Applied Coursework

Technology for Homeland Security Course Paper

Author:
Reba Gonzales
Cohort 0801/0802

Lead Instructor:
Richard Bergin
IS 4010 – Technology for Homeland Security

Case Study: Crisis Information Management Information Systems

Reba Gonzales
OCTOBER 24, 2008
Introduction

The 9/11 Commission Report identified the lack of overall situational awareness as a contributing factor for uninformed decision-making and an ineffective incident command structure. Subsequently, the absence of implementing the Incident Command System (ICS) resulted in inconsistent strategic objectives, inefficient coordination of on scene resources, and the inability to communicate information and intelligence. (9/11 Commission, 2004, p. 321) Situational awareness was hampered by divergent cultural and political priorities and the non-existence of an established conduit for disseminating real-time intelligence.

“One clear lesson of September 11 was the need to improve the sharing of information.” (The Whitehouse, 2007, p. 7) The 9/11 Commission Reports’ assertion that the greatest impediment to all-source intelligence analysis was the human or systemic resistance to sharing information and resulted in the Intelligence Communities (IC) failure to “connect the dots. (9/11 Commission, 2004, p. 416). Consequently, situational awareness was hampered by divergent cultural and political priorities and the non-existence of an established conduit for disseminating real-time intelligence.
The Lessons Learned\textsuperscript{1} from 9/11 demonstrate the criticality of implementing incident management functions, interagency collaboration and sharing information and intelligence beyond the traditional methods of tacit expectations and working in isolation. To achieve this level of institutional change requires developing relationships, incorporating best practices and leveraging innovative technology to maximize knowledge management and information sharing.

In response to the systemic failures of 9/11, the federal Government created the Department of Homeland Security (DHS) to serve as a catalyst to transform the emergency response architecture pursuant to several Presidential Directives. Presidential directive (HSPD-5), Management of Domestic Incidents, directed the Secretary of Homeland Security to develop and administer a National Incident Management System (NIMS). Implementation of NIMS by state, tribal and local response organizations is a condition for federal grants and contracts. The purpose of NIMS is to augment emergency responders’ capabilities to prepare for, prevent, respond to, and recover from terrorism and man-made or natural disasters using a “single, comprehensive approach to domestic incident management.” (The Whitehouse, 2003)

HSPD-8 addresses National Preparedness and established policies to strengthen the level of preparedness to “prevent and respond” to threatened or actual domestic terrorist attacks, major disasters and established mechanisms for efficient delivery of Federal assistance. (The Whitehouse, 2003, p. 1)

\textsuperscript{1} Lessons Learned refers to the best practices for emergency responders and homeland security officials. It is founded in the national Lessons Learned Information Sharing network. https://www.llis.dhs.gov/index.do
To meet the intent of HSPD 5 and 8, public safety leaders were called to redefine existing roles, responsibilities and work together to achieve mission success by improving capabilities, capacity and inter agency cooperation. Unfortunately, the response to Hurricane Katrina was evidence that despite their best intentions, emergency managers and first responders lacked proficiency with interagency collaboration, situational awareness and implementing the incident command structure.

These examples magnify systemic issues and reinforce the ineffectiveness of the status quo. Likewise, they provide opportunities to introduce technology as a strategic initiative to curtail similar outcomes. Specifically, utilizing collaborative applications for knowledge management, information sharing and to overcome issues related to interoperability.

At the request of Emergency Managers, in early 2002 the National Institute of Justice and the Office for Domestic Preparedness funded the Crisis Information Management Systems (CIMS) Test Bed Project to compare and contrast commercially available software. (United States Department of Justice, 2002, p. 8) To assist Emergency Managers in the selection and procurement of commercially available software, the CISM Test Bed Project developed Guidelines and created the Feature Comparison Matrix Tool.

CIMS computer applications are designed to collect information from geographically displaced agencies which allow evaluation of the aggregate information and intelligence in a timely manner by multiple agencies across several jurisdictions.

Initially, the most common usage of CIMS was limited to Emergency Operation Centers (EOC) where it supported the management of crisis information and the corresponding response by public safety agencies. (United States Department of Justice, 2002, p. 1). With the
advances of technology, a variety of products have been designed to improve situational awareness by enhancing command and control capabilities. Today, commercial software developers design applications specifically geared to meet the demands of first responders.

According to a report by the Institute for Security Technology Studies at Dartmouth College, various expert commissions and the first responder community made recommendations suggesting that with a broader use of technology, the value-added could improve their incident emergency management and enhance their efforts to prevent and respond to events of terrorism. (Institute for Security Technology Studies, Dartmouth College, 2004, p. 5)

Furthermore, The National Strategy for Information Sharing, states that gathering, analyzing and the sharing of information and intelligence is paramount for the prevention and deterrence of future terrorist acts against the homeland. The Strategy identified that a multi-directional flow of information must include state, local and tribal partners to prevent future terrorist attacks, counter and respond to threats. (The Whitehouse, 2007, p. 3)

The National Strategy for the Fire Service Intelligence Enterprise (FSIE) delineates that Fire Service 2 personnel need ongoing support of intelligence products that include potential or actual incident threats so that Executive Fire officers can leverage resources toward preparation and response capabilities. (Department of Homeland Security, 2008, p. 6)

In the case of the Seattle Fire Department, the organizational drivers for CIMS technology began with the need for an incident management tool that supported ICS functions and build

---

2 For the purpose of this memorandum, the term “Fire Service” includes, firefighting, fire prevention activities, fire investigation, emergency medical services, hazardous materials operations, technical rescue and marine operations
internal capacity for incident and event planning that can be used for day to day operations and as a functional tool and a conduit to share information with the Seattle Police Department.

Analysis

Selection of any technology should be a collaborative effort that includes the end user, the technical support staff, the developer/vendor and a conceptual idea of what the technology should provide. As previously noted; to assist in the selection of a CIMS product the Department of Justice developed guidelines and a matrix tool from surveys of the Emergency Management Agencies during the CIMS Test Bed Project. In addition, the Feature Comparison Matrix tool was designed to augment the procurement process by evaluating common functions and assign a weighted score based on the agencies internal requirements.

Guidelines for CIMS:

- Be affordable
- Be user friendly
- Be easy to maintain by existing EMA Staff with access to vendor’s technical support
- Be easy to tailor to the conditions and policies of the agency
- Allow for remote access by authorized users located outside the LAN
- Comply with the provisions and standards for Incident Command System (ICS)
- Comply with the provisions of the Emergency Support Functions (ESF)
- Integrate with other systems such as mapping, other CIMS, and telephonic alert notification systems
- Integrate public health into emergency management.
- Operate within a variety of network configurations
- Have a wide range of features.
- Offer help desk support 24/7 (United States Department of Justice, 2002, p. 7)

Feature Comparison Matrix:
The tool works by applying a priority factor to the scores that resulted from the feature comparison process. Where appropriate, it also provides a high-level description of the logic behind the calculations. Once the inputs to the Feature Comparison Matrix are processed and the products that best match the agency’s priorities are revealed, the agency can take these results as well as other priorities not addressed in the Feature Comparison Matrix into its decision process for final product comparison and selection (United States Department of Justice, 2002, p. 40).  

Another important consideration is the sharing of information between different application vendors. To address issues of interoperability between technologies, the Emergency Interoperability Consortium (EIC) was launched in October 2002. The EIC requires that there is open sharing of information between different applications, so it should not be an issue if you are using product “x” while another agency is using product “Z”. (Department of Homeland Security Office for Interoperability and Compatibility, 2004)

The EIC objectives are to create a nationwide standard for data sharing through a public/private effort. They encourage web-based services to support the exchange of information during emergency incidents and make appropriate information available to the public for use in the development process.

The Disaster Management (DM) Standards Initiative works to include practitioners in the collaboration and management of their incident response efforts across multiple jurisdictions and disciplines, even if their software, systems, and devices are different (Department of Homeland Security Office for Interoperability and Compatibility, 2004)

Furthermore, there are several messaging standards that will help the first responder. The Common Alerting Protocol (CAP) is used in all-hazard emergency alerts. The Distribution Element (DE) Standard enables responders to send information and files from one system to

---

3 See Appendix A – Feature Weighted Survey for example of survey
another in a uniform way. Hospital AVailability Exchange (HAVE) enables the exchange of hospital status, capacity, and resource availability between medical and health organizations.

Using the aforementioned criteria, Lenny Roberts, the Seattle Fire Departments Director of Management Information Systems conducted an evaluation of commercially available products and determined the top three CISM applications were: E*SPONDER from Convergence, E*TEAM from IBM and WebEOC from ESI. Below is a summation of his findings.

- **E Team** from IBM
  - Used by NYC on September 11th as well as during Hurricane Katrina and several Super Bowls.
  - Built on Crystal Reports.
  - Web-based and uses both predefined and customized reports.
  - Information can be sorted and exported to common business applications.
  - Uses technology that is incompatible with City of Seattle standards

- **Web EOC** from ESI
  - The first web-based emergency information sharing application.
  - Allows users locally or worldwide to share and view information in real-time.
  - Currently being used by national, state and local agencies.
  - Cannot be used by Medic One and AMR.  

---

4 Medic One and AMR are two agencies that SFD has a contractual working relationship with to manage emergencies.
- Does not have an out-of-the-box capability to integrate with Fire Department and the other City systems.
- Is not secure enough to allow external agency access therefore it cannot be used on an inter-jurisdictional basis for managing events.

- **E*SPONDER from Convergence**
  - A highly customizable disaster management software solution.
  - Based on Microsoft Sharepoint.
  - Can conduct planning with all of the agency’s stakeholders.
  - Command and control functions during events and incidents.
  - Review and evaluate performance during After Action Reviews.
  - Learning curve zero – built on Microsoft office – the standard in City of Seattle⁵

![E*SPONDER from Convergence](image)

**Figure 1 - E*SPONDER⁶**

Following the evaluation and analysis process, the E*SPONDER application was selected as it fulfills the departments’ communication, situational awareness, and data management needs. It provides a variety of usable, accessible tools, generates automated incident plans and ICS forms, and it can link documents and resources. These features allow the Seattle Fire

---

⁵ See Appendix – B for additional factors to support the selection.
⁶ See Appendix – C for additional E*SPONDER screens.
Department to use the application daily for a multitude of business processes in the Fire Marshal’s Office. E*SPONDER has the capability to provide real-time resource status that is supported by its’ alerting system. As incident commanders anticipate the need for additional resources, they can make mass requests using the software’s alerting system. Contact information can be preloaded by exporting an excel spreadsheet to populate database. Once a group is selected, the alert is transmitted via voice, email and text messaging. Moreover, this function tracks responding personnel with the call back status. Lastly, the E*SPONDER application works in a mobile environment and can communicate in real-time.

Conclusion

The extent of this case analysis was to look for plausible answers to the question, “how can situational awareness, intelligence sharing and implementation of the Incident Command System be enhanced with the inclusion of technology?”

Experts warn that the traditional compartmentalized approach to collection and analysis will not work with the new, more dynamic terrorists threats (The Markle Foundation, 2002, p. 69). This analysis validates the need for a working framework and mechanism to gather and share information, as well as the dissemination of intelligence to firefighters that is “timely, tailored, digestible and clear.” (Lowenthal, 2006, p. 139)

7 The Fire Prevention Division of the Seattle Fire Department, commonly referred to as the Fire Marshal’s Office, provides the leadership and inspection services to help prevent fires and assure fire and life safety for people who live, work and visit in Seattle.
As history has revealed, lack of imagination and maintaining status quo can have catastrophic results. Moreover, it discounts the current threat assessment and recent National Intelligence Estimates that suggest terrorist groups continue to exist and remain a serious threat to the Homeland. (National Intelligence Council, 2007, p. 6)

The benefits of a CISM tool will allow daily collaboration between the Seattle Police Department and Seattle Fire Department as a means to share intelligence and information. Incorporating CISMS software will increase coordination, integration, and communication with our public-safety partners and undoubtedly enhance our ability to focus on our core mission of protecting lives. Finally, “building capacity to deal with the most probably events will increase capacity to deal with less probably events” (Waugh, 2004).
Each feature has a corresponding input field. This input field is used to determine the importance of this specific feature to the evaluating organization. This is done by entering a number from 0 to 5, with 0 being the least important and 5 being the most important. This weighting is used to compute the scores that the vendors received during the final step of the analysis. The following provides a definition for the different weighting options.

- **0**—Of no importance to the user whether or not the feature is provided.
- **1**—Possibly useful.
- **2**—Nice to have.
- **3**—Important.
- **4**—Very important.
- **5**—Extremely important

APPENDIX B – E*SPONDER Features

- Based on SharePoint (City de facto and soon-to-be-official standard for collaboration.
- Only product that incorporates Microsoft Office allowing common desktop software to be used for creating and managing information used in the E*SPONDER system.
- Integrates with Active Directory (City standard directory service) so creating an account in E*SPONDER automatically creates an Active Directory Account.
- Allows security/permission to be managed from Active Directory.
- Tightly integrates Outlook and Exchange (City’s new email-standard).
- Supports test-to-speech in it’s voice alerting module.
- Allows people who are alerted to send responses back to the system so commanders know whether the person alerted received the alert, will respond, will not respond, etc.
- Integrates Microsoft Live Communications Server which allows alerting through voice (telephone and cell phone), e-mail and pagers.
- Has a remote/mobile module (E*SPONDER Express) that contains virtually all of the functionality of the full E*SPONDER version (including alerting). E*SPONDER Express can be installed in a command vehicle and periodically synchronized with the primary E*SPONDER site via a wireless connection. Therefore, first responders will have a complete, up-to-date emergency management tool in the field in situations where network connections get interrupted and/or the field command post becomes isolated.
- Integrates Virtual Earth which is a common mapping tool used in the City (and is being considered as the standard for user electronic map presentations.)
Appendix C – E*SPONDER Screens