Not surprisingly, the protection of human life is a high priority for colleges and universities. The security of campus facilities and other physical assets is taken equally seriously, considering the consequences of fire, chemical spills, and other hazards. However, until recently, the protection of cyber assets has rarely risen to the attention of campus governing boards and administrators.

The National Campus Safety and Security Project—launched by the National Association of College and University Business Officers (NACUBO) and seven other higher education associations, including EDUCAUSE—conducted a survey in late 2008. The results of that survey reinforce the view that higher education institutions have made significant progress in securing their human and physical assets in the aftermath of hurricanes in the Gulf region, floods in the Midwest, and shooting incidents at Virginia Tech and Northern Illinois University. A large majority of survey respondents indicated that their campus had a designated emergency manager, with larger institutions more likely to have people in positions dedicated solely to emergency management. According to the survey results, campus emergency-preparedness plans cover “acts of violence” 97.9 percent of the time and “natural disasters” 96.9 percent of the time. However, preparedness for a “pandemic” is addressed in only three-fourths of the campus plans and a “cyber disruption” is just over one-half (51.6%). Whereas more than one-half of the survey respondents reported conducting field exercises for “acts of violence” and “natural disasters,” only one out of four reported conducting field exercises for a “pandemic” and a mere 14 percent for cyber disruptions. Colleges and universities thus appear to be unprepared to respond to a major cyber attack that could disrupt critical programs and services.

The good news is that campus IT professionals are participating in field exercises with increased frequency (58% of the time). Additionally, 80.7 percent of the survey respondents recognize the computing and telecommunications infrastructure as a priority service that needs to be operational in the immediate aftermath of an emergency, following closely behind the physical plant (82.2%) and the public safety/campus police (88.9%). The infrastructure necessary to provide emergency notifications was also considered a high priority, with the most common avenues of notification being identified as follows: e-mail, web page, text messaging/instant messaging, LAN line messaging, and voice-mail, and telephone trees.

In August 2008, EDUCAUSE held a summit focused on the role of IT in campus security and emergency management, exploring proactive approaches to and emerging technologies for emergency management. Participants included chief information officers, campus police officers, campus public safety chiefs, emergency managers, facilities managers, risk managers, and public relations officers, among others. Summit participants listed seven “hallmarks of effective emergency management,” which addressed responsibilities that require IT leadership, including assurance that critical technologies work without delay or interruption during and immediately after an emergency. Participants also identified a number of emerging technologies that contribute to a safer and more secure environment, including emergency communication systems, geospatial mapping tools, GPS technology, business continuity planning tools, learning management systems and virtual worlds, social networking tools, virtual emergency operations centers, intelligent monitoring, data mining and database tracking, and information sharing.

Overall, colleges and universities take emergency preparedness and campus safety and security seriously. The survey results from the National Campus Safety and Security Project demonstrate that higher education institutions are both proactive and systematic in addressing the four phases of emergency management: prevention/mitigation, preparedness, response, and recovery. In addition, the survey results, combined with the recommendations from the EDUCAUSE Summit, suggest that institutions need to strike a balance between the open, research-driven nature of the academic enterprise and the need for a safe campus environment. Furthermore, higher education must keep an eye on emerging technologies and constantly seek new opportunities to leverage technology for emergency management.

The threat of violent acts, natural disasters (e.g., hurricanes, fires, and tornadoes), cyber attacks, and pandemic influenza suggests that the scope of campus safety and security has become more complex and requires a risk-based treatment of all of the possible hazards. Planning for the protection of cyber assets lags seriously behind efforts to safeguard human and physical assets. Accordingly, it will be up to the CIO and information security community to supply the leadership and the initiative for ensuring that campus emergency-preparedness plans embrace an all-hazards approach.

Notes

Rodney J. Petersen, Government Relations Officer for EDUCAUSE and Director of the EDUCAUSE Cybersecurity Initiative, served as guest editor for this cybersecurity focus issue of EDUCAUSE Review.