Academia’s Role in Securing Cyberspace

In 2002, U.S. President George W. Bush appointed and in 2009 President Barack Obama reappointed Jared Cohon, President of Carnegie Mellon University, to the Homeland Security Advisory Council, where he has served as chairman of the Council’s Academe, Policy and Research Senior Advisory Committee. In the following EDUCAUSE Review interview (facilitated by Carnegie Mellon Vice Provost and CIO Joel M. Smith), Dr. Cohon discussed this work and the role of higher education in improving cybersecurity.

Q. What have you learned from serving on the Homeland Security Advisory Council (HSAC) for the U.S. Department of Homeland Security (DHS), and what are the implications for colleges and universities?

It has been a privilege to have served on HSAC since its creation in March 2002. Serving on the Council and seeing, up close, some of the work undertaken by DHS, I am impressed by the dedication of the people involved and the size of the challenge that they face. Protecting the nation is a daunting task, and integrating the many agencies and people of DSH into an integrated whole is an enormous undertaking.

Colleges and universities have much to offer in support of DHS’s mission. Science and technology can make significant contributions to all aspects of homeland security, and for some elements, like cybersecurity, science and technology are of central and crucial importance. In addition to conducting research that leads to new technologies, colleges and universities also educate the people who lead and staff homeland security functions. DHS has reached out to colleges and universities, but it needs to do more and find more ways to engage the academic community.

Q. You also serve as chair of the Academe, Policy and Research Senior Advisory Committee (APRSAC). What is the mission of that organization?

The APRSAC has a particularly broad mission among HSAC’s standing committees. It exists to serve DHS by analyzing and offering advice on timely policy issues, especially those with a research and educational component. Over the years, APRSAC has advised DHS on educational and training programs for homeland security, on risk assessment and management methodology, and on other issues.

Q. There is a growing concern that the United States has not done enough to safeguard cyber assets. What is your view on whether U.S. policy has taken sufficient steps to improve cybersecurity?

As president of Carnegie Mellon University, I am fortunate to be surrounded by some of the world’s leading experts on cybersecurity. The testimony that many of these faculty have provided to Congress and government agencies over the last decade has been sobering. Corporations, the security community, the academy, and policymakers have certainly responded, and in some ways, things have improved. But the major challenges of securing cyberspace remain or have intensified. And as technology changes, so must policy. As Pradeep Khosla, dean of Carnegie Mellon’s College of Engineering and founding director of Carnegie Mellon’s CyLab, stated in a recent white paper prepared for the White House cybersecurity chief, the device-centric approach that has dominated information security strategies until now is fundamentally flawed in a world in which both the number and the kinds of devices are proliferating so rapidly. Khosla argues instead for strategies and policies that take more of a “data-centric” approach to improve effectiveness and to ensure that the free flow of information is not impeded by a “moat and castle” model for security. Such proposed changes in approach exemplify the reality that as the landscape of use, research outcomes, and technologies change, policy will need to be revisited on a regular basis. Policymakers, industry leaders, and academics must partner more aggressively to ensure that policies and regulations accomplish our cybersecurity goals without unintended, deleterious consequences.

Q. What are Carnegie Mellon University and other institutions of higher education doing to make sure that the future workforce is capable of addressing this need for cybersecurity?

Carnegie Mellon, like many other colleges and universities, engages in a wide range of cybersecurity educational efforts, many of which are aligned with national efforts to provide the cybersecurity researchers and technical workforce for the future. For example, the National Security Agency and DHS jointly sponsor the Centers of Academic Excellence in Information Assurance Education and the Centers for Academic Excellence in Research programs. Carnegie Mellon has attained both designations for its interdisciplinary education and research programs in...
information assurance. Students enrolled in Carnegie Mellon and other designated schools are eligible to apply for scholarships through the Federal Cyber Service: Scholarship For Service (SFS) program. The SFS program is specifically designed to strengthen and increase the pool of information assurance professionals who protect the nation’s information technology infrastructure.

Carnegie Mellon has also used National Science Foundation funding for faculty fellowship programs, specifically the Information Assurance Capacity Building Program (IACBP). The IACBP is an intensive, in-residence summer program designed to help faculty build information assurance education and research capacity at their respective colleges and universities. The IACBP has produced tremendous results at colleges and universities across the nation, ranging from the creation of new courses, certifications, and degree programs to the development of grant proposals and publications. Several participating schools have been designated as Centers of Academic Excellence in Information Assurance Education. In addition, CERT, part of Carnegie Mellon’s Software Engineering Institute, offers courses and certifications in topics ranging from incident handling to information security management.

The wide range of cybersecurity educational activities at Carnegie Mellon reflects the complexity of the educational tasks. Colleges and universities are providing a combination of specialized education paths, for those who will focus on security, and broadened computer science, engineering, information systems, and management curricula that include education in many facets of cybersecurity.

Q. What steps are being taken by colleges and universities to address the research and development challenges for cybersecurity?

A very broad range of cybersecurity research is happening throughout the academy. At Carnegie Mellon, much of this research falls under CyLab, an interdisciplinary unit. Virtually every kind of cybersecurity issue is being researched somewhere at a college or university. For example, of particular concern for the United States is the fact that much of its physical infrastructure, like the power grid, is controlled by its cyberinfrastructure. Many research programs are addressing the threats created by this dependence, including efforts to develop a next-generation secure Internet.

The particular value of academic research is its ability to look further ahead than much of corporate research. Companies must find solutions that can ship next year. The academy, by contrast, can look at longer-term solutions that may ultimately have more impact. At Carnegie Mellon, we also tend to take more of an interdisciplinary approach—including issues of economics, human factors, and policy with technology—when we seek solutions to cybersecurity problems. For all these reasons, academic research on information security plays a critical role in the overall national effort to secure information and communications.

Q. Colleges and universities operate some of the world’s largest collections of computers and high-speed networks. What role does higher education as a sector need to play to make sure that its own cyber systems and networks are secure?

Higher education’s traditions of openness, decentralization, and entrepreneurship coupled with our distributed computing power, high-speed networks, electronic data stores, and intellectual property make us particularly vulnerable to cyber threats. Our educational mission, research, administrative and residential operations, internationalization, and funding dependencies place us at the crossroads of legal and regulatory requirements. Our challenge is to find the right balance, protecting and supporting the openness on which research, collaboration, and innovation depend while meeting our own high standards as well as external requirements for data protection and system survivability.

We can bridge the theoretical and the practical by applying our research to our operations. For example, five years ago Carnegie Mellon, informed by its cybersecurity research, created a dedicated office to coordinate an information security program. Since that time, various research collaborations have produced mutual benefits in such areas as phishing awareness, spam filtering, and malware analysis. Collaborating nationally, Carnegie Mellon supports the efforts of the higher education community at large to monitor, analyze, share, and respond to threats to individual and shared computing and networking infrastructures via the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC).

Finally, those of us in higher education must contribute our technical and policy expertise to the national and international agenda on cybersecurity. This is a critical part of our mission to transfer to society.

Q. What advice would you give to other institutional leaders about the importance of cybersecurity to the overall well-being and future of higher education?

Along with the leaders of many kinds of organizations, college and university presidents bear a basic responsibility to ensure that appropriate efforts are made to protect the personal information entrusted to their institutions. Although colleges and universities are devoted to the free exchange of ideas, the authors of those ideas have the right to control when and how they are communicated. Since the means of storage and communication of information are almost exclusively digital, assuring our communities that the new knowledge they create is under their control means we must effectively manage the complexities of cybersecurity. Unfortunately, securing our information and communications represents an added expense for something that does not contribute directly to our core missions. Thus, given the complexity of cybersecurity across multiple dimensions—technologies, organizations, and policies—perhaps the best advice I can give is that no institution should try to address all the issues alone. Higher education can and should expand its efforts to collaborate where possible to solve common challenges in cybersecurity in order to make those efforts as effective and cost-effective as possible.

Note

Jared Cohon is President of Carnegie Mellon University.