

Summary of Briefing to CSIS Commission on Cyber Security for the 44th Presidency

By Rodney Petersen and Jack Suess on behalf of the
EDUCAUSE/Internet2 IT Security Task Force

The briefing is available at <http://www.educause.edu/ir/library/pdf/CSD5363a.pdf>.

Introduction to the Higher Education Sector

1. The higher education sector is extremely diverse and complex, with over 6,000 colleges and universities, of which 4,200 are nonprofit organizations. It includes a system of private and public schools.
2. Higher education's interests and expertise with respect to cybersecurity:
 - a. Through its core mission of *teaching and learning*, it is the main source of our future leaders, innovators, and technical workforce.
 - b. Through *research*, it is the basic source of much of our new knowledge and subsequent technologies.
 - c. As complex institutions, colleges and universities *operate* some of the world's largest collections of computers and high-speed networks.
3. The EDUCAUSE/Internet2 Computer and Network Security Task Force works to improve information security and privacy across the higher education sector by actively developing and promoting effective practices and solutions for the protection of critical IT assets and infrastructures.

Successes and Challenges of the Past Five Years

1. Higher education as a sector is far more organized today than five years ago.
2. Cybersecurity is a much higher priority on campuses.
3. The community is actively developing and sharing effective practices and solutions.

Questions We Have Posed to the Higher Education Community

1. What role has the federal government played to improve cybersecurity these past few years that has been useful for the higher education sector?
2. Are there ways in which the federal government has hindered progress? If so, please describe.
3. Are there new initiatives you would like to see from the federal government to help improve cybersecurity?

Conclusions and Recommendations

1. Continue to invest in resources such as the FTC, NIST, NCSA, and US-CERT that will serve the government and nonprofit educational sector.
2. Strive for laws, regulations, standards, and guidelines that are more uniform in approach and less complex in execution.
3. Continue to exert pressure and influence on the IT sector to improve the security of products and services.
4. Make cybercrime a priority for federal criminal law enforcement.
5. Elevate the participation of higher education as a "critical asset" or "key resource" for purposes of cybersecurity preparedness and response.