I. COURSE CHANGES

BUSINESS ADMINISTRATION (BUAD)

ADD

BUAD 589 Immersion Experience for Online Students (0) Provides an orientation and networking opportunity for students in enrolled in Haslam College of Business online programs.
Registration Restriction: Must be graduate student in the Haslam College of Business.
Rationale: This course fills a need for graduate students in the college. Financial and staffing impact: None.

DEPARTMENT OF ACCOUNTING AND INFORMATION MANAGEMENT

(INMT) Information Management

ADD

INMT 561 Foundations of Business Cybersecurity (3) Provides students with a foundational knowledge of concepts, theories, technologies, and procedures underlying the protection of information assets. Students work with a variety of tools to enhance their knowledge and technology skills in this ever-changing area.
Registration Restriction(s): Must be online student and Master of Science – Business Cybersecurity major.
Comment(s): or permission of the instructor.

INMT 562 Security Governance and Ethics (3) Designed to help students to gain an understanding of the regulatory environment, governance, and ethical issues relating to cybersecurity. The objective of the course is for students to understand how an organization effectively controls information technology (IT) security and manages associated ethical issues.
(RE) Corequisite: INMT 561.
Comment(s): or permission of the instructor.

INMT 563 Business Communications and Network Security (3) Provides students with a foundational knowledge of communication system and network design. It builds on this foundation to define and identify internal and external sources of business network security risk. Students will work with various tools, techniques, and methods to assess communication networks and develop and communicate mitigation strategies to reduce network and overall cybersecurity risk.
(RE) Corequisite: INMT 561.
Comment(s): or permission of the instructor.

INMT 564 Business Information Asset Security (3) Introduces the components, processes and techniques associated with protecting organizational information assets. Students will work with a variety of modern database management and monitoring tools to develop business and technical skills related to management and protection of a broad range of information assets.
(RE) Corequisite: INMT 561.
Comment(s): or permission of the instructor.

INMT 565 Risk Management and Business Continuity (3) Introduces the process and techniques of corporate risk management and business continuity, including its major activities such as risk assessment, risk mitigation, and risk control. Students will learn how to assess, develop, and implement effective risk management practices to meet business continuity objectives.
(RE) Corequisite: INMT 561.
Comment(s): or permission of the instructor.

INMT 566 Organizational Security Management (3) Provides students with an understanding of the human and organizational aspects of security and methods to mitigate risks associated with these areas. Students will work with various tools, techniques, and methods to assess organizational security practices and develop and communicate strategies to reduce overall cybersecurity risk.
(RE) Corequisite: INMT 561.
Comment(s): or permission of the instructor.

Rationale: New courses listed above are to be required of students enrolled in the online MS in Business Cybersecurity (MSBC). Impact on other units: None expected. Financial impact: Cost of instruction included in cost of MSBC degree program, to be offset by tuition revenue generated by this program. Additional documentation: None required.
INMT 567 Business Security Architecture and Systems (3) Covers the fundamentals of designing and implementing a multi-tier security architecture, focusing on the processes and tools used to protect assets and resources housed on organization servers. Students will work with a variety of tools and techniques to develop knowledge and technical skills related to the assessment, design, and management of an organization’s security architecture.
(Re) Corequisite: INMT 561.
Comment(s): or permission of the instructor.

INMT 568 Business Software Development Security (3) Designed to help students to gain fundamental knowledge of secure software development practices. The objective of the course is for students to understand how an organization formulates and manages software development processes where security is built in and ensures confidentiality, integrity, and availability in software applications. Students will work with various tools, techniques, and methods associated with the development, implementation, and management of organizational software applications.
(Re) Corequisite: INMT 561
Comment(s): or permission of the instructor.

INMT 569 Emerging Topics in Business Cybersecurity (3) A seminar designed to study technology innovations that are impacting (disrupting and transforming) the dynamic field of business cybersecurity. The course will focus on the potential opportunities and risks associated with currently trending emerging technologies.
(Re) Corequisite: INMT 561.
Comment(s): or permission of the instructor.

INMT 570 Business Cybersecurity Capstone (3) A capstone project course, enabling students to integrate their learning from prior coursework. Students will work on a broad array of contemporary cybersecurity problems and issues experienced by organizations. Students will have the opportunity to assess, analyze, and solve cybersecurity problems and present their results and solutions as aspiring cybersecurity managers.
(Re) Corequisite: INMT 561 and INMT 562 and INMT 563 and INMT 564 and INMT 565 and NMT 566 and INMT 567 and INMT 568 and INMT 569.
Comment(s): or permission of the instructor.

Rationale: New courses listed above are to be required of students enrolled in the online MS in Business Cybersecurity (MSBC). Impact on other units: None expected. Financial impact: Cost of instruction included in cost of MSBC degree program, to be offset by tuition revenue generated by this program. Additional documentation: None required.

DEPARTMENT OF FINANCE

(FINC) Finance

REVISE TO ADD (Re)PREREQUISITE

FINC 525 Investment Analysis and Portfolio Management (3)
(Re)Prerequisite(s): FINC 507.
Formerly: None.
Rationale: Ensures students have appropriate background knowledge. Impact on other units: None. Financial impact: None.

REVISE (Re)PREREQUISITES

FINC 512 Problems in Financial Management (3)
(Re)Prerequisite(s): FINC 507.
Formerly: (Re)Prerequisite(s): Business Administration 518.

FINC 535 Financial Markets and Institutions (3)
(Re)Prerequisite(s): FINC 507.
Formerly: (Re)Prerequisite(s): Business Administration 518.

FINC 540 Fixed Income Analysis and Markets (3)
(Re)Prerequisite(s): FINC 507.
Formerly: (Re)Prerequisite(s): Business Administration 518.

Rationale: BUAD 518 no longer exists. Impact on other units: None. Financial impact: None.
FINC 545 Financial Derivatives (3)  
(RE)Prerequisite(s): FINC 507.

Formerly: (RE)Prerequisite(s): Business Administration 518.

FINC 555 Financial Management: Theory and Practice (3)  
(RE)Prerequisite(s): FINC 507.

Formerly: (RE)Prerequisite(s): FINC 505, and FINC 506, and FINC 507 and BZAN 507.

REVISE TO DROP (DE)PREREQUISITE AND ADD (RE)PREREQUISITE

FINC 571 International Finance (3)  
(RE)Prerequisite(s): FINC 507.

Formerly: (DE)Prerequisite(s): Business Administration 518.

REVISE DESCRIPTION AND (RE)PREREQUISITE

FINC 581 Real Estate Investment and Finance (3) Explores the major concepts, principles, analytical methods, and tools used to evaluate the financing of and investment in real property. Emphasis is also placed on understanding the factors influencing the dynamics of commercial real estate markets.  
(RE) Prerequisite(s): FINC 505 and FINC 506.

Formerly: Financial and market analysis used to make real estate investment decisions. Effects of variety of financing options on rate of return on income-producing properties. Effect of various financing options on consumer’s decisions to purchase. Relationship between primary and secondary mortgage markets and impact of those markets on cost and availability of funds for real estate lending. Effects of government intervention (taxation, subsidization, and regulation) in both real estate and mortgage markets.  
(RE) Prerequisite(s): Business Administration 518.

Rationale: BUAD 518 no longer exists. Impact on other units: None. Financial impact: None.

DEPARTMENT OF SUPPLY CHAIN MANAGEMENT

(SCM) Supply Chain Management

ADD

SCM 521 Strategic Supply Management & Sustainability (3) Designed for the Tri-Continent SCM master’s program: addresses the processes that facilitate the structure, creation, and management of value-added transactions and relationships between supplier and customer organizations in a channel, supply chain, and integrated value system context with a particular focus on financial techniques to better manage supply chain costs. Will learn how to apply financial measures to supply chain decision-making problems and also to become an effective and efficient supply chain manager. Identifies and advocates for sustainable approaches to sourcing and SCM in general. This is a highly interactive class using cases, simulations and in-class exercises to better align with “real-world” thinking while focusing on foundations of the supply chain and the interactive role of supply management within an organization and as a boundary spanner.  
Knoxville Campus  
Registration Restriction: Graduate students in the Haslam College of Business.

Rationale: This course is specifically designed to fill a gap in Tri-Continent Master’s Program.

SCM 541 Supply Chain Planning and Analysis for Operations (3) Designed for the MBA program: covers the Development of plans for executing supply chain processes to support integration of the supply chain across major functional areas of the business including logistics, marketing, manufacturing, and procurement. To facilitate achievement of these objectives, will introduce analytical tools and techniques that provide a cause and effect understanding linking operational plans with corporate objectives.  
Registration Restriction: Graduate students in the Haslam College of Business.

Rationale: This course is added to fill a gap in the MBA program.

SCM 576 Logistics and Network Management (3) Designed for the Tri-Continent SCM master’s program: addresses strategic decision making related to the physical network design and operation of the supply chain, including the location and capacity of suppliers, plants and warehouses in a logistics network that delivers products and services to end customers. Content in this course will explore the tradeoffs inherent to physical network decision making with special emphasis on managing demand and
lead time variability, matching capacity to demand, centralization and pooling of inventory, and achieving a total value solution. Will apply analytic methods learned in other courses to the problems of supply chain network design and strategic inventory positioning, in order to explore theoretical relationships and to provide students with decision making skills needed in practice.

Knoxville Campus
Registration Restriction: Graduate student in the Haslam College of Business.

Rationale: This course is specifically designed to fill a gap in the Tri-Continent Master’s Program.

REVISE TITLES AND DESCRIPTIONS

SCM 621 Strategic and Sustainable Sourcing: Theoretical Foundations (3) Survey of concepts, frameworks, theory, research issues, and empirical research in content areas related to global strategic and sustainable sourcing. Focus on understanding the theoretical foundations used in the field. Covers conceptual foundations, issue controversies, and future research directions. Registration Restriction(s): Minimum student level – graduate.

Formerly:
Operations and Purchasing Management (3)
Survey of concepts, frameworks, theory, research issues, and empirical research in content areas related to manufacturing and service operations management and purchasing. Conceptual foundations, issue controversies, and future directions.

Rationale: To better reflect content of the course.

SCM 622 Supply Chain Operations, Planning, and Analysis (3) Survey of concepts, frameworks, theory, research issues, and empirical research in content areas related to operations management and planning. Focus on understanding the trade-offs of different empirical research methods. Conceptual foundations, issue controversies, and future directions.

Registration Restriction(s): Minimum student level – graduate.

Formerly: Supply Chain Management Thought (3)
Survey of concepts and research methods of interorganizational systems. Supply chains will be studied from multiple perspectives including the following: institutional design and structure, transaction cost economics, operations and logistics cost economics, exchange behaviors and strategies, supply chain relationship types, and evaluation of supply chain performance.

Rationale: To better reflect content of the course.

II. PROGRAM CHANGES

DEPARTMENT OF ACCOUNTING AND INFORMATION MANAGEMENT

ADD NEW MAJOR AND DEGREE

Major: Business Cybersecurity
Degree: Master of Science

In the 2023 Graduate Catalog, add program and program requirements (pending THEC and SACSCOC approvals)

*This program is pending approval from the Tennessee Higher Education Commission and the Southern Association of Colleges and Schools Commission on Colleges. Students will be admitted to the major should the program be approved.

The online Master of Science in Business Cybersecurity (MSBC) prepares both traditional, full-time students and working professionals attending school part-time with motivation and interest, but not necessarily a technical background, to pursue cybersecurity roles or take on cybersecurity responsibilities within their existing organizational position or future opportunities for those looking for new jobs. There is increasing demand for qualified cybersecurity professionals, encompassing a broad range of roles in organizations, which existing supply cannot meet. This program takes an engagement-based, integrative approach to expand upon traditional technical skills by building understanding of the business context, the regulatory environment, and the managerial and organizational implications of risk and value-generation associated with cybersecurity policies and systems.

Delivery Method: Distance Education

Campus Code: Distance Education
Options Available: Coursework Only Without Comprehensive Exam

Admission Standards/Procedures:

The HCB admissions group will perform reviews of student files along with the faculty program leader from the departments of Accounting and Information Management and Graduate and Executive Education. This group will review all applications and recommend prospective students for admission to the program. The following criteria will be considered when determining applicant admission into the program:

- Meets requirements for admission to the UT Graduate School;
- Holds an undergraduate degree in business (or equivalent) from an accredited program. Applicants with non-business degrees will be reviewed on an individual basis and may be required to complete non-credit training programs and/or additional coursework prior to enrolling in the MSBC program;
- Two applicant recommendation letters are required, and additional evaluation materials (such as GMAT or GRE scores) may be required;
- Applicants whose native language is not English may have to submit results of the Test of English as a Foreign Language (TOEFL) or the International English Language Testing System (IELTS); and
- All students must adhere to all UTK ethical and professional standards (see Hilltopics).

Procedure for Application to Program
- Complete Haslam College of Business Application Form.
- Adhere to application deadlines and other requirements as posted on the Haslam College of Business website.

Academic Standards
- A minimum grade of C in all HCB courses.
- A 3.00 graduate cumulative GPA is required for continuation in the program.
- Students must adhere to ethical and professional standards.

Credit Hours Required:
- 30 graduate credit hours

Required Courses:
Core and Sub-core Requirements (30 graduate credit hours). The MSBC program requires completion of 30 Semester Credit Hours (SCH) distributed as follows (for a semester by semester schedule see Example Full-Time Course Schedule and Example Part-Time Course Schedule below):

<table>
<thead>
<tr>
<th>Course Number</th>
<th>Course Title</th>
<th>SCH</th>
</tr>
</thead>
<tbody>
<tr>
<td>INMT 561*</td>
<td>Foundations of Business Cybersecurity</td>
<td>3</td>
</tr>
<tr>
<td>INMT 562</td>
<td>Security Governance and Ethics</td>
<td>3</td>
</tr>
<tr>
<td>INMT 563</td>
<td>Business Communications and Network Security</td>
<td>3</td>
</tr>
<tr>
<td>INMT 564</td>
<td>Business Information Asset Security</td>
<td>3</td>
</tr>
<tr>
<td>INMT 565</td>
<td>Risk Management and Business Continuity</td>
<td>3</td>
</tr>
<tr>
<td>INMT 566</td>
<td>Organizational Security Management</td>
<td>3</td>
</tr>
<tr>
<td>INMT 567</td>
<td>Business Security Architecture and Systems</td>
<td>3</td>
</tr>
<tr>
<td>INMT 568</td>
<td>Business Software Development Security</td>
<td>3</td>
</tr>
<tr>
<td>INMT 569</td>
<td>Emerging Topics in Business Cybersecurity</td>
<td>3</td>
</tr>
<tr>
<td>INMT 570**</td>
<td>Business Cybersecurity Capstone</td>
<td>3</td>
</tr>
</tbody>
</table>

Electives:
- No formal course electives are offered as part of the program.

*INMT 561 must be taken in the first semester. It is a co-requisite for all other courses.
**INMT 570 must be taken in the final semester. All other courses are co-requisites.

While MSBC will begin with the introductory course (INMT 561) and ends with the capstone course (INMT 570), students can take the remaining coursework in a manner that best fits with their schedule and finances allow. This flexibility would allow students to complete the program in as little as 12 months or more slowly based upon their individual situations. Thus, MSBC will not strictly be using a cohort system. Leave of Absences (LOA) will be allowed but students must complete the degree requirements in 6 years.

Example Full-Time Course Schedule (12 months):

<table>
<thead>
<tr>
<th>Course Number</th>
<th>Course Title</th>
<th>SCH</th>
</tr>
</thead>
<tbody>
<tr>
<td>INMT 561</td>
<td>Foundations of Business Cybersecurity</td>
<td>3</td>
</tr>
<tr>
<td>INMT 562</td>
<td>Security Governance and Ethics</td>
<td>3</td>
</tr>
<tr>
<td>INMT 563</td>
<td>Business Communications and Network Security</td>
<td>3</td>
</tr>
<tr>
<td>INMT 564</td>
<td>Business Information Asset Security</td>
<td>3</td>
</tr>
</tbody>
</table>

SPRING TERM
INMT 565  Risk Management and Business Continuity  3
INMT 566  Organizational Security Management  3
INMT 567  Business Security Architecture and Systems  3
INMT 568  Business Software Development Security  3

SUMMER TERM
INMT 569  Emerging Topics in Business Cybersecurity  3
INMT 570  Business Cybersecurity Capstone  3

Example Part-Time Course Schedule (variable time period not to exceed 6 years):

<table>
<thead>
<tr>
<th>Course Number</th>
<th>Course Title</th>
<th>SCH</th>
</tr>
</thead>
<tbody>
<tr>
<td>FALL I TERM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INMT 561</td>
<td>Foundations of Business Cybersecurity</td>
<td>3</td>
</tr>
<tr>
<td>INMT 564</td>
<td>Business Information Asset Security</td>
<td>3</td>
</tr>
<tr>
<td>SPRING I TERM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INMT 562</td>
<td>Security Governance and Ethics</td>
<td>3</td>
</tr>
<tr>
<td>INMT 568</td>
<td>Business Software Development Security</td>
<td>3</td>
</tr>
<tr>
<td>SUMMER TERM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INMT 563</td>
<td>Business Communications and Network Security</td>
<td>3</td>
</tr>
<tr>
<td>INMT 565</td>
<td>Risk Management and Business Continuity</td>
<td>3</td>
</tr>
<tr>
<td>FALL II TERM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INMT 566</td>
<td>Organizational Security Management</td>
<td>3</td>
</tr>
<tr>
<td>INMT 567</td>
<td>Business Security Architecture and Systems</td>
<td>3</td>
</tr>
<tr>
<td>SPRING I TERM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INMT 569</td>
<td>Emerging Topics in Business Cybersecurity</td>
<td>3</td>
</tr>
<tr>
<td>INMT 570</td>
<td>Business Cybersecurity Capstone</td>
<td>3</td>
</tr>
</tbody>
</table>

Graduation / Academic Standards
To be eligible for graduation, students must:

- complete the entire curriculum plan per UTK Graduate School policies as specified by the University of Tennessee.
- have a 3.00 graduate GPA to graduate.

RATIONALE: SUPPORTING INFORMATION:

Academic/Institutional need. The MSBC program is consistent with the goals and priorities of UTK, striving to contribute toward the university's stated goals and mission to "empower learners of all ages and backgrounds to achieve their dreams through accessible and affordable education, advance the prosperity, well-being, and vitality of communities across Tennessee and around the world through our research, teaching, service, and engagement, and commit to excellence, equity, and inclusion within the university, across the state, and in all our global activities." In addition, although two Tennessee universities offer business concentrations in this area (East Tennessee State University and Middle Tennessee State University), this will be the first standalone, comprehensive cybersecurity MS degree offered through a college of business in the State of Tennessee. This new program is significantly distinguishable from the University of Tennessee's existing Master of Science in Computer Science concentration in Cybersecurity, and similar programs from a Computer Science or related department, in both its target market and curriculum focus. The Computer Science program targets students with an undergraduate in Computer Science or a background in similar technical and mathematical skillsets, focusing on a deep dive into the technical aspects of cybersecurity and employment in associated technical positions. In contrast, this program is developed to enable individuals without a technical undergraduate program to transition into cybersecurity positions where the skillsets require competency and knowledge of the technical aspects but have a stronger emphasis on the intersection of the technology and the business context in terms of policy, risk, governance, communication, and management.

Student demand. The department of Accounting and Information Management currently offers courses in cybersecurity at both the undergraduate and graduate levels. These students, as well as alumni of our existing programs, have increasingly expressed interest in a graduate degree in Business Cybersecurity at the Haslam College of Business as a way of deepening their knowledge of cybersecurity, enhancing their employment opportunities, and earning potential, or transitioning from their current position into a cybersecurity role.

Following up on these conversations, we conducted a survey of students enrolled in an information management course (BUAD 342) taken by Haslam College of Business students in the fall semester of 2021. Course instructors of BUAD 342 invited all Haslam students enrolled in 14 sections to participate in the online survey. To maximize the response rate, instructors provided time during class for students to complete the survey. Five hundred seventeen (517) students completed the survey, yielding a 62% response rate.
rate. Key findings from the survey indicate a strong interest, and potential demand, among current Haslam students for such an offering. A majority (75%) of respondents indicated they would consider pursuing a master’s degree within five years of completing their bachelor’s degree. Additionally, 61% of respondents indicated they would consider pursuing a master’s degree within two years or less after completing their bachelor’s degree. Independent of the likelihood of pursuing a master’s degree in the future, when asked about their potential interest in a Master of Business Cybersecurity program at Haslam College of Business, a majority (65%) of respondents indicated some level of interest.

When asked how likely they would consider enrolling in a Master of Business Cybersecurity program at Haslam College of Business, 19% (n=96) of respondents indicated they were either likely or certain to enroll in the program, and 37.14% (n=192) of respondents indicated they could enroll in the program.

Survey findings also indicate a strong interest in a program that caters to working professionals. Most respondents indicated they would work either full-time (34%) or part-time (47%) while enrolling in a master’s degree program. As for reasons to pursue a master’s degree (respondents were allowed to choose multiple reasons), “to improve earning potential” (24%) and “to expand employment opportunities” were the top two reasons indicated by respondents.

Additionally, a market study was conducted by Noodle to capture the competitive landscape and interest in a master’s degree in business cybersecurity. Key findings from the market report indicate a strong market of potential students, with a 10-year growth rate of 13.7%. Findings also indicate an increase in demand for online programs in this area.

Employer need. According to the International Information Systems Security Certification Consortium (ISC)² Workforce Study, the workforce needs to grow 65% to meet current demand for qualified cybersecurity professionals. In the United States, there are over 597,000 open cybersecurity positions as of March 2022 and a supply of cybersecurity professionals to fill only 68% of those roles. The workforce gap is similarly concerning in Tennessee (73% of 6,729 jobs) and adjacent states (e.g., Georgia 67% of 21,868 jobs, North Carolina 67% of 21,010 jobs, and Virginia 68% of 53,767).

In response to this workforce gap, the Tennessee Higher Education Commission Supply and Demand Report pursues both traditional and new pathways for growing the cybersecurity workforce. Of the six universities in Tennessee that offer a master’s program related to cybersecurity, four offer a program in computer science or a related department, focusing primarily on the technical aspects of cybersecurity. Only three universities (Virginia Tech, Georgia State University, and the University of South Florida) offer a program in computer science or a related department, focusing on the technical aspects of cybersecurity. Two programs offered in the college of business (East Tennessee State University and Middle Tennessee State University) offer only a concentration in this area. Meanwhile, few research universities in the southeast region offer cybersecurity-related master’s programs. Like universities in Tennessee, most of these universities offer a program in computer science or a related department, focusing on the technical aspects of cybersecurity. Only three universities (Virginia Tech, Georgia State University, and the University of South Florida) offer the program in the college of business; among them, the University of South Florida is the only one that has a standalone, comprehensive cybersecurity program.

The proposed MSBC is well positioned to address a portion of the cybersecurity workforce gap. Although demand remains high for purely technical roles in cybersecurity, business leaders are recognizing that cybersecurity represents a major component of core business operations. This expansion of cybersecurity outside the technical domain is emphasized by high demand for skills that blend technical skills with complimentary business and organizational knowledge, such as risk management, governance, and regulatory compliance (see footnote 2). This program will be distinctive in that it takes an integrated approach that expands upon traditional technical skills by emphasizing the broader implications of cybersecurity in the business context. Beyond cutting-edge coursework, the program will leverage industry partnerships to bring current practices into the classroom and ensure students are “job-ready” upon graduating. The curriculum will enable students to fulfill many underserved roles in the market (i.e., those focused on risk management, governance, project management, security awareness, training, etc.) that require individuals who can liaise between system developers and other functional units.

In tandem with this expansion of the cybersecurity domain, there has been a shift in the path and entry point to a career in cybersecurity. A little over half of cybersecurity professionals are now entering the cybersecurity careers without a cybersecurity or similar technical background, transitioning from unrelated career fields or pursuing cybersecurity education on their own (see footnote 2). This program is developed to enable individuals without a technical undergraduate program to transition into cybersecurity positions where the skillsets require competency and knowledge of the technical aspects but have a stronger emphasis on the intersection of the technology and the business context. Additionally, the program is designed intentionally to be flexible and accessible to meet the needs of working professionals and individuals who cannot be full-time, on-campus students.

Staffing impact. Two additional tenure-track faculty have been approved for hire prior to the launch of the new program. One new non-tenure track faculty member will be funded through revenues generated from the program. Anticipated support staff will be funded through revenues generated from the program.

Financial Impact.

<table>
<thead>
<tr>
<th></th>
<th>Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2023-24</td>
</tr>
<tr>
<td>Program Fees</td>
<td>$464,101</td>
</tr>
</tbody>
</table>

1. [ISC² Workforce Study](https://www.isc2.org/Research/Workforce-Study)
2. [CyberSeek.org](https://www.cyberseek.org)
3. [8 Reasons Why Cybersecurity Strategy and Business Operations are Inseparable](https://www.isc2.org/Research/Workforce-Study)
<table>
<thead>
<tr>
<th></th>
<th>$0</th>
<th>$464,101</th>
<th>$2,024,648</th>
<th>$2,513,597</th>
<th>$3,146,455</th>
<th>$3,723,033</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total Revenue</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Expenditures</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fees - UTK</td>
<td>$27,909</td>
<td>$83,727</td>
<td>$130,388</td>
<td>$167,891</td>
<td>$200,161</td>
<td>$1,213,011</td>
</tr>
<tr>
<td>OPM Upfront Fees*</td>
<td>$867,693</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>OPM Annual Operating Costs</td>
<td>$1,213,011</td>
<td>$992,645</td>
<td>$1,274,784</td>
<td>$1,417,768</td>
<td>$1,397,512</td>
<td>$1,963,941</td>
</tr>
<tr>
<td>HCB Operating Costs</td>
<td>$161,000</td>
<td>$390,425</td>
<td>$380,188</td>
<td>$360,243</td>
<td>$355,601</td>
<td>$366,269</td>
</tr>
<tr>
<td><strong>Total Expenditures</strong></td>
<td>$1,028,693</td>
<td>$1,631,345</td>
<td>$1,456,560</td>
<td>$1,765,415</td>
<td>$1,941,259</td>
<td>$1,963,941</td>
</tr>
<tr>
<td><strong>Total Contribution HCB</strong></td>
<td>($1,028,693)</td>
<td>($1,167,244)</td>
<td>$568,088</td>
<td>$748,182</td>
<td>$1,205,196</td>
<td>$1,759,092</td>
</tr>
</tbody>
</table>

*Includes course buildouts, marketing and recruiting costs and first-year operating expenses.

Revenues are based upon a 6-hour progression, with one course taken in summer. Projected new enrollments each year, based upon the initial market study by Noodle are: 30 in the first year, 46 in year two, 60 in year three, 75 in year four, and 84 by year five.

**Impact on other units.**

This new program is expected to have impact in a few important ways:

- **Graduate student recruiting.** The MSBC program would increase the number of graduate students on the UTK campus by approximately 30 in year one and more in subsequent years. Given the target market could include students with limited or no work experience along with working professionals, it is also anticipated that the University will be able to retain top undergraduates who would otherwise leave to pursue graduate studies in cybersecurity or related majors elsewhere. Once successful, this program would also serve as a solid foundation for future expansion of graduate level business cybersecurity education. As an example, we could launch graduate business cybersecurity certificates geared toward focused cybersecurity topic areas, such as risk management, identity access and control, or governance and compliance.

- **Research output and collaborations.** Having a vibrant master’s program will help foster greater research productivity by providing a greater opportunity for Accounting and Information Management research faculty to leverage teaching topics that align more closely with the research they conduct, increasing idea generation and synergy between those activities. The potential for RAs with similar field of interest and knowledge could also enhance research productivity. Given the implications of cybersecurity across research disciplines, research output will be strengthened and broadened in the Department of Accounting and Information Management and enhance potential for collaboration with other departments in the Haslam College of Business and across the university.

- **Benefits to the State of Tennessee.** This proposal responds to the State of Tennessee’s focus on Student Success by broadening the range of students that can pursue an education and career in business cybersecurity. The program is intentionally flexible to reach individuals across the state and beyond who cannot be full-time, on-campus students. Partnering with Noodle to develop an engaging, interactive and personalized learning environment allows for better student engagement and retention, increasing the chances for students to successfully complete the program. The program will also help meet industry demand for cybersecurity professionals who have the skillset to work in roles at the intersection of technology and business.

- **Learning objectives supported.**

Proposed learning outcomes may include:

- Demonstrate understanding of the impacts of cybersecurity on the business environment;
- Demonstrate awareness and implications of regulations and external factors associated with organizational cybersecurity;
- Demonstrate the ability to leverage key technologies for the design, implementation, and protection of organizational assets;
- Demonstrate understanding of policy, operations, and management of organizational business processes; and
- Demonstrate the ability to apply cybersecurity skills and knowledge to real-world business scenarios.

These learning objectives will be paired with program assignments and course grades.

**Evidence from Assessment Activities**

None identified as this is a new program, but external evidence regarding student demand and employer need is reported above.