

EKU Cybersecurity Programs 2023-2024

Eastern Kentucky University's Digital Forensics and Cybersecurity bachelor's, master's levels and certificate programs offer students the knowledge and skills needed to fight cybercrimes and help public and private sector organizations avoid the devastating financial and reputation losses caused by data and information breaches.											
College	Program Title	Degree Level	Degree Designation	100% F2F	100% Distance Learning	F2F and Distance Learning	Min Credit Hours	Max Credit Hours	Employer advisory boards	Please list employers involved on advisory boards.	Please note any distinctive qualities of your academic programs (e.g. faculty recognition, research expertise, partnerships with employers).
Science, Technology, Engineering, and Mathematics	Computer Science	Baccalaureate	BS	Y	N	N	120	121	The EKU Department of Computer Science and Information Technology has one advisory board for the Computer Science and Digital Forensics and Cybersecurity programs.	SITEK, IBM, OpenText, Galmont Consulting, Alltech, Churchill Downs Interactive, Toyota, Wendell Willison Consulting, Lexmark, Kentucky State Policy Electronic Crime Branch, Suran Systems, Ashland, Cadre Information Security, eLink Design, Kentucky Employer's Mutual Insurance, RoundTower Technologies.	We have a partnership with the Department of Kentucky State Police which operates a fully functioning digital forensics lab on campus and accepts the students in the program for internships each semester. Dr. Shuangteng Zhang is a certified with ACE (AccessData Certified Examiner) that identifies individuals familiar with the FK Forensics Toolkit, the Password Recovery Toolkit, the FTK Imager, and the Registry Viewer. He also published two papers regarding forensic science in 2020. Dr. Lan Kong has completed AccessData Forensic Toolkit Basic training in 2021.
Science, Technology, Engineering, and Mathematics	Cyber Systems Technology	Baccalaureate	BS	Y	N	N	120	120	EKU has an advisory board for the Cyber Systems Technology BS, MS, and Certificate programs.	Kentucky Employers Mutual Insurance (KEMI), Centr Alert, Trane Technologies, Amazon, Expree Credit Union, Okonite, Matrix Team, Triveni Digital Eastern Kentucky University (EKU), Hitachi Astemo Electric Motor Systems America, Clark Regional Medical Center	The broad scope of the undergraduate technical program prepares students through foundational laboratory- and project- based experiences to support, administer, maintain, secure, and manage computer networks and electronic systems. Graduates work in a broad range of industrial sectors spanning healthcare, education, mining, manufacturing, banking and insurance, web, print, and publishing servies, security of cyber systems, military and government, supporting the software and hardware IT infrastructure. In the past two academic years, over 91% of the BS degree grads have completed an advisor approved IT certification.
Science, Technology, Engineering, and Mathematics	Technology Management- Cyber System Technology Security Concentration	Master's	MS	Y	Y	N	30	30	EKU has an advisory board for the Cyber Systems Technology BS, MS, and Certificate programs.	Kentucky Employers Mutual Insurance (KEMI), Centr Alert, Trane Technologies, Amazon, Expree Credit Union, Okonite, Matrix Team, Triveni Digital Eastern Kentucky University (EKU), Hitachi Astemo Electric Motor Systems America, Clark Regional Medical Center	The holistic nature of these undergraduate and graduate technical programs prepares students through foundational laboratory- and project- based experiences to support, administer, maintain, secure, and manage computer networks and electronic systems. Graduates work in a broad range of industrial sectors spanning healthcare, education, mining, manufacturing, banking and insurance, web, print, and publishing servies, security of cyber systems, military and government, supporting the software and hardware IT infrastructure. The MS degree concentration emphasizes the planning, implementation, and management of technology related projects, including the security of cyber systems in various environments.

Science, Technology, Engineering, and Mathematics	Computer Science-Cyber Security Concentration	Master's	MS	Y	Y	N	30	30	The EKU Department of Computer Science and Information Technology has one advisory board for the Computer Science and Digital Forensics and Cybersecurity programs.	SITEK, IBM, OpenText, Galmont Consulting, Alltech, Churchill Downs Interactive, Toyota, Wendell Willison Consulting, Lexmark, Kentucky State Policy Electronic Crime Branch, Suran Systems, Ashland, Cadre Information Security, eLink Design, Kentucky Employer's Mutual Insurance, RoundTower Technologies.	We have a partnership with the Department of Kentucky State Police which operates a fully functioning digital forensics lab on campus and accepts the students in the program for internships each semester. Dr. Shuangteng Zhang is a certified with ACE (AccessData Certified Examiner) that identifies individuals familiar with the FK Forensics Toolkit, the Password Recovery Toolkit, the FTK Imager, and the Registry Viewer. He also published two papers regarding forensic science in 2020. Dr. Lan Kong has completed AccessData Forensic Toolkit Basic training in 2021.
Justice, Safety, and Military Science	Security Management	Undergraduate Certificate 9-29 semester credit hours	UCERT6	Y	Y	N	24	24	The Security Management Certificate does not have an advisory board.	We do not have a formal advisory board, but rather consult with professionals from the U.S. Dept. on Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) and others here in Kentucky, and keep abreast of cybersecurity threats and responses as published by DHS and through the work of other academic partners such as the Center for Homeland Defense and Security. Specifically, we have met multiple times with Mr. Colin Glover, DHS Cybersecurity Advisor for Kentucky. Some of our adjunct instructors who work in law enforcement are familiar with cybersecurity topics; this includes an IT professional who works for the Dept. of Criminal Justice Training.	A distinctive quality of our programs is the view of cybersecurity in relation to physical security and critical infrastructure security and resilience more broadly. Physical and cyber systems operate in tandem, so vulnerabilities to one have cascading impacts on the other. As such, we promote systems thinking in our courses when conducting comprehensive risk assessments, which evaluate threats/hazards, vulnerabilities, and consequences. Another distinctive quality of our programs is the focus on understanding the cyber threat environment such as how international terrorist and domestic groups use the web to advance their ideologies, how nation states carry out cyberattacks, and how others conduct criminal activity online. This threat environment is complex and increasing in significance for those who work in governments and the private sector, as well as individuals and their families. Finally, the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST organizes cybersecurity functions under seven categories. The EKU Homeland Security program primarily addresses the Oversee and Govern, and Protect and Defend categories (two of seven). We educate security managers, intelligence analysts, and emergency managers who need a basic situational awareness of cyber threats and responses, especially those relating to organizational policies and procedures. As such, we focus our programming at this managerial level. The courses that support the Certificate in Intelligence Studies reach into the Analyze and Collect and Operate areas to some degree.

Justice, Safety, and Military Science	Intelligence Studies	Undergraduate Certificate 9-29 semester credit hours	UCERT6	Y	Y	N	24	24	The Intelligence Studies Certificate does not have an advisory board.	We do not have a formal advisory board, but rather consult with professionals from the U.S. Dept. on Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) and others here in Kentucky, and keep abreast of cybersecurity threats and responses as published by DHS and through the work of other academic partners such as the Center for Homeland Defense and Security. Specifically, we have met multiple times with Mr. Colin Glover, DHS Cybersecurity Advisor for Kentucky. Some of our adjunct instructors who work in law enforcement are familiar with cybersecurity topics; this includes an IT professional who works for the Dept. of Criminal Justice Training.	A distinctive quality of our programs is the view of cybersecurity in relation to physical security and critical infrastructure security and resilience more broadly. Physical and cyber systems operate in tandem, so vulnerabilities to one have cascading impacts on the other. As such, we promote systems thinking in our courses when conducting comprehensive risk assessments, which evaluate threats/hazards, vulnerabilities, and consequences. Another distinctive quality of our programs is the focus on understanding the cyber threat environment such as how international terrorist and domestic groups use the web to advance their ideologies, how nation states carry out cyberattacks, and how others conduct criminal activity online. This threat environment is complex and increasing in significance for those who work in governments and the private sector, as well as individuals and their families. Finally, the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST organizes cybersecurity functions under seven categories. The EKU Homeland Security program primarily addresses the Oversee and Govern, and Protect and Defend categories (two of seven). We educate security managers, intelligence analysts, and emergency managers who need a basic situational awareness of cyber threats and responses, especially those relating to organizational policies and procedures. As such, we focus our programming at this managerial level. The courses that support the Certificate in Intelligence Studies reach into the Analyze and Collect and Operate areas to some degree.
Science, Technology, Engineering, and Mathematics	Digital Forensics and Cybersecurity	Baccalaureate	BS	Y	N	N	120	120	The EKU Department of Computer Science and Information Technology has one advisory board for the Computer Science and Digital Forensics and Cybersecurity programs.	SITEK, IBM, OpenText, Galmont Consulting, Alltech, Churchill Downs Interactive, Toyota, Wendell Willison Consulting, Lexmark, Kentucky State Policy Electronic Crime Branch, Suran Systems, Ashland, Cadre Information Security, eLink Design, Kentucky Employer's Mutual Insurance, RoundTower Technologies.	We have a partnership with the Department of Kentucky State Police which operates a fully functioning digital forensics lab on campus and accepts the students in the program for internships each semester. Dr. Shuangteng Zhang is a certified with ACE (AccessData Certified Examiner) that identifies individuals familiar with the FK Forensics Toolkit, the Password Recovery Toolkit, the FTK Imager, and the Registry Viewer. He also published two papers regarding forensic science in 2020. Dr. Lan Kong has completed AccessData Forensic Toolkit Basic training in 2021.
Science, Technology, Engineering, and Mathematics	Cyber Systems & Network Security	Undergraduate Certificate 9-29 semester credit hours	UCERT6	Y	Y	Y	24	24	EKU has an advisory board for the Cyber Systems Technology BS, MS, and Certificate programs.	Kentucky Employers Mutual Insurance (KEMI), Centr Alert, Trane Technologies, Amazon, Expree Credit Union, Okonite, Matrix Team, Triveni Digital Eastern Kentucky University (EKU), Hitachi Astemo Electric Motor Systems America, Clark Regional Medical Center	Tightly focused technical course activities provide students with opportunities support, administer, maintain, secure, and manage computer electronic networks, devices, and systems in lab-based environments.

Science, Technology, Engineering, and Mathematics	Cyber Security and Digital Forensics	Post-Baccalaureate Certificate	GCERT1	Y	Y	Y	12	15	The ECU Department of Computer Science and Information Technology has one advisory board for the Computer Science and Digital Forensics and Cybersecurity programs.	SITEK, IBM, OpenText, Galmont Consulting, Alltech, Churchill Downs Interactive, Toyota, Wendell Willison Consulting, Lexmark, Kentucky State Policy Electronic Crime Branch, Suran Systems, Ashland, Cadre Information Security, eLink Design, Kentucky Employer's Mutual Insurance, RoundTower Technologies.	We have a partnership with the Department of Kentucky State Police which operates a fully functioning digital forensics lab on campus and accepts the students in the program for internships each semester. Dr. Shuangteng Zhang is a certified with ACE (AccessData Certified Examiner) that identifies individuals familiar with the FK Forensics Toolkit, the Password Recovery Toolkit, the FTK Imager, and the Registry Viewer. He also published two papers regarding forensic science in 2020. Dr. Lan Kong has completed AccessData Forensic Toolkit Basic training in 2021.
Business	Financial Technology and Cybercrime	Undergraduate Certificate 9-29 semester credit hours	UCERT6	Y	Y		21	21	The Certificate in Financial Technology and Cybercrime is an interdisciplinary University Certificate between the College of Business and the College of Justice, Safety, and Military Science, housed in the Evans Banking and Financial Services Program. While there is no formal advisory board for this certificate, the two colleges held an industry roundtable session early in the process of developing the certificate to receive direction from industry experts on what type of academic program is needed in our region to meet the needs of industry. We have worked closely with multiple government agencies and industry employers in different phases of the development of the certificate.	There is no advisory board specifically for the certificate. Some members of the College of Business Advisory Board and the Evans Banking and Financial Services Program Advisory Board have provided valuable input for the development of the certificate. The following agencies, industry partners, and individuals have provided us valuable feedback on current industry needs related to the development of the certificate: U.S. Congressman Andy Barr's Office – Megan Guillinan, Financial Services Policy Advisor Kentucky Department of Financial Institutions – Kentucky Commissioner of Banking Several community and regional banks Commonwealth Credit Union ISACA – Information Systems Audit and Control Association U.S. Secret Service Department of Homeland Security	The Certificate in Financial Technology and Cybercrime is supported by a Professorship gifted by Commonwealth Credit Union because they feel strongly about the need for more banking professionals having an understanding of cybersecurity controls, cybercrime, and financial technology. To ensure the content in the courses remains current and relevant to current issues that industry is facing, we are partnering with ISACA, a national association that specializes in continuing education for IT and cybersecurity professionals, to assist in providing content for the capstone courses in the certificate. Additionally, professors with industry experience are selected to teach the capstone courses in the certificate. In addition to traditional/current students enrolling in the Certificate, we have a partnership with the KY Department of Financial Institutions, which is sending multiple employees each year to enroll in the certificate.

Justice, Safety, and Military Science	Cyber and Security Management		GCERT I					The Cybersecurity Management Certificate does not have an advisory board.	We do not have a formal advisory board, but rather consult with professionals from the U.S. Dept. on Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) and others here in Kentucky, and keep abreast of cybersecurity threats and responses as published by DHS and through the work of other academic partners such as the Center for Homeland Defense and Security. Specifically, we have met multiple times with Mr. Colin Glover, DHS Cybersecurity Advisor for Kentucky. Some of our adjunct instructors who work in law enforcement are familiar with cybersecurity topics; this includes an IT professional who works for the Dept. of Criminal Justice Training.	A distinctive quality of our programs is the view of cybersecurity in relation to physical security and critical infrastructure security and resilience more broadly. Physical and cyber systems operate in tandem, so vulnerabilities to one have cascading impacts on the other. As such, we promote systems thinking in our courses when conducting comprehensive risk assessments, which evaluate threats/hazards, vulnerabilities, and consequences. Another distinctive quality of our programs is the focus on understanding the cyber threat environment such as how international terrorist and domestic groups use the web to advance their ideologies, how nation states carry out cyberattacks, and how others conduct criminal activity online. This threat environment is complex and increasing in significance for those who work in governments and the private sector, as well as individuals and their families. Finally, the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST organizes cybersecurity functions under seven categories. The ECU Homeland Security program primarily addresses the Oversee and Govern, and Protect and Defend categories (two of seven). We educate security managers, intelligence analysts, and emergency managers who need a basic situational awareness of cyber threats and responses, especially those relating to organizational policies and procedures. As such, we focus our programming at this managerial level. The courses that support the Certificate in Intelligence Studies reach into the Analyze and Collect and Operate areas to some degree.
---------------------------------------	-------------------------------	--	---------	--	--	--	--	---	--	---

Please describe basic or applied research efforts at your institution related to cybersecurity.

EKU Homeland Security faculty have conducted basic research and published the following two books that address cybersecurity among other topics:

Baggett, R. & Simpkins, B. (2018). Homeland Security and Critical Infrastructure Protection, Second Edition. Praeger Security International.

Baggett, R., Foster, C. & Simpkins, B. (2017). Homeland Security Technologies for the 21st Century. Praeger Security International.

In addition, as ECU Finance faculty members prepare to teach a new course, Financial Technology and Security, they are recognizing research opportunities. Future research initiatives include the impact of cybersecurity on bank valuation, acquisitions of fintech targets, and market reaction of including cybersecurity in non-financial public companies.

The faculty and students in the Digital Forensics and Cybersecurity program have been conducting research in the area of Digital Forensics and Cybersecurity. Some of the research projects include: A New Botnet Command & Control Mechanism Using Ethereum Platform, Steganography Detection Using Machine Learning (ML), Instagram Forensic Artifacts on Windows® Systems, Known Source Artifacts Examination with Digital Forensic Tools, and Blockchain Exposure Using Worms.

Please describe any cybersecurity needs assessments that have been conducted in your region or at the state level that have informed your academic programming and research efforts.

The Center for Homeland Defense and Security has a wealth of information on cybersecurity needs as a salient topic, and we keep abreast of the resources published both here and made available by DHS CISA.

In collaboration with the Kentucky Bankers Association, two faculty members conducted a survey of Kentucky banks related to cybersecurity practices and needs. Results of this research were published as a KBA White Paper and were presented during the 2022 KBA Convention. This research laid the foundation for subsequent development of the Financial Technology and Cybercrime Certificate.

In 2017, the Digital Forensics and Cybersecurity Institute in the Department of Computer Science and Information Technology conducted a thorough cybersecurity needs assessments at the state level which resulted in the creation of the BS degree program in Digital Forensics and Cybersecurity.