Interdisciplinary Approach Cybersecurity Curriculum

Rebecca Badu

Old Dominion University

Problem

I want to become a Cyber Security Analyst after my studies here at ODU. The main duty of a cyber security analyst is to defend a company's systems and network from online threats. In order to do this, it is necessary to do future IT trend research, develop backup plans, examine suspicious activity, report security breaches, and inform the rest of the organization about security precautions. Cybersecurity analysts use a combination of technical and workplace skills to assess vulnerabilities and respond to security incidents. Daily duties for a cybersecurity analyst include monitoring systems, taking preventative action, and conducting data analysis. Additionally, they might examine network traffic to look for any potential dangers. People in this profession are frequently talented in: Problem Awareness: Being aware of problems as they arise. Reading and comprehending what is written is known as written comprehension. Generalizing or deriving conclusions from a wealth of specific knowledge is known as inductive reasoning. Using rules to answer problems is known as deductive reasoning. The combination of two or more academic disciplines into one job role, by using this approach I will have to draw information from a variety of other academic disciplines, such as Science, technology, engineering, and math which are together known as STEM. The emphasis on creativity, problem-solving, and critical thinking is shared by these four fields.

Job

Cyber Security Analyst

https://www.careeronestop.org/Toolkit/Careers/Occupations/Occupation-profile.aspx?keyword=Information%20Security%20Analysts&onetcode=15121200&location=20110

Classes

MATH 162M PRECALCULUS I.

CYSE 270 LINUX SYSTEM FOR CYBERSECURITY

CYSE 300 INTRODUCTION TO CYBERSECURITY

CYSE 495 TOPICS IN CYBERSECURITY

Interdisciplinary Approach

The discipline will be able to assess each discipline independently and together using the IDS approach to see if the abilities taught in each subject will transfer to a future position as a cyber security analyst. Cybersecurity analysts evaluate vulnerabilities and respond to security issues using a combination of technical and professional skills. Some of the technical skills may already be present if you have an IT background, and many workplace abilities are transferable across a wide range of occupations.

Relevant Discipline

MATH 162M PRECALCULUS I. 3 Credits

The first course in a two-course sequence designed to provide a strong preparation for calculus. Topics include algebraic operations, equations and inequalities, graphs and functions, polynomial functions, theory of equations, systems of equations, exponential functions, and logarithmic functions. Prerequisite: qualifying score on SAT or ACT, or qualifying score on a

placement test administered by the University Testing Center or a grade of C or better in Math 102M or Math 103M.

CRJS 310CYBERCRIMINOLOGY: FOUNDATIONS 3 Credits

Students will learn about computer-related crimes and how law enforcement personnel investigate them in this course. The first part of the course describes the new environment that information and communication technology have produced and how it supports various forms of behavior. The course then proceeds on to defining and outlining the many computer-related crimes, the methods utilized by law enforcement, and the legal complications associated with countering cybercrime. Prerequisite: CRJS 215S

CYSE 406 CYBER LAW 3 Credits

This course tackles two major cyber law subjects. The first part of the course examines various U.S. laws and legal considerations that impact the digital and cyberspace worlds from traditional civil, and to a lesser extent, traditional criminal perspectives. The second part will familiarize cyber operations professionals about the extent of and limitations on their authorities to ensure operations in cyberspace follow U.S. law, regulations, directives and policies. The course will also introduce students to miscellaneous cybersecurity topics such as the Federal Acquisition Requirements. Prerequisite: junior standing.

Literature Search

Common Theme: All the required classes related to Information Security Environment

Conflict: The Social Science class, Cyber Law and mathematics are all slightly different type of skill and perspective wise but are all very important because Computer science's technical subject of cybersecurity necessitates strong analytical abilities from job candidates.

Knowledge Relates to Job:

Mathematics: Cyber security Analyst need to have a basic understanding of the concepts described here: Deductive Reasoning - Using rules to solve problems. binary number theory, Boolean and linear algebra, and cryptography. These are also the math skills you'll need to secure most cybersecurity certifications, which most employers prefer entry-level candidates to have.

Social Science: A solid understanding of social science and how it influences behavior can help companies build and support a security awareness.

Cyber Law: Cybersecurity or cybercrime laws are regulations that protect information technology with the aim of requiring businesses and organizations to use a variety of defenses to protect their systems and data against intrusions.

Adequacy In each Discipline

Discipline	Classification	History	Perspective/World View	Content	Research

Math	**Natural Science**	The history of mathematics deals with the origin of discoveries in mathematics and the mathematical methods and notation of the past. Before the modern age and the worldwide spread of knowledge, written examples of new mathematical developments have come to light only in a few locales.	Solving Problem for mathematicians who work with abstract, quantitative data. that investigates and makes an effort to verify several theorems	Empirical Data	Quantitative
Social Science	**Sociology**	According to sociology, human interactions in each particular culture come in all their variety and complexity. Sociology is interested in a variety of subcultures' perspectives, institutional studies, and how bureaucracy and vested interests affect daily life.	A collection of attitudes, values, stories and expectations about the world around us, which inform our every thought and action. Worldview is expressed in ethics, religion, philosophy, scientific beliefs and so on	Empirical Data	**Qualitative**

Criminal Justice/Cyber Law	**Applied Field**	Criminal Justice sees people's particular actions through different theories on human nature, societal structure, social order, concepts of law. This allows them to investigate and go through the necessary steps to find out if they are innocent or not	With the rapid development of computer technology and internet over the years, the problem of. Cyber-crime has assumed gigantic proportions and emerged as a global issue. It has created an. entirely new set of problems for law enforcement agencies all over the world	Empirical Data	Qualitative

Analysis of the Problem

Mathematic Strength: Deductive Reasoning - Using rules to solve problems. In dept understanding of the concepts described here: binary number theory, Boolean and linear algebra, and cryptography. **Weakness:** Inductive Reasoning - Making general rules or coming up with answers from lots of detailed information.

Social Science Strength: Complex Problem Solving - Noticing a problem and figuring out the best way to solve it. **Weakness:** Systems Analysis - Figuring out how a system should work and how changes in the future will affect it.

Criminal Justice/Cyber Law Strength: Yields legal recognition to electronic documents and a structure to support e-filing and e-commerce transactions and also provides a legal structure to reduce, check cyber-crimes. **Weakness:** Keeping up with the system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

How each discipline contributes to the career of a cyber security analyst: Mathematics (MATH 162 Precalculus) will help me develop Deductive Reasoning - Using rules to solve problems; Social Science (CYSE 201S Cybersecurity & Social Science) helps figure out how a system should work and how changes in the future will affect it; Criminal Justice/Cyber Law (CYSE 406 CYBER LAW) helps to Implement security measures for computer or information systems and to help mitigate cybercrime by the law.

Substitution or adding discipline: There isn't really any substitution or the need to add any othe discipline since these major classes may be sufficient enough to provide the education and background I need to become a Cybersecurity Analyst.

Effect of Conflict

Each discipline approaches challenges from a different angle. Cyber analysts use technology to solve problems in a very analytical, logical manner. They also have practical engineering science

and technology knowledge. To create and produce a variety of goods and services, this includes using principles, techniques, procedures, and equipment.

In order to build the approach and develop techniques and systems, mathematicians adopt a quantitative, data-driven procedure. The practice of qualitative analysis is used in social science to increase field knowledge. Cyber law uses qualitative approach to fully comprehends malware, cyberattacks, and the actions of hackers, and actively works to foresee and stop these attacks.

Due to their disparate points of view and various methods for tackling problems, the pure forms of all three disciplines could cause dispute among cybersecurity analysts. A mathematician would struggle to see the need for a social scientist to utilize Inductive Reasoning to examine data and generate generalizations or conclusions from a wealth of detailed information. Likewise, a social science and criminal justice/cyber law individual would conflict because the cyber law individual may not see why a social science person might have to know how to analyze a cyber-crime by using a complex data including open source data, individual and organized hackers, and require practical and theoretical abilities to gather, critically assess, and creatively synthesize the data, with the end goal of applying the findings to a variety of contexts, instead of using applicable knowledge.

If only three disciplines mathematics, social science, and criminal law were taught, the curriculum would be weaker because disciplinary conflicts may confuse pupils.
These classes' subfields, but especially those in social science like Cyber Law and Criminal Justice like cybercriminology, aid in highlighting the value of all three curricula.

Common Ground

Students in social science, mathematics, and criminal justice/cyber law can readily find common ground because each of these subjects offers components that help a cyber security analyst perform well in the workplace. Using the NIST Framework and cyber best practices, CYSE 300 serves as an introduction to cybersecurity. A future analyst will be well-prepared to approach CYSE 495 topics in cybersecurity if they have a solid foundation in technical knowledge, as this course provides a more in-depth understanding of the advanced study of particular cybersecurity topics that enable small groups of qualified students to work on topics of shared interest. The learner who is receiving education is now ready with knowledge of the vulnerabilities to search for and hopefully mitigate. After that, the student will be prepared to enroll in CYSE 270, which offers a conceptual foundation and an introduction to the fundamental operations in popular Linux distributions for cybersecurity utilizing both a graphical and command line interface. Students will gain knowledge of user authentication, file system management, shell scripts, and the fundamentals of Linux installation and configuration. This course serves as the technological foundation for students interested in majoring in cybersecurity.

An in-depth understanding of all three of the key subject's mathematics, criminal justice, and social science is not a part of the common ground. This would result in more conflicts than common ground, as was said in the conflict section.

Integration

According to Career One Stop, a cybersecurity analyst must have understanding of computers, electronics, and computer hardware and software, including applications and programming. They also need to be familiar with circuit boards, processors, chips, and other electrical devices. English Language Understanding of the grammatical and lexical principles, as well as the structure and content of the English language, including word meanings and spellings. Knowledge of business and management principles that are involved in strategic planning, resource allocation, human resource modeling, leadership approach, production methods, and the coordination of people and resources can be acquired from CYSE 495. They'll demand Engineering and technology: Understanding of engineering science and technology in practice. To create and produce a variety of goods and services, This includes applying principles, techniques, procedures, and equipment to the design and production of various goods and services. Telecommunications - Knowledge of transmission, broadcasting, switching, control, and operation of telecommunications systems which is taught in CYSE 300. And they will also need to Deductive Reasoning - Using rules to solve problems and an understanding of binary math helps cybersecurity analysts understand and create the unique programs that keep networks safe and facilitates understanding weaknesses in existing code which can be taught in MATH 162.

Testing

The conclusion that three courses MATH 162 Precalculus, CYSE 495 Topics in Cybersecurity, and CYSE 300 Introduction to Cybersecurity for educators help prepare a Cyber Security Analyst for employment may be reached after an in-depth interdisciplinary analysis of all the courses, disciplines, and sub-disciplines. The CareerOneStop list of necessary abilities and the

skills taught in these classes can be compared to show how close their material is. There is more in common across the courses that can be integrated into the future career of Cyber Security Analyst than differences in perspective, content derivation, and problem-solving techniques.

Reference:

https://www.careeronestop.org/Toolkit/Careers/Occupations/Occupation-profile.aspx?keyword=Information%20Security%20Analysts&onetcode=15121200&location=20110

https://catalog.odu.edu/courses/cyse/