Technology Must Be a Central Part of Emergency Management Planning

By Chuck Miller

Utter the phrase "emergency management" and people imagine sirens blaring, rising water, downed trees, blocked roads and detours. But an emergency management plan will fall short if it only includes public safety and public works departments and fails to involve the information technology department at the front end. Technology has permeated every aspect of municipal services delivery, so the IT department must be at the table during the emergency planning process.

From the IT perspective, the emergency management plan is but one element of a full-scale business continuity plan. As with any risk management situation, there is a challenge in balancing the likelihood of a particular event with the cost required to mitigate such an event. So it is essential that key departments work closely with IT to identify, quantify and mitigate risks.

Chuck Miller is the Director of Information Technology for the town of Lincoln and President of the Massachusetts Government Information Systems Association.

Awareness of risks must be combined with an intimate knowledge of how these potential risks could affect critical operations. When these risks are minimized, misunderstood or miscommunicated, the emergency plan is compromised. Business continuity and disaster recovery are relevant to the entire organization; they are not the sole responsibility of IT, but are part of a joint planning effort. This cohesive planning is essential to ensure that there is a unified response to emergency situations and consensus regarding the execution of the recovery process after a crisis.

In developing an emergency management plan, there are two distinct elements: Business Operations and Information Technology. It is important to understand that when the lights go out, processes and procedures will trump technology. Effective analysis of all business operations is the bedrock of the plan. All municipal business organizations must work together in the planning process to assess the risks and analyze the impact upon daily operations. Then they must develop a Crisis Management Plan and Business Contingency Plan. Based upon those deliverables, the IT department develops the Disaster Recovery Plan, which addresses the IT infrastructure, application recovery and data recovery.

For IT to assume all business continuity planning in a vacuum would be fruitless. All departmental stakeholders must be part of the process and take ownership in setting priorities, crafting the plan and acting upon its execution. This is essential in order to ensure that everyone understands their responsibilities and that there is consensus among all organizations. The planning process must be taken seriously and done well in advance of a pending crisis. Hurricane season is the time to meet to discuss the escalation process required to execute the emergency plan; it is not the time to whip a plan together with a few department heads.

All departmental stakeholders must be part of the process and take ownership in setting priorities, crafting the plan and acting upon its execution.

ELEMENTS OF A CONTINUITY PLAN

Fortunately, technologies once available only to large corporate clients have been scaled down to serve the small to medium business market, where you will find most municipalities. These key building blocks will lay the foundation for a Business Continuity Plan.

PC virtualization and application virtualization create a scenario where all systems can potentially be restored in a fraction of the time it would take to rebuild and configure all devices from scratch.

Virtualization: Most IT operations have morphed into their current form over a period of many years. There may be a mix of hardware and software platforms, state-of-the-art technologies and applications, and legacy applications that cannot be replaced. This means recovery is not likely to be as simple as ordering new servers and restoring a backup tape. This fact supports the need to integrate server virtualization as a key element of the municipal IT infrastructure. Virtualized servers provide the flexibility of running aged or obsolete applications on new equipment, by "spinning up" new virtual servers that emulate the obsolete environment. This not only extends the life of the applications, but also provides a mechanism for restoring backups of not only the lost data set but the entire virtual server image on a new piece of hardware. PC virtualization and application virtualization are also within the grasp of many communities, creating a scenario where all systems can potentially be restored in a fraction of the time it would take to rebuild and configure all devices from scratch.

Smartphones Provide Connection When Internet Is Unplugged

On the evening of October 29, 2011, much of Massachusetts went to bed without power. An unusually early snowstorm wreaked havoc with wiring throughout the region, taking with it electricity, phone service, cable television and the Internet. At Lincoln Town Hall, the generator kicked in and we never missed a beat, but I was unaware of this because my home in Ayer was in the dark. No electricity meant no Internet, and that meant no remote access to monitor and manage systems in Lincoln.

Public safety personnel didn't call me on my cell phone, so I knew systems were still available to them, even though I had no access from home. Due to fallen trees, it would be another eighteen hours before I could get out of my house to check on the data center in Lincoln. It would be three more days before I had electricity at home.

During the storm, my smartphone was my link to the world. I was able to check email that was still flowing in and out of the exchange server in town hall. I was able to text personnel. I was able to check various websites for updates. I was able to receive ConnectCTY notices from the Lincoln Police Department.

The biggest challenge that came with my newfound dependence on my iPhone was battery life. Normally this would be a mere inconvenience, but when you cannot simply dock your phone in a charger you need to be creative. [To prolong battery life when the power goes out, check the system preferences on your phone, turn off Bluetooth and dim the screen brightness.]

If you don't have a generator for your home, what are your choices? I found several, even though I was caught unprepared. First, I shut down my home computer and all peripherals and plugged the phone charger into the USB battery; I was able to charge the phone a couple times this way. Whenever I got in my truck, I took the phone and plugged it in. The third option was my emergency weather radio with a generator crank that powers USB devices; this worked for my wife's phone, but not mine.

When I arrived at work after a couple of days without power, I brought every battery-operated device I had and charged them while I worked. When I returned home to camp out in my living room, I had fully charged flashlights, lanterns, cell phones and a laptop, which were a comfort.

What are the "take-aways" for anyone who needs to be connected when local power and Internet providers are down? At this time the answer seems to be cell technology; iPhones, 3G-capable iPads and Android phones can provide Web and email access even when your cable modem has let you down. My old laptop still functions with a cellular aircard, which provided me with remote access to my data center once I had fully charged the batteries. The key to this contingency plan is battery life and charging capabilities. When the next storm knocks us down, we may be out of lights and heat, but we don't have to be out of touch.

—*Chuck Miller*

Secure Remote Access: Another key element of municipal IT infrastructure should be secure remote access for authorized users. I sometimes refer to this as the "Starbuck's model"; any authorized user should be able to access appropriate applications from a coffee shop, home or emergency work center. They would do so through a secure virtual private network that provides appropriate application access on any computer with a broadband Internet connection (SSL VPN). This technology is usually already in place on a small scale within municipalities, as it is what many IT departments use to remotely manage the servers and network from home during off hours.

Offsite Storage: Having last night's backup tapes locked up in a cabinet will be of little use if your primary data center is destroyed by fire or flood. Offsite data storage is critical. This may be in the form of disks or tapes that are securely stored in another building, ongoing disk replication to another location or "cloud storage." In communities that are running a virtualized server farm in their data center, these server images can also be backed up to simplify the rebuilding of the data center.

Cloud Computing: The "cloud" is another infrastructure element that greatly simplifies the ability to function in the event of a severe weather event or a disaster. This is typically a fully supported server and service arrangement with a software vendor, with secure access available to authorized users. A tremendous benefit is that these servers are often hundreds of miles away, so weather-related events that affect your city or town are unlikely to have affected the remote location. In addition, these vendors are usually fully redundant, so if their Site A data center is affected, operations go to another site B, without clients experiencing downtime. The downside of cloud solutions is that not all vendors have the means to provide such levels of service, and those that do charge a premium price.

Emergency Power: Three years ago, a severe ice storm crippled much of central Massachusetts for more than a week. Many homeowners and businesses saw how devastating a long-term loss of power can be. Such a scenario demonstrates that backup power is essential for municipal operations. An emergency plan should include a generator of sufficient power to keep town or city hall open for days. Where it is available, natural gas-fueled generators are preferred over those using diesel fuel, since they do not depend on fuel deliveries at a time when roads may be impassable. The generator should be equipped with an automatic transfer switch. All servers, storage systems and network equipment should be equipped with sufficient battery backup power so that server functionality will not be lost during the switch over to the generator.

Internet Access: Communities have at least some possibility of direct control or influence over the factors above, but the same is not true of Internet access, where communities are extremely vulnerable. As a society, we have placed a disproportionate amount of our eggs in this communication medium's basket. When a municipality loses Internet access, it loses access to state and federal advisories, email, municipal bulletins, websites, and valuable cloud computing resources. It is essential to have contingency plans. It may be worth investigating what is required to have redundant Internet service providers (ISPs), such as Comcast and Verizon.

Citizen Advisory Services: "Reverse 911" is a valuable Web-based tool that allows officials to keep the public and employees informed about emergency services, travel advisories, and so forth. One of the most significant benefits of this tool is its versatility. Notices can be posted by phone or a Web interface, and constituents can receive messages by landline, cell phone or email; in other words, the service has several delivery contingencies built right into it. Though geographic data is adequate for automatically calling a landline awithin a given telephone exchange or map radius, cell phones and email notices require the citizen to subscribe in order to receive information.

Testing: Once redundancies are built into the municipal IT infrastructure, they must be tested to ensure that they will live up to expectations in the event of a crisis. The generator should be tested weekly to ensure that it cuts over properly and that servers and the network remain online. Test restorations of virtual servers should be performed, and data should be backed up nightly. Officials should send out test bulletins on their reverse 911 system to a select group of people to ensure that it works well and that staff is proficient in posting notices. Social media such as Facebook and Twitter should be used to maximize the outreach to employees and residents who use smartphones.

It is important to focus on the business first and technology second; that's why it's called business continuity, not IT continuity.

Given the growing importance of technology in our society, IT may need to take the initiative in facilitating this planning process (though management must retain overall responsibility). It is important, however, to focus on the business first and technology second; that's why it's called business continuity, not IT continuity.