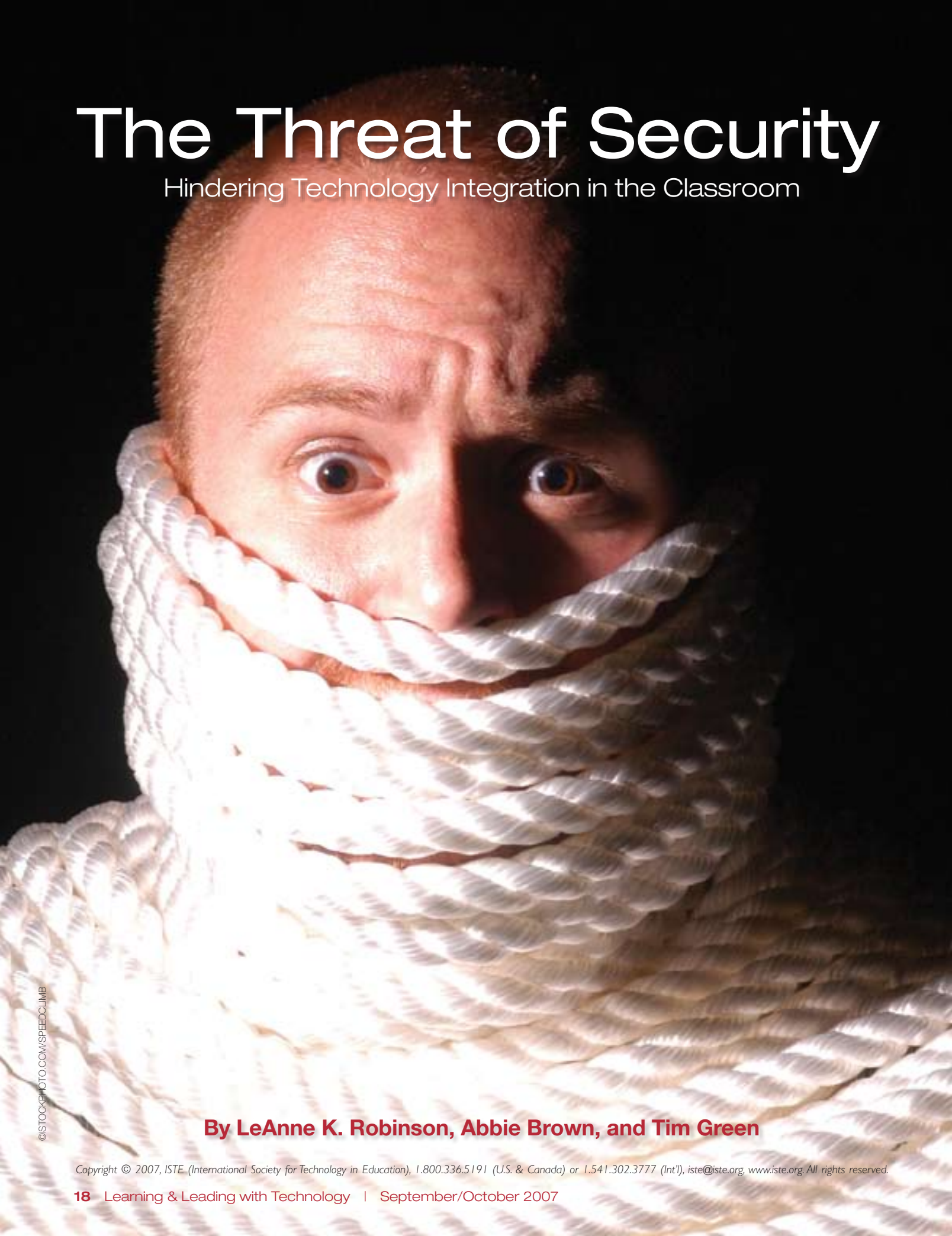
The Threat of Security

Hindering Technology Integration in the Classroom



©ISTOCKPHOTO.COM/SPEEDCLIMB

By LeAnne K. Robinson, Abbie Brown, and Tim Green

A dedicated teacher who spends much of his summer break in his classroom shared an interesting story regarding his alleged inappropriate use of the Internet:

> I spent last Saturday in my classroom, getting ready for back to school. Before I left, I ordered half a dozen bulbs from an online flower company. Don, the personnel director, sent me an e-mail and stopped by my classroom to inform me that I was now being monitored for inappropriate uses of the Internet. He said that repeated violations would be noted in my personnel file.
> —*Tom, high school science teacher*

This teacher also shared that new computers purchased for his classroom were equipped with inoperable CD-RW drives. When he inquired as to why he couldn't burn a CD of a PowerPoint presentation, he was told "The drives will not be made available for open use. Teachers may violate copyright laws if they are allowed to freely burn CDs." This teacher's conclusion? He has decided to avoid computing technology in his classroom, no longer wanting to deal with the conflicts and increased permissions needed to use the available technological resources:

> I am a good teacher. Sure, technology may be beneficial, but it is much easier to continue doing what I know works than to attempt to use technology that is riddled with roadblocks.

Unfortunately, this teacher's story is similar to the experiences of many others. When we shared these two incidents with several colleagues, it turned out that they too had been collecting stories. For the last year we have been gathering examples of how perceived "threats of security" are hampering the integration of technology in teaching and learning. After examining several anecdotes from K–12 schools and institutions of higher education, we asked ourselves the question, "Could our concern over security be generating a fear that is now hindering the integration of technology?" It is our hope that educators will examine both the challenges of increased security demands and ways in which security might enhance, rather than detract from, the use of technology for learning.

Where We Are

First, let us state that we feel security *is* important. The safety of our children is paramount and the financial investment in networks, hardware, software, and infrastructure should be protected. Most of us have experienced the grinding halt to productivity that occurs when a system is attacked by a virus. However, if protecting our investment actually decreases or impedes the use of technology, then our goal of improving student learning through the integration of technology becomes harder to achieve.

Barriers to the integration of technology include such things as a lack of appropriate hardware and software, training, administrative support, and even collegial jealousy. The lack of security, as far as we have found, has not been identified as a barrier in the literature. Studies indicate that teachers who use technology in their classrooms tend to develop and implement more constructivist learning activities. Therefore, researchers believe that the presence of technology in PK–12 classrooms is a contributing factor in the development of more authentic and opportunistic learning environments. The full integration of technology into teaching and learning has been a relatively slow process, especially in PK–12 schools. Access to technology has been identified as a contributing barrier to technology integration, and the CEO Forum identified increased access as a necessary goal during earlier integration efforts. Lack of access is a primary barrier to technology integration, and ISTE explicitly states that access is one of the necessary conditions for full integration. Schools across the nation have spent billions of dollars on computing technologies. The concerted effort to provide access to computing technology has resulted in wired schools, where students and educators have educational technology available in a large percentage of teaching and learning situations.

With the ongoing development of computing infrastructure and increased access, school districts have begun to examine issues of security. Early security measures in PK–12 schools focused on cybersecurity for students, including limiting access to inappropriate Web sites. Schools purchased programs that blocked student access to certain sites. In attempts to protect students, limit liability, and receive federal funding, district technology committees implemented Internet Use Policies (now commonly referred to as Acceptable Use Policies or AUPs) that had to be signed by parents, students, and teachers. Students who violated agreements lost Internet privileges. In addition, school districts purchased antivirus software, made efforts to increase firewall security, and started backing up data. A third line of security included the development of protocols for accessing network information.

In addition, educators have become increasingly aware of copyright law. They are expected to monitor potential copyright infringement associated with digital information accessed through the Web. Districts created policies and systems to make sure that software usage adheres to licensing policies. Although these initial protections were often inconvenient for staff, the policies made sense.

Ironically, the mere presence of technology is not generating access.

Although technologies may be present, many students and educators, both in PK–12 and higher education, are increasingly reporting problems with using technologies due to increased security measures. Employee monitoring software that has been used in business is being used by administrators to monitor faculty use of the Internet and e-mail. Additionally, faculty members, like their students, are increasingly expected to read and sign strict AUPs. Although security measures appear to be well grounded, there is increasing evidence that many policies being imposed by administration as efforts to protect students and personnel from lawsuits are actually decreasing the availability and utility of integrating technology into teaching and learning. The more anecdotal information we gather, the clearer it becomes that increased use of security and monitoring software is having a negative effect on students and educators.

Identifying the Threats

E-mail. There is no question that e-mail has altered how we communicate. Educators are expected to check and respond to e-mail, just as they are expected to check and respond to phone messages. Interestingly, the same codes of conduct that are applied to the phone—which is considered district property—do not transfer to the use of e-mail. In our experience, no one questions a teacher when he or she makes a personal call before or after school, and phone conversations are not recorded and monitored. This is not true with e-mail. Citing the rationale that computers are public property, e-mail is often monitored and staff use is often highly restricted. As an example, let us look at one school district's written policy for e-mail:

"No staff member shall access, create, transmit, retransmit or forward material or information:

- that promotes violence or advocates destruction of property including, but not limited to access to information concerning the manufacturing or purchasing of destructive devices or weapons
- that is not related to district educational objectives
- that contains pornographic, obscene or other sexually oriented materials…"

There is nothing wrong with this policy's first and last bulleted points, but the second bullet point may be interpreted very narrowly to a point where almost no e-mail message sent or received by a teacher would be deemed appropriate (one might interpret a message home asking about a student who was ill as an infraction).

Trying to regulate the use of e-mail has resulted in lengthy inservices and fear:

There is increasing evidence that many policies being imposed by administration as efforts to protect students and personnel from lawsuits are actually decreasing the availability and utility of integrating technology into teaching and learning.

We were told that all of our e-mail was being monitored. I am afraid to check my e-mail after school because sometimes people, even parents, will send me stuff that may be offensive to the person monitoring the e-mail. We had a big district meeting and it was made clear that under no circumstances should we use our e-mail for personal purposes, not even to make plans for the weekend with people we work with.
—Monica, special education instructional assistant

Trying to regulate the use of e-mail has resulted in lengthy inservices and fear.

©ISTOCKPHOTO.COM/PETER AUSTIN

Networks. At one university, campus labs have been equipped with an automatic logoff script that closes the account of an inactive user after 15 minutes. The purpose is to protect the information of those students who have forgotten to log off. An instructional computer lab, used for classroom instruction anywhere from four to 10 hours a day, recently had the same script installed by the college technology service. Because students in classes are often engaged in small group activities and work with other individuals, they are frequently logged out when away from the computer. The instructor had to remember to move the mouse on the machine designated for demonstration. Because he was often engaged with both individuals and groups of students, he would forget to return to the demonstration machine and consequently had to re-log on to the machine several times during a class period. When the instructional technology instructor asked to have the script altered, he was

told that the logoff scripts were necessary for security. A solution offered was to add another four-minute logoff script that would save students' work to the desktop. Once the logoff script was executed, the user was forced to wait for the entire four minutes and then restart the machine.

> The funny part is that the threat to security being mentioned doesn't really exist in the classroom labs. Students are much more concerned about losing their work during class than they are about someone accessing their personal folders. … A fluid use of technology is more difficult to model for our preservice teachers. Many of them come into technology courses with a negative attitude about computers. It is almost like we are showing our students that computers, like challenging students, have to be monitored constantly. I don't think this is the message that we really should be sending.
> *—Judy, instructional technologist*

Web sites. Preservice teacher education candidates are often encouraged to create classroom Web sites. Schools have Web sites, and it is not uncommon for teachers to develop their own classroom pages—and frequently, creating a Web page for one's classroom is a requirement for inservice coursework in educational technology. Although this is considered a best practice, many district policies designed to combat corresponding threats to security actually discourage the use of the Web:

> … our school has a filter and I tried to get on my Freewebs site… It wouldn't let me through…. probably the word "free." Freewebs is a great site for creating Web pages at no cost. All you have to do is include a link somewhere on your page that goes back to the Freewebs home page, and that page does not have to have ads on it.
> *—Molly, elementary teacher*

> My district forbids teachers from posting Web pages outside sites that relate to their classroom. All pages must reside on the county server.
> *—Jeff, middle school teacher*

These teachers are forbidden to use their own resources to create a class-related site, and the district server limits what can and cannot be posted. This is the equivalent of saying that they cannot use their own money to buy pencils and markers, or that they cannot purchase bulletin board materials on their own. Worse yet, this is the equivalent of saying they cannot create a bulletin board display on their own but must follow a strict, district-supplied template.

Filters. Instructional technologists are well aware of potential problems associated with children's personal information being available online and the need to monitor the use of the Internet in classrooms. The Children's Internet Protection Act (CIPA) makes it clear that a minor's access to potentially harmful sites be restricted. School districts have taken action, schools have installed various types of filters, and professional literature has provided recommendations as to how teachers and administrators should safeguard their schools. For example, the April 2004 *Superintendent's Insider* gave the following advice: "Before a staff member tests the filtering software, he should be sure to get authorization to avoid the appearance of impropriety." Should teachers and librarians also get permission before previewing books for inappropriate content? Would a teacher who was testing filtering software *not* contact the technology coordinator if they had concerns? And shouldn't the technology coordinator (or appropriate party) have checked the filters prior to purchase? It makes sense to test filtering software and if there is a problem it should be reported, but extreme recommendations and regulations create fear.

> I am a science teacher. With that being said, you must assume that I typically look at numbers involved in a study in order to form an opinion. In the article "Safeguarding the Wired Schoolhouse" by CoSN it is suggested that in "July of 2000 there would be 2.1 billion Web pages and 7 million new pages created each day." Now that is a lot of Web pages. However, the article goes on to say that 72,000–100,000 of these sites even suggest any type of "inappropriate" material. If you do the math, that means that .003-.005% of the sites on the Web in 2003 were considered inappropriate. Does this mean that our government should spend millions of dollars to protect our children from these sites by using filters? … as a teacher I personally don't want students pulling up these sites in class, but I think I'll take the cheaper route and simply tell them to turn off their computer … because they have used poor judgment in my classroom.
> —*Sherry, science teacher*

Where We Need To Go

Threats to security are real, but they need to be seen in perspective. As instructional technologists, we must balance the need for the protection of our students and our tools with the need for accessible and flexible applications of technology. We must find ways to encourage fearless and safe use of computing tools and innovative technologies. We must empower teachers to fully integrate these tools and technologies into their classroom settings in ways that are both safe for the individual and satisfying for the learner. We are concerned that current security measures are more punitive than supportive; that they will cause teachers to avoid integrating technology for fear of negative repercussions. In the worst-case scenario, teachers would make no attempt to experiment with or creatively apply innovative technologies to their teaching practice for fear of administrative reprimand. We who believe in the power of computing tools as a positive force in the classroom must find ways to create environments in which the potential dangers of the tools are minimized without minimizing teachers' opportunities for professional growth.

Resources

Becker, H. J. (2000). Findings from the teaching, learning, and computing survey: Is Larry Cuban right. *Education Policy Analysis Archives, 8*(51).

CEO Forum. (1999). *The CEO Forum School Technology and Readiness, Report 2: Professional Development, A link to Better Learning.* Washington DC: CEO Forum on Education and Technology

Cuban, L., Kirkpatrick, H., and Peck, C. (2001). High access and low use of technologies in high school classrooms: Explaining an apparent paradox. *American Educational Research Journal, 38*(4), 813–834.

Ertmer, R. A., Addison, P., Lane, M., Ross, E., & Woods, D. (1999). Examining teachers' beliefs about the role of technology in the elementary classroom. *Journal of Research on Computing in Education, 32*(1), 54–62.

ISTE (2000). *National educational technology standards for teachers*. Eugene, OR: International Society for Technology in Education.

Kalkowski, M. A. (2001) Focus on learning and technology. *Communication: Journalism Education Today, 34*(4), 19–22, 25, 27.

Lane, M., Ross, E., & Woods, D. (1999). Examining teachers' beliefs about the role of technology in the elementary classroom. *Journal of Research on Computing in Education, 32*(1), 54–62.

Robinson, L. (2003). *Diffusion of educational technology and education reform: A qualitative study of educators' perceived barriers.* Unpublished doctoral dissertation.

Robinson, L., Brown, A., & Green, T. (2004). *The threat of security: Increased technology access limitations on teachers and students.* Paper presented at the Association of Educational Communications and Technology Annual Conference, Chicago, IL.

LeAnne K. Robinson, PhD, is an associate professor of special education and instructional technology at Western Washington University.

Abbie Brown, PhD, is an associate professor at East Carolina University in the Department of Library Science and Instructional Technology.

Tim Green, PhD, is an associate professor at California State University, Fullerton in the Department of Elementary and Bilingual Education.