INSIDE HIGHER ED

# Our Greatest Strength Is Our Greatest Vulnerability

> The greatest strength of online learning is the anytime and anywhere characteristic, but the online aspect is also our greatest vulnerability.

By **Ray Schroeder**

December 18, 2019

We tend to think often about the worldwide reach and impact of online learning. Through online, we have the power to change lives and societies. However, we are seriously vulnerable, more so, one might argue, than our campus-based colleagues. The online digital nature of our field is such that we are subject to outages and cyberattacks. One might be able to convene a campus-based class without the network, without an LMS, without asynchronous communication features. But without these capabilities, our online classes would be crippled.

In the early days of online learning -- the mid and late 1990s -- I recall setting up a telephone bridge with bulletin board software to enable a rudimentary backup to a potential disruption of the internet. Contingency plans included contacting students via phone or snail mail with instructions on how to connect through dial-up modem connections. As enrollments grew larger, we obtained high-speed DVD copying devices so that copies of courseware could be distributed via snail mail in case of network disruption. This involved altering the course display so that it was not dependent on the LMS system. We then implemented VM server solutions at remote locations to provide backup emulation and virtualization. And much of our software moved to the cloud with relatively robust backups in place. All of these actions are part of the historical record of attempts to assure continuity of the online learning programs. Yet today, despite our ever more sophisticated backups and hardened security, we remain vulnerable to network disruption at the user

side, software corruption, personal identity theft, intellectual property theft and a host of other vulnerabilities through nefarious actors and actions.

On the geopolitical front, on Nov. 1, Russia implemented its sovereign internet law, effectively enabling the government to cut off all outside internet sources to the country. Russia is only the latest; a number of other countries have put similar measures in place. Even more recently, Iran blocked the entire net, not just foreign sites, but for nearly all of the country. Our international students are left to struggle with such interruptions.

As we move toward the integration of more "smart" AI applications such as neural networks, other concerning strategies are emerging. Intelligent chat boxes, "smart" assistant programs and learner face- or voice-recognition programs all carry vulnerabilities due to the emergence of adversarial machine learning, creating another approach to compromising our online learning programs. Matthew Harris does an excellent job of introducing the principles of adversarial machine learning in his article in *Towards Data Science*: "Essentially, attacks on neural networks involve the introduction of strategically placed noise designed to fool the network by falsely stimulating activation potentials that are important to produce certain outcomes." These approaches can enable altering the artificial intelligence perception of inputs and sources without directly breaking into the computer or coding.

How do we prepare for such incursions in the 2020s? The first step may be to identify the problem. I serve on a systemwide cybersecurity task force for my university. We are looking at vulnerabilities, impacts and solutions. It is unlikely that any single task force will be able to anticipate every single potential eventuality. Certainly, this is a moving target with technologies, networks and applications constantly evolving. As Dan Carfagno reports in his enlightening article "Why Is Higher Education the Target for Cyber Attacks?" "Cyber-attacks will not happen the same way in the future. Hackers have learned over time to adapt to changes in security methods. Some more pressing problems today faced by IT departments will include hackers using

their entry for creating severe disruptions to university operations and affect more than just data."

Taking action to protect the university is not a single simple action. It takes a multiprong approach that is constantly assessed and reassessed, as hackers are constantly evolving their methods in higher education attacks.

Ongoing proactive vigilance is necessary to assure that we are meeting the challenge. The consequences of failing to create an effective comprehensive program put students, faculty and the credibility of the university at risk. It is important that all parts of the university are engaged in this process so that all interests and vulnerabilities are represented.

What are you doing to advance cybersecurity at your university? Have you begun benchmarking your practices against other universities? What practices have you targeted? I plan to continue to follow and write on this topic, so let me know what you and your peers are doing to lead in this field.

https://insidehighered.com/digital-learning/blogs/online-trending-now/our-greatest-strength-our-greatest-vulnerability?utm_source=Inside+Higher+Ed&utm_campaign=8d364b5e55-InsideDigitalLearning_COPY_01&utm_medium=email&utm_term=0_1fcbc04421-8d364b5e55-200040001&mc_cid=8d364b5e55&mc_eid=20a6b0e480