Center for Cybersecurity
Dr. Kenneth Knapp

Director of the Cybersecurity Program

Contact Dr. Knapp by email at
kknapp@andersonuniversity.edu
Cybersecurity Program

- Cybersecurity at Anderson University begins fall, 2020
  - Will have dedicated Cyber Lab for courses
- Cybersecurity Academic Programs
  - Cybersecurity Major (123 Credit Hours)
  - Three Interdisciplinary Majors:
    - Cybersecurity and Criminal Justice (123 Credit Hours)
    - Cybersecurity and Mathematics (123 Credit Hours)
    - Cybersecurity and Analytics (121 Credit Hours)
  - Cybersecurity Minor (18 Credit Hours) – available to all AU Majors
  - Cybersecurity Professional Certificate (18 Credit Hours) – six online courses

*Pending approval by the Southern Association of Colleges and Schools Commission on Colleges.

**Information in this document is provided for information purposes until the Anderson University catalog is officially updated.
Cybersecurity Major

- The Bachelor of Science in Cybersecurity gives graduates the knowledge and skills needed to enter the dynamic field of Cybersecurity. Students learn how to protect the confidentiality, integrity and availability of data, networks and computer systems. Anderson students also learn the ethical considerations that impact the Cybersecurity profession. To do this, students gain a balanced Cybersecurity education that includes both the technical and risk management aspects of the field.

- In all Cybersecurity classes, faculty integrate hands-on learning exercises to ensure students gain the necessary skills with tools that are used in the field.

- Today, all types of companies hire Cybersecurity professionals in fields as diverse as finance, insurance, retail, healthcare, hospitality, information technology, consulting, transportation, manufacturing, law enforcement, public utilities, government, defense and more. The Anderson Cybersecurity program gives the essential knowledge and skills for students to get jobs in these industries. In addition to careers in cybersecurity, the program of study prepares students to pass professional certification exams as well as earn acceptance into graduate school for those planning to continue their education.
Cybersecurity Major Requirements

Twelve required CYB courses = 37 Cr. Hrs.

100-level Basic
- Cryptography: CYB 210 (F)
- Cloud Security: CYB 310 (F)
- Cybersecurity Contingency Planning: CYB 410 (F)

200-level Development
- Programming for Security: CYB 220 (F)
- Cyber Threat Intelligence: CYB 320 (F)
- Ethical Hacking: CYB 420 (4 CH)

300-level Intermediate
- Network Security: CYB 230 (S)
- Digital Forensics: CYB 330 (S)
- Risk Management & Compliance: CYB 340 (S)

400-level Advanced
- Cybersecurity Foundations & Ethics: CYB 101 (F and S)
- Security with Linux: CYB 110 (S)
- Certification Preparation: CYB 450 (S)

Prereq: Any one CYB 3xx course

Pre-requisite
- Pre or Co-requisite
Cybersecurity Major

TOTAL CREDIT HOURS
41 + 37 + 15 + 18 + 12 = 123 Credits

AU Core (41 credit hours). Must include these two courses:

- MAT 108: Finite Probability & Statistics 1 (3 CH) (Part of AU Core)
- Scientific Inquiry: BIO 104, BIO 150 or CHE 104 (4 Cr. Hrs.)

Cybersecurity Core Requirements (37 credit hours)

- CYB 101: Cybersecurity Foundations & Ethics
- CYB 110: Security with Linux
- CYB 210: Cryptography
- CYB 220: Programming for Security
- CYB 230: Network Security
- CYB 310: Cloud Security
- CYB 320: Cyber Threat Intelligence
- CYB 330: Digital Forensics
- CYB 340: Risk Management & Compliance
- CYB 410: Cybersecurity Contingency Planning
- CYB 420: Ethical Hacking
- CYB 450: Certification Hacking

Cognate Cybersecurity Requirements (15 credit hours)

- CIS 120: Intro to Information Processing Systems 3 Cr. Hrs.
- CIS 352: Management of Information Systems 3 Cr. Hrs. | Pre: CIS 120, Jr. standing
- ENG 301: Business Communications 3 Cr. Hrs. | Pre: ENG 102
- BUS 251: Legal Environment of Business 3 Cr. Hrs.
- CRJ 101: Intro to Criminal Justice 3 Cr. Hrs.
- OR
- OR
- CRJ 150: Criminology 3 Cr. Hrs.

Major Elective Options (must = 12 credits)
choose any four classes from either list below:

Business Electives

- ACC 201: Introduction to Financial Accounting 3 Cr. Hrs.
- ACC 202: Introduction to Managerial Accounting 3 Cr. Hrs. | Pre: ACC 201
- MGT 360: Project Management 3 Cr. Hrs.
- MGT 210: Principles of Management 3 Cr. Hrs. | Pre: PSY 101, SOC 101
- ECO 211: Principles of Microeconomics 3 Cr. Hrs.
- ECO 212: Principles of Microeconomics 3 Cr. Hrs.

Computing/Math Electives

- CIS 202: Computer Science I 4 Cr. Hrs. | Pre: CIS 120, MAT 106 or higher
- CIS 203: Computer Science II 4 Cr. Hrs. | Pre: CIS 202
- CIS 310: Introduction to Database Systems 3 Cr. Hrs. | Pre(s): CIS 202 (Fall)
- DA 301: Introduction to Data Analytics 4 Cr. Hrs. | Pre: BUS 230, CIS 202
- BUS 230: Business Statistics 3 Cr. Hrs. | Pre: MAT 108, CIS 120
- CDG 111: Coding I 3 Cr. Hrs.
- CDG 112: Coding II 3 Cr. Hrs. | Pre: CDG 111
- CDG 205: Introduction to Mobile Interface Design 3 Cr. Hrs. | Pre: CDG 111
- MAT 160: Introduction to Discrete Methods 3 Cr. Hrs. | Pre: See Catalog
- CYB 495: Cybersecurity Special Topics (3)
Cybersecurity Course Descriptions

All CYB courses are 3 credit hours, except when noted. They will be entered into the catalog for the 2020-2021 academic year.

**CYB 101 Cybersecurity Foundations & Ethics**
An introduction to the principles of the cybersecurity field. The course covers how to protect the confidentiality, integrity and availability of information systems. The domains examined include networks, access control, risk management, cryptography, cybercrime and legal issues. We address ethical issues that arise from our interconnected world involving topics such as cyberwar, surveillance, privacy, censorship and hacking. Special consideration is given to promoting personal security best practices.

**CYB 110 Security with Linux**
This course covers the fundamentals of a computer operating system (OS) and contrasts the common systems used today. Then, we focus on the Linux OS covering topics such as command line interface, file systems, networking, scripting basics, logging, controlling file permissions and the Linux kernel. We highlight how Linux is used in security and pen-testing.

**CYB 210 Cryptography**
Covers the principles and technologies used in the computerized encoding and decoding of information. Topics include cryptography basics, encryption & decryption methods, symmetric versus asymmetric systems, hashing, public-key infrastructures, cryptanalysis and attack types. A focus is given to solutions such as blockchain, tokenization, hardware security modules, format-preserving encryption and cloud-based cryptographic technologies. Concepts are reinforced with hands-on exercises.

**CYB 220 Programming for Security**
An introduction to programming principles using a modern language. Students create simple computer scripts and programs to automate operations and solve problems. The course emphasizes important practices in developing secure and quality code. Applications and exercises that are relevant to the cybersecurity industry are explored.
CYB 230 Network Security
An introduction to the operation and security of computer networks. Topics include network security architectures, topology, routing, protocols, IP addressing, wireless networking. The OSI and TCP/IP protocol suite are covered in depth. Security mechanisms such as firewalls, intrusion prevention systems, network hardening and honeypots are addressed. Students are given hands-on exercises using industry standard tools.

CYB 310 Cloud Security
An introduction to the concepts of securing cloud-based technology systems. The course covers architectural and security design requirements of cloud systems. Topics include data security, virtual networks and storage, visualization architectures, platform administration, application security and identity management. Governance, legal and compliance issues that impact cloud systems are examined. Students will build and secure a virtual private cloud service provider.

CYB 320 Cyber Threat Intelligence
An exploration of the concepts, methods, and tools used to gather and analyze cyber threat data. Threat intelligence is knowledge that allows organizations to prevent or mitigate cyberattacks. In this course we investigate cyber threats and describe different types of attacks and their characteristics. To detect malicious activity, we examine system logs, intelligence data, and indicators of compromise. We utilize both internal and external data sources, including open source intelligence.

CYB 330 Digital Forensics
An introduction to the practice of digital forensics. The course surveys the knowledge needed to forensically analyze computer hosts and networks and how to properly collect, analyze, report and present such evidence. Students learn to examine computer memory, storage, file systems, and cloud based systems. Legal topics are covered to include chain of custody, e-discovery and authentication of evidence.
CYB 340 Risk Management and Compliance
This course covers the management of information security programs in organizations. Students are introduced to various standards that define best practices for creating and maintaining security policies and performing an enterprise risk assessment. Students are exposed to legal, regulatory and compliance requirements of cybersecurity. The course requires students to solve real-world security problems using a risk management approach through group project work and writing assignments.

CYB 410 Cybersecurity Contingency Planning
This covers incident response, disaster planning and business continuity as it relates to cybersecurity. Students learn the different organizational roles of key personnel in the planning process as well as develop organization specific contingency strategies. Contingency planning for critical infrastructures is addressed. Additionally, the course covers contingency planning from within a boarder homeland security and emergency services framework.

CYB 420 Ethical Hacking. 4 Credit Hours
The course covers the hacking methodologies used to plan, organize and perform penetration testing on a target computer system. Emphasis is placed on understanding attack types and using security tools to find and exploit system vulnerabilities. Hacking ethics and legal issues are emphasized. Penetration testing in a cloud environment is addressed. The stages of organized cyber operations and pen testing are practiced with hands-on labs.

CYB 450 Certification Preparation
In the Cybersecurity field, employment prospects are significantly improved if the job seeker holds a professional certification(s). The course provides a comprehensive and intense preparation for an entry-level cybersecurity certification. Students sharpen test taking skills with practice questions and exams. At the end of the course, students are encouraged to take an actual certification exam. Contact the instructor to inquire what exam is being covered during a particular semester.
The Bachelor of Science in Cybersecurity & Criminal Justice gives graduates an in-depth education in two related fields. This interdisciplinary program combines courses from the Cybersecurity and Criminal Justice majors to give graduates the knowledge and skills needed to enter either the Cybersecurity or Criminal Justice field with significant opportunities where the fields overlap.

In this program, students learn how to protect the confidentiality, integrity and availability of computer systems while examining the foundations of the criminal justice system and its component parts. Students take courses in digital forensics, ethical hacking, contingency planning, cyber threat intelligence, cryptography, risk management, police systems, criminal law, investigations, judicial systems, constitutional law and more.

Today the government agencies at all-levels are expanding their cybersecurity, digital forensics and cybercrime unites. Likewise, many businesses are expanding their cybersecurity teams including those in industries such as finance, insurance, healthcare, security consulting, utilities and military/defense. The Anderson Cybersecurity and Criminal Justice program gives graduates the preparation to earn jobs in these industries.

In addition to careers in cybersecurity and criminal justice, the program of study prepares students for graduate school for those planning to continue their education.
Cybersecurity & Criminal Justice Major

Not a double major, but an interdisciplinary major.

**TOTAL CREDIT HOURS**

$$41 + 34 + 33 + 3 + 12 = 123\text{ Credits}$$

**AU Core (41 credit hours)**. Must include these two courses:

- MAT 108 Finite Probability & Statistics 1 3CH (Part of AU Core)
- SOC 101 (Social Inquiry)

**Cybersecurity Core Requirements (34 credit hours)**

- CYB 101 Cybersecurity Foundations & Ethics
- CYB 110 Security with Linux
- CYB 210 Cryptography
- CYB 220 Programming for Security
- CYB 230 Network Security
- CYB 310 Cloud Security
- CYB 320 Cyber Threat Intelligence
- CYB 330 Digital Forensics
- CYB 340 Risk Management & Compliance
- CYB 410 Cybersecurity Contingency Planning
- CYB 420 Ethical Hacking

**Criminal Justice Major Core Requirements (33 credit hours)**

- CRJ 101 Introduction to Criminal Justice 3 Cr. Hrs.
- CRJ 150 Criminology 3 Cr. Hrs.
- CRJ 215 American Police Systems 3 Cr. Hrs.
- CRJ 230 Criminal Law 3 Cr. Hrs.
- CRJ 251 Criminal Investigation 3 Cr. Hrs.
- CRJ 275 Correctional Systems 3 Cr. Hrs.
- CRJ 301 Research Methods in Criminal Justice 3 Cr. Hrs.
- CRJ 350 Judicial Systems and Practices 3 Cr. Hrs.**
- CRJ 450 Ethics in Criminal Justice 3 Cr. Hrs.
- CRJ 475 Constitutional Law 3 Cr. Hrs.
- CRJ 490 Senior Seminar in Criminal Justice 3 Cr. Hrs.

**Cognate Requirements (3 credit hours)**

- PS 101 American National Government

**General Electives (12 credit hours)**

**Prereq:** PS 101
The Bachelor of Science in Cybersecurity and Mathematics gives graduates an in-depth education in these two related fields. This interdisciplinary program integrates cybersecurity and math courses into a relevant, challenging major. The major provides students the knowledge and skills needed to enter the Cybersecurity field equipped with a strong mathematics background.

In this program, students learn how to protect the confidentiality, integrity and availability of computer systems while examining topics relevant to cybersecurity such as discrete methods, probability & statistics and linear algebra. Students take courses covering topics such as network security, digital forensics, ethical hacking, programming, scripting, cryptography, linear programming, differential equations and calculus.

This relevant, interdisciplinary major prepares students to work in both Government agencies and private companies that depend on mathematics. Graduates with backgrounds in both cyber and math can work on interdisciplinary teams to help formulate complex mathematical and cryptographic solutions to today’s cybersecurity problems.

Graduates can work in any industry that hires cybersecurity professionals—especially those in data-intensive sectors such as finance, insurance, healthcare, software development, intelligence and military/defense. The major also prepares students for careers in cybersecurity consulting, auditing as well as graduate work in Cybersecurity or Mathematics.
Cybersecurity & Mathematics Major

Not a double major, but an interdisciplinary major.

TOTAL CREDIT HOURS
42 + 34 + 38 + 9 = 123 Credits

AU Core (42 credit hours). Must include these courses:
- MAT 140  Quantitative Literacy
- PHY 201
- PHY 203  Scientific Inquiry

Cybersecurity Core Requirements (34 credit hours)
- CYB 101  Cybersecurity Foundations & Ethics
- CYB 110  Security with Linux
- CYB 210  Cryptography
- CYB 220  Programming for Security
- CYB 230  Network Security
- CYB 310  Cloud Security
- CYB 320  Cyber Threat Intelligence
- CYB 330  Digital Forensics
- CYB 340  Risk Management & Compliance
- CYB 410  Cybersecurity Contingency Planning
- CYB 420  Ethical Hacking

Math Major Core Requirements (38 credit hours)
- MAT 160  Introduction to Discrete Methods 3 Cr. Hrs.
- MAT 190  Analytic Geometry & Calculus 4 Cr. Hrs.
- MAT 215  Linear Algebra 3 Cr. Hrs.
- MAT 240  Calculus with Several Variables 4 Cr. Hrs.
- MAT 270  Linear Programming 3 Cr. Hrs.
- MAT 280  Introduction to Probability & Statistics 3 Cr. Hrs.
- MAT 290  Differential Equations 3 Cr. Hrs.
- MAT 340  Probability & Statistical Theory & Methods 3 Cr. Hrs.
- MAT 380  Probability & Statistical Theory & Methods 3 Cr. Hrs.
- MAT 390  Advanced Calculus 3 Cr. Hrs.
- MAT 420  Abstract Algebra 3 Cr. Hrs.
- MAT 496  Senior Research in Mathematics 3 Cr. Hrs.

General Electives (9 credit hours)
Cybersecurity and Analytics Major

• The Bachelor of Science in Cybersecurity and Analytics gives graduates an in-depth education in these two related fields. This interdisciplinary program integrates cybersecurity, business and data analytics courses into a dynamic, combined major. The major gives students the knowledge and skills needed to enter the Cybersecurity field equipped with an understanding of the key technologies and concepts of data analytics.

• In this program, students learn how to protect the confidentiality, integrity and availability of computer systems as well as the foundations to problem analysis and big data tools. Students take courses covering topics such as network security, digital forensics, ethical hacking, scripting, cyber threat intelligence, risk management, cloud security, database systems, analytics programming, data science processes and statistical tools.

• Today, organizations of all types use data analytics to hunt for indicators of compromise in computer networks and systems. Cyber analytics professionals use their skills to protect businesses form the constantly evolving threat landscape facing modern organizations.

• This relevant, interdisciplinary major prepares students to work in any industry that hires cybersecurity professionals and especially those in information-intensive sectors such as finance, insurance, retail, healthcare, accounting and military/defense. The major also prepares students for careers in cybersecurity consulting, auditing, cyber operations and threat hunting.
Cybersecurity & Analytics Major

Not a double major, but an interdisciplinary major.

TOTAL CREDIT HOURS

$41 + 34 + 22 + 15 + 9 = 121$ Credits

**AU Core (41 credit hours).** Must include the following course:

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAT 108</td>
<td>Quantitative Literacy</td>
</tr>
</tbody>
</table>

**Cybersecurity Core Requirements (34 credit hours)**

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYB 101</td>
<td>Cybersecurity Foundations &amp; Ethics</td>
</tr>
<tr>
<td>CYB 110</td>
<td>Security with Linux</td>
</tr>
<tr>
<td>CYB 210</td>
<td>Cryptography</td>
</tr>
<tr>
<td>CYB 220</td>
<td>Programming for Security</td>
</tr>
<tr>
<td>CYB 230</td>
<td>Network Security</td>
</tr>
<tr>
<td>CYB 310</td>
<td>Cloud Security</td>
</tr>
<tr>
<td>CYB 320</td>
<td>Cyber Threat Intelligence</td>
</tr>
<tr>
<td>CYB 330</td>
<td>Digital Forensics</td>
</tr>
<tr>
<td>CYB 340</td>
<td>Risk Management &amp; Compliance</td>
</tr>
<tr>
<td>CYB 410</td>
<td>Cybersecurity Contingency Planning</td>
</tr>
<tr>
<td>CYB 420</td>
<td>Ethical Hacking</td>
</tr>
</tbody>
</table>

**Analytics Requirements (15 credit hours)**

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS 202</td>
<td>Computer Science 1 Cr. Hrs.</td>
</tr>
<tr>
<td>CIS 310</td>
<td>Introduction to Database Management Systems 3 Cr. Hrs.</td>
</tr>
<tr>
<td>DA 301</td>
<td>Introduction to Data Analytics 4 Cr. Hrs.</td>
</tr>
<tr>
<td>DA 401</td>
<td>Intermediate Data Analytics 4 Cr. Hrs.</td>
</tr>
</tbody>
</table>

**Required Business Courses (22 credit hours)**

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACC 201</td>
<td>Introduction to Financial Accounting 3 Cr. Hrs.</td>
</tr>
<tr>
<td>ACC 202</td>
<td>Introduction to Managerial Accounting 3 Cr. Hrs.</td>
</tr>
<tr>
<td>BUS 110</td>
<td>Investigating Business 1 Cr. Hrs.</td>
</tr>
<tr>
<td>BUS 203</td>
<td>Business Statistics 3 Cr. Hrs.</td>
</tr>
<tr>
<td>CIS 120</td>
<td>Introduction to Information Processing Systems 3 Cr. Hrs.</td>
</tr>
<tr>
<td>CIS 352</td>
<td>Management of Information Systems 3 Cr. Hrs.</td>
</tr>
<tr>
<td>FIN 310</td>
<td>Financial Management 3 Cr. Hrs.</td>
</tr>
<tr>
<td>BUS 251</td>
<td>Legal Environment of Business 3 Cr. Hrs.</td>
</tr>
</tbody>
</table>

**General Electives (9 credit hours)**

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
</table>
Open to all Anderson Majors
Requires 18 credit hours
• *Mandatory Courses: CYB 101, 110, 230
• Choose any three additional CYB courses

- Cryptography: CYB 210 (F)
- Programming for Security: CYB 220 (F)
- Cloud Security: CYB 310 (F)
- Cyber Threat Intelligence: CYB 320 (F)
- Cybersecurity Contingency Planning: CYB 410 (F)
- *Network Security: CYB 230 (S)
- Digital Forensics: CYB 330 (S)
- Ethical Hacking: CYB 420 (4 CH)

*Cybersecurity Foundations & Ethics: CYB 101 (F and S)
*Security with Linux: CYB 110 (S)

Certification Preparation: CYB 450 (S)

Prereq: Any one CYB 3xx course

Pre-requisite
Pre or Co-requisite
Cybersecurity Professional Certificate

For Online students through CIDL
Requires 18 credit hours

- *Mandatory Courses: CYB 101, 110, 230
- Choose any three additional CYB courses

**Cybersecurity Foundations & Ethics**
- **CYB 101** (F and S)
  - Fall
  - Spring

**Security with Linux**
- **CYB 110** (S)
  - Fall
  - Spring

**Network Security**
- **CYB 230** (S)
  - Fall
  - Spring

**Digital Forensics**
- **CYB 330** (S)
  - Fall

**Risk Management & Compliance**
- **CYB 340** (S)
  - Fall

**Ethical Hacking**
- **CYB 420**
  - 4 CH (S)
  - Fall

**Certification Preparation**
- **CYB 450** (S)
  - Fall

---

100-level
Basic

200-level
Development

300-level
Intermediate

400-level
Advanced

Pre-requisite
Pre or Co-requisite
Online (and seated)
Seated Only

Gold Text
Grey Text

Prereq: Any one CYB 3xx course