



**ITPRO.TV**

# **Cybersecurity Course Guide**

**College**



**WILEY**

# Associate's Degree (A.A.S.) in Cybersecurity

## Program Description

The Cybersecurity A.A.S. program provides students with a core set of competencies in information systems security necessary to manage and safeguard the technological infrastructure of organizations from both internal and external threats. Students' competencies will be developed through courses encompassing both network administration and business. The program also focuses on industry experience through an extensive externship opportunity.

*Note: This program is based on 60-70 credit hours with 35-40 credits in major area. The credit/clock hours are flexible. The program length is 5 full-time semesters.*



## Program Objectives

Upon completion of the program, students will be able to:

1. Understand how to troubleshoot a computer system and how hardware and software work together.
2. Produce professional business documents using various computer applications.
3. Understand network protocols.
4. Identify and troubleshoot computer and network security software issues.
5. Understand networking theory and concepts as applied to information systems security as well as the OSI model and TCP/IP security concerns.
6. Implement information systems security policies and procedures.
7. Recognize and solve business problems through project management and team-building.
8. Communicate effectively both in writing and orally.
9. Practice information technology security competencies and related skills in the field.



Click on an ITProTV course to learn more.

## SEMESTER I

### Introduction to Computers and Business Applications

This course introduces basic elements of the computer system. Topics include: file management; database management; word processing; spreadsheets; email; web browser applications; and computer concepts, language and terms. Students will practice hands-on exercises for basic proficiency using computer hardware and software.

*Prerequisite: none*

IT Fundamentals-FC0-U51 ▶  
MTA Windows Operating System  
Fundamentals-98-349 ▶

### Introduction to Networking

This course provides foundational knowledge in local area networks (LANs), including networking topologies and media, the Open Systems Interconnect (OSI) model, Transmission Control Protocol/Internet Protocol (TCP/IP), network design and implementation, and intermediate routing and switching principles.

*Corequisite: Introduction to Computers and Business Applications*

CCENT Course Subtitle: Cisco Certified  
Entry Networking Technician ▶  
GIAC Security Essentials ▶  
A+ 900 Series ▶  
Network+- N10-006 ▶  
MTA - Windows Operating System  
Fundamentals - 98-349 ▶  
CCENT Course Subtitle: Cisco Certified  
Entry Networking Technician ▶

### Computer Hardware and Software

This course explores PC hardware and software installation and configuration. Hardware topics include: system boards and memory; computer processors; I/O boards and devices; CMOS configuration; storage devices; printers; and PC networking hardware. Software topics include: installations and configuration of various applications; and basic client/server software installation and configuration.

*Corequisite: Introduction to Computers and Business Applications*

IT Fundamentals Overview ▶  
Network+- N10-006 ▶  
A+ 900 Series ▶

## SEMESTER II

### Information Systems Security Foundations

This course introduces students to basic information systems security concepts and issues. Students learn the importance of information systems security to the overall mission of organizations, including best security practices related to organizational policies, procedures, and standards. The importance of user training, auditing, risk analysis, and disaster recovery related to information systems security will be covered. Ethical implications related to network security, including ethical hacking, will also be explored.

*Prerequisite: Introduction to Computers and Business Applications*

Security Fundamentals Course Subtitle:  
Core Security Concepts ▶  
Security Fundamentals ▶  
Security+-SY0-401 ▶  
CCNA-210-260 ▶  
CompTIA Advanced Security  
Practitioner Course Subtitle: CASP ▶  
CISA Course Subtitle: Certified Information  
Systems Auditor ▶  
System Center 2012 Configuration  
Manager-70-243 ▶

## Network Administration I

This course requires students to use Microsoft Windows operating systems to manage local and wide area networks. Students will install and configure a Windows server operating system on both the client and server sides as well as configure it for various services, including file and print sharing, remote access services, terminal services and Active Directory. Additional Windows features and security will also be covered.

*Corequisite: Introduction to Networking*

Network+- N10-006 ▶  
 MCSA Windows 7-70-680 ▶  
 MCSA Windows 7-70-680 ▶  
 MCSA Windows 8.1-70-687 ▶  
 MCSA Windows 8.1-70-688 ▶  
 MCSA Windows 10-70-697 ▶  
 MCSA Windows 10-70-698 ▶  
 MCSA Windows Server 2012-70-410 ▶  
 MCSA Windows Server 2012-70-411 ▶  
 MCSA Windows Server 2012-70-412 ▶

MCSA Windows Server 2016-70-740 ▶  
 MCSA Windows Server 2016-70-741 ▶  
 PowerShell ▶  
 Supporting Windows 7 ▶  
 Windows 10 Security ▶  
 CCENT Course  
 Subtitle: Cisco Certified Entry  
 Networking Technician ▶  
 System Center 2012 Configuration  
 Manager-70-243 ▶

## Computer Forensics

This course provides students with instruction in current and emerging issues and trends that have significance in computer forensics. Through the use of course activities, students will investigate and analyze computer and network security breaches, applicable security standards, protocols, and laws. Topics will include an assortment of computer-related crimes, legal and ethical issues, securing computerized systems, electronic evidence, and data storage and retrieval.

*Prerequisite: Introduction to Networking*

CHFI v8 ▶  
 Digital Forensic Investigator ▶

## SEMESTER III

### Internal Network Protection

This course explores safeguarding a network from malicious intent from the internal network perspective. Students will learn how to implement internal intrusion detection methods using a variety of hardware and software to help secure a network from unauthorized employees or others with malicious intent. Topics include firewall configuration, hacking methods, network intrusion detection utilities, access control and auditing, and virtual private network intrusion detection and prevention.

*Prerequisite: Network Administration I*

CEH v9 ▶  
 CHFI v8 ▶  
 CCNA Security 640-554 Course Subtitle:  
 Cisco Certified Network Associate Security ▶

### Wireless Network Technology I

This course introduces wireless networking technology from both the hardware and software perspectives. In a lab environment, students learn how to connect, troubleshoot and secure wireless networking components using associated networking hardware and software. Current wireless networking protocols are discussed as well as emerging wireless protocols and technology in relation to mobile device security.

*Prerequisite: Network Administration I*

A+ 900 Series Course Subtitle: 900 Series ▶  
 Security+ ▶  
 CHFI v8 ▶  
 CEH v8 ▶  
 MTA - Mobility and Devices Fundamentals  
 - 98-368 ▶  
 A+ 900 Series ▶

### Information Assurance Foundations

This course introduces students to various information technology network threats that can derive through several mediums. Students will analyze threats that can exist through hacking, web-based scripting, operating system vulnerabilities, database design flaws, and web browser and e-mail client vulnerabilities. Other internet and network security topics will also be explored, including internet protocol (IP) security, encryption, user authentication, protocols, security-suite software, and firewalls. Securing mobile devices using a variety of related technologies will also be discussed.

*Prerequisite: Information Systems Security Foundations*

CyberSec First Responder ▶  
 Security+-SY0-401 ▶  
 CEH v8 ▶  
 CEH v9 ▶  
 SSCP ▶

## SEMESTER IV

**Operating Systems Security**

This course introduces students to security issues related to both Microsoft Windows-based and Linux-based network operating systems. Students will learn to configure and test various security settings in both systems while recognizing the similar and unique security vulnerabilities of each system. Students will explore file system security, auditing and logging, access control methods and other related security services and tools.

*Prerequisite: Network Administration I*

- MCSA Windows 7-70-680 ▶
- MCSA Windows 8.1-70-687 ▶
- MCSA Windows 8.1-70-688 ▶
- MCSA Windows 10-70-697 ▶
- MCSA Windows 10-70-698 ▶
- MCSA Windows Server 2012-70-410 ▶
- MCSA Windows Server 2012-70-411 ▶
- MCSA Windows Server 2012-70-412 ▶
- MCSA Windows Server 2016-70-740 ▶
- MCSA Windows Server 2016-70-741 ▶
- PowerShell ▶
- Supporting Windows 7 ▶
- Windows 10 Security ▶
- Linux+ Course Subtitle: Powered by LPI ▶
- Kali Linux ▶
- SSCP ▶
- Mac Integration Basics 10.9 ▶
- Certified Support Professional 10.10 ▶
- Certified Technical Coordinator 10.10 ▶
- Mac Management Basics 10.11 ▶
- Mac Integration Basics 10.11 ▶
- Certified Support Professional 10.11 ▶
- Certified Technical Coordinator 10.11 ▶
- Certified Technical Coordinator 10.11 ▶

**Perimeter Network Protection**

This course explores network security infrastructure issues. Students will learn how to design and implement network infrastructure defenses. Topics include firewall configuration, authentication and access, load-balancing, wireless access, transport protocols, and domain name systems. Internet, e-mail, hacking, and other web security threats will be addressed as well as the strategies to detect and defend against these vulnerabilities.

*Prerequisite: Network Administration I*

- MTA - Security Fundamentals - 98-367 Course Subtitle: Security Fundamentals ▶
- Cisco ASA Express Security ▶
- CCNA Security Course Subtitle: Cisco Certified Network Associate Security ▶
- CCNA Security 640-554 Course Subtitle: Cisco Certified Network Associate Security ▶
- pfSense (2016) Course Subtitle: pfSense build 2.3.2 ▶
- CEH v9 ▶
- CHFI v8 ▶

**Information Technology Disaster Prevention and Recovery I**

This course covers the planning, prevention and recovery from events that can threaten organizations' vital technology assets and associated business functions. Students learn best-case planning strategies, while developing disaster prevention methods and necessary recovery plans. Throughout the course, students will review industry case studies and practice both feed-forward and feedback controls.

*Prerequisite: Information Assurance Foundations*

- CHFI v8 ▶
- CASP-CAS-002 ▶
- Security+-SY0-401 ▶
- Eliminating Malware ▶
- Working with SSH ▶
- Certified Information Systems Security Professional (UPDATED 2016) Course Subtitle: CISSP ▶

## SEMESTER V

**Externship**

This is the capstone course in the Cybersecurity Associate of Applied Science program. Students practice essential network security skills while being supervised in a real-world information technology environment.

*\*Required in last semester only\**

# Bachelor's Degree (B.S.) in Cybersecurity

## Program Description

The Cybersecurity B.S. program provides students with skills in computer networking, information systems security and business. Students' competencies will be developed through several core areas encompassing information systems security from both internal and external threats and its relation to both network administration and business. The program prepares students in information systems security management, network administration and business concepts. Project management and its relation to information systems security are also explored. The program includes requisite industry experience through an extensive externship opportunity.

*Note: This program is based on 120-130 credit hours with 60-65 credits in major area. The credit/clock hours are flexible. The program encompasses 8 full-time semesters.*



## Program Objectives

Upon completion of the program, students will be able to:

1. Understand how to troubleshoot a computer system and how hardware and software work together.
2. Produce professional business documents using various computer applications.
3. Understand network protocols.
4. Identify and troubleshoot computer and network security software issues.
5. Understand networking theory and concepts as applied to information systems security as well as the OSI model and TCP/IP security concerns.
6. Perform enterprise information systems risk assessment, identify security vulnerabilities, develop security policies, and implement security plans to safeguard information technology assets.
7. Implement information systems security policies and procedures.
8. Recognize and solve information systems security problems through advanced project management and team-building.
9. Communicate effectively both in writing and orally.
10. Practice information technology security competencies and related skills in the field.



Click on an ITProTV course to learn more.

## SEMESTER I

### Introduction to Computers and Business Applications

This course introduces basic elements of the computer system. Topics include: file management; database management; word processing; spreadsheets; email; web browser applications; and computer concepts, language and terms. Students will practice hands-on exercises for basic proficiency using computer hardware and software.

*Prerequisite: none*

IT Fundamentals-FC0-U51 ▶  
MTA Windows Operating System  
Fundamentals-98-349 ▶  
System Center 2012 Configuration  
Manager-70-243 ▶

### Introduction to Networking

This course provides foundational knowledge in local area networks (LANs), including networking topologies and media, the Open Systems Interconnect (OSI) model, Transmission Control Protocol/Internet Protocol (TCP/IP), network design and implementation, and intermediate routing and switching principles.

*Corequisite: Introduction to Computers and Business Applications*

CCENT Course Subtitle: Cisco Certified  
Entry Networking Technician ▶  
GIAC Security Essentials ▶  
A+ 900 Series ▶  
Network+- N10-006 ▶  
MTA - Windows Operating System  
Fundamentals - 98-349 ▶  
CCENT Course Subtitle: Cisco Certified  
Entry Networking Technician ▶

### Computer Hardware and Software

This course explores PC hardware and software installation and configuration. Hardware topics include: system boards and memory; computer processors; I/O boards and devices; CMOS configuration; storage devices; printers; and PC networking hardware. Software topics include: installations and configuration of various applications; and basic client/server software installation and configuration.

*Corequisite: Introduction to Computers and Business Applications*

IT Fundamentals Overview ▶  
Network+- N10-006 ▶  
A+ 900 Series ▶

## SEMESTER II

### Information Technology Project Management

This course explores traditional project management with heavy emphasis on information technology. Students will define projects and manage the project lifecycle, resource requirements, proposals and contract requirements for IT projects and related case studies.

*Prerequisite: Introduction to Computers and Business Applications*

ITIL Foundation ▶  
Project Management Professional ▶  
Microsoft Project 2013 - 74-343 ▶  
Project+ ▶  
Lean Six Sigma ▶

### Computer Forensics

This course provides students with instruction in current and emerging issues and trends that have significance in computer forensics. Through the use of course activities, students will investigate and analyze computer and network security breaches, applicable security standards, protocols, and laws. Topics will include an assortment of computer-related crimes, legal and ethical issues, securing computerized systems, electronic evidence, and data storage and retrieval.

*Prerequisite: Introduction to Networking*

CHFI v8 ▶  
Digital Forensic Investigator ▶

## Information Systems Security Foundations

This course introduces students to basic information systems security concepts and issues. Students learn the importance of information systems security to the overall mission of organizations, including best security practices related to organizational policies, procedures, and standards. The importance of user training, auditing, risk analysis, and disaster recovery related to information systems security will be covered. Ethical implications related to network security, including ethical hacking, will also be explored.

*Prerequisite: Introduction to Computers and Business Applications*

Security Fundamentals Course Subtitle:  
Core Security Concepts ▶  
Security Fundamentals ▶  
Security+-SY0-401 ▶  
Linux+- LPI-LX0-103/LX0-104 ▶  
CCNA-210-260 ▶  
CompTIA Advanced Security  
Practitioner Course Subtitle: CASP ▶  
CISA Course Subtitle: Certified Information  
Systems Auditor ▶  
System Center 2012 Configuration  
Manager-70-243 ▶

## SEMESTER III

### Technology Management

This course goes beyond information technology (IT) project management to concentrate on enterprise management of technological resources. Students will learn how to analyze enterprises' IT requirements and ensure uniformity of systems and required IT processes. Students will develop and manage effective IT solutions by exploring internal resources and outsourcing alternatives.

*Prerequisite: Information Technology Project Management*

MCSA Windows 8.1-70-687 ▶  
MCSA Windows 8.1-70-688 ▶  
MCSA Windows Server 2012-70-411 ▶  
MCSA Windows Server 2012-70-412 ▶  
MCSA Windows Server 2016-70-740 ▶  
MCSA Windows Server 2016-70-741 ▶  
Mac Integration Basics 10.9 ▶  
Mac Management Basics 10.11 ▶  
Mac Integration Basics 10.11 ▶  
pfSense ▶

### Information Assurance Foundations

This course introduces students to various information technology network threats that can derive through several mediums. Students will analyze threats that can exist through hacking, web-based scripting, operating system vulnerabilities, database design flaws, and web browser and e-mail client vulnerabilities. Other internet and network security topics will also be explored, including internet protocol (IP) security, encryption, user authentication, protocols, security-suite software, and firewalls. Securing mobile devices using a variety of related technologies will also be discussed.

*Prerequisite: Information Systems Security Foundations*

### Network Administration I

This course requires students to use Microsoft Windows operating systems to manage local and wide area networks. Students will install and configure a Windows server operating system on both the client and server sides as well as configure it for various services, including file and print sharing, remote access services, terminal services and Active Directory. Additional Windows features and security will also be covered.

*Prerequisite: Introduction to Networking*

Network+- N10-006 ▶  
MCSA Windows 7-70-680 ▶  
MCSA Windows 7-70-680 ▶  
MCSA Windows 8.1-70-687 ▶  
MCSA Windows 8.1-70-688 ▶  
MCSA Windows 10-70-697 ▶  
MCSA Windows 10-70-698 ▶  
MCSA Windows Server 2012-70-410 ▶  
MCSA Windows Server 2012-70-411 ▶

MCSA Windows Server 2012-70-412 ▶  
MCSA Windows Server 2016-70-740 ▶  
MCSA Windows Server 2016-70-741 ▶  
PowerShell ▶  
Supporting Windows 7 ▶  
Windows 10 Security ▶  
CCENT Course Subtitle: Cisco Certified  
Entry Networking Technician ▶  
System Center 2012 Configuration  
Manager-70-243 ▶



## SEMESTER IV

## Network Administration II

This course introduces students to the Linux operating system. Topics include: command-line administration using a Linux shell; features of the operating system on both the client and server sides; Open Source Software (OSS) benefits and implications; and Linux interoperability with other hardware and software systems.

*Prerequisite: Network Administration I*

Linux+- LPI-LX0-103/LX0-104 ▶

Working with SSH ▶

Kali Linux ▶

Accelerated CCENT Course Subtitle:  
Cisco Certified Entry Network Technician ▶

Systems Security Certified  
Practitioner Course Subtitle: SSCP ▶

## Information Technology Disaster Prevention and Recovery I

This course covers the planning, prevention and recovery from events that can threaten organizations' vital technology assets and associated business functions. Students learn best-case planning strategies, while developing disaster prevention methods and necessary recovery plans. Throughout the course, students will review industry case studies and practice both feed-forward and feedback controls.

*Prerequisite: Information Assurance Foundations*

CHFI v8 ▶

CASP-CAS-002 ▶

Security+-SY0-401 ▶

Eliminating Malware ▶

Working with SSH ▶

Certified Information Systems Security  
Professional (UPDATED 2016) Course  
Subtitle: CISSP ▶

## Information Privacy and Security

This course explores the legal and regulatory compliance issues in regards to information technology. Both national and international legal and regulatory compliance issues will be covered, with an emphasis on relevant regulations, treaties, cases and associated laws that govern information technology. Students will study numerous cases and learn how they can protect organizations' technology assets and enforcing their rights against those who commit security violations.

*Prerequisite: Information Assurance Foundations*

Certified Information Systems Security  
Professional (UPDATED 2016) Course  
Subtitle: CISSP ▶

CompTIA Advanced Security  
Practitioner Course Subtitle: CASP ▶

## SEMESTER V

## Wireless Network Technology I

This course introduces wireless networking technology from both the hardware and software perspectives. In a lab environment, students learn how to connect, troubleshoot and secure wireless networking components using associated networking hardware and software. Current wireless networking protocols are discussed as well as emerging wireless protocols and technology.

*Prerequisite: Network Administration I*

A+ 900 Series Course Subtitle: 900 Series ▶

Security+ ▶

CHFI v8 ▶

CEH v8 ▶

MTA - Mobility and Devices Fundamentals  
- 98-368 ▶

A+ 900 Series ▶

## Operating Systems Security

This course introduces students to security issues related to both Microsoft Windows-based and Linux-based network operating systems. Students will learn to configure and test various security settings in both systems while recognizing the similar and unique security vulnerabilities of each system. Students will explore file system security, auditing and logging, access control methods and other related security services and tools.

*Prerequisite: Network Administration I*

- MCSA Windows 7-70-680 ▶
- MCSA Windows 8.1-70-687 ▶
- MCSA Windows 8.1-70-688 ▶
- MCSA Windows 10-70-697 ▶
- MCSA Windows 10-70-698 ▶
- MCSA Windows Server 2012-70-410 ▶
- MCSA Windows Server 2012-70-411 ▶
- MCSA Windows Server 2012-70-412 ▶
- MCSA Windows Server 2016-70-740 ▶
- MCSA Windows Server 2016-70-741 ▶
- PowerShell ▶
- Supporting Windows 7 ▶

- Windows 10 Security ▶
- Linux+ Course Subtitle: Powered by LPI ▶
- Kali Linux ▶
- SSCP ▶
- Mac Integration Basics 10.9 ▶
- Certified Support Professional 10.10 ▶
- Certified Technical Coordinator 10.10 ▶
- Mac Management Basics 10.11 ▶
- Mac Integration Basics 10.11 ▶
- Certified Support Professional 10.11 ▶
- Certified Technical Coordinator 10.11 ▶
- Certified Technical Coordinator 10.11 ▶

## Wireless Network Technology II

This course builds-upon the foundation of Wireless Network Technology I and requires students to design and plan large-scale wireless networks. Planning implications of wireless networks are discussed. Additionally, students explore the integration of various networking topologies and technologies, both wired and wireless, in forming large-scale networks. Additional topics in wireless technologies are discussed including cellular and satellite networks.

*Prerequisite: Wireless Network Technology I*

- Certified Information Systems Security Professional (UPDATED 2016) Course Subtitle: CISSP ▶
- Accelerated CCENT Course Subtitle: Cisco Certified Entry Network Technician ▶

## SEMESTER VI

### Internal Network Protection

This course explores safeguarding a network from malicious intent from the internal network perspective. Students will learn how to implement internal intrusion detection methods using a variety of hardware and software to help secure a network from unauthorized employees or others with malicious intent. Topics include firewall configuration, hacking methods, network intrusion detection utilities, access control and auditing, and virtual private network intrusion detection and prevention.

*Prerequisite: Network Administration I*

- CEH v9 ▶
- CHFI v8 ▶
- CCNA Security 640-554 Course Subtitle: Cisco Certified Network Associate Security ▶

### Information Technology Disaster Prevention and Recovery II

This course builds up Information Technology Prevention and Recovery I by implementing lab exercises comprising relevant disaster prevention and recovery scenarios. Students will learn best-case prevention, detection, recovery and documentation methods to prevent and recover from harmful events in a hands-on environment. Students will also be exposed to various hardware as well as software tools to help plan, document and prevent harmful events.

*Prerequisite: Information Technology Disaster Prevention and Recovery I*

- CHFI v8 ▶
- CASP-CAS-002 ▶
- Security+-SY0-401 ▶
- Eliminating Malware ▶
- Working with SSH ▶
- Certified Information Systems Security Professional (UPDATED 2016) Course Subtitle: CISSP ▶



## Perimeter Network Protection

This course explores network security infrastructure issues. Students will learn how to design and implement network infrastructure defenses. Topics include firewall configuration, authentication and access, load-balancing, wireless access, transport protocols, and domain name systems. Internet, e-mail, hacking, and other web security threats will be addressed as well as the strategies to detect and defend against these vulnerabilities.

*Prerequisite: Network Administration I*

MTA - Security Fundamentals - 98-367  
Course Subtitle: Security Fundamentals ▶  
Cisco ASA Express Security ▶  
CCNA Security Course Subtitle: Cisco Certified Network Associate Security ▶  
CCNA Security 640-554 Course Subtitle: Cisco Certified Network Associate Security ▶  
pfSense (2016) Course Subtitle: pfSense Build 2.3.2 ▶  
CEH v9 ▶  
CHF1 v8 ▶

## SEMESTER VII

### Wireless Network Security

Most organizations rely on mobile wireless communications to help share data. This course focuses on wireless device and software security. Students will learn about various ways others can obtain unauthorized wireless access or cause security issues, including MAC spoofing, "man-in-the-middle" and denial-of-service (DOS) attacks. Prevention of unauthorized access will be explored, including the use of Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), IP-addressing methods, and MAC id filtering. This course will also explore mobile security concerns and issues.

*Prerequisite: Wireless Network Technology II*

Security+ Course Subtitle: Vendor-neutral IT Security ▶  
CISA Course Subtitle: Certified Information Systems Auditor ▶  
MTA - Security Fundamentals - 98-367 ▶  
Certified Information Systems Security Professional (UPDATED 2016) Course Subtitle: CISSP ▶  
Accelerated CCENT Course Subtitle: Cisco Certified Entry Network Technician ▶

### Advanced Network Security

This course provides students with extensive hands-on skills in safeguarding networks. Students practice network security risk assessments, while preventing and detecting various security vulnerabilities. Students will also practice network intrusion detection, response and documentation methods and strategies. Network authentication, access control, firewall configuration, cryptography and other security prevention methodologies will be discussed and practiced.

*Prerequisite: Perimeter Network Protection*

Security+ ▶  
CompTIA Advanced Security Practitioner Course Subtitle: CASP ▶  
Certified Information Systems Security Professional (UPDATED 2016) Course Subtitle: CISSP ▶  
CEH v9 ▶  
CEH v8 ▶

## SEMESTER VIII

### Externship

This is the capstone course in the Cybersecurity Bachelor's Degree program. Students practice essential network security skills while being supervised in a real-world information technology environment.

*\*Required in last semester only\**

CONTACT US TODAY

Learn more about the cybersecurity courses available from Wiley and ITProTV.

WILEY