8-2022

Crafting a Degree, Empowering Students, Securing a Nation: The Creation of a Modern Cyber Security Degree for the 21st Century

Mahmoud K. Quweider
The University of Texas Rio Grande Valley

Fitratullah Khan
The University of Texas Rio Grande Valley

Liyu Zhang
The University of Texas Rio Grande Valley, liyu.zhang@utrgv.edu

Hangsheng Lei
The University of Texas Rio Grande Valley

Recommended Citation

Quweider, M., & Khan, F., & Zhang, L., & Lei, H. (2022, August), Crafting a Degree, Empowering Students, Securing a Nation: The Creation of a Modern Cyber Security Degree for the 21st Century Paper presented at 2022 ASEE Annual Conference & Exposition, Minneapolis, MN. https://peer.asee.org/41292

ASEE 2022 ANNUAL CONFERENCE
Excellence Through Diversity

MINNEAPOLIS, MINNESOTA, JUNE 26TH-29TH, 2022 ASEE

Paper ID #37468

Crafting a Degree, Empowering Students, Securing a Nation: The Creation of a Modern Cyber Security Degree for the 21st Century

Mahmoud K Quweider (Professor)

Fitratullah Khan (Professor)

Liyu Zhang

Hansheng Lei

Crafting a Degree, Empowering Students, Securing a Nation: The Creation of a Modern Cyber Security Degree for the 21st Century

Abstract

In today's ever-expanding cyberspace world with its host end systems, networks, communications links, software applications, data, and human users, the field of Cyber Security is becoming integral part of each of these components in order to defend against malicious software (Malware) in all its forms, from viruses to worms, rootkits, trojan horses, ransomware, spyware, adware, and even to social engineering. The importance of such a field has created great opportunities for new careers such as cyber security specialists, cyber-crime analysts, incident and intrusion analysts, IT auditors, and many others. Unfortunately, there is not enough graduates to fill these vacancies, and many governmental entities such as NIST and NSA have sounded the alarm about the shortage of cyber security graduates in the US which puts our nation at risk.

While many universities have added new security courses to their existing programs in Information Systems, Computer Science, or Engineering, we felt the need to create a new degree from scratch. With the field expected to grow at an unprecedented rate of 28% through 2026 with a global cyber security market worth $300B by 2024 as indicated by the U.S. Bureau of Labor Statistics (BLS), we set out to address not only the technical part of the degree, but also the legal, corporate, policy, procedure, and human aspects as well.

In this paper, we present our answer to how we went about creating the new bachelor's degree in cyber security, as our university proactively sought to heed the nation's call for skilled cyber security professionals who are ready to tackle the ever-growing threats that are being faced by almost every aspect of life. In the paper, we will present:

- The holistic approach to the structure of the bachelor's degree as unique collaborative effort in three areas: Technical (Computer Science), Legal and Business (Business & Computer Information Systems), and Policy and Governance (Criminal Justice).
- The complete degree plan with all prerequisites including mathematics and statistics.
- Innovative requirements for the delivery of the degree courses using course management tools, on-line, and in-class delivery options.
- Certification and accreditation requirement for the degree: as a field that is certification heavy, we designed our degree so that our students would achieve two entry level certifications before they graduate.
- Collaboration with local schools to create pipeline to the degree.
- Support activities to ensure the creation of a close-knit community with national peer to peer connections.
- Support activities to promote and develop soft skills among participants including leadership, communications skills, and teamwork.
- By presenting our efforts, we hope that other institutions who are considering expanding their programs of study can benefit from our experience by adopting best practices while avoiding pitfalls.

Keywords:

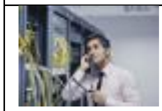
Cyber Security, Cyber Security Education, Collaborative Degrees, Career Pathways, NIST

Introduction and Motivation

As cyber security is becoming an integral part of every business and personal digital asset, the demand for cyber security professionals is at an all-time high, especially with the exponential rise in cyber-related crimes that are affecting businesses from government agencies to hospitals and health care clinics, banks and financial institutions, schools and universities, and to corporates and private businesses [7-13]. In fact, according to the quarterly data breach analysis report published by the Identity Theft Resource Center, we are poised to break records this year [1] when it comes to statistics on data breaches, ransomware, and phishing. Therefore, protecting digital assets and defending against internal and external digital threats in all forms is essential to the country's continued economic, social, and military success, especially in an ever-changing, global, connected, competitive, and technology-driven world.

To highlight how high the demand for cyber security professionals is, the US government agency, the Bureau of Labor Statistics [5], predicts that the number of cyber security jobs will increase 28 percent by 2026. According to the U.S. Department of Labor Employment Occupational Outlook Handbook, cyber security related jobs are projected to grow 33 percent from 2020 to 2030 alone, much faster than the average for all other occupations. These jobs will include skilled analysts, managers, and administrators. The numbers don't include closely related fields, shown in Table 1. for reference. The growth for the Information Security Analyst field (ISA) alone translates to about 16,300 openings each year, on average, over the decade. As we can see in the table, these are well-paying jobs with a median salary of $103,000.00 for the ISA jobs.

Table 1. U.S. Department of Labor Security/Security Related Outlook Comparison

	Occupation	**Job Duties**	**Entry-level Education**	**2020 Median Pay**
	Information Security Analysts	Information security analysts plan and carry out security measures to protect an organization's computer networks and systems.	Bachelor's degree	$103,590
	Computer and Information Systems Managers	Computer and information systems managers plan, coordinate, and direct computer-related activities in an organization.	Bachelor's degree	$151,150
	Computer Network Architects	Computer network architects design and build data communication networks, including local area networks (LANs), wide area networks (WANs), and Intranets.	Bachelor's degree	$116,780
	Computer Programmers	Computer programmers write and test code that allows computer applications and software programs to function properly.	Bachelor's degree	$89,190

	Computer Support Specialists	Computer support specialists provide help and advice to computer users and organizations.	AAS degree	$55,510
	Computer Systems Analysts	Computer systems analysts study an organization's current computer systems and find a solution that is more efficient and effective.	Bachelor's degree	$93,730
	Database Administrators and Architects	Database administrators and architects create or organize systems to store and secure data.	Bachelor's degree	$98,860
	Network and Computer Systems Administrators	Network and computer systems administrators are responsible for the day-to-day operation of computer networks.	Bachelor's degree	$84,810
	Software Developers, Quality Assurance Analysts, and Testers	Software developers design computer applications or programs. Software quality assurance analysts and testers identify problems with applications or programs and report defects.	Bachelor's degree	$110,140
	Web Developers and Digital Designers	Web developers create and maintain websites. Digital designers develop, create, and test websites or interface layouts, functions, and navigation for usability.	Bachelor's degree	$77,200

With such a high and steady demand for cyber security professionals with their noticeable short supply, it becomes imperative that academic institutions such as colleges and universities continue their innovative educational efforts to expand opportunities in these highly sought-after career fields that will help in securely modernizing the country's physical and electronic infrastructure to accommodate the ever-expanding use of 5G, drones, big data, cloud computing and IoT, modern database systems, web technologies, social media platforms, and AI and Machine Learning algorithms [7,8]. In doing this, the academic institutions should ensure to have a diverse workforce, one that has good representation of minority students, economically disadvantaged students, as well as females so that the society as a whole participates, and benefits from its young and creative upcoming workforce.

As an academic institution that is minority serving, we saw a great opportunity to create a new unique degree that will produce the much-needed next generation of cyber security professionals that reflects US's diversity and inclusion. As a new degree, we had a chance to define the characteristics of the degree and incorporate the latest technological and pedagogical advances.

Built from scratch, the cyber security degree addresses several aspects from enrollment, to pedagogy, delivery, accreditation, infrastructure and labs, student support activities, faculty recruitment and human resources, to infrastructure and labs. In the following sections, we go in great details over all these aspects.

Degree Design and Organization

Overall Architecture

Structured around a blend of theory and practice; confluence of technology, humans, law, and organizations; as well as collaboration with other departments within the university, the **Bachelor of Science in Cyber Security** is a degree, separate from Computer Science, and is offered by the Department of Informatics and Engineering Systems which is a part of the College of Engineering and Computer Science at The University of xx [3]. It is a Brownsville Signature Program with all courses required for the degree offered at the Brownsville Campus with on-line and synchronous options allowed for all students residing outside of Brownsville. With **Cyber Security** defined as the study of science, technologies, processes, and practices designed to protect computers, networks, smart devices, software programs, and data from attack, damage, or unauthorized access, our cyber security degree is a collaborative inter-disciplinary degree which follows a holistic approach that integrates technical, legal, business, and policy skills by using existing computer science courses with support courses from Business, Information Systems and Criminal Justice.

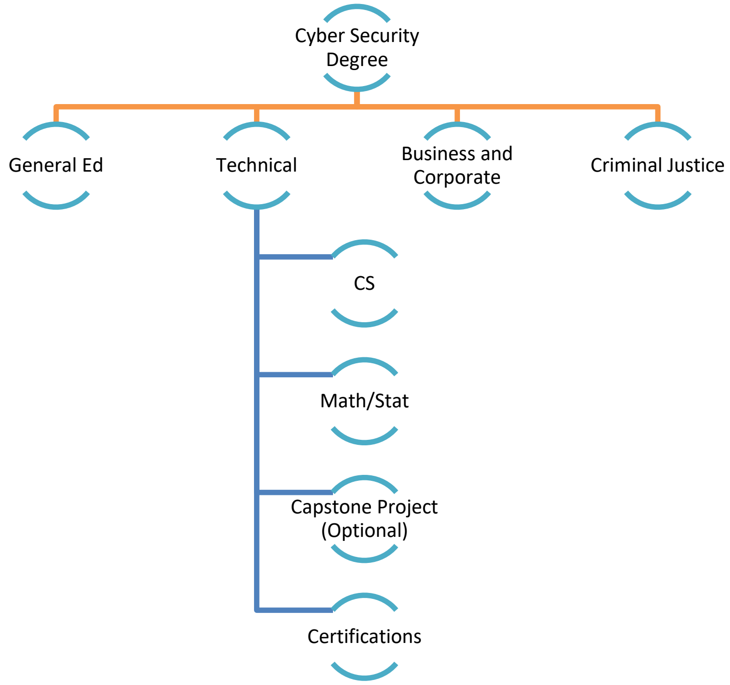


Figure 1. Cyber Security Degree Architecture

Major Areas of Study Beyond General Education

The new holistic multi-disciplinary B.S. Degree is built on a solid foundation of the following four areas:

1. Mathematics Skills—Precalculus and Statistics
    a. MATH 2412: Precalculus
    b. MATH 2334: App Stats Health
    c. Discrete Math and CS related topics recommended by the ABET are covered in a new course called Foundation of Systems (CSCI-2322)
2. Technical Skills—Computer Science
    a. 50 Adv. Hrs.
3. Investigation Procedures and Policies—Criminal Justice

   a. CRIJ 1301: Intro to Crim Justice
   b. CRIJ 3316: Crime Investigation & Proof
4. Legal and Ethical Principles—Business
   a. INFS 3308: Bus Info Infra
   b. BLAW 333:7 Bus Law I
   c. Corporate and Ethical Principles—Business
   d. INFS 4312: E-Commerce Design (Elective)
   e. INFS 4330: Business Intelligence (Elective)
   f. INFS 4391: Information Security (Elective)
   g. INFS 4397: Health Computer Information Systems (Elective)

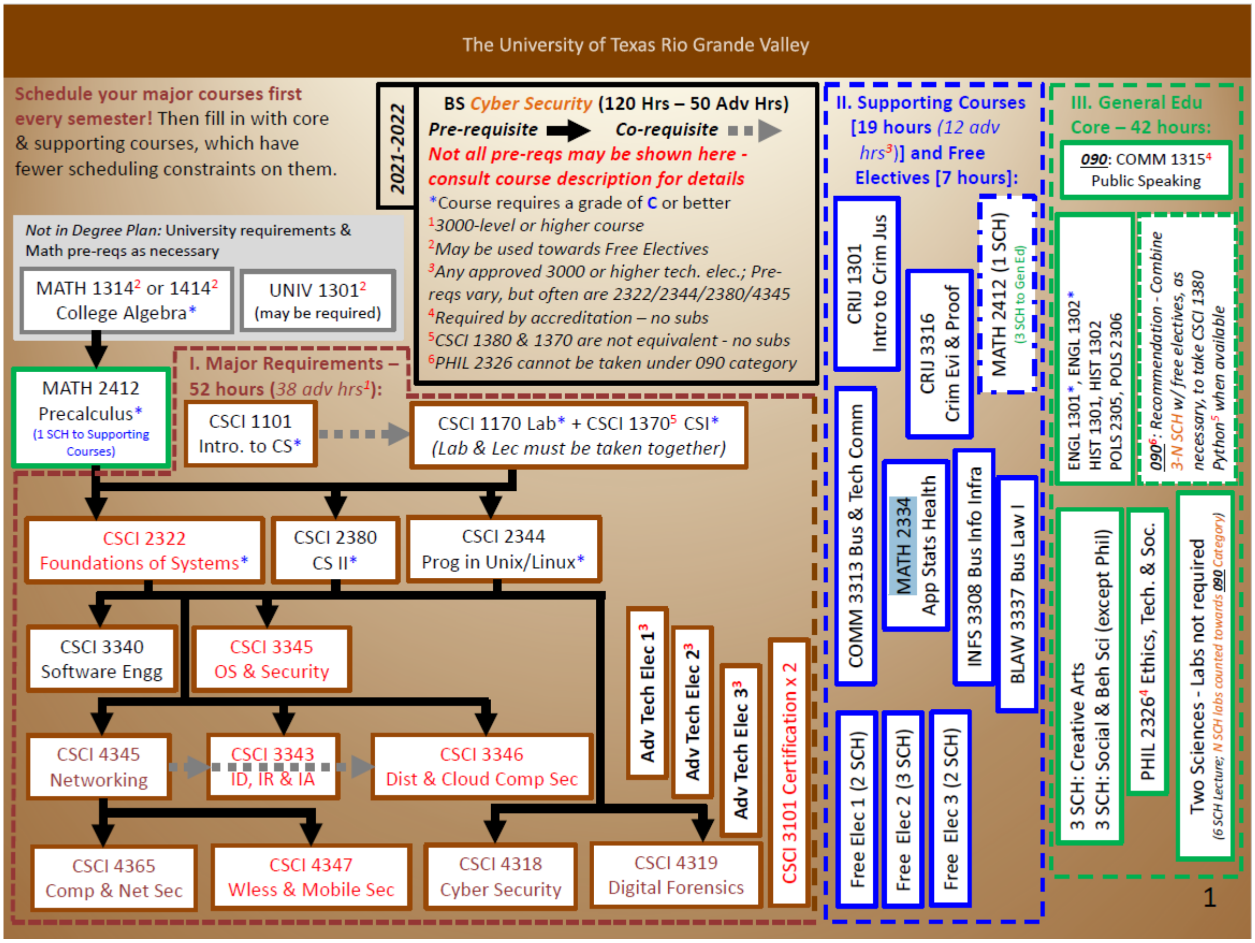

The University of Texas Rio Grande Valley
Schedule your major courses first every semester! Then fill in with core & supporting courses, which have fewer scheduling constraints on them.
2021-2022
BS Cyber Security (120 Hrs – 50 Adv Hrs)
Pre-requisite
Co-requisite
Not all pre-reqs may be shown here - consult course description for details
*Course requires a grade of C or better
[1]3000-level or higher course
[2]May be used towards Free Electives
[3]Any approved 3000 or higher tech. elec.; Pre-reqs vary, but often are 2322/2344/2380/4345
[4]Required by accreditation – no subs
[5]CSCI 1380 & 1370 are not equivalent - no subs
[6]PHIL 2326 cannot be taken under 090 category
Not in Degree Plan: University requirements & Math pre-reqs as necessary
MATH 1314[2] or 1414[2] College Algebra*
UNIV 1301[2] (may be required)
MATH 2412 Precalculus* (1 SCH to Supporting Courses)
I. Major Requirements – 52 hours (38 adv hrs[1]):
CSCI 1101 Intro. to CS*
CSCI 1170 Lab* + CSCI 1370[5] CSI* (Lab & Lec must be taken together)
CSCI 2322 Foundations of Systems*
CSCI 2380 CS II*
CSCI 2344 Prog in Unix/Linux*
CSCI 3340 Software Engg
CSCI 3345 OS & Security
CSCI 4345 Networking
CSCI 3343 ID, IR & IA
CSCI 3346 Dist & Cloud Comp Sec
CSCI 4365 Comp & Net Sec
CSCI 4347 Wless & Mobile Sec
CSCI 4318 Cyber Security
CSCI 4319 Digital Forensics
Adv Tech Elec 1[3]
Adv Tech Elec 2[3]
Adv Tech Elec 3[3]
CSCI 3101 Certification x 2
II. Supporting Courses [19 hours (12 adv hrs[3])] and Free Electives [7 hours]:
CRIJ 1301 Intro to Crim Jus
CRIJ 3316 Crim Evi & Proof
MATH 2412 (1 SCH) (3 SCH to Gen Ed)
COMM 3313 Bus & Tech Comm
MATH 2334 App Stats Health
INFS 3308 Bus Info Infra
BLAW 3337 Bus Law I
Free Elec 1 (2 SCH)
Free Elec 2 (3 SCH)
Free Elec 3 (2 SCH)
III. General Edu Core – 42 hours:
090: COMM 1315[4] Public Speaking
ENGL 1301*, ENGL 1302* HIST 1301, HIST 1302 POLS 2305, POLS 2306
090[6]: Recommendation - Combine 3-N SCH w/ free electives, as necessary, to take CSCI 1380 Python[5] when available
3 SCH: Creative Arts 3 SCH: Social & Beh Sci (except Phil)
PHIL 2326[4] Ethics, Tech. & Soc.
Two Sciences - Labs not required (6 SCH Lecture; N SCH labs counted towards 090 Category)
1

Figure 2. Cyber Security Degree/Flow Chart

Fig. 2 shows the details of the degree. It has a total of 120 hours with 50 advanced hours (core, technical electives, and support courses). As we can see, the degree is a balanced blend of theory and practice. When designing the degree, we followed closely the ABET recommendation for Cyber Security" Program Criteria. The courses descriptions which will be available on the department's website details the topics covered in each course. The course on Ethics & Technology complements the areas above and prepares the graduate to join the work force immediately. Another thing to note on the degree is that it allows a student to be specialized (and certified) in an area of one’s choice. These areas are determined through the technical electives. Here are some of the supported areas.

Cyber Security Areas

Principal areas of study within cyber security include:

- Applications Security
- Network Security
- Data Security
- Cloud Security
- System and Hardware Security
- IoT (Internet of Things) and Mobile Security
- Intrusion Detection and Incident Response
- Information Assurance
- Digital Forensics
- Malware Analysis
- Reverse Engineering

We are currently working on becoming a National Center of Academic Excellence in Cyber Defense and an ABET (Accreditation Board for Engineering and Technology) accredited program in the coming years. These efforts will be supported by a recent $399K grant we received to align the curriculum to achieve our accreditation and stacked certification goals.

Course Delivery

The degree was launched in the Fall of 2021. The original design was to have all classes in Brownsville in a traditional face-to-face with on-line synchronous (where a student attends on-line during the class set days and times) option for students outside the valley (The Rio Grande Valley). However, the COVID crisis negated the face-to-face option, and all courses were moved to on-line and on-line synchronous.

Incidentally, the crisis strengthened the degree academically in unexpected ways including a flux of software and hardware devices, expediated intensive on-line learning/teaching workshops that emphasized maintaining quality and interactive and immersive learning environment. One additional advantage was the deployment of several virtual machine (VM-based) labs that can be run in the cloud or downloaded and run locally on client machines. These labs allowed for realistic simulation of networks that include clients, servers, services, and IoT devices in different topologies. We plan to continue the course offering modalities to accommodate local and remote students (attending other xx campuses) who enroll in the program. As Covid restrictions ease, the program will be as advertised as a ***signature program*** at the Brownsville Campus, with the first two years available at both Edinburg and Brownsville campuses. We will continue to leverage educational technology, such as Learning Management System (LMS) and Interactive TV (ITV), to accommodate students from all xx distributed campuses.

Enrollment Data

Table 2. shows the current enrollment as of Fall-2022. In our original projections, we expected 50 students at this time. Our enrollment numbers far exceed our projection and indicate the strong demand for the specialized degree. Currently, we are in the process of hiring new faculty to meet the demand and maintain a healthy faculty to student ratio, high quality research, and impactful service to the university and the community.

Table 2. Cyber Security Enrollment

Total	209
Cyber Security	184
Cyber Security (Unofficial Minor)	12 (Not counted in Total)
Master of IT (MSIT)	25

Certification

Following a model of study, certify, work, we integrated nationally accredited certifications into our degree to give our graduates a competitive edge. As we know, employers in the cyber security fields require different levels of skills from well qualified workers. National certifications show employers that our candidates already have the skills to implement state-of-the-art current and emerging technologies. In cyber security, students need to remain up to date in a field where the technology is always changing. This has the positive effect of making lifelong learning a critical topic in every course. Learning to learn independently is an essential requirement. Two (2) required hours earning professional certifications through two one (1) hour certification increase a student's exposure to the current state of the profession and its organizations and associations. A student in cyber security can pursue many certifications that will make one stand out among candidates and increases one's earning potential. Table 3 Shows a sample of the certifications that are accepted by the department.

Table 3. Cyber Security Certifications

Cyber Security-Vendor-Neutral	• Certified Ethical Hacker (CEH) • CompTIA Network+ • CompTIA Security+ • Certified Information System Security Professional (CISSP) • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • NIST Cybersecurity Framework (NCSF) • Certified Cloud Security Professional (CCSP) • Computer Hacking Forensic Investigator (CHFI)
Digital Forensics Vendor-Neutral	• Certified Forensic Computer Examiner (CFCE) • Certified Computer Examiner (CCE) • Global Information Assurance Certification (GIAC)

Degree Support & Resources

With a new degree comes the need for several support services and activities. In addition to administration and faculty recruitment, the areas showed in Fig. 3 were addressed and tackled in detail in systematic way. The following sections deal with the details.

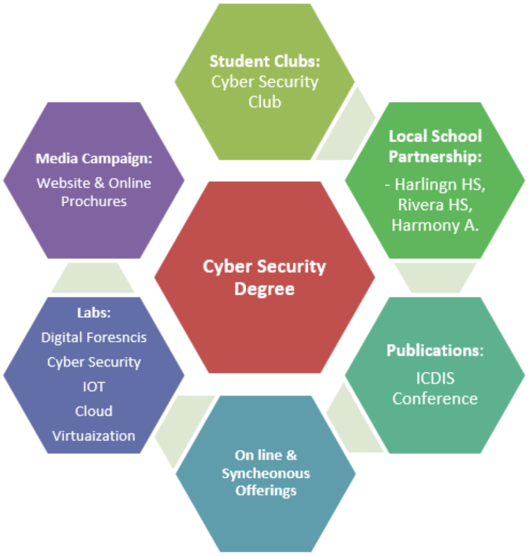


Figure 3. CS Degree Support

Cyber Security Computer Labs

Our labs provide an opportunity to the students to collaborate on ideas, team-up on class team projects, and to ask questions! We have two labs, hosted in one large physical space in SET 1.508, the former being the primary **Open Lab** for Cyber Security research and development, and for students to work on their projects and class work.

- Digital Forensics (primarily in BSETB 1.508): Research Theme: Mobile forensics, Memory Forensic, and File System Forensic.
- Security Enhancement (primarily in BSETB 1.508): Research Theme: Cryptography Engineering, Cloud/Mobile/IoT Security, and Blockchain.
- Secure System Design (primarily in BSETB 1.508): Research Theme: Hardware Security, System Security, and Adversarial Machine Learning.
- Open Team or Individual Projects (primarily in BSETB 1.508): General Theme: Students work on their team/individual projects and other class work.

Cyber Security Clubs

In addition to the University's fraternities and sororities, the **Cyber Security Club** was exclusively created with the new degree to support students majoring in it. The Club has the following as part of its main mission:

- Support students to stay abreast of the cyber security field
- Nurture a sense of professional community through networking with local and national peers
- Promote an ethical approach to the practice of cyber security
- Mentor the next generation of cyber security professionals
- Help raise awareness about the importance of cyber security within our community

The club also has strong collaboration with the following well-established clubs: ACM (Association for Computing Machinery) and the IEEE (Institute of Electrical and Electronic Engineers).

Local Schools Partnership

To ensure the success of the new degree, the department established several partnerships with local high schools in order to establish long term supportive networks and pathways. The partnerships were created at different levels ranging from serving on advisory boards to offering dual enrollment courses, to participating in College Days, and offering virtual and physical tours with detailed presentations about the new program and career opportunities. Currently, the partnerships include xx, Harlingen Collegiate High, Rivera HS, Brownsville Early College, and Harmony Academy.

Media & Marketing Campaign

The marketing campaign includes a dedicated web site [4] with complete material including:

- Bachelor of Science in Cyber Security (BSCS) Degree Plan
- Road Map (Guide for students for planning a path to the degree)
- Flowcharts (Quick reference of what courses to take & when)
- Checklist (Track what one has taken so far)
- Class Planning Worksheet
- Course Offering Cycle
- Course Descriptions

Additionally, several brochures and pamphlets have been created to email to interested students. A sample of such high-quality professionally designed material is included in appendix A. The current xx sponsored conference on Data, Intelligence, and Security (ICDIS)[6] founded by faculty members of the new degree will be used as the preferred to disseminate research conducted students and faculty of the program.

Conclusions and Future Work

In this paper we presented the unique design of our cyber security degree with our holistic multi-disciplinary approach that includes Technical Skills—Computer Science, Investigation Procedures and Policies—Criminal Justice, Legal and Ethical Principles—Business. We also showed how the degree allows for a quick entry into the work force through our curriculum and integrated national vendor-neutral certifications that offer job seekers a distinct competitive edge.

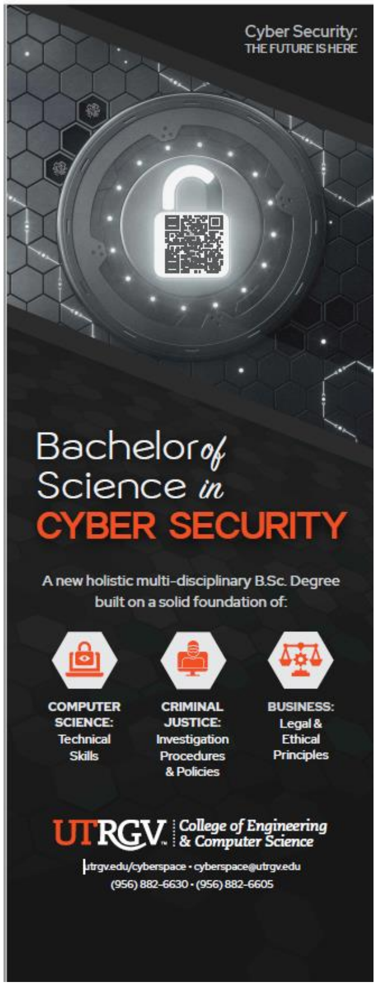
As an integral part of the degree, we detailed many of the support resources and activities that go side-by-side with the academic and curricular activities, from students' clubs, to specialized labs, dedicated media and web platforms, partnership agreements with local high schools, and to diverse set of delivery offerings and learning tools.

Finally, we presented current and projected enrollment numbers that exceeded our expectations by leaps and bounds. Future work will further detail how we are integrating NICE curriculum and certification in every course to meet the objectives of every certification by the time the certification test is taken.

References

1. https://www.statista.com/topics/1390/nonprofit-organizations-in-the-us/
2. https://www.idtheftcenter.org/
3. https://www.utrgv.edu/cyberspace/academics/index.htm.
4. www.chronicle.com/article/Cybersecurity-Rising/239270.
5. https://www.bls.gov/ooh/
6. https://www.icdis.org/submission
7. E. A. Fischer, “Cybersecurity issues and challenges: in brief,” Congressional Research Service Report prepared for Members and Committees of Congress, 2014.
8. Justin Wang, Dennis Brylow, Debbie Perouli, Implementing Cybersecurity into the Wisconsin K-12 Classroom, COMPSAC 2019, the 43rd Annual IEEE Computer Software and Applications Conference, Milwaukee, Wisconsin, July 2019.
9. Gaby Galvin, https://www.usnews.com/news/stem-solutions/articles/2016-11-23/study-girls-less-interested-in-stem-fields-perceived-as-masculine
10. Bonwell, C., and Eison, J. Active Learning: Creating Excitement in the Classroom. ASHE-ERIC Higher Education Report 1, 1991.
11. ODEP. (2016). Essential skills to getting a job. Retrieved from http://promotions.usa.gov/odep/essential_job_skills.pdf
12. Julia Evetts” Women and careers in engineering: management changes in the work organization,” Women in Management Review Volume 12, Number 6, pp. 228–233, 1997.
13. McRae, S., Devine, F. and Lakey, J., Women into Science and Engineering, Policy Studies Institute, London, 1991.

Appendix A. Sample Cyber Security Program Brochure



Cyber Security:
THE FUTURE IS HERE

Bachelor *of* Science *in* CYBER SECURITY

A new holistic multi-disciplinary B.Sc. Degree built on a solid foundation of:

COMPUTER SCIENCE: Technical Skills

CRIMINAL JUSTICE: Investigation Procedures & Policies

BUSINESS: Legal & Ethical Principles

UTRGV | *College of Engineering & Computer Science*

utrgv.edu/cyberspace • cyberspace@utrgv.edu
(956) 882-6630 • (956) 882-6605