklin et al., 2004). The population grew steadily and in 1987 Dublin qualified to become a city (City of Dublin, 2010b). Dublin is home to several well-known corporations and is approximately 25 square miles, has nearly 42,000 residents, and collects roughly $66 million in tax revenues (City of Dublin, 2011a; U.S. Census Bureau, 2011). Dublin is run as a council-mayor form of government and has a mayor and a city manager (Svara, 2005).

The research was guided by three research questions:

1. To what extent will the "type, degree, content, extent, and formality of user participation" affect the Dublin Division of Police's design for incorporating a CRG in conjunction with their EMS? (Butler & Fitzgerald, 2001, p. 14).
2. To what extent will the organizational context of the Dublin Division of Police affect the implementation of a CRG? (Qu et al., 2009; Wu et al., 2008). Organizational context refers to the Dublin Division of Police's policies and management necessary to facilitate the implementation of a CRG.

3. Can a CRG address communication issues during emergencies in cities similar in size and demographics to Dublin, Ohio? (Jaeger et al., 2007; Qu et al., 2009; Wu et al., 2008).

The case study investigation was conducted in four phases (USDOJ, 2003):

1. Phase 1 or the Initiation Phase: Identification of the project, development of the business case, and assignment of Dublin Division of Police resources.
2. Phase 2 or the System Concept Development Phase: Establishment of the feasibility, appropriateness, and scope of the proposed solution.
3. Phase 3 or the Planning Phase: Identification of the success criteria and planning elements of the system.
4. Phase 4 or the Requirements Analysis Phase: Identification of functional user requirements to identify data, system performance, security, and maintainability.

Throughout each of these phases, related information and emergency response requirements of the Dublin Division of Police were collected.

A literature review provided the grounding for this study and included the areas of EMSs, incident categorization, and CRGs. The foundation for modern EMSs is NIMS (USDHS, 2008a), which was a response to the attacks on the World Trade Center on September 11, 2001, in New York City. Since that time, NIMS has served as the cornerstone for local, state, and federal emergency response organizations to develop plans for managing command, preparedness, communications, and maintenance activities. Although NIMS is a benchmark in terms of helping emergency organizations to respond to large-scale disasters, Buck et al. (2006) and Crowe (2010) noted the following deficiencies in the NIMS standard: (a) the lack of accommodation for social

media in communication strategies and (b) unorganized and volunteer group emergency response.

CRGs are designed to be implemented primarily as a Web portal and should support mobile access (e.g., mobile-enabled Web pages and smartphone apps). CRG portals should contain four primary features (Jaeger et al., 2007): (a) a function that enables new users to register, (b) a reporting function that allows users to make an account of an incident, (c) a function that allows one to request assistance from others as well as to respond to requests from others, and (d) a function that allows the communicating of basic information about events and happenings in the neighborhood and community groups to which users belong. These features are typically implemented as a Web application that is hosted in a data center (Jaeger et al., 2007).

Chapter 3 presented the methodology and included detailed information about the above-noted four phases as well as the sources of data: (a) Dublin Division of Police documentation, (b) the author's direct observations during his interactions with Dublin Division of Police, and (c) comments made during the workshops with the Dublin Division of Police.

The critical results of the investigation, presented in Chapter 4, are as follows:

1. The CRG supported the Dublin City Council goals for 2010-2011 to develop a strategy to provide for a robust public safety and emergency management infrastructure (City of Dublin, 2012a).
2. The residents of Dublin, Ohio, expected that the Dublin Division of Police would post and respond to social media messages (Participant A, personal communication, October 5, 2010), even though social media was not the official

channel for communicating emergency information to the Dublin Division of Police.

3. The cost to implement a CRG for the Dublin Division of Police was estimated to cost between $160,000 and $495,000, with a mode value of approximately $319,000. Rough estimates placed the total completion time of the project at approximately 400 days.
4. Data classification for this system will be comprised of two categories: public data and exempt data. According to Participant F (personal communication, October 29, 2010), all data should initially be classified as public data, with the exception of the exempt data category, which includes data required for ongoing investigations.
5. Participant F (personal interview, October 29, 2010) expected minimal legal exposure in the operation of the CRG because, according to Ohio Revised Code § 2744.01, all governments in Ohio have immunity against civil action. Thus, when the CRG becomes a part of the normal operation of the City of Dublin, its operations would be immune to lawsuits.
6. The CRG should support the following user types: general, member, moderator, and administrator (Participant A, personal communication, October 5, 2011), with member users having more privileges than general users and so on down the list.
7. Because the City of Dublin and the Dublin Division of Police did not own or lease a suitable web hosting environment, a hosting arrangement for the Web portal operations and software development is needed (Participant D, personal communication, October 14, 2010).

8. Potential risks to the successful completion of the project include a lack of project funding, cultural friction that limits adoption, and a lack of volunteers to serve as forum moderators (Participant K, personal communication, September 16, 2010; Participant A (personal communication, October 5, 2010; Participant G, personal communication, November 2, 2010).
9. The Dublin Division of Police plans to contract out the software development to a third party (Participant D, personal communication, October 14, 2010) to ensure that the needed functionality is delivered. In this case, quality assurance will be accomplished during UAT (Jiang et al., 2010).
10. Database tables for the CRG will be developed for (a) Users, (b) Groups, and (c) Content. Each of these tables will have a unique, automatically generated PK to identify each row of data. The Groups and Content tables will also contain the PK from the Users table (FK1), and the Content table will contain the PK from the Groups table (FK2).
11. According to Participant C (personal information, October 12, 2010), the information submitted to the CRG will be public data by default, and the privacy risk to a user of the system will be marginal. This is because most of the data collected in the system were already available in other formats, e.g., the phone book, public 911 call records.

In conclusion, the Dublin Division of Police indicated that a CRG would benefit the emergency management process in Dublin, Ohio. CRGs can provide city residents with the ability to report incidents and to respond to requests for assistance in their own communities. This investigation identified key factors that contribute to the success of

CRG implementations. These factors contribute to a paradigm for similar-sized cities that plan to implement a CRG for the benefit of their residents.

Appendix A

Letter Providing Consent for Use of Graphic

Science
AAAS

Permissions Letter

Ref # 08-27844

DATE: Friday, October 10, 2008

TO: John Freund
Nova Southeastern Univeristy
7985 Champaign Drive
Blacklick, OH 43004
United States

FROM: Elizabeth Sandler, Rights and Permissions
RE: Your request for permission dated 10/07/08 (submission id 37620)

Regarding your request, we are pleased to grant you non-exclusive, non-transferable permission to use the AAAS material identified below in your dissertation or thesis identified below, but limited to the formats identified below, and provided that you meet the conditions / requirements below. Such permission is for one time use and therefore does not include permission for future editions, revisions, additional printings, updates, ancillaries, other formats, translations, or promotional pieces, unless otherwise permitted below. This permission does not apply to figures / artwork that are credited to non-AAAS sources. This permission does not include the right to modify AAAS material.

The following credit line must be printed along with the AAAS material: "From [Insert Full Reference Citation]. Reprinted with permission from AAAS."

This permission covers the use of the AAAS material identified herein in the following format versions of your dissertation/thesis:
[x] print
[x] microform
[x] Digitized / electronic versions , provided the reprinted AAAS material remains in situ and is not made digitally available separated from your dissertation/thesis

AAAS agrees that ProQuest/UMI may supply copies of the dissertation/thesis on demand.

If the requested material is sourced to or references non-AAAS sources, you must obtain authorization from that source as well.

Permission fees are waived in this instance. AAAS reserves the right to charge for reproduction of AAAS controlled material in the future.

AAAS must publish the full paper prior to use of any text.

AAAS does not supply photos or artwork. AAAS material must not be used in a derogatory manner. Use of the AAAS material must not imply any endorsement by the American Association for the Advancement of Science. This permission is not valid for the use of the AAAS and/or SCIENCE logos.

Permission is valid for use of the following AAAS material only:
Fig w/ caption: A community response grid. from Ben Shneiderman and Jennifer Preece, SCIENCE 315:944 (2/16/2007)
In the following work only:
N/A, CONSTRUCTING A COMMUNITY RESPONSE GRID: THE DUBLIN, OHIO CASE STUDY published by UMI Proquest Digital Dissertations
Thank you for writing. If you have any questions please call me at (202) 326-7074 or write to me via fax at (202) 682-0816. For international calls, +1 is the country code for the United States.

Appendix B

Permission and Consent Letter

CITY OF DUBLIN.

Human Resources
5200 Emerald Parkway
Dublin, Ohio 43017-1090

Phone: 614-610-6400
Fax: 614-761-2965
Web Site: www.dublin.oh.us

5 May 2010

Mr. John Freund
Nova Southeastern University
School of Computer and Information Sciences
7985 Champaign Drive
Blacklick, OH 43004

Dear Mr. Freund:

I, Tom Hirschy, on behalf of the City of Dublin, Division of Police, approve the research to be conducted at the Dublin Justice Center. The research is being conducted by Ph.D. candidate John Freund of Nova Southeastern University entitled "Constructing a Community Response Grid (CRG): The Dublin, Ohio Case Study."

The City of Dublin, Division of Police has conducted an ethical review of the research proposal as well as the Nova Southeastern University Institutional Review Board for Research with Human Subjects (IRB) New Protocol Submission and we have found it satisfactory. We will continue to monitor this research as it progresses.

Sincerely,

Tom Hirschy
Emergency Management Coordinator/Law Enforcement Planner
City of Dublin
Dublin Division of Police

Appendix C

List of Acronyms Used in this Document

3G	Third Generation
AAAS	American Association for the Advancement of Science
AFIS	Automated Fingerprint Identification System
B3G	Beyond Third Generation
CCH	Computerized Criminal History
CDMA	Code Division Multiple Access
CIO	Chief Information Officer
CJIS	Criminal Justice Information Services
CLEC	Competitive Local Exchange Carrier
CRG	Community Response Grid
EMS	Emergency Management System
ERB	Executive Review Board
FBI	Federal Bureau of Investigations
FEMA	Federal Emergency Management Agency
FK	Foreign Key
FPT	Federal, Provincial, and Territorial
GPS	Global Positioning System
HOA	Homeowner's Association
HTTP	Hypertext Transfer Protocol
ICT	Information and Communications Technology
IS	Information Systems
ISO	International Organization for Standardization

IT	Information Technology
LAFD	Los Angeles Fire Department
LEADS	Law Enforcement Automated Data System
MDT	Mobile Data Terminal
MMS	Multimedia Messaging Service
NGOs	Non-governmental Organizations
NIMS	National Incident Management System
NRF	National Response Framework
OARnet	Ohio Academic Resources Network
PCs	Personal Computers
PDA	Personal Digital Assistant
PER	Professional Emergency Responder
PERT	Program Evaluation and Review Technique
PK	Primary Key
PMI	Project Management Institute
PRI	Primary Rate Interface
RFP	Request for Proposal
SARS	Severe Acute Respiratory Syndrome
SaaS	Software-as-a-Service
SDLC	Systems Development Lifecycle
SMS	Short Message Service
UAT	User Acceptance Testing
USDHS	United States Department of Homeland Security
USDOJ	United States Department of Justice

WBS	Work Breakdown Structure
XML	Extensible Markup Language

Appendix D

Institutional Review Board Approval

NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

MEMORANDUM

To: John Freund

From: Ling Wang, Ph.D.
Institutional Review Board

Date: May 21, 2010

Re: *Constructing a Community Response Grid (CRG): The Dublin, Ohio Case Study*

IRB Approval Number: wang02151002

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE REACTIONS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

3301 College Avenue • Fort Lauderdale, FL 33314-7796 • (954) 262-5369
Fax: (954) 262-3977 • Email: *inga@nsu.nova.edu* • Web site: *www.nova.edu/cwis/ogc*

References

Abrahamsson, M., Hassel, H., & Tehler, H. (2010). Towards a system-oriented framework for analyzing and evaluating emergency response. *Journal of Contingencies and Crisis Management, 18*(1), 14-25.

ADC Telecommunications, Inc. (2006). *TIA-942: Data center standards overview.* Retrieved from http://www.adc.com/Attachment/1270711929361/102264AE.pdf

Akkiraju, R., Bhattacharjya, D., Plaskon, J., & Jennings, D. (2011). Towards effective business process availability management. *2011 Annual SRII Global Conference*, 242-251.

Andersson, O. (2010). *Threat, risk, and vulnerability analyses during the development of IT systems in the Swedish Armed Forces*. (Unpublished master's thesis). Umeå University, Umeå, Sweden.

Bala, H., Venkatesh, V., Venkatraman, S., Bates, J., & Brown, S. H. (2009). Disaster response in health care: A design extension for enterprise data warehouse. *Communications of the ACM, 52*(1), 136-140.

Barnshaw, J., Letukas, L., & Quarantelli, E. L. (2008). *The characteristics of catastrophes and their social evolution: An exploratory analysis of implications for crisis policies and emergency management procedures.* Retrieved from http://dspace.udel.edu:8080/dspace/handle/19716/3766

Bartlett, J. G. (2006). Planning for avian influenza. *Annals of Internal Medicine, 145*(2), 141-144.

Besana, P. (2011). *The OpenKnowledge project*. Retrieved from http://research.nesc.ac.uk/files/openk-to-dir.pptx_.pdf

Buck, D. A., Trainor, J. E., & Aguirre, B. E. (2006). A critical evaluation of the incident command system and NIMS. *Journal of Homeland Security and Emergency Management, 3*(3), 1-27.

Bush, G. W. (2003). *Homeland security presidential directive 5: Management of domestic incidents*. Retrieved from http://www.dhs.gov/xabout/laws/gc_1214592333605.shtm

Bush, G. W. (2010). *Decision points*. New York: Crown.

Butler, T., & Fitzgerald, B. (2001). The relationship between user participation and the management of change surrounding the development of information systems: A European perspective. *Journal of End User Computing, 13*(1), 12-25.

Carver, L., & Turoff, M. (2007). Human-computer interaction: The human and the computer as a team in emergency management information systems. *Communications of the ACM, 50*(3), 33-38.

Catarci, T., de Leoni, M., Marrella, A., Mecella, M., Salvatore, B., Vetere, G., et al. (2008). Pervasive software environments for supporting disaster response. *IEEE Internet Computing, 12*(1), 26-37.

Chen, R., Sharman, R., Rao, R., & Upadhyaya, S. (2008). Coordination in emergency response management. *Communications of the ACM, 51*(5), 66-73.

City of Dublin. (2010a). *City charter*. Retrieved from http://www.dublin.oh.us/gov/charter/

City of Dublin. (2010b). *History.* Retrieved from http://www.dublin.oh.us/about/history/

City of Dublin. (2010c). *Police: Flagship agency*. Retrieved from http://www.dublin.oh.us/police/news/flagship.php

City of Dublin. (2010d). *Welcome to Twitter*. Retrieved from http://www.dublin.oh.us/community/twitter.php

City of Dublin. (2011a). *Profile.* Retrieved from http://www.dublin.oh.us/about/index.php

City of Dublin. (2011b). *Quarterly activity report, July-September 2011*. Retrieved from http://www.dublin.oh.us/police/pdf/quarterlyreport3-11.pdf

City of Dublin. (2012a). *Council goals.* Retrieved from http://www.dublin.oh.us/council/goals/

City of Dublin. (2012b). *Dublin police (dublinpolice) on Twitter*. Retrieved from https://twitter.com/#!/dublinpolice

City of Dublin. (2012c). *Volunteer Services.* Retrieved from http://www.dublin.oh.us/volunteer/wearedublin.php

Commission of Accreditation for Law Enforcement Agencies, Inc. (2010). *Law enforcement accreditation*. Retrieved from http://www.calea.org/content/law-enforcement-program-standards

Creswell, J. W. (2003). *Research design* (2nd ed.). Thousand Oaks, CA: Sage.

Crowe, A. (2010). The elephant in the JIC: The fundamental flaw of emergency public information within the NIMS framework. *Journal of Homeland Security and Emergency Management, 7*(1), 1-4.

Crowe, A. (2011). The social media manifesto: A comprehensive review of the impact of social media on emergency management. *Journal of Business Continuity & Emergency Planning, 5*(1), 409-420.

Davies, T. R. (2008). *The rise and fall of transnational civil society: The evolution of international non-governmental organizations since 1839.* Retrieved from http://www.staff.city.ac.uk/tom.davies/CUWPTP003.pdf

de Nooy, W., Mrvar, A., & Batagelj, V. (2005). *Exploratory social network analysis with Pajek*. New York: Cambridge University Press.

Dilmaghani, R. B., & Rao, R. R. (2007). Hybrid communication infrastructure and social implications for disaster management. *Proceedings of the 40th Hawaii International Conference on System Sciences,* 1-9.

Draheim, D., & Pirinen, R. (2011). Towards exploiting social software for business continuity management. *2011 22nd International Workshop on Database and Expert Systems Applications,* 279-283.

Ellison, N. B., Lampe, C., & Steinfield, C. (2009, January and February). Social networking sites and society: Current trends and future possibilities. *Interactions Magazine, 16,* 1.

Franklin, P. D., Kehoe, E., & The City of Dublin. (2004). *Dublin's journey* (1st ed.). Dublin, OH: The City of Dublin.

Freeman, L. C. (2004). *The development of social network analysis: A study in the sociology of science*. Vancouver, BC, Canada: Empirical Press.

Ghosh, S. (2011). *Transparent and commercialized? Managing the public-private model for data production and use* (University of Wisconsin Law School, Legal Studies Research Paper Series Paper No. 1155). Retrieved from http://ssrn.com/abstract=1780486

Gordon, J. (2007). The mobile phone and the public sphere: Mobile phone usage in three critical situations. *Convergence: The International Journal of Research into New Media Technologies, 13*(3), 307-319.

Gunawan, L. T. (2008). Collaboration-oriented design of disaster response system. *Proceedings of CHI EA '08 Extended Abstracts on Human Factors in Computing systems.* New York: ACM.

Guth, S. (2009). *Project procurement management: A guide to structured procurements.* Alexandria, VA: Guth Ventures.

He, J., & King, W. R. (2008). The role of user participation in information systems development: Implications from a meta-analysis. *Journal of Management Information Systems, 25*(1), 301-331.

Horan, T. A., Marich, M., & Schooley, B. (2006). Time-critical information services: Analysis and workshop findings on technology, organizational, and policy dimensions to emergency response and related e-governmental services. *ACM International Conference Proceeding Series, 151*, 115-123.

Horan, T. A., & Schooley, B. (2005). Interorganizational emergency medical services: Case study of rural wireless deployment and management. *Information Systems Frontiers, 7*(2), 155-173.

Hubbard, D. W. (2010). *How to measure anything: Finding the value of intangibles in business*. Hoboken, NJ: John Wiley & Sons.

Hunter, M. G. (2004). Qualitative research in information systems: An exploration of methods. In M. E. Whitman & A. B. Woszezynski (Eds.), *The handbook of information systems research* (pp. 291-304). Hershey, PA: Idea Group.

International Organization for Standardization (ISO). (2005). *ISO/IEC 27001: 2005 information technology: Security techniques: Information security management systems: Requirements.* Geneva, Switzerland: Author.

Jaeger, P. T., Shneiderman, B., Fleischmann, K. R., Preece, J., Qu, Y., & Wu, P. F. (2007). CRGs: E-government, social networks, and effective emergency management. *Telecommunications Policy, 31*(10-11), 592-604.

Jenson, J. (2011). The current NIMS implementation behavior of United States counties. *Journal of Homeland Security and Emergency Management, 8*(1), 1-25.

Jenson, J. A., & Yoon, D. K. (2011). Volunteer fire department perceptions of ICS and NIMS. *Journal of Homeland Security and Emergency Management, 8*(1), 1-19.

Jiang, Z. M., Avritzer, A., Shihab, E., Hassan, A. E., & Flora, P. (2010). An industrial case study on speeding up user acceptance testing by mining execution logs. *2010 Fourth International Conference on Secure Software Integration and Reliability Improvement*, 131-140.

Juszczyk, L., & Dustdar, S. (2008). A middleware for service-oriented communication in mobile disaster response environments. *Proceedings of the 6th international workshop on Middleware for pervasive and ad-hoc computing* (MPAC '08), 37-42.

Kumar, R., Novak, J., & Tomkins, A. (2010). Structure and evolution of online social networks. In P. S. Yu, J. Han, & C. Faloutsos (Eds.), *Link mining: Models, algorithms, and applications* (pp. 337-357). New York: Springer.

Kwak, H., Lee, C., Park, H., & Moon, S. (2010). What is Twitter, a social network or a news media? *Proceedings of the 19th International Conference on World Wide Web*, 591-600.

Latonero, M., & Shklovski, I. (2010). Respectfully yours in safety and service: Emergency management & social media evangelism. *Proceedings of the 7th International ISCRAM Conference*. Retrieved from http://ssrn.com/abstract=1566423

Lawton, G. (2011). 4G: Engineering versus marketing. *Computer, 44*(3), 14-16.

Marchese, M., Vaccari, L., Trecarichi, G., Osman, N., McNeill, F., & Besana, P. (2009). An interaction-centric approach to support peer coordination in distributed emergency response management. *Intelligent Decision Technologies, 3*(1), 19-34.

Markus, M. L., & Mao, J-Y. (2004). Participation in development and implementation—Updating an old, tired concept for today's IS contexts. *Journal of the Association for Information Systems, 5*(11-12), 514-544.

Mattson, M. (2009). *Flu wiki*. Retrieved from http://www.fluwikie.com/

Nixle, LLC. (2011). *Nixle*. Retrieved from http://www.nixle.com/

O'hEocha, C., & Conboy, K. (2010). The role of the user story agile practice in innovation. In P. Abrahamsson & N. Oza (Eds.), *Lean enterprise software and systems* (pp. 20-30). New York: Springer.

Ohio Administrative Code § 4501:2-10-10 (H) (1999). Retrieved from http://codes.ohio.gov/oac/4501%3A2-10-10

Ohio Revised Code § 149.43 (1999). Retrieved from http://codes.ohio.gov/orc/149.43

Ohio Revised Code § 703.01 (1999). Retrieved from http://codes.ohio.gov/orc/703.01

Ohio Revised Code § 2744.01 (1999). Retrieved from http://codes.ohio.gov/orc/2744.01

Okolloh, O. (2011). *Ushahidi*. Retrieved from http://www.ushahidi.com/

Palen, L., Hiltz, S. R., & Liu, S. B. (2007). Online forums supporting grassroots participation in emergency preparedness and response. *Communications of the ACM, 50*(3), 54-58.

Pelfrey, W. V. (2005). The cycle of preparedness: Establishing a framework to prepare for terrorist threats. *Journal of Homeland Security and Emergency Management, 2*(1), 1-21.

Project Management Institute. (2008). *A guide to the project management body of knowledge* (PMBOK Guide). Philadelphia: Author.

Public Safety Canada. (2011). *An emergency management framework for Canada*. Retrieved from http://www.publicsafety.gc.ca/prg/em/emfrmwrk-2011-eng.aspx

Qu, Y., Wu, P. F., & Mahindrakar, S. (2009). Design and prototyping of a community response grid (CRG) for a university campus. *2009 International Conference on Complex, Intelligent and Software Intensive Systems,* 772-777.

Saleem, K., Luis, S., Deng, Y., Chen, S.-C., Hristidis, V., & Li, T. (2008). Towards a business continuity information network for rapid disaster recovery. *ACM International Conference Proceeding Series: Proceedings of the 2008 International Conference on Digital Government Research, 289,* 107-116.

Satyanarayanan, M. (2010). Mobile computing: The next decade. *Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond,* 1-6.

Schafer, W. A., Carroll, J. M., Haynes, S. R., & Abrams, S. (2008). Emergency management planning as collaborative community work. *Journal of Homeland Security and Emergency Management, 5*(1), 1-17.

Scholl, H. J. (2009). Mobile computing in the public sector: Practices, opportunities, and arduous challenges. *The Proceedings of the 10th International Digital Government Research Conference.* Marina del Rey, CA: Digital Government Society of North America.

Schooley, B., Marich, M., & Horan, T. A. (2007). Devising an architecture for time-critical information services: Inter-organizational performance data components for emergency medical service (EMS). *Proceedings of the 8th Annual International Conference on Digital Government Research: Bridging Disciplines & Domains, 228,* 164-172.

Shirky, C. (2009). *Here comes everybody: The power of organizing without organizations.* New York: Penguin Group.

Shklovski, I., Palen, L., & Sutton, J. (2008). Finding community through information and communication technology during disaster events. *Proceedings of the ACM Conference on Computer Supported Cooperative Work (CSCW 2008),* New York: ACM Press.

Shneiderman, B., & Preece, J. (2007). 911.gov. *Science, 315*(5814), 944.

Stair, R., & Reynolds, G. (2011). *Principles of information systems*. Boston: Course Technology.

Starbird, K., & Palen, L. (2010). Pass it on? Retweeting in mass emergency. *Proceedings of the 7th International ISCRAM Conference,* 1-10.

State of Ohio. (2011). *STS contracts*. Retrieved from http://procure.ohio.gov/proc/contractsSTS.asp

Stephenson, M. (2005). Making humanitarian relief networks more effective: Operational coordination, trust, and sense making. *Disasters, 29*(4), 337-350.

Stephenson, M. (2009). Coordination in humanitarian relief chains: Practices, challenges and opportunities. *International Journal of Production Economics.* doi:10.1016/j.ijpe.2009.09.008

Structured Data, LLC. (2008). *RiskAMP Monte Carlo add-in library* (Version 2.97) [Computer software]. New York. Retrieved from http://www.riskamp.com/

Sullivan, D. K. (2011). *Higher education emergency management survey*. Retrieved from http://205.128.1.22/EMIWeb/edu/surveys/Sullivan%20-%202011%20Higher%20Education%20Emergency%20Management%20Survey%2010-26-11.pdf

Svara, J. H. (2005). Exploring structures and institutions in city government. *Public Administration Review, 65*(4), 500-507.

Sylves, R., & Cumming, J. D. (2004). FEMA's path to homeland security: 1979-2003. *Journal of Homeland Security and Emergency Management, 1*(2), 2-21.

Taylor, J. G., Gillette, S. C., Hodgson, R.W., & Downing, J. L. (2005). Communicating with wildland interface communities during wildfire. *Open File Report 2005-1061*. Fort Collins, CO: U.S. Geological Survey, Fort Collins Science Center.

Tipton, H. F., & Nozaki, M. K. (2012). *Information security management handbook, Vol. 5*. Boca Raton, FL: CRC Press.

Truong, H-L., Manzoor, A., & Dustdar, S. (2009). On modeling, collecting and utilizing context information for disaster responses in pervasive environments. *Proceedings of the First International Workshop on Context-Aware Software Technology and Applications (CASTA '09).* New York: ACM.

U.S. Census Bureau. (2011). *State and county QuickFacts for Dublin (city), Ohio*. Retrieved from http://quickfacts.census.gov/qfd/states/39/3922694.html

U.S. Department of Homeland Security. (2008a). *National incident management system*. Retrieved from http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf

U.S. Department of Homeland Security. (2008b). *National response framework*. Retrieved from http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf

U.S. Department of Justice. (2003). *The Department of Justice SDLC guidance document*. Retrieved from http://www.usdoj.gov/jmd/irm/lifecycle/table.htm

Van de Walle, B., & Turoff, M. (2007). Emergency response information systems: Emerging trends and technologies. *Communications of the ACM, 50*(3), 29-31.

Walsh, D. W., Christen, H. T., Lord, G. C., Miller, G. T., Maniscalco, P. M., Callsen, C. E., & Dolan, N. J. (2012). *National incident management system: Principles and practice*. Sudbury, MA: Jones and Bartlett Learning.

Wang, Z., Hämäläinen, M., & Lin, Z. (2008). An open community approach to emergency information services during a disaster. *2008 International Symposium on Information Science and Engineering*, 649-654.

World Wide Web Consortium. (2008). *Extensible Markup Language (XML) 1.0*. Retrieved from http://www.w3.org/TR/REC-xml/

Wu, P. F. (2008). Motivation for adopting emergency response technology in community settings. *Proceedings of the 22nd British CHI Group Annual Conference on HCI 2008: People and Computers XXII: Culture, Creativity, Interaction, Vol. 2,* 259-260.

Wu, P. F. (2009). *User acceptance of community emergency alert technology: Motivations and barriers* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3359323)

Wu, P. F., Qu, Y., Preece, J., Fleischmann, K., Golbeck, J., Jaeger, P., et al. (2008). Community response grid (CRG) for a university campus: Design requirements and implications. *Proceedings of the 5th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2008)*, 34-43.

Yates, D., & Paquette, S. (2011). Emergency knowledge management and social media technologies: A case study of the 2010 Haitian earthquake. *International Journal of Information Management, 31*(1), 6-13.

Yin, R. K. (2003). *Case study research: Design and methods* (3rd ed.). Thousand Oaks, CA: Sage.

Zittrain, J. (2009). *The future of the Internet—and how to stop it*. New Haven, CT: Yale University Press.