Cybersecurity is a computing-based discipline involving technology, people, information, and processes to protect computing systems from adversaries. It involves the creation, operation, analysis, and testing of secure computing systems. Cybersecurity professionals know how to secure websites, mobile apps, operating systems, databases, networks, and embedded computing systems. They stay current on the latest computer vulnerabilities, help prevent employees from falling victim to social engineering attacks, collaborate with leadership to mitigate and manage risks, monitor systems to identify intruders, and respond effectively when successful attacks occur. Penetration testers, also known as Red Team members, are hired by companies and organizations to identify vulnerabilities by ethically hacking into systems. Digital forensics investigators use sophisticated tools to track down attackers and capture evidence that can be used in court. Because of the

<table>
<thead>
<tr>
<th>University Core Requirements</th>
<th>Suggested Sequence of Courses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>University Core Requirements:</strong></td>
<td><strong>FRESHMAN YEAR</strong></td>
</tr>
<tr>
<td>Requirements</td>
<td>1st Semester</td>
</tr>
<tr>
<td><strong>Religion Cornerstones</strong></td>
<td></td>
</tr>
<tr>
<td>Teachings and Doctrine of The Book of Mormon</td>
<td>1</td>
</tr>
<tr>
<td>Jesus Christ and the Everlasting Gospel</td>
<td>1</td>
</tr>
<tr>
<td>Foundations of the Restoration</td>
<td>1</td>
</tr>
<tr>
<td>The Eternal Family</td>
<td>1</td>
</tr>
<tr>
<td><strong>The Individual and Society</strong></td>
<td></td>
</tr>
<tr>
<td>American Heritage</td>
<td>1-2</td>
</tr>
<tr>
<td>Global and Cultural Awareness</td>
<td>1</td>
</tr>
<tr>
<td><strong>Skills</strong></td>
<td></td>
</tr>
<tr>
<td>First Year Writing</td>
<td>1</td>
</tr>
<tr>
<td>Advanced Written and Oral Communications</td>
<td>1</td>
</tr>
<tr>
<td>Quantitative Reasoning</td>
<td>1</td>
</tr>
<tr>
<td>Languages of Learning (Math or Language)</td>
<td>1</td>
</tr>
<tr>
<td><strong>Arts, Letters, and Sciences</strong></td>
<td></td>
</tr>
<tr>
<td>Civilization 1</td>
<td>1</td>
</tr>
<tr>
<td>Civilization 2</td>
<td>1</td>
</tr>
<tr>
<td>Arts</td>
<td>1</td>
</tr>
<tr>
<td>Letters</td>
<td>1</td>
</tr>
<tr>
<td>Biological Science</td>
<td>1</td>
</tr>
<tr>
<td>Physical Science</td>
<td>1</td>
</tr>
<tr>
<td>Social Science</td>
<td>1</td>
</tr>
<tr>
<td><strong>Core Enrichment: Electives</strong></td>
<td></td>
</tr>
<tr>
<td>Religion Electives</td>
<td>3-4</td>
</tr>
<tr>
<td>Open Electives</td>
<td>Variable</td>
</tr>
</tbody>
</table>

*THESE CLASSES FILL BOTH UNIVERSITY CORE AND PROGRAM REQUIREMENTS

| Graduation Requirements: | | |
| Minimum residence hours required | 30.0 | |
| Minimum hours needed to graduate | 120.0 | |
BS in Cybersecurity (396527)
2021-2022 Program Requirements (77 Credit Hours)

**THE DISCIPLINE:**
Cybersecurity is a computing-based discipline involving technology, people, information, and processes to protect computing systems from adversaries. It involves the creation, operation, analysis, and testing of secure computing systems. Cybersecurity professionals know how to secure websites, mobile apps, operating systems, databases, networks, and embedded computing systems. They stay current on the latest computer vulnerabilities, help prevent employees from falling victim to social engineering attacks, collaborate with leadership to mitigate and manage risks, monitor systems to identify intruders, and respond effectively when successful attacks occur. Penetration testers, also known as Red Team members, are hired by companies and organizations to identify vulnerabilities by ethically hacking into systems. Digital forensics investigators use sophisticated tools to track down attackers and capture evidence that can be used in court.

Because of the influence and leadership roles we expect graduates to have, our students will be encouraged to develop high moral and ethical standards as well as being conversant with and compliant with professional and legal standards.

**CAREER OPPORTUNITIES:**
The field has grown tremendously in recent years and is expected to continue rapid growth in the coming decades. BYU’s Cybersecurity program is recognized as a National Center of Academic Excellence in Cyber Defense by the NSA/DHS and has placed students in the public and private sector at top companies both small and large. Graduates fill roles as penetration testers, forensics computer analysts, network and systems administrators, data security engineers, information security analysts, security architects, IT security engineers, and Chief Information Security Officers.

**MAP DISCLAIMER**
While every reasonable effort is made to ensure accuracy, there are some student populations that could have exceptions to listed requirements. Please refer to the university catalog and your college advisement center/department for complete guidelines.

**DEPARTMENT INFORMATION**
Information Technology & Cybersecurity
School of Technology
265 Crabtree Building
Brigham Young University, Provo, UT 84602
Telephone: 801-422-6300

**ADVISEMENT CENTER INFORMATION**
Samuel Cardenas Academic Advisor, School of Technology
250 Snell Building
Brigham Young University, Provo, UT 84602
Telephone: 801-422-1818
sot_advisement@byu.edu

---

**REQUIREMENT 1 Complete 7 courses**
- IT&C 412 - Introduction to Computer Programming 3.0
- IT&C 235 - Data Structures and Algorithms 3.0
- IT&C 236 - Discrete Structures 3.0
- *MATH 112 - Calculus 1 4.0
- PHYSICS 121 - Introduction to Newtonian Mechanics 3.0
- STAT 201 - Statistics for Engineers and Scientists 3.0
- WRTG 116 - Technical Communication 3.0

**REQUIREMENT 2 Complete 1 course**
ENG T 231 - (Not currently offered)

**REQUIREMENT 3 Complete 1 course**
IT&C 233 - Ethics, Globalization, & Leadership 3.0

**REQUIREMENT 4 Complete 15 courses**
- **NOTE: IT&C 210A AND 212 MUST BE COMPLETED WITH A GRADE OF C OR HIGHER PRIOR TO ENTERING ANY 300-LEVEL IT COURSE.**
- IT&C 101 - Cornerstone: Information Technology & Cybersecurity 3.0
- IT&C 124 - Introduction to Computer Systems 3.0
- IT&C 210A - Fundamentals of Web-Based Information Technology 2.0
- IT&C 210B - Fundamentals of Web-Based Information Technology 2.0
- IT&C 252 - Computer Architecture and Organization 3.0
- IT&C 293 - Professional Seminar 0.5
- IT&C 327 - Digital Communications 4.0
- IT&C 344 - Operating Systems 3.0
- IT&C 347 - Computer Networks 3.0
- IT&C 350 - Database Principles and Applications 3.0
- IT&C 366 - Information Assurance and Security 3.0
- IT&C 446 - Senior Project / Capstone 1 3.0
- IT&C 447 - Senior Project/Capstone 2 3.0
- IT&C 566 - Digital Forensics 3.0
- IT&C 567 - Cybersecurity and Penetration Testing 3.0

**REQUIREMENT 5 Complete 1.5 hours from the following course(s)**
TAKING THE FOLLOWING 3 TIMES:
- IT&C 291R - Seminar 0.5

**REQUIREMENT 6 Complete 6.0 hours from the following course(s)**
COURSES OUTSIDE OF THOSE LISTED MUST BE PRE-APPROVED BY THE PROGRAM. IT&C 492R AND 515R MUST HAVE A CYBERSECURITY-RELATED TOPIC.
- IT&C 492R - Special Problems in Information Technology & Cybersecurity 3.0
- IT&C 515R - Special Topics in Information Technology & Cybersecurity 3.0v
- IT&C 529 - Advanced Networking 3.0
- IT&C 544 - System Administration 3.0
- IT&C 548 - Cyber-Physical Systems 3.0
- MATH 485 - Mathematical Cryptography 3.0

**REQUIREMENT 7**
Students must complete 200 hours of pre-approved cybersecurity-related work after declaring the major and must submit a signed letter from an employer during the IT&C 447 course.

**REQUIREMENT 8**
Complete department packet and exit interview.

---

Students must have a minimum of 120 total hours to graduate with this major.

**REQUIREMENT 8**
Students must complete 200 hours of pre-approved cybersecurity-related work after declaring the major and must submit a signed letter from an employer during the IT&C 447 course.

Major.

Students must have a minimum of 120 total hours to graduate with this major.

**REQUIREMENT 5**
Complete 7 courses
- IT&C 412 - Introduction to Computer Programming 3.0
- IT&C 235 - Data Structures and Algorithms 3.0
- IT&C 236 - Discrete Structures 3.0
- *MATH 112 - Calculus 1 4.0
- PHYSICS 121 - Introduction to Newtonian Mechanics 3.0
- STAT 201 - Statistics for Engineers and Scientists 3.0
- WRTG 116 - Technical Communication 3.0

**REQUIREMENT 2**
Complete 1 course
ENG T 231 - (Not currently offered)

**REQUIREMENT 3**
Complete 1 course
IT&C 233 - Ethics, Globalization, & Leadership 3.0

**REQUIREMENT 4**
Complete 15 courses
NOTE: IT&C 210A AND 212 MUST BE COMPLETED WITH A GRADE OF C OR HIGHER PRIOR TO ENTERING ANY 300-LEVEL IT COURSE.
- IT&C 101 - Cornerstone: Information Technology & Cybersecurity 3.0
- IT&C 124 - Introduction to Computer Systems 3.0
- IT&C 210A - Fundamentals of Web-Based Information Technology 2.0
- IT&C 210B - Fundamentals of Web-Based Information Technology 2.0
- IT&C 252 - Computer Architecture and Organization 3.0
- IT&C 293 - Professional Seminar 0.5
- IT&C 327 - Digital Communications 4.0
- IT&C 344 - Operating Systems 3.0
- IT&C 347 - Computer Networks 3.0
- IT&C 350 - Database Principles and Applications 3.0
- IT&C 366 - Information Assurance and Security 3.0
- IT&C 446 - Senior Project / Capstone 1 3.0
- IT&C 447 - Senior Project/Capstone 2 3.0
- IT&C 566 - Digital Forensics 3.0
- IT&C 567 - Cybersecurity and Penetration Testing 3.0

**REQUIREMENT 5**
Complete 1.5 hours from the following course(s)
TAKING THE FOLLOWING 3 TIMES:
- IT&C 291R - Seminar 0.5

**REQUIREMENT 6**
Complete 6.0 hours from the following course(s)
COURSES OUTSIDE OF THOSE LISTED MUST BE PRE-APPROVED BY THE PROGRAM. IT&C 492R AND 515R MUST HAVE A CYBERSECURITY-RELATED TOPIC.
- IT&C 492R - Special Problems in Information Technology & Cybersecurity 3.0
- IT&C 515R - Special Topics in Information Technology & Cybersecurity 3.0v
- IT&C 529 - Advanced Networking 3.0
- IT&C 544 - System Administration 3.0
- IT&C 548 - Cyber-Physical Systems 3.0
- MATH 485 - Mathematical Cryptography 3.0

**REQUIREMENT 7**
Students must complete 200 hours of pre-approved cybersecurity-related work after declaring the major and must submit a signed letter from an employer during the IT&C 447 course.

**REQUIREMENT 8**
Complete department packet and exit interview.

THE DISCIPLINE:
Cybersecurity is a computing-based discipline involving technology, people, information, and processes to protect computing systems from adversaries. It involves the creation, operation, analysis, and testing of secure computing systems. Cybersecurity professionals know how to secure websites, mobile apps, operating systems, databases, networks, and embedded computing systems. They stay current on the latest computer vulnerabilities, help prevent employees from falling victim to social engineering attacks, collaborate with leadership to mitigate and manage risks, monitor systems to identify intruders, and respond effectively when successful attacks occur. Penetration testers, also known as Red Team members, are hired by companies and organizations to identify vulnerabilities by ethically hacking into systems. Digital forensics investigators use sophisticated tools to track down attackers and capture evidence that can be used in court.

Because of the influence and leadership roles we expect graduates to have, our students will be encouraged to develop high moral and ethical standards as well as being conversant with and compliant with professional and legal standards.

---

**CAREER OPPORTUNITIES:**
The field has grown tremendously in recent years and is expected to continue rapid growth in the coming decades. BYU's Cybersecurity program is recognized as a National Center of Academic Excellence in Cyber Defense by the NSA/DHS and has placed students in the public and private sector at top companies both small and large. Graduates fill roles as penetration testers, forensics computer analysts, network and systems administrators, data security engineers, information security analysts, security architects, IT security engineers, and Chief Information Security Officers.