Developing Cybersecurity Degree Programs to Meet Workforce Needs

Donald Heier
Department of Mathematics, Computer Science and Statistics
Saint Mary's University of Minnesota
Winona, MN 55987
dheier@smumn.edu

Abstract

Saint Mary's University of Minnesota is a private, nonprofit university that includes an undergraduate college with 59 majors plus schools of graduate and professional studies with 60 programs offering a variety of masters, doctoral or specialists' degrees. In 2016, after a period of careful study, the university committed to launching an effort into cybersecurity education. This paper details the steps and processes undertaken to bring forward an online master's degree in cybersecurity that was immediately followed by the addition of a cybersecurity track to the bachelor's degree in computer science.

1 Introduction

Saint Mary's University of Minnesota is a private, nonprofit university that includes an undergraduate college with 59 majors plus schools of graduate and professional studies with 60 programs offering a variety of masters, doctoral or specialists' degrees. In 2016, after a period of careful study, the university committed to launching an effort into cybersecurity education. This paper details the steps and processes undertaken to bring forward an online master's degree in cybersecurity that was immediately followed by the addition of a cybersecurity track to the bachelor's degree in computer science.

In the fall of 2017, the university hired a program director / professor of computer science to lead the effort. A working group of cybersecurity professionals was formed to bring in expert experience and knowledge to help set the direction for program development. After several months of bi-weekly meetings, a vision for the graduate program began to emerge. This vision fed into research on cybersecurity programs throughout the country about what types of courses a cybersecurity program would include and how this collection of courses could be adapted, modified and added to. Research was also undertaken into various cybersecurity certifications in order to ensure that graduates would be prepared to pass many of these exams upon the completion of their coursework. This led to the development of a set of 12 graduate courses that have many unique features and fit well with the market and educational leadership that Saint Mary's has had great success in. This program is designed to prepare graduates to have leadership roles in the cybersecurity programs. It features courses that extend beyond the technology and cybersecurity management skills by implementing courses that focus on leadership, communication and ethics.

The knowledge gained from the development of the master's program was utilized a couple months later thru the addition of the cybersecurity track to the revised computer science bachelors' program. The bachelor's program was designed to provide traditional computer science and technology skills that could flow into a series of courses focused on cybersecurity topics which will effectively prepare students for entry level positions in cybersecurity.

2 Design Considerations

Saint Mary's University of Minnesota put together a development team that started on February12, 2016 to investigate degree programs for cybersecurity. The development team consisted of administrators and technical staff from the university along with a working group of eight industry leaders in cybersecurity. In August of 2016 they recommended the university move forward with curriculum development for a M.S. in information security, a B.S. completion degree in information security, and a four year undergraduate degree in information security on the Winona campus. They cited many industry trends to support their recommendation based primarily on the rapid growth in the field and the number of cybersecurity positions that employers were not able to fill.

It was decided to first design the online master's degree, then follow up shortly after with the bachelors programs. Early on in the development, a vision for the program was refined that fit well with the current offerings from Saint May's University. That vision focused on 3 main areas: Technical skills, management skills, and leadership abilities. Threes three areas formed the framework for an array of course offerings.

Patrick Joyce, a member of the development team, and CISO of Medtronic stated the following: "Ability to communicate and the strong communication/interpersonal skills are absolutely critical. You can be incredibly good at the tech, but without the softer skills to communicate laterally and up and down, you won't succeed. You need the ability to bring people along with you. You must be able to speak succinctly and make the complex understandable via meaningful business terms. If you can't do that, you are DOA (1)." Aaron Wampach, also a development team member and a security architect for Health Partners stated the following when asked what the biggest weakness he saw in cybersecurity job applicants today, "The ability to synthesize something down to a concept that an executive or board of directors would be able to understand. You can be a brilliant professional with great technical acumen, but that will only get you so far." He also suggested "A big important trait is the ability to make quick decisions based on data analysis. They really need to have the critical thinking skills (2)."

With recommendation such as those above, the endeavor to design and implement a successful master's program began. The design was completed in December of 2017 and the first courses were launched in August of 2018. Section 3 of this paper outlines the design of the master program.

Section 4 outlines the design on the undergraduate bachelors program. The cybersecurity program was designed as a track under the computer science program and essentially brought in a selection courses that were foundational in nature, and had a strong applied component. There were essentially adapted from the already designed master's courses to give students practical hands on skills.

3 Master's Program Design

The M.S. in Cybersecurity degree is geared toward people who have some experience with information technology, and seek to focus on managing information security within organizations (3). Students are not required to have a bachelor's degree in information technology, but must at least have computer networking as a foundational course. The program advances students' technical knowledge in information security along with leadership skills to manage security information business planning and implementation. The program addresses organizations' need to hire information security professionals with sound technology skills coupled with strong communication, consultative, and conflict management skills. Information security professionals are frequently called upon to interact with unknowing end users in order to teach, lead, change behaviors, or mandate compliance with company policy or laws.

Currently the program is designed as a streamlined, 36-credit degree without electives. Courses include communication, leadership and ethics, change management, along with cybersecurity technical courses.

The program description, outcomes/indicators, course plan, course descriptions and student learning objectives, and curriculum map follow.

3.1 Program Description

The Master of Science in Cybersecurity equips students to manage information security programs in organizations. The program provides up-to-date knowledge and skills in the technology and application of cybersecurity. Students will learn to apply risk management frameworks, methods, and strategies; enhance the protection of enterprise-wide information assets; and detect and plan for cyber-attacks on networks and computer systems. Students will be prepared to manage security information functions and teams in all business, nonprofit, healthcare, government, educational, and other sectors.

3.2 Program Outcomes and Indicators

Upon completion of the program, graduates are expected to be able to do the following:

1) Demonstrate business management skills relevant to administering information security programs in organizations**.**

a) Integrate best practices of business administration functions into a security plan.
b) Identify legal issues, the sources of law, and compliance bodies related to computer security for an organization.
c) Analyze business alignment, risk appetite, and risk aversion in program implementation.
d) Develop administrative security policies, procedures, and enforcement plans.
e) Evaluate security requirements and implementation for vendors, consultants, and contractors.

2) Apply leadership skills in information security planning.

a) Articulate a shared vision for security operations.
b) Incorporate an understanding of ethical and social responsibility into information security decisions regarding the interaction of human beings, information objects, and social computing technologies.
c) Develop high performing work teams.
d) Apply systems theory to security operations.
e) Monitor the impact of organizational change and decision making affected by ongoing and diverse external and internal security threats.

f) Evaluate new information available related to current cybersecurity issues, threats, and recovery.

3) Demonstrate proficiency in communicating technical information.

a) Effectively present formal reports, documentation, and oral presentations to corporate management, users, and information technology professionals.
b) Demonstrate a professional manner and style in all communications.
c) Analyze how the practitioner's perspectives and culture shape interpersonal communication.
d) Apply the principles of communication theory as it applies to interpersonal and group communication.

4) Develop a strategic balance between business needs and overall information security architecture planning.

a) Incorporate security policy, industry and regulatory standards, and technology into security architecture planning.
b) Integrate formal frameworks for privacy-enhancing technologies and models of privacy protection.
c) Evaluate security policy, standards, procedures, and guidelines.
d) Apply security governance principles of confidentiality, integrity, and availability.
e) Analyze legal and regulatory issues that pertain to information security in a global context.
f) Lead the implementation and management of physical security with both perimeter and internal security controls.
g) Secure information resources through asset management and configuration management techniques.
h) Apply foundational security operations concepts such as least privilege, separation of duties, job rotation, and service level agreements.

5) Evaluate risk management frameworks, methods and strategies.

a) Analyze multiple risk management frameworks, models, processes, and tools.
b) Conduct risk and vulnerability assessments of existing and proposed information systems.
c) Develop plans to operationalize risk management in an organization or government agency.
d) Apply threat modeling concepts and methodologies.
e) Select security controls based upon systems security requirements through an understanding of the security capabilities of information systems.
f) Apply risk-based management concepts to core business processes.
g) Articulate fundamental concepts in IT security audit and control processes.

6) Plan for cyber-attacks on networks and computer systems.

a) Devise a mitigation plan against both external and internal vulnerabilities to enterprise computer infrastructures and sensitive digital assets.
b) Integrate current tools and methods that involve response, mitigation, and policy.
c) Develop methods for identifying, acquiring, preserving, and analyzing electronic evidence from single machines, networks, and internet.
d) Analyze both technical and legal issues of computer forensics investigations.
e) Apply evidence recovery theory and practice of computer file systems, memory, registry, network logs, and communications for security incidents.
f) Utilize digital forensics, biometrics database security, intrusion detection, and prevention to improve systems security.
g) Conduct logging and monitoring activities to assist with intrusion detection and prevention, and event management.
h) Conduct incident management through all stages of a breach with knowledge of detection, response, mitigation, reporting, recovery, and remediation.

7) Protect enterprise-wide information assets.

a) Apply effective industry accepted information and risk management techniques that include proactive security testing methods.
b) Implement secure design principles in network architectures with an understanding of various protocols and network models, software defined networks, and wireless networks.
c) Conduct security control testing that involves a vulnerability assessment, penetration testing, log reviews, synthetic transactions, code review and interface testing.
d) Operate detective and preventive measures using firewalls, intrusion detection and prevention systems, and third-party provided security services.
e) Demonstrate recovery strategies such as backup, recovery sites, multiple processing sites, and fault tolerance.

3.3 Course Plan

Degree Requirements: 36 credits: Recommended Sequence:

1) CYBR600 Foundations of Cybersecurity (3 cr.) (required first course)
2) CYBR605 Security Architecture (3 cr.)
3) CYBR610 Network Security and Intrusion Detection (3 cr.)
4) CYBR615 Cybersecurity Change Management (3 cr.)
5) CYBR620 Operational Security Policy (3 cr.)
6) CYBR625 Risk Management (3 cr.)
7) CYBR630 Communication for Cybersecurity Professionals (3 cr.)
8) CYBR635 Data Privacy (3 cr.)

9) CYBR640 Leadership and Ethics (3 cr.)
10) CYBR645 Incident Response and Investigation (3 cr.)
11) CYBR650 Ethical Hacking and Defense (3 cr.)
12) CYBR690 Security Operations and Leadership (3 cr.) (capstone course)

Students must have a transcripted undergraduate or graduate computer networking course completed before taking CYBR610. CYBR590 Computer Networking is provided for those who need the prerequisite knowledge. This foundational course does not count toward the 36-credit degree.

3.4 Course Descriptions

1) CYBR590 Computer Networking (3 cr.)
The course introduces the foundations of network infrastructures and network technology. It covers the OSI model in depth, including TCP/IP, and introduces basic switching and routing concepts. Students investigate the standards, design, architecture, and operation of LAN, WAN, and telecommunications.

2) CYBR600 Foundations of Cybersecurity (3 cr.)
This course provides an overview and foundational understanding of concepts essential to the cybersecurity professional to evaluate best practices in implementing security systems within the enterprise. This course covers key bodies of knowledge in security, privacy, and compliance. Topics include security planning, risk management, security technologies, basic cryptography, digital forensics, application security, intrusion detection and prevention, physical security, and privacy issues.

3) CYBR605 Security Architecture (3 cr.)
This course introduces the student to the importance of security architecture design in enterprise security. Students are presented with a structured approach to the steps and processes involved in developing comprehensive and layered security architectures. Students evaluate the principles, attributes, and processes used in designing and deploying architecture that supports the business objectives of the enterprise.

4) CYBR610 Network Security and Intrusion Detection (3 cr.)
Prerequisite: CYBR590 Computer Networking or equivalent
This course provides a comprehensive overview of network security and intrusion detection. Students focus on methods for securing networks, and utilize these methods in basic architectural design. Students apply these methods into a cohesive network security strategy. Topics include investigation of areas such as network analysis, perimeter defense strategies, network monitoring, vulnerability and intrusion detection, and security in mobile and wireless environments.

5) CYBR615 Cybersecurity Change Management (3 cr.)
This course describes the business context in which a cybersecurity professional must function within an organization. Students examine the interplay between business process

and cybersecurity issues in mitigating security threats. An overview of audit, compliance, regulation, and liability for business security, along with how to construct effective continuity and disaster recovery plans, are provided.

6) CYBR620 Operational Security Policy
In this course, students examine the role of security policies, standards, and procedures in addressing business and technical security risks. Students explore the types of policies that are part of an overall security strategy. Policies are discussed that drive computer security, including discretionary access control, mandatory access control, and role-based access control types of policies, and how these are used in organizations. Students develop policies and deployment plans as part of the comprehensive strategic plan for the enterprise.

7) CYBR625 Risk Management
This course includes a study of the existing risk management frameworks, models, processes, and tools to provide students with the theory and practical knowledge to operationalize risk management in an organization or government agency. Additionally, fundamental concepts in information technology security audit and control processes for an organization are discussed. Students learn to create a control structure and audit an information technology infrastructure.

8) CYBR630 Communication for Cybersecurity Professionals
This course introduces students to the foundations of communication in a business setting as a critical component for success in the workplace. Students develop a foundation for designing effective messages, both written and oral, from concept to delivery. This course emphasizes elements of persuasive communication: how to design messages for diverse and possibly resistant audiences and how to present that information in a credible and convincing way.

9) CYBR635 Data Privacy (3 cr.)
This course introduces techniques for information distribution in such a way that data privacy is protected. It discusses models and frameworks for privacy protection that support privacy enhancements from economic, legal, and policy perspectives. Fundamentals of cryptographic theory and practice along with its applications are introduced in topics such as classical and contemporary ciphers, encryption and decryption, breaking ciphers, cryptographic protocols, and analysis tools.

10) CYBR640 Leadership and Ethics (3 cr.)
This course focuses on the development of leadership skills used in managing a successful security program. Students analyze the role of a leader in business with a focus on decision making, management of group dynamics, workplace stress and conflict, motivation of employees, and planning. Ethics and social responsibility will be emphasized throughout the course.

11) CYBR645 Incident Response and Investigation (3 cr.)

This course introduces the principles and best practices for incident response, along with an overview of digital forensics. Students understand the goals of incident response and learn how to prepare and respond to information security incidents and understand how the incident occurred. Students understand the process of collecting and analyzing data, and the process of remediation. The course outlines the investigative and analysis process, tools, digital evidence, and applicable law with a focus on computer, mobile, network, and database forensics.

12) CYBR650 Ethical Hacking and Defense (3 cr.)
This course includes a study of theoretical and practical aspects of network and web application penetration testing. Students are able to evaluate the security of a network or system's infrastructure and outline how hackers find and attempt to exploit any vulnerabilities. Included in the course are in-depth details on ethical hacking, including reconnaissance, vulnerability assessment, exploitation, maintaining access, and covering tracks. A focus on current tools and methodologies is stressed.

13) CYBR690 Security Operations and Leadership Capstone (3 cr.)
Prerequisites: All required coursework completed or co-requisite
This course provides an opportunity for students to integrate their learning across the program in a case study project. Students complete a risk analysis, vulnerability and threat analysis, security infrastructure requirements, logical design, physical design, management design, pricing, and implementation planning.

4. Bachelors' Program

In the spring of 2018, Saint Mary's University completed the renewal of the computer science major with the belief that a solid computer science program will help support the university's vision of providing advanced knowledge, skills and critical thinking abilities to prepare tomorrow's leaders. The primary goal of the revised major was to make it current with industry trends and prepare graduates for a wide variety of positions in computer technology (4). The redesign of the program was well supported by national standards, career outlooks and relevant research papers. The primary source of the revisions emanates from the Curriculum Guidelines for Undergraduate Degree Programs in Computer Science released in 2013 by The Joint Task Force on Computing Curricula which includes the Association for Computing Machinery (ACM) and IEEE Computer Society (5).

4.1 Program Description

The existing computer science major consisted of three tracks: Programming, Geographic Information Science and Data Analytics. These tracks were maintained even though the

Computer science core was modified. A new track in cybersecurity was added to meet the growing demand for cybersecurity professionals.

Table 1 outlines the computer science core.

Computer Science Core		
Course	Description	Credits
CS101	Computer Science Fundamentals	3
CS110	Computer Science I	3
CS210	Computer Science II	3
CS220	Discrete Math	3
CS255	Database Design	3
CS300	Networking	3
CS307	Introduction to Cybersecurity	3
Total Credits		**21**

Table 1: Computer Science Core

Table 2 outlines the cybersecurity track.

Computer Science: Cybersecurity		
Course	Description	Credits
	CS Core	21
CS305	Server Systems	3
CS317	Network Security	3
CS327	Risk Management	3
CS337	Forensics and Incident Response	3
CS357	Cyberwarfare and Hacker Techniques	3
CS490	Capstone Project	3
Choose 9 credits from the following		9
CSxxx	CS electives	
CS496	Internship (3-6)	
Total Credits		**48**

Table 2: Cybersecurity Track

4.1 Course Descriptions

The following are key courses in the cybersecurity track:

1) CS307 Introduction to Cybersecurity (3 cr.)
This course provides an overview of modern security concepts. Topics covered will include security terminology, risk management, security policy and strategy, security awareness, cryptography, operating system security, network security, physical security and digital forensics. The course will contain a lab component where students will investigate current hardware and software tools for vulnerability analysis and penetration testing. This course is designed to assist students to:
Understand information security's importance in our increasingly computer-driven world; Master the foundational concepts of information security; Develop a "security mindset" by learning how to critically analyze situations of computer and network usage from a security perspective.

2) CS317 Network Security (3 cr.)
This course provides a comprehensive overview of network security with a focus on methods for securing networks, and utilizing these methods in basic architectural design. The methods are then applied to the design of a cohesive network security strategy. Topics include investigation of areas such as network analysis, perimeter defense strategies, network monitoring, vulnerability and intrusion detection, and security in mobile and wireless environments. This course is designed to assist students to: Identify key concepts in network security; Implement these concepts as security attacks/controls in a lab environment; Relate course material to real-world events and situations.

3) CS327 Risk Management (3 cr.)
This course includes a study of the existing risk management frameworks, models, processes, and tools to provide students with the theory and practical knowledge to operationalize risk management in an organization or government agency. This course is designed to assist students to: Engage in active discovery of risk management principles; Prepare to function in a business environment, developing an awareness of the challenges, the tools, and the process of designing and implementing a risk management program; Help evaluate various strategies to treat risk and select strategies appropriate to the goals and objectives of the business.

4) CS337 Forensics and Incident Response (3 cr.)
This course introduces the principles and best practices for incident response, along with an overview of digital forensics. The goals of incident response; preparation and response to information security incidents; and understanding how incidents occur are covered. Computer and digital media resources are used to explore basic digital forensic investigation techniques. This course is designed to assist students to:
Correctly define and cite appropriate instances for the application of computer forensics; Correctly collect and analyze computer forensic evidence; Identify the essential and up-to-date concepts, algorithms, protocols, tools, and methodology of computer forensics; Obtain basic knowledge on dealing with system security related incidents; Increase knowledge on potential defenses and counter measures against common threat vectors/vulnerabilities.

5) CS357 Cyberwarfare and Hacker Techniques (3 cr.)
This course includes a study of theoretical and practical aspects of network and web application penetration testing. The evaluation of the security of a network or system's infrastructure and the process of how hackers find and exploit vulnerabilities are covered. In-depth details on ethical hacking, including reconnaissance, vulnerability assessment, exploitation, maintaining access, and covering tracks are discussed. This course is designed to assist students to: Understand the elements of security; Identify the phases of the hacking cycle; Identify the different types of hacker attacks; Understand hacktivism; Understand ethical hacking; Understand vulnerability research and identify tools assisting in vulnerability; Identify steps for conducting ethical hacking; Understand computer crimes and implications; Describing the security threats facing modern network infrastructure.

4. Conclusion

This paper details the steps and processes undertaken to bring forward an online master's degree in cybersecurity that was immediately followed by the addition of a cybersecurity track to the bachelor's degree in computer science.

The master's program involved the development of a set of 12 graduate courses that have many unique features and fit well with the market and educational leadership that Saint Mary's has had great success in. The knowledge gained from the development of the master's program was utilized a couple months later thru the addition of the cybersecurity track to the revised computer science bachelors' program. It is early in the implementation process, but so far the response from the community and students has been very positive. The master's program currently has approximately 40 students enrolled and that number will likely double in the next 6 months. We are in the beginning phases of marketing the undergraduate program and are recruiting students for next year. Local employers have already reached out with an interest in our students for internships and future full time employment.

References

[1] Joyce, Partick. Personal Interview. 23 February 2018

[2] Wampach, Aaron. Personal Interview. 23 February 2018

[3] Saint Mary's University of Minnesota. (2019). *2018-2019 Academic Catalog.* Retrieved from: http://catalog.smumn.edu/index.php?catoid=25

[4] Occupational Outlook Handbook, United States Department of Labor – Bureau of Labor Statistics. Retrieved from*:* https://www.bls.gov/ooh/computer-and-information-technology/home.htm

[5] Association for Computing Machinery (ACM), IEEE-Computer Society - Joint Task Force on Computing Curricula. (2013). *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science.* Retrieved from: http://www.acm.org/education/CS2013-final-report.pdf