Master of Science in Cybersecurity

Program Director: Henry Collier

Please note: The Norwich Board of Trustees has authorized the renaming of the Master of Science in Information Security and Assurance program (MSISA). In March 2020 it became the Master of Science in Cybersecurity program. Student who enrolled in the Masters of Science in Information Security and Assurance may continue their studies and receive their MS in Information Security and Assurance, or they may petition the Registrar to change their program of study to the the MS in Cybersecurity program.

The Master of Science in Cybersecurity program delivers state-of-the-art, high-quality, and convenient education to busy professionals committed to furthering their careers in information security and assurance. In particular, the Master of Science in Cybersecurity program appeals to chief information, technology, and information security officers of business and governmental organizations and is designed for security administrators, network administrators, information technology specialists, professionals in the information technology field, including military personnel. Master of Science in Cybersecurity graduates are leaders and innovators in information security and assurance, bringing sound interdisciplinary perspectives to the field.

The program balances academic rigor with convenience. This combination maintains and respects Norwich University's long educational heritage while it meets the needs of today's working students. The program hires instructors who are academically and professionally qualified in their respective fields of expertise. Please note that a case study is a required part of the Master of Science in Cybersecurity program.

Throughout the program, students:

- Study various aspects of information security and assurance
- Analyze the situation at their workplace or case study site
- Complete written assignments
- Use research findings to prepare a report with recommendations

Depending upon the concentration chosen, students are able to

- Perform penetration tests,
- Analyze cyber law, cybercrime and critical infrastructure protection
- Understand international perspectives on cyber space
- Manage Computer Incident Response Teams
- Apply best practices in digital forensics

Requirements

Curriculum Map/Plan of Study

Term 1		
GI 512	Foundations and Historical Underpinnings of Information Assurance	6
Term 2		
GI 522	Information Assurance Technology	6
Term 3		
GI 532	Human Factors and Managing Risk	6
Term 4		
GI 542	Information Assurance Management and Analytics	6
Term 5		
One Concentration Course		6
Term 6		
One Concentration Course		6
Culminating Academic Requirement		
GI 595	Residency [1]	0
Total Cr.		**36**

[1] Students are required to attend a one-week, on campus Residency Conference the June following or concurrent with their final course.

Curriculum Requirements

Four of the six seminars in the 36 credit hour program are core requirements and two courses comprise an elective concentration. All courses are focused on providing an opportunity for students to acquire and exercise the knowledge and skill expected of top-level managers of information security and assurance in today's demanding security environment.

Required Core Courses (24 credits)

GI 512	Foundations and Historical Underpinnings of Information Assurance	6
GI 522	Information Assurance Technology	6
GI 532	Human Factors and Managing Risk	6
GI 542	Information Assurance Management and Analytics	6
Culminating Academic Requirement		
GI 595	Residency	0
Total Cr.		**24**

Concentrations (12 credits)

One of the following two-seminar, 12-credit concentrations is required to complete the 36 credit hour program: Project Management, Forensics, Critical Infrastructure Protection and Cyber Crime, Vulnerability Management, Cyber Law and International Perspectives on Cyber Space.

Project Management Concentration

The Project Management concentration offered to the MS Cybersecurity students uses a sequential approach to provide a thorough understanding of all aspects of project-management theory and practice. Academic objectives of this program are mapped to *A Guide to Project Management Body of Knowledge* (PMBOK® Guide). MS Cybersecurity students enrolled in this concentration will be taking advantage of the experience of the Project Management faculty in conjunction with MS Cybersecurity faculty members who specialize in cyber security and information assurance. More importantly, the Project Management students establish a firm foundation in project management tools, techniques and practices. MS Cybersecurity students are required to take two of the three Project Management concentration courses. The courses offer in-depth study, specifically addressing each project management process area from a project leadership perspective.

Project Management Seminars		
GB 544	Project Management Techniques, Tools and Practices	6
GB 554	Project Management Leadership, Communications and Teams	6
or GB 564	Strategic Management in Project Management	
Total Cr.		**12**

Computer Forensic Investigation/Incident Response Team Management Concentration

In this concentration, students learn to analyze and apply the key points in creating and managing a computer security incident response team (CSIRT) also known as a computer incident response team (CIRT) or a computer emergency response team (CERT). Students use the

case study developed in the four required core courses to apply their knowledge to real-world situations and prepare recommendations for the establishment of a new CSIRT or improvement of their existing CSIRT. This concentration also provides the broad understanding that information assurance professionals must have of the management, investigation, and analysis of digital incidents.

Computer Forensic Investigation/Incident Response Team Management Seminars		
GI 551	Computer Forensic Investigations	6
GI 554	Computer Security Incident Response Team Management	6
Total Cr.		**12**

Critical Infrastructure Protection and Cyber Crime Concentration

This concentration explores the nature of conflict in cyber space focusing on two major Internet-based threats to the U.S. national security: cyber terrorism and cyber crime, and the security of information in computer and communications networks within infrastructure sectors critical to national security. These include the sectors of banking, securities and commodities markets, industrial supply chain, electrical/smart grid, energy, transportation, communications, water supply, and health. The seminars in this concentration provide a risk management framework to help information leaders leverage the benefits of internet technologies while minimizing the risks that such technologies pose to their organizations. Special attention is paid to the risk management of information in critical infrastructure environments through an analysis & synthesis of assets, threats, vulnerabilities, impacts, and countermeasures. Critical consideration is given to the role of Supervisory Control and Data Acquisition (SCADA) systems in the flow of resources such as electricity, water, and fuel.

Critical Infrastructure Protection and Cyber Crime Seminars		
GI 556	Cyber Crime	6
GI 566	Critical Infra. Protection	6
Total Cr.		**12**

Vulnerability Management Concentration

The basics of penetration testing constitute the core of this concentration. Students utilize a virtual lab to gain experience through hands-on lab exercises. Students learn to use the well-known open-source Metasploit computer security project to understand security vulnerabilities, study to use this tool for penetration testing, testing the control tools, and learn to conduct monitoring of an enterprise. Students are introduced to: system security and vulnerability analysis, the most common system exploits and vulnerabilities, system “pivoting” and client-side exploits. Students learn how to assess enterprise security controls and system vulnerability, and to document their findings. Students study the rules of engagement, and how to conduct legal and ethical security tests and vulnerability assessments using known open-source tools (Metasploit , John the Ripper, Wireshark) to understand security vulnerabilities as well as to use this tool for penetration testing, testing the control tools, and how to conduct monitoring of an enterprise. This concentration is designed for penetration testers, system security, and network administrators.

Vulnerability Management		
GI 562	Vulnerability Management and Penetration Testing I	6
GI 563	Vulnerability Management II	6
Total Cr.		**12**

Cyber Law and International Perspectives on Cyber Space Concentration

This concentration presents a comprehensive overview of ethical issues, legal resources and resources, and public policy implications inherent in the evolving online society. Complex and dynamic state of the law as it applies to behavior in cyberspace is introduced, and the pitfalls and dangers of governing in an interconnected world are explored. Ethical, legal, and policy frameworks for information assurance are addressed. Various organizations and materials that can provide assistance to operate ethically and legally in cyberspace are examined. Topics include intellectual property protection, electronic contracting and payments, notice to consent from e-message receipts, non-repudiation and cyber crime, and the impact of ethical, moral, legal, and policy issues on privacy, fair information practices, equity, content control, and freedom of electronic speech using information systems. It also provides an overview of the issues surrounding transnational cyberspace policies, international investment strategies and implementation of communication and information technologies that affect the global economy and transforms the flow of information across cultural and geographic boundaries. The concentration examines various global governance frameworks, and organizations that shape and transform cyberspace such as the International Telecommunications Union, the World Bank Information and Communications Technology Sector, and the U.S. Federal Communications Commission.

Cyber Law and International Perspectives on Cyber Space Seminars		
GI 557	Cyber Law	6
GI 567	International Perspectives on Cyberspace	6
Total Cr.		**12**

Procurement and Government Contract Management

After completing this concentration, students will have the ability to analyze data and craft plans to conduct and actively engage public procurement, contracting, and contract management processes from a functional and management vantage.

Procurement and Government Contract Management Courses		
AD 568	Government Procurement and Contract Management	6
AD 578	Government Contract Management	6
Total Cr.		**12**

One-Week Residency

All degree candidates of the MS Cybersecurity are required to attend a one-week Residency Conference (https://catalog.norwich.edu/onlineprogramscatalog/academicpolicies/graduationrequirements/) on the Norwich University campus, during which they may attend professional presentations, participate in roundtable discussions with faculty, and present papers. The one-week residency is a degree requirement.

Faculty

Faculty Member	Institution at which highest degree was earned
Donald Holden, MBA, CISSP-ISSMP	University of Pennsylvania
Christopher King, MS	Carnegie Mellon University
John Mason, MBA, CISA, CISM, CFE, CFSSP, CFS	University of Phoenix
Matthias Plass, MS	University of Maryland, University College

George Silowash, MSIA, CISSP	Norwich University
Brent Kennedy, MS	Carnegie Mellon University
Bill Powers, PhD	Bellevue University
Peter Sullivan, MISA	Norwich University
Jimmie Flores, DMgt, PhD	University of Phoenix
Jerry Dixon, MISA	Norwich University
Tom Hyslip, DS	Capitol College
Michael Albrethsen, MS	University of Pittsburgh
Charles Lorbeer, PhD	Walden University
Stuart McCubbrey, MIS	University of Michigan