

IMPLEMENTING PUBLIC AND PRIVATE
HIGHER EDUCATIONAL INSTITUTION
CYBER SECURITY ARTICULATION
AGREEMENTS IN 9-12 SCHOOLS

COURSE:
CYBER SECURITY FUNDAMENTALS

Presenter:

Dr. Thomas Rzemyk, Ed.D., CHPP, CAS

PURPOSE

- Communicate strategies, best practices, and recommendations that our institution has taken to be successful in implementing cyber security curriculum at the 9-12 grade levels.
- Outline the importance of partnerships with *public* and *private* educational institutions to establish valuable articulation agreements that serve the best interests of our students.
- Explore future opportunities to further enhance curriculum and student experiences.

PRESENTATION OVERVIEW

- Importance of cyber security education in 9-12 schools
- Mount Michael Benedictine School Overview & Mission Statement
- Why did we decide to pursue to pursue cyber security curriculum for our students
- Articulation Agreements
- Curriculum Overview (Part I & II)
- Topics & Subtopics
- University of Omaha Dual Enrollment
- Exploratory Trips
- Assessing Students
- Advanced After School I.T. Club
- Upcoming Publications

WHY IS CYBER SECURITY IMPORTANT IN GRADES 9-12?

- Increasing demand for young professionals both men and women to enter the cyber security sector.
- Career Opportunities
- Workforce Opportunities
- Networking Opportunities
- Practical Level Experience Opportunities
- Imperative to integrate this type of curriculum in college preparatory institutions and those offering advanced Information Technology courses.
- Develops cognitive skills and abilities to complete complex technical tasks



MOUNT MICHAEL BENEDICTINE HIGH SCHOOL OVERVIEW

- Mount Michael Benedictine School is a Catholic, college-preparatory residential & day high school. At Mount Michael the core of the academic program enables students to become inquiring learners, appreciative of their heritage, responsive and committed to the challenges of the future.
- At Mount Michael the monks, lay faculty, and staff instill the value of moral leadership so that they may live in harmony with each other, their families, and the community at large. At Mount Michael the search for God is fundamental to understanding the meaning of life; Christian charity is grounded in our relationships with ourselves, our families, and all whom we meet. As gifts of God, individual talents are to be developed fully and shared generously.

MOUNT MICHAEL BENEDICTINE HIGH SCHOOL MISSION STATEMENT

- Mount Michael Benedictine School is a Catholic college preparatory residential/day high school rooted in Benedictine values for young men committed to excellence. Students develop spiritually, intellectually, and socially through the comprehensive curriculum and communal experience to become future leaders.

GOALS & STEPS FOR ESTABLISHING ARTICULATION AGREEMENTS

- Mount Michael Benedictine School's goal was to offer a cyber security course that allowed our students to earn *college credit* while covering advanced concepts
- First Step: Network with local public & private institutions
 - (i.e. University of Nebraska-Omaha, Creighton University, etc.)
- Second Step: Determine if the prospective college/university meets your institutions goals
- Third Step: Create a dialogue with key stakeholders emphasizing the overall goals of your program and prospective course (Email, call, go to the host institution for a visit)
- Fourth Step: Align with schools that have a strong support system, STEM program, cyber security program, faculty, administration, accreditation, etc.
- Fifth Step: Submit a syllabus for review/approval to the host college/university

INNOVATIVE & ENGAGING CURRICULUM

- Mount Michael is of the first schools in the state of Nebraska to offer a Cyber Security focused course at the high school level
- We are the first school in the state of Nebraska and possibly in the Midwest to offer an all in one cyber security course on both public policy and cyber security network fundamentals
- Advanced level concepts taught over two semesters (one academic school year August-May)
- Over 250 topics covered over one academic school year
- Exploratory Day Trips (i.e. data centers, secure facilities, UNO STEM Labs)
- Guest Speakers (Industry Professionals, Public Officials, Cyber Experts, Criminal Investigators)

CYBER SECURITY FUNDAMENTALS COURSE DESCRIPTION

- *This course will provide students an overview into the field of cyber security to include public policy concepts. It will focus on several components of computer science and networking theories .*
- *Topics include cyber security policy, cyber security law, cyber security research, cyber operations, ethical hacking, protocols, cyber architecture, security architecture, digital forensics, intrusion detection, malware, cloud computing, and computer networking.*
- *This course will also offer hands on practical and virtual labs*

GOALS & STEPS FOR ESTABLISHING ARTICULATION AGREEMENTS

- Sixth Step: Work closely with the faculty of the host institution to make changes/revisions/edits
- Seventh Step: Communicate! Communicate! Communicate! (wants/needs/deadlines/approvals, etc)
- Eighth Step: Many institutions will require that the syllabus go through a curriculum committee as part of the approval process
- Ninth Step: For our course we took a standard syllabus and added content, thus creating a custom course that offers public policy and network fundamentals
- Final Step: Be flexible throughout the process and during the first year of the course. Provide feedback!

PART 1: PUBLIC POLICY

- In the first semester students learn about “all” elements of cyber security.
- It is important to understand the *foundational* concepts and practices of cyber security
- Why is cyber security such a buzz word?
- What does the term cyber security stand for?
- Why is public policy, law, and ethics important in cyber security?

PART II: ADVANCED NETWORKING FUNDAMENTALS

- In the second semester, students learn about *basic* to *advanced* networking concepts.
- Students leave the course understanding terminology, concepts, objectives, and the peripherals involved with cyber security.
- Students experience hands-on labs both inside and outside of the classroom.

FIRST SEMESTER

- We will cover topics ranging from:
- Cyber Law
- Cyber Ethics
- Cyber Legislation (State, Federal, International)
- Cyber Careers
- Public Policy
- Cyber Terrorism
- Cyber Crimes
- Domestic Cyber Security
- Global Cyber Security
- White Collar Crime
- Cyber Warfare
- And much more!

SECOND SEMESTER

- We will cover topics ranging from:
- Cyber Security Concepts
- Networking Principals
- Networking Peripherals & Equipment
- Wireless Security
- Cyber Warfare
- Information Assurance
- IT System Components
- Cloud Computing
- Risk Assessment & Vulnerability Analysis
- Auditing
- And much more!

UNIVERSITY OF NEBRASKA AT OMAHA: DUAL ENROLLMENT COURSE

- College level advanced course
- Students earn (3) college credits (this will change next year to 4-6 college credits as more topics are covered)
- Credits can be applied to an undergraduate information security UNO or to more than 92% of schools around the country
- 1:8 Teacher to Student Ratio

UNIVERSITY OF NEBRASKA-OMAHA: *REQUIREMENTS & STANDARDS*

- As outlined in the articulation steps, the course must be approved and offered as a dual enrollment course
- Students must register within the first two weeks of the course
- Students must maintain a cumulative GPA of 3.0 or they are not granted college credits
- Must participate in all college activities associated with the course

DUAL ENROLLMENT BENEFITS

- Course costs 25% of a normal college course at UNO
- Students have access to *all* of the university resources to include the online electronic library
- Gain experience and confidence
- Students demonstrate competitiveness for admissions to universities and scholarships

DUAL ENROLLMENT CHALLENGES

- Course work is demanding for students
- Requires effective and efficient time management skills as there is a significant amount of work completed outside of the classroom
- Commitment required by all faculty members to meet and exceed host institutions expectations

SCOTT DATA CENTER EXPLORATORY FIELD TRIP

Purpose:

To expose students to a real world operating secure data center

TOUR DETAILS

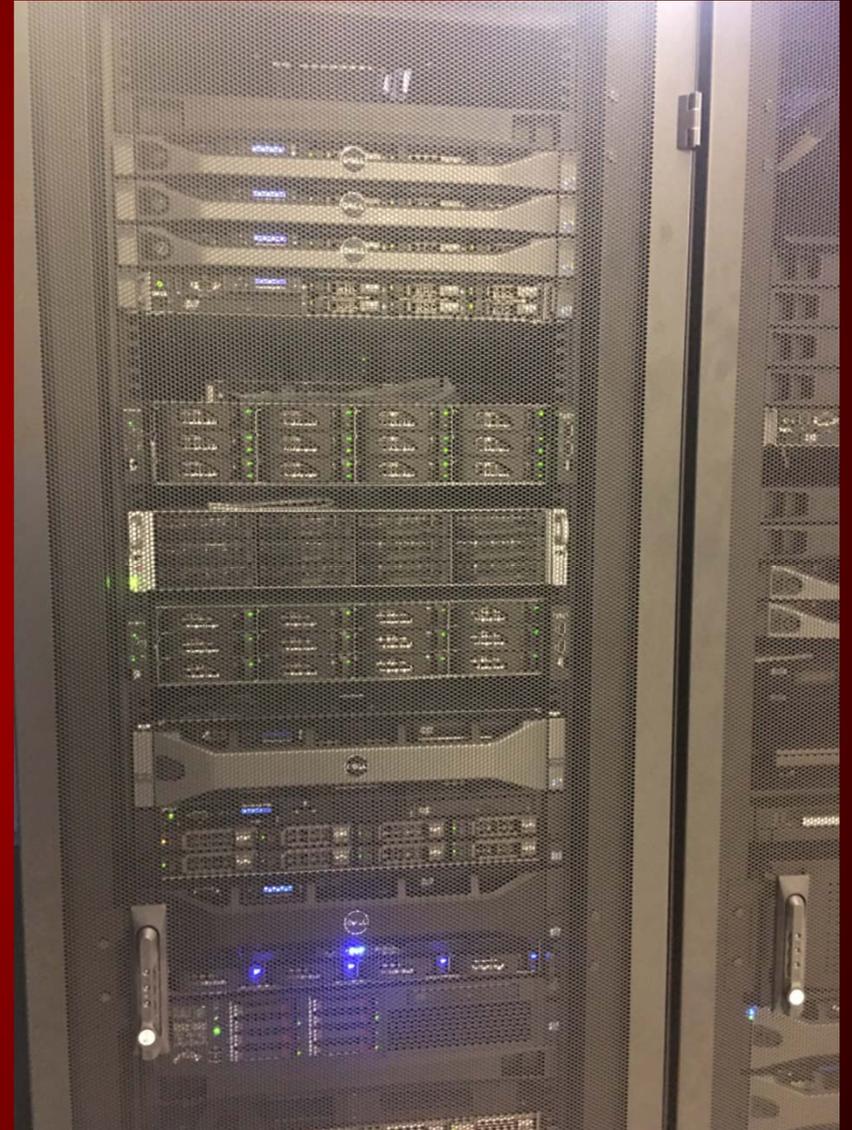
- One of the largest data centers in the state
- Non profit data center hosted by the University of Nebraska-Omaha
- Certified Tier III facility by the Uptime Institute
- Facility can withstand 285+MPH Winds
- Facility was built in 2003 and originally housed cyber operations for Offutt AFB in Bellevue, Nebraska
- Facility can operate off the grid and has its own powerplant and water cooling turbines
- Self sustained facility (i.e. uses the heat from the server room to heat 35,000 sq ft.)

PHOTOS FROM THE SCOTT DATA CENTER TOUR





ADDITIONAL PHOTOS



SURVEY INSTRUMENT: *GATHERING FEEDBACK*

- One of the key elements to ensuring that a class is going well and according to plan, is to *assess* students and gather feedback
- Four times per year, random surveys are given to the students to assess if a certain project, exploratory trip, assessment, etc., was in line with the learning objectives for the course.
- Assessments also gauge if an activity or exploratory trip was engaging, relative to the course content, etc.
- For example, after the Scott Data Technology Center exploratory trip, I sent students a 40 question survey instrument to assess what they learned
 - Survey results showed 100% of the class enjoyed the trip, found it engaging, learned at least five different things, etc.

FUTURE OF COURSE

- The course will continue to develop into new areas and concepts.
- Assess/Survey students at *least* four times per year (once a quarter) to determine if the course is meeting the expectations of the students.
- A second cyber security class in development which will focus on advanced concepts.
- Additional dual enrollment opportunities will be sought out.
- Continue positive relations with partner colleges and universities.
- Maintain constant communication with dual enrollment staff.

ADVANCED AFTER SCHOOL I.T. CLUB

- Allows students to explore concepts and learning objectives more in-depth and in flexible format
- Students can conduct hands-on physical labs with networking equipment
- Students can conduct virtual labs
- Students can brainstorm
- Students can assist with real-world technology troubleshooting on campus
- Students can conduct research
- Establish a coding club

UPCOMING TEXTBOOK PUBLICATIONS

- Volume I (Scheduled Release 10/2017)
- Title: ***Cybersecurity: Introduction and Public Policy and Procedures***
- The first textbook will focus on cyber security and public policy at the *public* and *private* levels while examining, local, state, federal, and global concepts. It will cover cyber security topics to include: policies, procedures, ethics, warfare, terrorism, espionage, cybercrime, white collar crime, cyber law, cyber legislation, digital forensic, career opportunities, government agencies, private information technology agencies, and much more.

UPCOMING TEXTBOOK PUBLICATIONS *CONTINUED*

- Volume II (Scheduled Release 10/2018)
- Title: ***Cybersecurity: Network Basics***
- The second textbook will focus on cyber security networking fundamentals and applying the concepts from the first textbook in the volume to the public and private sectors. It will cover cyber security topics to include: network security concepts, networking principles, network peripherals, onsite/offsite vulnerabilities, cryptography, wireless security and protocols, cloud computing, information assurance, risk management, auditing, compliance, and much more.



QUESTIONS?

trzemyk@mountmichael.org

402-213-8300