

FOR IMMEDIATE RELEASE

CODE ORANGE – IS YOUR HOSPITAL PREPARED FOR EMERGENCIES

By David A. Kipp and Ihab Osman, Ross & Baruzzini

January 7, 2008 – According to the Law of Large Numbers (LLN), hospitals and major medical centers know it is only a matter of time until disaster strikes. While no one can predict whether it will be a major pandemic like the avian flu, a natural catastrophe, or a terrorist attack that compromises significant regional resources, there is no doubt that the threats are real and many medical institutions remain woefully vulnerable.

The reality is that no amount of planning for patient safety and security is complete without a conducting a comprehensive impact analysis to determine to what extent an institution's functionality can be preserved while under duress. This should include a detailed evaluation of operational processes and physical facilities, as well as technology requirements to ensure that personnel, equipment, communications and procedures are fully integrated for maximum survivability and effectiveness.

Every detail is important. Although the hospital may have an excellent emergency plan in place, it may still have a plethora of vulnerabilities because of a computer system that could be hacked, an electrical system that could be completely disabled, security cameras that are poorly placed or have limited range, or an older facility with too many nooks and crannies that create convenient hiding places for potentially dangerous explosives or individuals.

Mission Critical Operations

In terms of performing an emergency management evaluation, hospitals might consider how other mission critical operations such as airports are setting the standard for disaster management through process planning and reengineering.

From Boston to Los Angeles, airports are identifying the critical processes that govern the detection of risk, delay of impact, incident response and operational recovery. These largely unseen strides are resulting in improved awareness and response, while maintaining a modicum of pleasant travel conditions on the ground. These concepts and lessons translate directly to hospitals, as well as other institutional environments.

Although there obviously are fundamental differences between medical facilities and airports, there are also some strategic similarities. For example, in both a detailed analysis of functionality can help prioritize risk factors under duress. Important factors include determining what risks necessitate immediate changes and resources and which can be addressed by using specific alternative approaches.

In the aftermath of a crisis, resuming operations as quickly as possible can be critical to effectively dealing with the emergency itself. In addition, it is essential to have the resources to facilitate and coordinate regional collaboration, especially if one or more facilities is either completely or even partially non-functional.

In all instances, technology infrastructure must be ready to assume mission critical operations instantly. Having the capability to create seamless intercommunications and interoperations functions using remote nodes is a necessity that cannot be ignored in a disaster, especially considering the high cost of NOT having these capabilities in place.

Analyzing Facility Security & Operations

Another set of solutions can emerge from enlarging the view of security, from the narrow view of crime or disaster prevention to a series of processes that go beyond prevention to embrace detection and response. In fact, in the rapidly evolving world of homeland security, the phrase D3R is being used to describe a broadened security philosophy that addresses Deterrence, Detection, Delay and Recovery.

As horribly demonstrated by 9/11 and the more recent Virginia Tech tragedy, determined and deranged people cannot always be reliably stopped. Nor can anyone prevent tornadoes, earthquakes, typhoons and hurricanes, all of which can wreak devastation and fatalities. Yet these realities do not preclude actions that can mitigate the risk of loss by more rapidly and accurately detecting the situation, delaying its impact or implementing activity designed to recover normal operations.

Regardless of whether a hospital is a non-profit or for-profit institution, security and back office operations also have bottom line implications. A detailed analysis can identify opportunities where technology can be used most effectively. Options can range from video intelligence tools designed to help reduce staff and potential exposure to lawsuits to RFID technology that can generate significant savings by tracking materials handling and provide asset management.

Success Depends on Processes

But the bottom line is that security is about preventing and minimizing loss. And as we have learned from recent events, there are new ways to think about security that are more relevant to hospitals than ever before.

The foundation of security is the development of critical operations processes, not the installation of hardware and electronics or the provision of armed forces. Hardware, electronics and force protection are only effective to the extent that they are enabled by knowing and doing the right things in an emergency situation. Planning these operational processes, establishing preparedness and having a response and recovery approach comes first.

About the Authors:

David A. Kipp, PE is Senior Vice President and Chief Operating Officer and Ihab Osman is Chief Technology Officer for Ross & Baruzzini. The firm specializes in providing professional technology and engineering consulting for facilities and infrastructure challenges in the healthcare, education, government, aviation and maritime industries. Ross & Baruzzini has been ranked as one of the top engineering and architectural firms in the United States by *Consulting-Specifying Engineer* magazine. Founded in 1953, the company is headquartered in St. Louis and has regional offices in Miami and Indianapolis. More information is available at www.rossbar.com.