Cybersecurity Minor

Description
Cybersecurity is a hot topic in the world of information technology. We are faced with an increasing number of computer crime and computer-supported hacking activities. New technologies such as wireless communication and the Internet of Things will continue to develop and evolve, opening new threats to the industry - increasing the need for cybersecurity professionals and incident response teams. System hacking and cracking can range from theft of personal identity and data on up to hijacking system resources from the intended system users. Malware – computer viruses, worms, trojan horses, root kits, spyware and adware – are continuously obstructing everyday computer use. Cybersecurity personnel need to expand their understanding of computer security issues, system hacking and cracking, the nature of malware, forensic processes, and their understanding of investigative and preventive measures.

Students completing the Cybersecurity Minor program will be prepared to enter the field of cybersecurity in a public or private environment as computer security technicians, internet security analysts and computer forensics analysts. Individuals currently working in this or a related field will substantially enhance their knowledge and skills.

Cybersecurity Requirements (16 credits required)

CS 232	Cybersecurity System Administration	*(CS 105)*	4 cr	[FA]
CS 233	Cybercrime, Technology and Countermeasures	*(CS 232)*	4 cr	[WI]
CS 333	Computer Forensics	*(CS 216; CS 232; CS 233)*	4 cr	[FA]
CS 433	Cybersecurity	*(CS 333)*	4 cr	[WI]

Criminal Justice Requirements (3 credits required)

CJ 315	Private Security	*(None)*	3 cr

Legend:
Items in [ ] indicate semesters in which CSIS courses are offered
Items in ( ) indicate the prerequisites to a specific course