UCLA Extension

CYBER SECUTITY certificate
16 UNITS - 3 MONTHS

To ensure that our programs and courses reflect the most current and relevant academic content, **you will be required to complete your program requirements within five years,** including any courses taken prior to establishing candidacy if you wish them to count toward your requirements.

Learn essential cybersecurity skills in our 4-course Cybersecurity Certificate. Quickly gain the knowledge you need to protect your technology infrastructure from physical and virtual threats.

This program is perfect for...

- IT professionals looking to advance into the cybersecurity area
- Managers who oversee a security team, and want a higher level understanding of cybersecurity
- Those in the technology field who want to learn about securing networks, infrastructure, and how to defend against cyber attacks
- Entrepreneurs who want to mitigate their cybersecurity risk by avoiding common pitfalls in security

What you can learn.

- Learn about securing applications, cryptography, common attack vectors, cyber attacks, and exploits
- Hands-on experience with OSI stack security, hacking methodology and mitigation, penetration testing, and defensive strategies
- Create security policies, risk assessments, disaster recovery plans and post attack protocols, and procedures
- Learn concepts needed for the CISSP, CCNA, CompTIA, and other certifications

UCLA Extension

About this certificate.

Cybersecurity is an essential component of every organization. The risks involved in a cyber attack include loss of data, intellectual property, brand equity, and possible legal ramifications. Understanding how cyber attacks happen is your best defense against them. Whether you're an entrepreneur who wants to protect your business against cyber intrusions, or you manage people responsible for cybersecurity, our Cybersecurity Certificate will quickly give you the knowledge you need. Our courses are taught by industry experts who are up-to-date on the latest trends in cybersecurity.

Courses

1 course = 4 units

Required Courses 4

Fundamentals of Cybersecurity COM SCI X 420.1

This course combines theoretical security models with practical examples for a comprehensive intro and should benefit auditors, system administrators, or anyone else with a basic understanding of information technology.
Topics include security policies, risk analysis, cryptography, and network security. Course material is consistent with relevant portions of the Certified Information System Security Professional (CISSP) certification exam's Common Body of Knowledge (CBK).

- Understand the role of a security policy and how an organization can manage information security
- Understand how security relates to risk and the role of risk analysis
- Understand the strengths and weaknesses of various authentication methods
- Understand how proper software development can reduce security risks, and describe the types of vulnerabilities poorly written software can experience
- Understand the importance of hardware security mechanisms in enforcing all other technical security controls
- Know how the various layers of the network protocol stack contribute to security

UCLA Extension

Information Systems Infrastructure Security Management COM SCI X 420.3

This security course covers physical and logical security over data centers and offices. It defines a management program that protects assets across all levels of tech and core components that support that technology.
In addition, the course analyzes hacking methodology and how to create a functioning IT Infrastructure program for businesses, whether large or small, and includes change management scenarios and how to approach daily business security issues from an IT perspective. Much of the challenge of IT security remains the fundamental fact that management does not see it as a profit center, and as long as there has been no reported breach, there is clearly nothing to worry about. With this as a starting point, you investigate how best to explore the myriad options for network security.

- Create, develop, test, and maintain a disaster recovery and business resumption plan for a client
- Identify and plan for threats to the information infrastructure
- Learn how to successfully conduct a risk assessment

Network, Operating System, and Database Security COM SCI X 420.5

This course delivers a step-by-step methodology to secure any infrastructure by enhancing defenses to the core components of networks and databases, integrating cyber threat/risk management, defense-in-depth, and more.
Cyber-based attacks and data breaches are a critical risk for organizations of any size. Effective defenses to the cyber threat are usually not well-understood or applied. This course delivers a step-by-step methodology to secure any infrastructure by enhancing defenses to the core components of networks, operating systems, and databases. The approach integrates cyber threat and risk management, defense-in-depth, network monitoring, cloud, and mobile devices. Also provides effective strategies for security testing, mitigating the insider threat, and recovering from a security incident. Current events case studies illustrate key concepts. Cyber defense techniques are demonstrated in computer and DIY device (Beaglebone) labs. Final project enables students to apply the methodology to secure an infrastructure of their choice. This course is relevant for security and IT professionals, students, technical users, management, and anyone seeking an understanding of the key principles of cyber defense.

- Identify motivations and tactics for the major categories of cyber threat actors
- Recognize common types of cyber attacks and exploits
- Demonstrate understanding of risk management as it applies to information security management
- Apply lessons learned from an APT case study
- Demonstrate a basic understanding of modern network protocols
- Identify the components of an enterprise network architecture

UCLA Extension

Cybersecurity Lab (Defensive Tools) COM SCI X 420.9

This hands-on course introduces defensive methodology and tools. Defensive security practices require a strong understanding of current risks and exploits. Leveraging the knowledge acquired from the Information System Security Lab (offensive tools), this course builds on the remediation strategies for thwarting off active offensive attacks. This course introduces core defensive strategies for various environment types and provides hands-on experiences of security defensive tools.

- Be familiar with what to look for while on the defensive side of the Cyber game, the tools used to detect and prevent attacks, and the underlying protocols used in order to do so.
- Build a layered defense architecture to test with
- Add web servers, intrusion detection and firewalls to your test network
- Deploy honeypots and decoys on your network

options

- Optional Internship Elective
- COM SCI X 460.100 Digital Technology Internship may be taken as an optional elective course. It is not required for the certificate.
- Digital Technology Internship
- COM SCI X 460.100
- Typically Offered: Fall, Winter, Spring, Summer

INSTRUCTORS

Vincent LEVEQUE : MS, business information security officer, AIG
Gary SEVELIN : MS, information systems security officer, U.S. Department of Defense, U.S. Special Operation Command
Wayne WHEELER : MS, Senior Security Analyst, Aerospace Corporation