CYBERSECURITY
AND DATA PRIVACY
CERTIFICATION PROGRAM
Powered by Southern University Law Center

Charles Winnsboro
AFRICA, UNCHAINED

Cybersecurity and Data Privacy – Spring 2023

The objective of this course is to introduce students to cybersecurity and data privacy. The field is incredibly vast and diverse, encompassing a wide range of disciplines and careers. Some of the most common careers in this field include cybersecurity analysts, information security managers, data privacy professionals, cyber risk analysts, forensic analysts, and penetration testers.

One of the key areas of focus for cybersecurity and data privacy professionals is the protection of data. Data breaches can have severe consequences for organizations, including financial losses, damage to reputation, and loss of customer trust. Cybersecurity and data privacy professionals must have a thorough understanding of data protection laws and regulations, including the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States.

Another important aspect of cybersecurity and data privacy is incident response planning. Incident response plans (IRPs) are critical for organizations to have in place in the event of a data breach or other security incident. An IRP outlines the steps that an organization should take in the event of a security incident, including identifying the incident, containing it, investigating it, and restoring normal operations.

In addition to protecting data and developing incident response plans, cybersecurity and data privacy professionals also need to be knowledgeable about emerging threats and technologies. For example, the rise of the Internet of Things (IoT) has created new security risks, as more and more devices become connected to the internet.

Finally, cybersecurity and data privacy professionals must be able to communicate effectively with both technical and non-technical stakeholders. They must be able to explain complex technical issues in simple terms and be able to communicate the importance of data protection to business leaders.

In this course, you will learn about data protection laws and regulations, incident response planning, emerging threats and technologies, and effective communication with stakeholders. The course consists of an introductory week, three two-modules, and a capstone week. The first module covers data privacy and cybersecurity in the United States; the second, data privacy and cybersecurity in Europe (GDPR); and the third, data privacy and cybersecurity in select African countries. Throughout the modules, you will be working on a business case that requires you to adjust your fictional company's policies in response to a data breach. As you learn more about each region's laws and processes, you will be given additional facts and asked to further refine your policies. The capstone week is for you to prepare and finalize an Incident Response Plan that reflects everything you've learned.

[See following pages for a week-by-week overview of the course]

Cybersecurity and Data Privacy – Spring 2023

Section	Weeks		Description	Timeframe**
Overview	Week 1	Introduction to Cybersecurity & Data Privacy	This week introduces participants to cybersecurity and data privacy. Data privacy is defined and the sources and classification of data is described. Cybersecurity is defined and common threats and vulnerabilities are discussed. Participants are introduced to the fictitious company they'll work for over the next eight weeks.	May 8, 2023
Module 1: US Data Privacy & Cybersecurity	Week 2	Digital Privacy and Security Protections Under American Law	This week provides participants with an overview of US Data Protection and Privacy laws created to protect privacy and cybersecurity with a discussion of the American legal system and review of the origins of privacy protection in the US Constitution.	May 15, 2023
	Week 3	Applying US Data Protection and Privacy Law	This week participants will have an opportunity to apply what they've learned to begin development of their IRP. During this week participants also meet with the professors during office hours to review concepts learned in this section.	May 22, 2023
Module 2: European Data Privacy & Cybersecurity	Week 4	Overview of General Data Protection Regulation (GDPR)	This week introduces participants to the General Data Protection Regulation. The types of data that are protected are discussed and individual data rights for EU residents are explored.	May 29, 2023
	Week 5	Impact of GDPR Around the World	This week participants review eCommerce Privacy Policy and the impact of GDPR. Students apply GDPR rules to their IRPs and meet with professors.	June 5, 2023
Module 3: Data Privacy Laws in Africa	Week 6	Overview of Data Privacy Laws in Africa	This week introduces participants to data privacy laws in sub-Saharan Africa. The laws of several African countries are explored in a survey format, and commonalities and differences are highlighted. The African Continental Free Trade Agreement (AfCFTA) is introduced.	June 12, 2023

Cybersecurity and Data Privacy – Spring 2023

Section	Weeks		Description	Timeframe**
	Week 7	The State of Cybersecurity in Africa	This week follows up on the preceding week and analyzes the current state of cybersecurity in sub-Saharan Africa. Potential threats, challenges and opportunities are explored, including among others the IT adoption rate, crypto and other scams, and the transformative potential of AfCFTA.	June 19, 2023
Capstone	Week 8	Wrap-up and Capstone	This week participants complete their IRPs and submit their presentations. Office hours are available this week.	June 26, 2023

Technology requirements: To complete this course, participants must have access to a laptop, desktop, or other computing device that has MS Office at a minimum. Additionally, participants will be required to record a presentation and will need some type of recording device that at least has audio – i.e. computer, cell phone.

Learning requirements: To earn a Certificate of Completion from Southern University Law Center, participants must thoughtfully complete materials for all eight weeks, including "**Met**" expectations of the associated assignments by stated guidelines.