At Least It Wasn’t a Football Weekend: The Notre Dame Tunnel Fire

Dewitt Latimer, University of Notre Dame
On Friday morning, August 28, 2009, the University of Notre Dame experienced what began as a minor fire in a utility tunnel. The impact of the fire escalated into a significant emergency and an extended, widespread communications outage that affected thousands of people on campus. The fire destroyed a substantial portion of the campus communications infrastructure, severing 36 buildings from the outside world and sending faculty, staff, and students scrambling into the cold, rainy morning.

This incident occurred at a terrible time—during the first week of fall classes—when the campus was heavily populated and in high gear. Thankfully, it didn’t happen a week later, which would have been the first home football game weekend of the season!

Notre Dame’s response and handling of the event is a textbook example of the benefits of a well-constructed incident response plan, the creation of a formal incident response and emergency operations center (EOC), an ongoing disaster recovery and business continuity initiative, and, most importantly, repeated testing of the various plans using realistic emergency simulations. The event also illustrated how dependent complex organizations are on communications and how even seemingly obscure elements of your campus infrastructure can test the best laid plans.

This research bulletin discusses how the University of Notre Dame created and refined its incident response plan, how the utility tunnel fire of August 28 played out within that framework, the challenges of the subsequent week-long recovery phase, and how lessons Notre Dame learned can be applied at other colleges and universities.

Highlights of an Emergency Response Framework

In September 2006, the University of Notre Dame, following the aftermath of Hurricane Katrina and in response to recent federal regulations requiring compliance with national incident response frameworks, began to review its existing campus response plan(s) and its ability to respond adequately and cohesively to a large-scale campus or regional emergency. Over the following year, the university created a unified campus incident response plan compliant with the National Incident Management System (NIMS), which was developed by the Department of Homeland Security (DHS).

The University of Notre Dame’s Campus Emergency Preparedness & Response Plan outlines policies and procedures for managing major emergencies that could threaten the health and safety of the campus community or significantly disrupt its programs and activities. The plan provides a structure for coordinating preparedness, response, and recovery efforts of Notre Dame personnel and resources. It applies to a broad range of major emergencies, including but not limited to fires, explosions, extended power outages, mass casualty events, hazardous materials releases, information security breaches, financial malfeasance, and other events impacting the life and safety of campus constituents and the physical condition or credibility of the university. The plan is intended for major emergencies and is activated when an emergency reaches a level beyond the capacity of routine departmental response procedures. It provides for a comprehensive approach in which both first responders and executive management can respond strategically to large-scale emergencies.
Incident Command System

In response to the events of September 11, 2001, DHS mandated the widespread use of NIMS within the federal government itself. After Hurricane Katrina, the federal government then required that all state and local entities become compliant with the NIMS standard. Universities and any other entity receiving federal funds were subject to that mandate. The Notre Dame plan is modeled not only on NIMS but also includes many elements from the Incident Command System (ICS), a standardized construct for an integrated emergency management organization structure.

ICS and NIMS provide guidance for a consistent and integrated framework for the management of emergencies. Moreover, federal, state, and local government emergency agencies (e.g., the Federal Emergency Management Agency [FEMA], state DHS, local fire departments, emergency medical services [EMS], law enforcement, and departments of health and public works) responding to an incident at Notre Dame will easily recognize, understand, and follow a well-established protocol, permitting a coordinated response. Finally, ICS and NIMS provide a standardized framework for communications and information sharing at all levels of incident management, ensuring that all affected constituents receive consistent information regarding the emergency.

Essential characteristics of ICS and NIMS include provisions to

- accommodate the changing dynamics of an incident, by smoothly adding and releasing resources based on need;
- outline authority and responsibilities inherent to incident response roles; to assign individuals to such roles on a temporary basis and reassign, replace, or release them as needed; and
- promote proper span of control and unity of command.

Organization and Reporting Structure

An organization’s structure during an emergency response likely will not resemble its day-to-day operations. Employees may report to individuals to whom they do not ordinarily report. Furthermore, if the severity of an emergency increases, assignments may change in the organizational structure, therefore changing an employee’s position during the course of a single emergency.

The organizational structure of Notre Dame’s plan includes four major components:

- Traditional first-responding agents (e.g., Notre Dame Security Police, Notre Dame Fire and Rescue)
- Executive Emergency Policy Committee
- Emergency Operations Center Management Team
- Localized Department Operations Centers

Traditional first responders include those agents that would initially respond to the scene of an incident, such as fire, rescue, and police departments. First responders are responsible for staffing and operating field command posts near the scene of an incident or at staging
areas nearby. As necessary, first responders coordinate efforts with off-site governmental authorities under a unified command.

The Executive Emergency Policy Committee at Notre Dame includes the president, provost, executive vice president, vice president for student affairs, vice president for public affairs and communication, and vice president and general counsel. The Policy Committee is the senior-most team responsible for developing a strategy and overall direction during major campus-wide emergencies. Moreover, the Policy Committee evaluates the impact of an emergency on human life and the long-term operations of the university in terms of service delivery, local community impact, government regulation, and institutional reputation.

The appropriate Liaison Officer notifies the Policy Committee in the event of an emergency, regardless of its magnitude. Should the emergency reach proportions beyond the capacity of routine first responders, the Policy Committee would activate the response plan and assume ultimate responsibility for activation, oversight, and deactivation of the university’s EOC. The Policy Committee may declare a state of emergency throughout the whole campus or a portion of the campus and, following the university’s response under the plan, can officially downgrade the state of emergency to business-as-usual.

The EOC is the physical location where university leaders gather during an emergency to coordinate response and recovery actions and resources. The EOC is not an incident command post used by first responders; rather, it is the operations center where coordination and management decisions are facilitated.

Finally, college and departments can activate local Department Operations Centers, which are essential to facilitating communication to and from the EOC.

**EOC Operations and Management**

The EOC Management Team serves as the operational arm of the Policy Committee during a declared emergency. In its role, the EOC Management Team creates plans to implement strategies developed by the Policy Committee, evaluates the incident as it unfolds, and further enhances strategies for an effective response. The management team also serves as the single point of contact for first responders and other field emergency response operations. Communication between these parties ensures coordination of university-wide response efforts between on-scene responders, departments, and executive management.

Upon activation of the plan, all primary EOC Management Team members report to the EOC. Once seated, the team establishes specific objectives and strategies for the particular incident at hand. EOC team members agree on a response strategy, and the EOC Leader might release those individuals not required for the specific incident. Members of the EOC include the following:

**Liaison Officer:** In the event of a significant campus emergency, first responders are required to notify the Liaison Officer. Regardless of the severity of an incident, the Liaison Officer notifies all members of the Policy Committee. The Liaison Officer provides a description of the emergency and an initial assessment of the magnitude of the event to the Policy Committee. The Policy Committee performs an incident assessment to determine the appropriate emergency level and, if necessary, the activation of the EOC. Information technology incidents are reported to the Office of Information Technology Liaison Officer (the
CIO or designate); hazardous materials incidents are reported to the Risk Management & Safety Liaison Officer, and all other incidents are reported to the Notre Dame Security Police Liaison Officer.

**EOC Leader:** The president, in consultation with the Policy Committee, appoints the EOC Leader, who has overall responsibility for the management of emergency response and recovery efforts. After appointment, the EOC Leader assumes ultimate authority for all aspects of emergency response management, including the development and implementation of strategic and tactical response activities and post-emergency assessments. The corresponding Liaison Officer for the particular event category may be identified as the EOC Leader. The EOC Leader is responsible for ensuring that the Policy Committee has accurate information about injuries or major financial/reputational risks.

**EOC Coordinator:** The EOC Coordinator is responsible for the EOC facility, including supplies, communication equipment, and EOC support staff (e.g., field runners). The coordinator monitors the communication flow to and from the EOC and assists the EOC Leader as necessary.

**EOC Scribe:** The EOC Scribe maintains a complete and accurate record of all events that occur during and after the incident.

**Public Information Officer:** The Public Information Officer serves as the university’s representative for communication of information to internal and external stakeholders, including the media or other organizations seeking information about the incident or event. The Public Information Officer ensures that only authorized university officials issue such information and directs distribution of messages through the university’s various communication channels. The Public Information Officer clears all communication through the EOC Leader prior to distribution.

**Life Officer:** Working closely with representatives from student affairs, human resources, and the office of the provost, the Life Officer monitors the status of all students, staff, faculty and visitors following the incident. The Life Officer coordinates communication with students, parents, staff, and faculty, working closely with the Public Information Officer on the nature of messages. The Public Information Officer must approve all messages, but the Life Officer may assist in distribution of such messages. The Life Officer also is responsible for the coordination of volunteers, medical care, and shelter.

**Finance & Administrative Officer:** The Finance & Administrative Officer is responsible for engaging necessary resources to monitor all financial and cost-analysis aspects of the incident. The Finance & Administrative Officer also tracks incident-related costs, personnel records, and requisitions. This individual works with the Planning Officer to obtain a status of all resources available for recovery actions and coordinates the procurement of resources, supplies, and materials required to conduct an emergency response (e.g., supplies, construction contracts, trailers, and so forth).

**Planning Officer:** The Planning Officer is responsible for managing the university’s efforts in the recovery stage of the incident, including overseeing departmental contributions to campus recovery efforts. The EOC Leader appoints the Planning Officer, who contacts members of the university leadership as necessary and coordinates with various divisions.
the personnel and equipment necessary to return to normal campus operations. The Planning Officer must consider the following aspects of response and recovery:

- **Operations**: In conjunction with the Liaison Officer, manage various campus departments directly related to incident stabilization and resolution. Formulate tactical objectives and operation strategies for resolving an incident and returning the university to normal operations.

- **Planning and Intelligence**: Identify technical specialists and campus resources to assist in planning incident recovery strategies.

- **Logistics**: Provide facilities, services, and resources required for the safe and successful return to normal operations.

Examples of necessary coordination by the Planning Officer include but are not limited to the following:

- **Business Operations**: Obtain a status of all resources available for recovery actions.

- **Student Affairs/Human Resources/Academic Affairs**: In conjunction with the Life Officer, develop plans to house students, staff, and faculty during the response and recovery phases.

- **University Relations/Information Technology/Athletics/Research**: Depending on the nature of the incident, the Planning Officer or EOC Leader may call upon departments within these divisions for participation in the response plan.

**Unified Command Structure**

When necessary, the EOC Leader may request jurisdictions outside of Notre Dame to commit major resources and expertise to an emergency response. In such instances, a Unified Command Structure is implemented. The Unified Command Structure consists of key officials from all responding agencies working toward a common objective with a common strategy. In these circumstances, leaders from other agencies work with the EOC Leader, Liaison Officer, and Planning Officer to coordinate response and recovery efforts.

**Department Operations Centers**

Depending on the incident, the university may activate one or more Department Operations Centers in affected departments and colleges. In campus-wide emergencies, Department Operations Centers may be the execution arm of specific EOC response or recovery strategies, or they might disseminate information from the EOC to various departments, colleges, and schools. Each college or major division will maintain a Center to provide continuous communication with faculty, staff, or students. It is imperative that all faculty members receive current, consistent information, as students will most likely turn to faculty members for information and guidance.

**Deactivation of the EOC**

The Policy Committee, advised by the EOC Leader, will determine when to deactivate the EOC and begin transition to normal campus operations. If deactivation of the EOC is authorized by the Policy Committee, the EOC Leader will notify all EOC personnel. All personnel should ensure that any required forms or documentation are completed and...
provided to the EOC Scribe prior to deactivation. Documentation and forms are maintained by the university for a defined period following the incident response.

Summary

Creating a comprehensive incident response plan and formalizing an EOC are crucial to an institution’s ability to quickly and effectively respond to large-scale emergency events. Institution leaders should not trivialize the complexity and breadth of this undertaking, and they should dedicate appropriate resources and time to its creation. Campus personnel are normally not experts in incident response, so it is wise to consider hiring a professional firm to assist. Having a well-thought-out plan is not sufficient in and of itself. At least once a year, the campus should practice day-long realistic simulation exercises during which the plan is fully tested, particularly so that those playing a leadership role can gain confidence in their roles. The second and even third tier of leadership should participate in the simulations and become operationally familiar with the response plan, in case key leaders are traveling or otherwise unavailable during an actual incident.

The Fire

On Friday morning August 28, 2009, only two days after fall classes had started, a small fire broke out in one of our numerous steam and utility tunnels that run throughout campus. At approximately 8:30 a.m., three events almost simultaneously alerted university officials that something was occurring. The Office of Information Technology’s (OIT) central operations center noticed an increasing number of network devices going off-line across many different buildings. Meanwhile, the campus fire department noticed that numerous building monitoring systems were going into local mode indicating that the central monitoring panel had lost contact with the buildings. Finally, building smoke detectors began to pick up the light smoke that was making its way through the tunnels into the nearby buildings and setting off building evacuation alarms. The fire department and OIT were unaware of what each unit was seeing on their monitors at that very moment.

The Notre Dame fire department arrived on the scene within minutes of the first alarms, to find moderate smoke escaping from a tunnel access hatch. Faculty and staff were standing outside five evacuated campus buildings, and students were streaming from four nearby residential halls into the rainy, chilly South Bend morning. The fire chief immediately declared an emergency, called for backup support, and began establishing a local incident command post. By this time, the OIT had lost data communications to numerous buildings and widespread reports of Internet, telephone, and cable television (CATV) outages were streaming in to the help desk. The OIT was still unaware of the fire, but word was sent up to the chief technology officer and then on to the chief information officer that “something big” was happening. The communications outage by this time was affecting approximately one-third of the campus.

News of the fire and the magnitude of the disruption were communicated through the chain of command to the president and executive vice president, who consulted with the provost, declared a campus-wide level-three emergency, and activated the EOC. By this time, the OIT was aware of the fire and assumed that it was related to the loss of data communications. Hearing of the widespread communications infrastructure outages, the
executive vice president contacted the campus CIO to communicate the president’s decision to appoint the CIO as the EOC Leader for this event.

EOC Activation

The EOC activation notice was sent out via NDAlert at 9:33 a.m. informing all primary EOC members to report to the center. NDAlert is Notre Dame’s emergency alert system built upon Blackboard Connect’s emergency notification platform. By 10:03 a.m., the EOC was assembled, with the CIO assuming the EOC command lead. The chief technology officer assumed the IT Liaison Officer role. The associate vice president for student affairs assumed the Human Safety Officer role, and the associate vice president for public affairs became the Public Information Officer. The role of Planning Officer was filled by an individual who served as backup to the primary and secondary designates for this role, since the primary and secondary designates were otherwise engaged.

By 10:10 a.m., the initial assessment of the incident was completed. The Incident Command Post at the scene, from which the first responders operated, had been established since 8:45 a.m., and it reported to the EOC Leader that the fire department had largely contained the fire by flooding the tunnel with foam. The fire was confined to a small portion of the utility tunnel between Washington and LaFortune Halls on campus and, as we learned later, at a major intersection of two main tunnels on campus. The IT Liaison Officer informed the EOC Leader that complete communications had been lost to 36 buildings, slightly more than one-third of campus buildings.

The Response

The EOC Leader had five main problems to deal with:

1. Coordinating with the Incident Command Post as they worked to extinguish the fire.
2. Working with the Human Safety Officer and Planning Officer and their respective teams to move the large number of displaced individuals, many of them in their pajamas and robes, out of the rain and into shelter.
3. Working with the Public Information Officer to keep the campus community and various news outlets informed, even though a large portion of the communications infrastructure was inoperable.
4. Calling into action the requisite Department Operations Centers to lay the strategy for the recovery phase.
5. Maintaining contact and communications with the Policy Committee.

The portion of the tunnel in which the fire broke out was a major thoroughfare for the copper and fiber communications plant. All traditional (landline) telephone, data, CATV, networked public address (IP-PA) system, and building-control systems affecting fire, security, door control, and heat, ventilation, and air conditioning (HVAC) were down for approximately one-third of campus buildings. Moreover, two cellular distributed antenna system (DAS) nodes affecting AT&T and Verizon Wireless users were offline because of damaged fiber. Within the hour, it was determined that the fire took out the T3 circuit feeding the AT&T cellular base transmission station (BTS), thus rendering the other 17 cellular DAS nodes for AT&T effectively inoperable. The building housing the university switchboard lost its connection,
and the main university number was not ringing through. As the fire damaged more and more copper, low-voltage coils protecting the telephone switch began tripping, taking out sections of the campus not originally affected by the fire. The operation of the EOC itself was severely hampered by the difficulty of making reliable calls, either via campus PBX or cellular. Had it not been for the purposeful installation of external VoIP lines into the EOC via the local cable company through secondary communications conduits, the EOC would have been virtually cut off from voice communications. Had that been the case, the EOC would have relocated to its designated secondary location or a tertiary location off-campus.

Given the extent of the communications outage and the loss of the university switchboard, the EOC Leader asked that the OIT’s Department Operations Center be immediately activated. This group was crucial in assessing the damage and working with the IT Liaison Officer to communicate the extent of the damage to the EOC Leader. The switchboard was relocated to a room adjacent to the PBX, where temporary circuits could easily be run, and this allowed the main university number to be brought back on-line.

Like many campuses, Notre Dame built its emergency notification system using multiple communications modalities. This strategy proved particularly important during this incident, but challenges still surfaced. Although central e-mail was up and working, a large portion of the campus had no access to the campus network, so e-mail was not a reliable communication channel. Moreover, the IP-network-based PA system recently installed in every building was inoperable in the 36 affected buildings because of the loss of data communications. Voice communication, along with CATV, was impaired by the massive loss of copper and fiber. Finally, service to cell phones was unreliable due to the loss of cellular DAS nodes and because many students rushed out of their residence halls so quickly that they left their cell phones in their rooms. In the end, building custodians outfitted with their normal work radios proved to be an effective communications conduit to the building occupants.

The university web page was updated with news of the event and referred people to emergency.nd.edu, the university’s well-branded emergency web portal, for the most up-to-date and accurate information. As news of the fire broke across the AP wire, more and more parents began trying to reach their children. With cellular service disrupted and so many of the students evacuating their rooms without their cell phones, the newly established switchboard began experiencing an increased call volume from anxious parents. The Public Information Officer and the communications team quickly created a response script for the telephone operators to follow to accurately inform and comfort the concerned callers and point them to the emergency web portal for the latest updates.

About 90 minutes into the incident, the EOC Leader asked the vice president of research to assess whether there was any imminent danger to research animals or research in general and report back to the EOC. After conferring with his team, the vice president determined that no research was in immediate jeopardy.

The fire itself was quickly extinguished. Most of the evacuated buildings, however, were still closed because of concerns about air quality. The nearby North Dining Hall was established as a safe gathering place for affected students and employees. Without a means to verify meal plans (the point-of-service food system was also down) and given the size of the
population impacted, Food Services offered free drinks and food for all those gathering in the dining hall.

Several of the affected buildings housed classrooms. As one of their responsibilities, the Human Life Officer and his group have oversight of the teaching function of the university. After conferring with the EOC Leader, the Human Life Officer canceled a total of 10 classes because of the fire. The Human Life Officer sent word to the registrar through the Public Information Officer to that effect.

The Executive Policy Committee convened at 11:30 a.m., and the EOC Leader provided an update. They were very satisfied with the response to the incident thus far and the initial recovery strategies being established to return the campus to normal operations. One might naturally think that the president, provost, and executive vice president of the university would ordinarily be neck deep in a situation like this, but the purposeful separation of the EOC and Executive Policy Committee allows the top leaders to stay above the fray of the incident and think clearly and strategically about how the university needs to respond.

By 1:46 p.m., all buildings were cleared for reoccupation, and the crowds eventually dispersed. The EOC held its last briefing, charged the recovery teams with their responsibilities, and disbanded shortly thereafter.

The Recovery Phase

The recovery portion of an incident is a distinct phase of the emergency response plan. While the recovery phase may begin before the deactivation of the EOC, it is largely a free-standing process that continues after the EOC has disbanded and runs until normal campus operations resume.

Even though the tunnel fire at Notre Dame was probably small on a range between a smoldering cigarette and flames licking out the windows of a high rise, it caused extensive damage to the communications infrastructure. One of the OIT’s network personnel donned a haz-mat suit and entered the tunnel with emergency personnel shortly after 2:00 p.m. What he saw was a spaghetti-like mess of melted copper and fiber cable. We knew at that point that restoration would be measured in days, not hours.

All-in-all, over 10,000 pairs of copper and 800 strands of fiber-optic cable were damaged and had to be repaired or replaced. The fire started in probably the worst conceivable location: the main tunnel into which the phone switch and campus network feed. Much of the copper damaged was large (4-inch) 2,000-pair trunk lines, many dating back to the early 1960s, and large fiber bundles heading to other fiber distribution points (POPs) on campus and over to WNDU, the NBC affiliate on the west side of campus. The haz-mat team hired to clean out the tunnel was instructed to cut back and remove all cable 75 feet in three directions where the tunnel forms a T to feed other parts of campus.

AT&T had its emergency splice crews and large spools of cable on site by early Friday afternoon. Because of concerns about asbestos fibers from damaged insulation floating loose in the air, tunnel access for non-emergency personnel was delayed until 8:00 a.m. Saturday morning while the various tunnels were ventilated and air measurements taken throughout the night.
By 7:00 p.m. Friday evening, the AT&T cellular head-end was back on-line. With landlines long since removed from the dorms and the restoration phase entering into the weekend, the demand to restore voice services was much different from what it might have been otherwise. The restoration of services fed by fiber took on a much different tone from copper, however. The lack of Internet, CATV, and building-control systems affecting fire, security, door control, and HVAC placed a much higher priority on getting the fiber infrastructure repaired. Door locks were still operating in “local mode,” which means they were enforcing the last downloaded access control list.

Notre Dame has the classic hub-spoke-ring fiber distribution model. Because of the route diversity of our tunnel system and the richness of fiber running through major fiber POPs, we were able to reroute many of the severed fiber trunk lines and bring back a considerable portion of data and CATV services within hours of the fire. For buildings to which the main feed had been cut, we began running armored cable over the ground from the nearest fiber POP to the main building wiring closet. It was decided early on that it would be quicker and cleaner to pull new fiber end-to-end than to try to splice the damaged fiber in the tunnels. With that in mind, we spent Friday afternoon and evening buying up every available large spool of fiber within a 100-mile radius of Notre Dame.

Every tragedy has at least one or two funny stories buried among its hardship. It is here that I would like to introduce Dan, the shoeless truck driver. Dan is a delivery truck driver for one of the fiber distribution houses outside of Chicago—and, it turned out, an avid Notre Dame “subway alum” (a fan who didn’t attend Notre Dame). Although Dan’s company had a large portion of the fiber we needed, it could not fill all our requirements from the warehouse with which Dan was affiliated. Dan promptly loaded up his truck and then drove to two other warehouses in the Chicago area to complete the order, and then drove to Notre Dame in South Bend, Indiana. We met Dan at the delivery docks shortly after midnight. Dan emerged from his truck wearing no shoes, and he spent the next 45 minutes helping us unload the fiber in a cold, driving rain. He wished us luck with the home opener against Nevada and was back on the road to Chicago by 1:00 a.m. Proving that no good deed goes unrewarded, Dan is getting an opportunity to come back to campus for the Notre Dame–Boston College football game as our guest—hopefully under much better circumstances. Needless to say, this is one subway alum who is ecstatic to have helped out that rainy evening.

By Sunday evening, with around-the-clock shifts of Notre Dame personnel working with Comcast and local electrical contractors, all 36 buildings were back on-line with everything but voice services. It took three AT&T splice crews working around the clock until Thursday morning to return all the voice lines to service.

What It Means to Higher Education

Any postsecondary institution that receives federal funds is required to establish compliance with various federal directives as it relates to emergency preparedness. Among those directives is Homeland Security Presidential Directive #5 (issued 2/28/2003), which requires the institution to be compliant with NIMS. Included within NIMS is a requirement that the campus adopt, understand, exercise, and train on the elements of the Incident Command System and embrace the concept of Unified Command when responding to local, state, or regional crises.
An inevitable fact of life is that “stuff happens,” whether it is hurricanes, threats from individuals, pandemics, or apparently insignificant tunnel fires. The demands placed on campus IT and communications infrastructure have never been greater, and they will only continue to increase. The “Google syndrome” has raised the performance bar in our users’ minds to a point that anything less than five 9s of availability is unacceptable; this “stuff” should never go down.

You can never plan for everything, but the process of planning and, more importantly, exercising and refining the plans using real-life simulations and other table-top exercises means that the institution will have greater maturity and skills to better handle emergency incidents when they do happen. Nothing in our plans would have prepared Notre Dame for the events of that August 28, 2009. As an institution, however, we responded quickly and strategically—not only because we took the time to write the plan but because we took the time to exercise it before an actual emergency.

Key Questions to Ask

- Is our campus incident response plan compliant with NIMS standards?
- How does our business continuity and disaster recovery planning address risks associated with seemingly obscure elements of the campus infrastructure and operations?
- What are some realistic simulation exercises that the university could undertake that will help us respond effectively to emergency incidents on campus?
- What program do we have in place to train the second tier of university leadership in emergency response in case primary leadership is unavailable?
- Does our emergency operations center have back-up voice and data communications that do not depend on either the campus telephone switch, campus-based cellular sites, or campus networking?
- Which key vendor relationships and contracts does our institution have in place that allow us to quickly execute our disaster recovery phase?
- How does the campus disaster recovery and business continuity plan integrate with the incident response plan?

Where to Learn More


Endnote


About the Author

Dewitt Latimer (dewitt@nd.edu) is Deputy CIO and Chief Technology Officer at the University of Notre Dame.