GRADUATE CERTIFICATE IN CYBERSECURITY

The Graduate Certificate in Cybersecurity provides students with the knowledge and skills needed to face the ever-changing need for information management and security. Upon completion of the courses, students are able to identify enterprise and IT-related risks for organizations and evaluate their potential impact. Students learn how to evaluate weaknesses in an organization's IT controls and make recommendations to improve regulatory compliance, reporting, and operational performance. Students learn basic programming concepts, demonstrate the ability to set-up and troubleshoot hardware and software for a computer network, and gain significant "hands-on" experience in both attacking and defending virtual systems. This certificate is compatible with our MCIS degree requirements, enabling certificate recipients to transition into the MCIS program and apply it to their degree. It is also compatible with some of the MBA requirements, allowing some MBA students to earn the certificate as part of their MBA degree.

Students interested in graduate work should refer to the Graduate and Professional Bulletin (http://catalog.colostate.edu/general-catalog/graduate-bulletin/).

Learning Objectives

Students will:

1. Design, construct, and test business application software infrastructure, including hardware, operating software, and communications networks.
2. Demonstrate the ability to set up and troubleshoot hardware and software for a computer network in Linux and Windows.
3. Compare and contrast various approaches to networking and learn how to select the best type of network to implement in a given situation.
4. Identify system vulnerabilities and common security problems, configure VMWare, perform risk and cost benefit analysis, configure web protocols, secure servers, configure a firewall, install intrusion detection systems, and understand forensic procedures.
5. Demonstrate an awareness of enterprise risk and internal control systems and be able to evaluate an organization's vulnerability due to organizational and regulatory environments.