Community Engagement for Security and Safety

As educators and IT professionals, we all are cognizant of how technological innovation is changing our world, our lives, and our future. But until April 16, 2007, I was blind to its dark side. On that day at 9:42 AM, I received a phone call from my daughter on the Virginia Tech campus. Not understanding her first words, I responded: “Melissa, I can’t understand you. What is that background noise?” “Dad, it’s gunfire. Someone’s shooting in the Norris classrooms across from my office!” By the time the gunfire stopped less than ten minutes later, a deranged student had shot and killed thirty faculty and students and wounded seventeen before killing himself as police entered the building. That call and that tragedy exposed me to a new facet of our responsibilities as educators and IT professionals in this new century.

Since the end of the Cold War, state-on-state wars have dramatically decreased, but the effectiveness of violence by individuals and small, often stateless groups has increased startlingly. Technological innovation has changed global, national and local economies; it has decreased the importance of physical distance but has increased the value of knowledge and human creativity and of timely, high-capacity access to these resources. The dark side of this change is that a single individual, or a small group, intent on leveraging readily available advanced technologies and increasingly deadly weapons can, at relatively low cost, research, organize, and execute a complex plan, acquiring critical components for horrible consequences.

A few days after the shooting at Virginia Tech, a former colleague, employed by one of the federal agencies involved in national security, told me that academic communities, especially college/university and school campuses, have been viewed as easy targets—“just so much low-hanging fruit”—for anyone intent on mayhem. Yet I suspect that many in education are convinced that what happened at Virginia Tech, at Sandy Hook, and in other educational communities cannot happen in theirs—or that the violence somehow relates to flaws in those communities. A year after the attack on our campus, a high-level politician in another state asked me: “Has Virginia Tech done the things necessary to guarantee that there will never be another such attack?” I am convinced that we have done more than any other higher education institution to ensure the safety of our community, but in our world today, it is quite naive and dangerous to think that safety from evil can be guaranteed.

I led the post-tragedy internal review of how campus and regional technology infrastructure at Virginia Tech was leveraged and how it performed on April 16, 2007. The report examined multiple areas, including the following: campus and regional data communications systems; web communications facilities; emergency radio communications systems; relevant local 911 systems; cellular service utilization and performance; traditional telephone service utilization and performance; video, campus cable television, and related broadcast systems; IT support services; data-preservation facilities and processes; data-retrieval facilities and processes; personal information management; command, control, and emergency communications centers; cyber-security; and the automated notification system. Although many think that the analysis must have focused on emergency communications during and after the shooting, believing that this is the only role for information technology in such events, the report documented weaknesses and failures in all elements of the local and regional communications infrastructure, including the cellular telephone systems, the public switched telephone network (PSTN), and the emergency responder radio communications systems. The report also listed more than 120 recommendations for improvement specific to particular functional areas. The IT interdependencies related to public safety go far beyond the communications technology elements triggered by a particular event.

The most important lesson we learned—one that is especially relevant to every human-initiated act of violence—is related to the following facts. First, the burden for preventing or mitigating the vast majority of these incidents has been and will be on poorly financed and supported local (community) security and first responder personnel and institutions. Second, although advances in information technology, communications, and computing have resulted in profound changes in the way we live and work, they have hardly touched how communities mitigate/prevent, prepare for, respond to, and recover from acts of violence. A significant disconnect exists between IT practitioners and public safety principals at the local community level, except in the case of a few major cities. There is no culture of experimentation with emerging technologies and capabilities or of innovation in front-line public safety institutions. Thus the key lesson learned is that college and university IT organizations should have advocates for activity and service in this arena and should have an appropriate-level liaison to those responsible for campus security and safety.

Emergency management consists of four phases: Mitigation/Prevention (avoidance and deterrence), Preparedness, Response, and Recovery. Traditionally, telecommunications systems have been critical components for the Response
phase. However, existing telecommunications systems, not just in southwest Virginia but throughout the United States, are not designed to support all of the innovations possible in emergency management, such as advancements in processing, visualization, sensors, and myriad other tools. We need an information architecture that is capable of facilitating all four phases of emergency management. (For example, see Figure 1.) This enhanced system would take advantage of the resilience inherent in Internet Protocol (IP) based networks to provide extremely high reliability and availability. It would integrate all types of communications including legacy voice, data, and video, and it would support a wide variety of IP-access devices. Employing innovative technologies such as massive sensor networks, intelligent threat-analysis systems, pervasive computing, and cognitive radio, the new architecture would enhance all the phases of emergency management.

Figure 1

The Role of Information Technology and Research in Emergency Management

Even given the promises of leveraging existing technological capabilities, the poignant realization for me, as an IT professional, is that few of our findings relevant to systems and capabilities in place in April 2007 would have been relevant to early detection or mitigation of the events of April 16 at Virginia Tech. Exploring and exploiting technology innovations and leveraging massive collaboration to address this aspect of community security is fertile ground for innovation. Although the public perceives security as a government problem and as the responsibility of the state, the higher education community should be engaged in this space. If there is one key lesson from the growth of the Internet, it is the unbounded value proposition of massive collaboration. Leveraging this opportunity requires enabling and instilling the idea that every connected person can be a sentinel for security, and it requires security policies and institutions that can selectively encourage and support openness, peering, and sharing.

Governmental agencies and their private-sector partners are beginning to explore how to leverage our highly networked world for “proactive” security. They are exploring systems and methodologies that are intended to predict impending threats and support the mitigation of those threats. The higher education community can bring to the engagement advanced infrastructure investments in ubiquitous computing and communications, early explorations of pervasive computing environments, and most important, above-the-norm competencies in using computational and advanced communications.

Anytime the political pressure for public security increases, there is danger of a shift in equilibrium against individual liberties. We must create safe and secure environments that reduce fear through enhanced security while preserving individual liberties. The academic community—with its free-thinking, push-the-boundaries culture—may be the community best-suited to develop and advocate for policies and mechanisms that will balance the need to protect individual privacy and liberties with the desire for public security. It is the only community that I trust to do so.

The first step is the creation of an information architecture to facilitate the four phases of emergency management, as noted above. But in addition, higher education needs to be more engaged in the related public debate on issues ranging from mental health to gun regulation. There is always a flurry of hand-wringing and proposed activity after a tragic event—followed soon by silence, with no real change in engagement by higher education. Violence can happen anywhere, on any of our campuses. Being ready is not someone else’s responsibility. It is up to each of us and all of us.

Notes
1. Earlier that morning, the student had shot and killed two other students, making a total of thirty-two murdered. An additional dozen students were injured by jumping out of windows to escape the shooter. A good reference for the tragedy is John P. Giduck, Shooter Down! The Dramatic, Untold Story of the Police Response to the Virginia Tech Massacre (Bailey, Colo.: Archangel Group, 2011).
3. For an example, see the description for the Executive Director, Converged Technologies for Security, Safety and Resilience position at Virginia Tech: http://it.vt.edu/ctssr/staff/director/.

Earving L. Blythe (blythe@vt.edu) is Vice President Emeritus, Information Technology, at Virginia Tech.

© 2013 Earving L. Blythe. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License (http://creativecommons.org/licenses/by-nc-nd/3.0/).