# CDS640 Executive Cyber Leadership
## (3 credit hours)
## Course Syllabus

---

## Course Description

Executive Cyber Leadership examines the aspects of leadership in a cybersecurity setting. This course will cover a variety of topics including supervision, decision making, communication, conducting evaluations, and more. It will detail on how leaders in cyber security execute decision-making and establish a vision and direction for an organization's cyber operations.

## Course Learning Outcomes

By the end of this course, you will be able to:

1. Describe the cyber security vulnerabilities of various industry technologies.
2. Describe current laws, regulation, policies, and ethics as they relate to cybersecurity
3. Develop a policy that reflects system security objectives.
4. Demonstrate via recording or observation how to communicate with all levels of management.
5. Propose a strategy for anticipating new security threats.
6. Use critical thinking skills to analyze organizational patterns and relationships.
7. Describe the relationship between strategy, business, and technology in the context of organizational dynamics.

## Required Textbook(s) and Resources

For this course you will need to purchase the following materials:

Textbook: Touhill, G. J. & Touhill, C. J. (2014). *Cybersecurity for executives: A practical guide,* (1st Ed). John Wiley & Sons, Inc. ISBN-10: 9781118888148; ISBN-13: 978-118888148

Note: this course may contain additional resources for specific activities. Be sure to read the instructions carefully for individual assignments or activities for those requirements. Where applicable, Tiffin University has obtained permission to use copyrighted material.

Visit the Tiffin University Library for access to databases, research help, and writing tips. A link is available in the Start Here section (Quick Links). You might consider registering for one of the library's many webinars on library research, source evaluation, copyright, and other topics, at the Library Events - Upcoming Events web page. If you register but cannot attend a live session, the library will email you a link to the session recording after the event. For further assistance email a librarian, at: library@tiffin.edu.

## Time Commitment

Effective time management is possibly the single most critical element to your academic success. To do well in this online class you should plan your time wisely to maximize your learning through the completion of readings, discussions, and assignments. Because of our accelerated, seven-week term, TU online courses are designed with the expectation that you dedicate a little over **six (6)** hours per credit hour to course activities and preparation **each week**. For example, for successful completion of a three-credit, seven-week online course you should reserve roughly **twenty (20) hours per week**.

To help plan your time and keep on track toward successful course completion, note the distinctive rhythm of assignment due dates:

1. All times assume Eastern Time (GMT-4).
2. Weeks begin at 12:00 a.m. ET on Monday and end at 11:55 p.m. ET on Sunday.
3. Unless otherwise noted, initial assignments or discussion posts are due by **11:55 p.m. ET** on **Wednesdays.**
4. Additional assignments or follow-up discussion posts are due by **11:55 p.m. ET** on **Saturdays, and**
5. Major assignments and reflections are typically due by **11:55 p.m. ET** on **Sundays.**

## Learning Activities

The learning objectives of this course, described above, are organized to build the capabilities and confidence you will need in the real-world as leaders and executives dealing with cybersecurity. Through weekly discussions that ask probing questions where you will be required to analyze, extract relevant information, evaluate the core requirement/concept, and present a logically based and defended post.

Weekly written assignments (papers) will build your knowledge base across the critical functions of any cybersecurity program (Identify, Protect, Detect, Respond, and Recovery). These will ultimately be demonstrated at the end of the course where you will pull all the distinct elements together to create a viable organizational level ***[Cyber]*** System Security Policy/Plan.

## Grading

The chart below identifies the individual contributions from each type of activity, per week.

| Week 1 | Week 2 | Week 3 | Week 4 | Week 5 | Week 6 | Week 7 | Total |
|---|---|---|---|---|---|---|---|
| **Discussions**<br>Activity 1.1<br>(n/a)<br>Activity 1.2<br>(30) | **Discussions**<br>Activity 2.1<br>(30) | **Discussions**<br>Activity 3.1<br>(30) | **Discussions**<br>Activity 4.1<br>(30) | **Discussions**<br>Activity 5.1<br>(30) | **Discussions**<br>Activity 6.1<br>(30) | **Discussions**<br>Activity 7.1<br>(30) | **210** |
| **Assignments**<br>Activity 1.3<br>(80) | **Assignments**<br>Activity 2.2<br>(80) | **Assignments**<br>Activity 3.2<br>(80) | **Assignments**<br>Activity 4.2<br>(80) | **Assignments**<br>Activity 5.2<br>(80) | **Assignments**<br>Activity 6.2<br>(80) | **Assignments**<br>Activity 7.2<br>(230)<br>Activity 7.3<br>(80) | **790** |
| **Reflection (Extra Credit)**<br>Activity 1.4<br>(15) | | **Reflection (Extra Credit)**<br>Activity 3.3<br>(15) | | **Reflection (Extra Credit)**<br>Activity 5.3<br>(15) | | **Reflection (Extra Credit)**<br>Activity 7.4<br>(15) | |
| **110** | **110** | **110** | **110** | **110** | **110** | **340** | **1000** |

## Grading Scale

| Grade | Percentage |
|---|---|
| A | 90-100% |
| B | 80-89% |
| C | 70-79% |
| F | ≤69% |

Please see the Academic Bulletin for grade appeal information.

## Course Schedule and Weekly Checklist

| Topic | **Learning Activities** (Due by 11:55 p.m. ET on day designated) |
|---|---|
| Start Here | ☐ MON: Activity 1.1: Meet Your Peers |
| **Week 1: Introduction & Overview**<br>● Leadership<br>● Management<br>● R&R of CIO/CISO | ☐ WED: Activity 1.2: Leadership vs. Management – Initial Post<br>☐ SAT: Activity 1.2: Leadership vs. Management – Secondary Responses<br>☐ SUN: Activity 1.3: CIO and CISO Organizational Impact<br>☐ SUN: Activity 1.4: Reflection (Extra Credit) |
| **Week 2: Laws, Regulations & Ethics**<br>● Laws & Regulations related to Cyber<br>● Ethics | ☐ WED: Activity 2.1: Cybersecurity Responsibilities – Initial Post<br>☐ SAT: Activity 2.1: Cybersecurity Responsibilities – Secondary Responses<br>☐ SUN: Activity 2.2: Three Types of Hackers |
| **Week 3: Critical Thinking & Risk Analysis**<br>● Critical thinking<br>● Risk & Risk Analysis | ☐ WED: Activity 3.1: Critical Thinking and Arguments – Initial Post<br>☐ WED: Activity 3.1: Critical Thinking and Arguments – Secondary Responses<br>☐ SUN: Activity 3.2: Critical Risk Analysis<br>☐ SUN: Activity 3.3: Cybersecurity Reflection (Extra Credit) |
| **Week 4: Strategic Approaches to Threat Analysis**<br>● Threat Analysis<br>● Scenario-Based Planning | ☐ WED: Activity 4.1: Breach Discovery – Initial Post<br>☐ SAT: Activity 4.1: Breach Discovery – Secondary Responses<br>☐ SUN: Activity 4.2: Modeling Technologies |

| | |
|---|---|
| **Week 5: Cyber Organizational Structures & Impacts**<br>• Cybersecurity Organizational Structures - light, medium, heavy<br>• Revisit: Leadership & Management Theories applied to Cybersecurity | ☐ WED: Activity 5.1: Executive Responsibilities – Initial Post<br>☐ SAT: Activity 5.1: Executive Responsibilities – Secondary Responses<br>☐ SUN: Activity 5.2: Organizational Charts and Business Operations<br>☐ SUN: Activity 5.3 Reflection (Extra Credit) |
| **Week 6: Economics of Cyber**<br>• Calculating cybersecurity costs<br>• Budgeting for Cybersecurity | ☐ WED: Activity 6.1: Budget Request – Initial Post<br>☐ SAT: Activity 6.1: Budget Request – Secondary Posts<br>☐ SUN: Activity 6.2: Cybersecurity Assessment Tool |
| **Week 7: Organizational Dynamics in the Cybersecurity Environment**<br>• Cyber organization structures<br>• Integrated System Security Policies/Plans | ☐ WED: Activity 7.1: The System Security Plan – Initial Post<br>☐ SAT: Activity 7.1: The System Security Plan – Secondary Posts<br>☐ SUN: Activity 7.2: Developing an SSP<br>☐ SUN: Activity 7.3: Briefing SSP to the Board<br>☐ SUN: Activity 7.4: SSP Reflection (Extra Credit) |

## Tips for Success

Successful online learning requires a good deal of self-discipline and self-direction. As seekers of the truth, we should be willing to challenge and review one another's academic work in a spirit of respectful comradery and constructiveness. You should accept constructive feedback as a gift. Your course is a place for you to stretch and grow as you benefit from the expertise, knowledge, experience and diverse perspectives of your instructor and peers. Constructive feedback will challenge you to stretch your own thinking, thereby expanding your knowledge, understanding and application.

To get the most out of your learning experience, you should actively engage (participate) in **ALL** course activities. Course elements in any given week are arranged chronologically. To complete a week, simply work your way "down the page" through all of the course materials and activities.

## Your Instructor Will Expect You to:

- Thoroughly review orientation materials (Start Here) within the first 48 hours of the term.
- Monitor your TU email account **daily** for important updates and announcements.
- Take ownership of your learning experience and act in a proactive, self-directed manner. That means:
    - Fully participate in all learning activities.
    - Complete assignments as described in rubrics or other instructions.
    - Submit all work on time and in the specified format (e.g. APA format for citations).
    - Utilize and incorporate instructor provided feedback to improve your work.
    - Ask questions so you can better understand course material or assignments.
    - Use the highest standards of intellectual honesty and integrity. For more information, see the TU Library guide: Digital Literacy: Netiquette and Internet Safety.
    - Treat others respectfully and demonstrate "netiquette" (online politeness and respectfulness) at all times. TU celebrates cultural uniqueness and expects all students to be considerate and thoughtful throughout their learning experiences.

## You Should Expect Your Instructors to:

In general, your instructors should advocate for your success as a learner and help guide you toward successful completion of the course activities and most importantly, attainment of the course learning outcomes. To accomplish this, your instructors should:

- Post an introductory announcement/email at the beginning of each week to provide updates and help you prepare for the week's activities.
- Maintain an active and engaged presence in all course activities and throughout the course.
- Respond to your emailed questions within 48 hours, if not sooner.
- Clearly communicate any absences or expected non-participation due to extenuating circumstances. For example, "I will be traveling to attend a funeral this week and may not be able to respond to questions or participate in forums for a couple of days."
- When grading your work, your instructors should:
    - clearly indicate their grading approach (what they like to see in submitted work as well as what types of errors they tend to penalize more harshly),
    - thoroughly review and evaluate your submissions in a timely manner (in less than 5 days for most assignments), and

- provide constructive feedback that indicates the strengths and weaknesses of your work and provides suggestions on how you can improve your performance on future assignments.

## Accommodations

The **Office for Disability Services** supports the institutional commitment to diversity by providing educational opportunities for qualified individuals with disabilities through accessible programs and services in compliance with Section 504 of the Rehabilitation Act of 1973 and Title III of the Americans with Disabilities Act (ADA) of 1990.

If you need reasonable accommodations due to a documented disability, contact the Office for Equity, Access, & Opportunity 419.448.3021 or via email at disabilityservices@tiffin.edu.

## Additional Resources & Support

For technical support, either email moodlesupport@tiffin.edu or call the 24/7 Technical Support Call Center at 855-664-1200.

If you need to consult an academic advisor refer to TU's Meet the Team page.

For information about TU's peer tutoring program see the Murphy Center's Tutoring Policies and Procedures page. Veterans and active military can seek assistance from TU's Veteran and Military Services Web Page.

## Comments or Concerns

TU's online programs are designed to be student *driven*: to empower you with a voice and stake in your learning. Our courses feature multiple and varied ways that you can share feedback, and we invite you to become an active voice and help drive our improvement efforts. In addition to providing in-course feedback, we encourage you to submit questions or comments directly to the online team at online@tiffin.edu.