

Final Project: Evaluating Information Security Analyst Using an Interdisciplinary Approach

Abstract

Information Security Analysts are responsible for the organization's information security. They keep threats and vulnerabilities under control, respond to security breaches, and propose appropriate procedures in case of violations. However, to become an effective Information Security Analyst, one must be knowledgeable about network security, information security, threat analysis, and more (Cybersecurity Career Pathway, n.d.). College teaches the theoretical knowledge of using software, fixing hardware issues, etc. College courses must teach practical skills to help recent graduates apply their knowledge. An interdisciplinary approach can facilitate the practical application of classes to real-world situations. Courses like MATH 163, ECE 455, and PHIL 355E can equip students with valuable knowledge and practical skills in various job roles.

Problem

Information Security Analysts ensure the security of the organization. They oversee the network traffic, respond to threats, and propose solutions to hacks, malware, and viruses (*Occupation Profile for Information Security Analysts* | *CareerOneStop*, n.d.). In addition, they actively find the best ways to protect the organization. Besides their technical knowledge, they have a good sense of analytical skills, problem-solving, and communication skills to work with others.

The primary focus is integrating an interdisciplinary approach in pertinent courses that teaches skills applicable to a profession. Schools teach theoretical knowledge to help students learn (Loveless, 2022). Hypothetical is not practical for students to respond in real-life situations. Courses such as MATH 163 Precalculus I, ECE 455 Network Engineering and Design, and PHIL 355E Cybersecurity Ethics help students prepare for the real world, where any scenario can happen at any given time. The listed courses are not the only possible courses that help students in the real world, but their distinct characteristics distinguish them from other classes. In summary, taking courses such as MATH 163, ECE 455, and PHIL 355E can help students prepare for potential situations and be better prepared as Information Security Analysts.

Interdisciplinary Approach

Interdisciplinary is a way to integrate different ideas and develop the best solution that satisfies both ideals. Moreover, the interdisciplinary approach ensures that strengths are applied while weaknesses are identified and resolved.

Courses have different skills that can be pertained to other jobs. Nevertheless, the interdisciplinary approach can help students taking classes gain the skills needed to be effective Information Security Analysts.

Relevant Disciplines

Many disciplines can contribute significantly to job applications. However, three fields present common skills that an Information Security Analyst should learn. Most, if not all, courses apply different skills that can be useful in the role of Information Security Analyst.

The first course is from the study of mathematics called Precalculus I or MATH 163. MATH 163 teaches students about exponential and logarithmic, trigonometry, vectors, complex numbers, and other related concepts. These help students be prepared for Calculus and help them gain a deeper understanding of the role of numbers in explaining various phenomena in the world.

The next course is ECE 455 or Network Engineering and Design. ECE 455 focuses on the comprehension of networking design principles. Additionally, it includes topics such as LAN, VLANs, internetworking principles, WAN design, and more. ECE 455 allows students to gain insight into a real-world network design application.

The third selected course is Cybersecurity Ethics, also known as PHIL 355E. The course focuses on the ethical issues in Information Technology, which are not limited to privacy, content control, social responsibility, cyber crimes, etc. PHIL 355W introduces students to ethical dilemmas faced by Information Security analysts or other tech jobs.

In conclusion, each course has skills for its specific discipline, but it can also be applied to become an Information Security Analyst. In addition, the interdisciplinary approach makes it possible to use skills from a particular field as Information Security Analyst.

Literature Search

All three courses teach critical thinking and problem-solving skills. The role of the teacher is to instruct students on various subjects. At the same time, it is the responsibility of students to gain the necessary knowledge and skills to apply the matter to their daily life. Engaging in critical thinking empowers students to effectively evaluate various scenarios and problems and comprehend the far-reaching implications of conflicts. MATH 163 serves to cultivate in students

an appreciation for the underlying processes involved in solving complex problems. Similarly, ECE 455 aims to equip students with the necessary tools and knowledge to deliberate on optimal solutions for networking challenges. Lastly, PHIL 355E will allow students to implicate the theories and question the idea of imposed solutions. Through this, students can learn about critical thinking about problems. In the workplace, critical thinking is slightly different from in classrooms because there's a consequence involved when the team or individual fails to address faults. Additionally, due to critical thinking, they hone their problem-solving skills.

Problem-solving is the byproduct of analyzing and assessing a problem and curing a solution that revolves around the root of the problem.

The three courses are by no means perfect. They contain flaws and weaknesses that may contradict each other. Each one of them teaches curriculum differently. For example, Cybersecurity Ethics (PHIL 355E) preaches cross-examining the ideal solution to a dilemma. Information Security Analysts determine their actions based on their current circumstances. Thus, PHIL 355E was a suitable course to learn about critical thinking and analyzing information. However, PHIL 355E focuses on understanding ethical issues and covers other fields, such as Information Technology (IT) and Cybersecurity (CYSE). On the other hand, Precalculus (MATH 163) illustrates steps to solving a complex problem. MATH 163, to an extent, deals with imaginary numbers, whereas Information Security Analyst deals with real numbers.

On the contrary, Precalculus and Information Security Analysts deal with numbers presenting information when processed correctly. Lastly, ECE 455 uses real-world scenarios to express the thought process in ways Information Security Analysts a solution choose a solution. Information Technology Analyst has to be sure about answers so that the company will save money in

creating and developing solutions. ECE 455 covers the physical aspects of Information Technology Analyst. In short, each discipline has weaknesses and strengths that can significantly affect the interdisciplinary approach in students applying theoretical knowledge to jobs.

Adequacy in Each Discipline

Mathematics is "the science of structure, order, and relation" (*Mathematics*, n.d.). Its history dates back to Egypt and Mesopotamia or perhaps even further. From their perspective, they seek to uncover the world's mysteries through numerical representations. Most of their content is both empirical and commentary and analysis. Their research is quantitative since they deal with proofs and models based on their empirical data. They hypothesize ideas and turn them into theories where they interpret the outcome of an experiment.

Information Security Analysts can apply mathematics to turn data into information.

Electronics and Computer Engineering is a relatively new field that focuses on designing and developing computer systems (*Electronics and Computer Engineering Technology*, n.d.). It is a combination of computer science and electrical engineering. The field falls upon applied science. Their perspective utilizes modern technology to create better and faster systems. The content is based on empirical data since they need to prove that their systems are efficient through numbers. Their research is both qualitative and quantitative, depending on the study. Some research can be theoretical representations of possible cost-effectiveness because they lack the funding to set up a complete implementation of a system. Furthermore, ECE can be utilized in Information Security Analyst to determine hardware and software problems.

Philosophy studies the experience and existence of humans (*Philosophy*, n.d.). Philosophy classifies as humanities. The history of philosophy goes back to the era of Socrates, at least in terms of Western philosophy (Nails, n.d.). Its perspective centered on the idea of human rational thinking. The content of philosophy is analysis and commentary. There is no visual representation of how humans think; however, humanity can express different reactions based on situations. The research is qualitative, where philosophers try to explain how the mind works through theories. Information Security Analysts can apply philosophy to think about ethical dilemmas.

Analysis of the Problem

Mathematics is strong in critical thinking, logical reasoning, and a deep understanding of abstract concepts. Therefore, math can be helpful in Information Security Analyst in many ways. For example, an Information Security Analyst needs to understand the inner workings of cryptography. At the basic level, cryptography turns plain text into cipher text using a complex math equation. Furthermore, by monitoring network traffic, math can help Information Security Analysts study and understand big data. The only caveat is that some people need help learning math; thus, people tend to avoid it.

Electronics and Computer Engineering are adept at teaching hardware, software, and networking essentials. They allow students to excel in learning the technical knowledge needed to be an Information Security Analyst. The drawback of Electronics and Computer Engineering is that non-technical people need help understanding jargon and their functionality. Information Security Analyst does not only imply technical knowledge, but some are about risk management.

Knowing Philosophy allows Information Security Analysts to express their concerns for the security and privacy of the company. As an Information Security Analyst, an organization must understand its responsibilities as a company that holds sensitive information.

Effect of Conflicts

The discipline of mathematics, electronics and computer engineering, and philosophy have different perspectives that can cause conflict when integrated into Information Security Analyst. For example, MATH and ECE may assert the idea of a secure system. However, PHIL may imply a concern for security and privacy. The conflict between technology and security must consider imposing a solution that satisfies both fields and the organization. The substitution or addition of different disciplines will allow solutions to be more flexible. However, the downside is that views of various disciplines may diverge from the ideology of Information Security Analysts.

Common Ground

Information Security Analysts can integrate the selected disciplines into a broad understanding of Information Security analysts. For example, philosophy examination of security, privacy, and accountability can create various solutions that address ethical concerns. Mathematics can provide logic and probability in analyzing systems and determining the effectiveness of security measures. Electronics and Computer Engineering can design systems that address security issues and network security implementation. The common ground is that all disciplines have strengths that can contribute to Information Security Analyst.

Integration

An Information Security Analyst can integrate disciplines such as mathematics, electronics and computer engineering, and philosophy to enhance their job performance and bring multidisciplinary viewpoints to tackle security challenges from various perspectives and make wise decisions that balance technical and ethical considerations.

Testing

Math provides an understanding of cryptography and statistics in risk assessment. Electronics and computer engineering allow the knowledge of network and security measures. Finally, philosophy can give a sense of ethical conflicts that may arise. Each of these disciplines addresses challenges and expands the knowledge of Information Security Analysts.

References

Occupation Profile for Information Security Analysts | *CareerOneStop*. (n.d.). CareerOneStop .

Retrieved April 27, 2023, from

<https://www.careeronestop.org/Toolkit/Careers/Occupations/occupation-profile.aspx?keyword=Information%20Security%20Analysts&location=United%20States&onetcode=15-1212.00>

Cybersecurity Career Pathway. (n.d.). Cyberseek. Retrieved April 27, 2023, from

<https://www.cyberseek.org/pathway.html>

Electronics and Computer Engineering Technology. (n.d.). Bowling Green State University.

Retrieved April 27, 2023, from

<https://www.bgsu.edu/technology-architecture-and-applied-engineering/schools-and-departments/engineering-technologies/electronics-and-computer-engineering-technology.html>

Loveless, B. (2022, March 10). *15 Learning Theories in Education (A Complete Summary)*. Education Corner. <https://www.educationcorner.com/learning-theories-in-education/>

mathematics. (n.d.). Encyclopædia Britannica; Encyclopædia Britannica. Retrieved April 27, 2023, from <https://www.britannica.com/science/mathematics>

Nails, D. (n.d.). *Socrates (Stanford Encyclopedia of Philosophy)*. Stanford Encyclopedia of Philosophy. Retrieved April 27, 2023, from <https://plato.stanford.edu/entries/socrates/>

philosophy. (n.d.). Encyclopædia Britannica; Encyclopædia Britannica. Retrieved April 27, 2023, from <https://www.britannica.com/topic/philosophy>