St. John's University’s new New York State Registered Master of Science Degree in Cyber and Information Security

Denise Dragos, Suzanna Schmeelk, Joan E. DeBello

St. John’s University, Queens, New York, United States of America

Abstract

The field of cybersecurity is expanding at an unprecedented rate. The rapid development is due in part to the ever increasing city, state, federal, and international regulations for the privacy and security of sensitive communications and the underlying data. This paper discusses the research and statistics involved in developing a New York State registered Master of Science degree in Cyber and Information Security at St. John’s University. The program is a 30 credit master’s program that combines cybersecurity and information science. It is designed with cybersecurity specialists, IT enterprise professionals, and data scientists in mind. The knowledge it provides can also serve the cybersecurity skill needs of the wider community of IT managers and computer professionals. Our research paper explores the courses chosen in the current program to keep-up with the pervasive nature of cyber threats. We discuss the appeal of the program to students who want to become cybersecurity specialists, change their careers, or improve their skills. Finally, we share the lessons learned creating the program.

Keywords: *Cyber Security, Cybersecurity, Information Security, Digital Forensics, Graduate Program, Master of Science, New York State, Online Distance Learning.*

1. Introduction

The need for information security and cybersecurity has been increasing at an unprecedented rate. The rapid changes are partially due to three main factors. First, there is an ever increasing number of new information systems being developed and deployed. Second, the regulatory and risk factors are being regularly redefined, improved, and developed. Third, incidents and breaches are occurring at an alarming rate.

Just several years ago there were few graduate degree granting institutions in the U.S. for cyber or information security. At the time of our application, there were only four similar programs in the entire New York City area.

St. John’s University is a Catholic four year private institution with its main campus in Queens NY. Its undergraduate program in cyber security systems and graduate program in cyber and information security are given through the Collins College of Professional Studies. The graduate program in cybersecurity will be offered in both traditional (face-to-face) and online distance learning formats. Our university is accredited by Middle States and the undergraduate cybersecurity program is currently going through ABET accreditation.

2. Review of Literature

The trend for using technology to make life more convenient is growing at a rapid rate due to the rise of the Internet of Things (IoT). Chandrashekhar et al. [11], reported in 2016 that it is estimated 75 billion devices will be connected in 2020. More and more people are getting and staying connected. The millennials are creating and using IoT devices daily, with generation Z not far behind. The developers need to secure these devices and keep consumers’ data protected. With so much connectivity, there is a growing interest in the area of cybersecurity and a growing demand for graduates who have the skills necessary to keep products, consumers and corporations safe and secure [11].

The cyber and information security curriculum has increasingly grown. What was once part of a program in computer science with a few courses, special track or option is now a full program of study at the undergraduate level which also has introductory fundamentals even in high school and more specialized programs at the graduate level of study with research [12].

The U.S. federal government, recognizing the growing importance of cybersecurity, has invested resources into education and specialized programs including the National Initiative for Cybersecurity Education (NICE) and the Department of Homeland Security (DHS) Cyber Skills Task Force [13].
Andel and McDonald [5] discuss formalized four year academic programs supporting cyber and information assurance requirements. Their work documents curriculum development that focuses on a systems level approach to cyber assurance education.

Chow, Crutchlow, and Cain [6] hosted a practitioner panel to provide perspectives on the cybersecurity workforce shortage based on personal experience, and share ways that the academic community can improve the pipeline of cybersecurity graduates with needed skills.

Goel and Kumar [2] presented a poster describing concepts around developing skills via a more complete cybersecurity ecosystem involving collaboration and synergy among the four main pillars of society: Academia, Government, Industry and Social Civil Societies.

Yamin and Katt [3] mapped job skills to their academic programs and evaluated map against two certification programs: (1) CREST registered penetration tester for red teams and (2) Securing web applications, Services and Servers for blue teams, which are not under US-DOD 8570 baseline, but are approved by UK GCHQ. They then identified that their map covered the basic security skills present in those certification programs.

3. Core MS Curriculum

The cybersecurity knowledge-base for the workforce varies by role. In depth skills, training in software tools, and ethics must be built into any effective graduate program to ensure student success and job placement. The St. John's graduate program was designed to give students all the necessary skills in core foundation courses as well as specific disciplined courses in more focus based areas of information technology, data science or cyber security [4].
Students enrolled in the cyber and information security graduate program will complete a master's thesis or capstone project. They'll work closely with faculty having specialized skills in cyber security, digital forensics, computer science, data science, artificial intelligence and machine learning. The dual teaching formats (traditional and online) make the program attractive to a variety of local, out of state, or international students. It's designed for students who have undergraduate degrees in computer science, IT, or are looking for a change in career (www.stjohns.edu).

4. Program Design to Meet Professional Needs

There will be 3.5 million unfilled cybersecurity jobs by 2021, while cybercrime costs are expected to hit six-trillion dollars annually. From 2017 to 2021 cyber spending will exceed one-trillion dollars [8]. Hanover rates computer and information systems security/information assurance as one of the highest growth fields within Computer and Information Technology Administration and Management [9]. This booming need inspired the 30 credit program. Students will all take core competency courses in foundations in cybersecurity, protection of digital infrastructure, cybersecurity laws regulations and best practices, and principles of secure scripting and cryptography. Given the needs for today's jobs and the skills necessary to get employed and do well within the job, they may optionally complete a specialization in data science or IT enterprise [1].

5. Lessons Learned and Future Research

There were many lessons learned during the creation of our program. These lessons along with experience gained from running the program will lead to different strands of future research.

5.1 Lessons Learned

We have learned many lessons in the development and accreditation of a new master's program. First, in order to create a new program there is a process that our faculty must follow which includes creating an initial proposal that is supported by both our dean and the deans of the other colleges within the university. Once approved, the proposal is completed by division faculty and approved internally. The proposal is reviewed by the college Curriculum and Education Committee before going to the college Faculty Council. Its next steps are the university Graduate Council and Board of Trustees. Once completely approved at the university level, the application is then sent to the NY

State Department of Education for final review and approval. Only then will the application be registered as an official degree program. This process took over two and a half years. Experience creating similar graduate programs in Data Science and Computer Science helped tremendously.

Second, marketing is essential for a new program. It is very important to identify websites listing relevant programs and get the new program included. Reaching current undergraduate students at the university can fast track applicants to the program. Undergraduate alumni from the cyber security systems, computer science, information technology, networking, and healthcare informatics have been informed of the new opportunity that the school has to offer. It's also important to host information sessions for interested students.

Additionally, the chair and program directors reach out to members of the advisory board and local professional organizations to promote the major and to gather input for continuously improving the program. Utilizing these resources helps to strengthen the program and provides the networking ties that our students and faculty can use to promote internships and possible job placement.

5.2 Future Research

There are many pathways for future research for our master's of science program. First, we can further expand and improve on the overall curriculum. Second, we can explore capstone and theses which have been studied in the program. For example, Freeman, Haigler, Schmeelk, Ellrodt and Fields [7] explored doctoral dissertations through the lens of machine learning. A similar study could transpire for our program. Third, we can explore research projects within the program. Fourth, we could explore further accreditation and industry job mappings for the program. Fifth we can also conduct research with faculty and students in the division's other graduate programs of study in computer science and data science and can collaborate on Artificial Intelligence, Healthcare Informatics and other topics where cybersecurity is essential and gaining interest.

6. Conclusions

Developing a new New York State cybersecurity program has been a significant undertaking but extremely rewarding. This program fills a program gap in the New York, Long Island, and Metropolitan area for students interested in cybersecurity especially for those interested in specializing in digital forensics, data science, information technology enterprise and who may be looking for a change of career.

References

[1] St. John's University (2020) M.S. in Cyber and Information Security. Retrieved from: https://www.stjohns.edu/academics/programs/ms-cyber-and-information-security

[2] Rajni Goel and Vineet Kumar. 2017. A Public-Private-Social Ecosystem: An Interdisciplinary Framework for Cybersecurity Capacity Building. In Proceedings of the 2017 ACM SIGMIS Conference on Computers and People Research (SIGMIS-CPR '17). Association for Computing Machinery, New York, NY, USA, 185–186.

[3] Muhammad Mudassar Yamin and Basel Katt. 2019. Cyber Security Skill Set Analysis for Common Curricula Development. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19). Association for Computing Machinery, New York, NY, USA, Article 37, 1–8. DOI: https://doi.org/10.1145/3339252.3340527

[4] H. Santos, T. Pereira and I. Mendes, "Challenges and reflections in designing Cyber security curriculum," 2017 IEEE World Engineering Education Conference (EDUNINE), Santos, 2017, pp. 47-51, doi: 10.1109/EDUNINE.2017.7918179.

[5] Todd R. Andel and J. Todd McDonald. 2013. A Systems Approach to Cyber Assurance Education. In Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference (InfoSecCD '13). Association for Computing Machinery, New York, NY, USA, 13–19. DOI:https://doi.org/10.1145/2528908.2528920

[6] Jonathan Chow, Eric Crutchlow, and Justin Cain. 2015. Industry Cybersecurity Workforce Development. In Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research (SIGMIS-CPR '15). Association for Computing Machinery, New York, NY, USA, 19.

[7] I. C. Freeman, A. J. Haigler, S. E. Schmeelk, L. R. Ellrodt and T. L. Fields, "What are they Researching? Examining Industry-Based Doctoral Dissertation Research through the Lens of

Machine Learning," 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, 2018, pp. 1338-1340, doi: 10.1109/ICMLA.2018.00217.

[8] Landivar, Muoi Tran (2018). Cybersecurity Career Guide: Who Works in Cybersecurity? How We Got Started. Why We Need You. Palo Alto Networks.

[9] Hanover Research Study (2017), Potential Professional Master's Degree Program Fields.

[10] Chandrashekhar et al. 2016 Security Fundamentals in Internet of Things. International Journal of Research (IJR). http://internationaljournalofresearch.org

[11] Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. Computers & Security, 75, 24-35.

[12] Bicak, A., Liu, X. M., & Murphy, D. (2015). Cybersecurity curriculum development: introducing specialties in a graduate program. Information Systems Education Journal, 13(3), 99.

[13] Conklin, W. A., Cline, R. E., & Roosa, T. (2014, January). Re-engineering cybersecurity education in the US: an analysis of the critical factors. In 2014 47th Hawaii International Conference on System Sciences (pp. 2006-2014). IEEE.