Master of Cyber Security Management (MCSM)

Course requirements
Cyber Security Management Curriculum

Overview

Required Courses

Complete fifteen units from the Required Courses:

- T81-560 Systematic View of Cyber Security and Information Assurance**
- T81-561 View from the Bridge: Leading an Information Security Team**
- T81-562 Applied Cyber Security Practices in Cyber Warfare**
- T81-567 Enterprise Network Security**
- T81-5502 The Art and Science of Risk Management**
- T81-581B Emerging Technologies and Innovation
- T81-612 Cyber Counterespionage — Case Study Analysis
- T81-546 Telecommunications Management*

*Telecommunications Management is the prerequisite for the capstone course.

** These courses are required to earn a Graduate Certificate in Cyber Security Management

Electives

Select nine units of the following:

- T55-524A Executive Perspectives for Technical Professionals
- T81-556 Advanced Risk Analysis and Response Planning
- T81-557 Privacy In The Digital Age
- T81-575 Data Warehousing
- T81-578 Security Auditing
- T81-586 Defensive Hacking
- T81-587 Mobile Security and BYOD
- T81-588 Cryptography

Complete nine units of the following Business and Organization Courses:

- T60-502 Financial Principles of the Company
- B63-529 Management and Corporate Responsibility
- B66-500 Creative Thinking and Leading the Creative Organization
- B66-524 Negotiation
- B66-565 Leading Change
- B67-577 Information Technology and Supply Chain Management
- T81-584 Public Speaking and Presentation Skills for Technical Professionals

All students in the MCSM program will be required to take the Capstone course as their final course in the program.

- T81-585 Capstone Course

The student can select the direction of their course of study by their selection within the Focus course areas.
Course Descriptions Select fifteen units of the following:

Required Courses:

Systematic View of Cyber Security and Information Assurance  
**Total Units: 3.0**  
Information security is paramount to the health of a successful enterprise. Learn what it takes to manage and operate an information security program in an enterprise. The focus is on areas such as risk assessment, risk management, incident handling and business continuity planning. Learn the vocabulary, vernacular and terminology used in the information security space. Learn what keeps Chief Security Officers, their teams and the business clients they serve “awake at night”, and what you can do, as an information security professional to protect your clients.

A View from the Bridge: Leading an Information Security Team  
**Total Units: 3.0**  
This class discusses the “How-To’s” in developing, organizing, staffing and leading an Information Security organization from inception through maturity. How it is supported by the CSIS Top 20 Critical Controls will also be a focal point of the course. We will discuss how to manage the harmony between regulatory standards, information security best practices and organizational practices and procedures in establishing and leading an effective Cyber Security organization. “Because organizations and their information systems constantly change, the activities within the security management process must be revised continuously, in order to stay up-to-date and effective. Security management is a continuous process and it can be compared to W. Edwards Deming’s Quality Circle (Plan, Do, Check, Act).” *(Control Case International 2012).* Students will study initial security policies that stipulate requirements about ethics, confidentiality and integrity. Techniques for implementing and technical controls for enforcing these policies are investigated, including, access control mechanisms, user authentication, configuration and vulnerability management techniques and networking tools such as firewalls and intrusion detection systems. This course explores, more deeply, the principles of information technology governance, focusing on IT control objectives (COBIT) and related internal controls. Coursework provides a deeper understanding of best practices for managing cyber security processes and meeting multiple needs of enterprise management by balancing the void between business risks, technical issues, control needs, and reporting metrics.

Applied Cyber Security Practices in Cyber Warfare  
**Total Units: 3.0**  
This course will provide the student with a basic understanding of information warfare. This course will build from a strategic understanding of warfare as reflected in the information realm. It will discuss both theoretical and practical aspects of dealing with information warfare. Included will be a discussion of how Information Warfare differs from cyber-crime, cyber-terrorism and other forms of on-line conflict. The course will equip the student with the current practices in detecting and mitigating incidences and the communication strategies to employ in educating not only senior management but also the employee body at large. Included will be best practices to design and implement an employee awareness campaign on Incidence Response.

Enterprise Network Security  
**Total Units: 3.0**  
Some of today’s most damaging attacks on computer systems involve the exploitation of network infrastructure, either as the target of attack or as a vehicle to advance attacks on end systems. This course provides an in-depth study of the ITIL methodology in securing the network against various attack techniques. It will explore ITIL methods to defend against them. Topics include firewalls and virtual private networks; network intrusion detection; denial of service (DoS) and distributed denial-of-service (DDoS) attacks; DoS and DDoS detection and reaction; worm and virus propagation; tracing the source of attacks; traffic analysis; techniques for hiding the source or destination of network traffic; secure routing protocols; protocol scrubbing; and advanced techniques for reacting to network attacks.

Art and Science of Risk Management  
**Total Units: 3.0**  
This course focuses on why many project managers miss requirements for schedule, budget or even both. The course concentrates on key Risk Management techniques practiced by leading Project and Program Managers and taught through fact filled lecture, case work and project execution as applied to information systems, engineering, financial, product/process and design projects/programs in today’s fast moving environment. Students will take away key value propositions including Risk Identification, Risk Quantification, Risk Monitoring, Risk Control and Risk Mitigation. This course will enable the student to address common Scope, Schedule, Quality and Cost risk events that occur on complex projects. Project Risk Management
examines the types of risk, with a focus on understanding the process of risk identification, assessment, prevention, mitigation, and recovery; governance, auditing, and control of the confidentiality; integrity; and availability of data. Using common operational, strategic, tactical, and technological scenarios, the coursework provides a comprehensive approach to the challenges faced by managers where global data is readily available, risk is pervasive, regulations are ever-increasing, and the threat of disruption from potential crises is real.

Emerging Technologies and Innovation

**Total Units: 3.0**

Understanding the role that new technologies can play in achieving the strategic vision and thus shareholder value of the firm will be the focus of this course. This includes reviewing appropriate ways of judging a technology and whether a re-positioned technology can drive business value. Students will participate in a process of discovery and judgment rationalization that will lead to understanding how to bring together the technical and commercial worlds in a profitable way. A discussion of the key concepts that it would take to distinguish between activities and outcomes. How do you distinguish between discoveries and technologies add value? Technological innovations (outcomes) are normally the result of product, process, market development and administrative capabilities. A discussion on strategy, visioning, formulation and execution. How does innovation and growth enter into it? Innovation and growth innovation in design; interaction with customers; in business processes; in management thinking? How do you build and innovation strategy will be the capstone of the course.

Cyber Counterespionage – Case Study Analysis

**Total Units: 3.0**

Students will study the management and the communication of information that could be presented in court or could be used to facilitate other information that would be presented in court. The course will review the federal and certain state laws pertaining to the collection of evidence and evidence related material and the successful submission of evidence to a court. In addition, strategies will be discussed as related to discovery of evidence and evidence related material and the use of attorney-client privilege and work product to protect the client’s interests with respect to such material. The students will also examine when reports should be drafted and examine the proper drafting and use of such reports as a submission to legal counsel, the court or to business. Further, the students will study effective testimony in a court of law that would include oral testimony and use of demonstrative evidence and material.

Telecommunications Management

**Total Units: 3.0**

This course reviews all areas of modern telecommunications from the application layer down through the routing and physical network layers for mobile access, global corporate networks, security and network management fundamentals. This course also highlights large scale corporate data collection over the W-W Internet for marketing research, security (i.e., cyber intelligence) and competitive business intelligence purposes.

All students in the MCSM program will be required to take the Capstone course as their final course in the program

**Electives:**

**Defensive Hacking**

**Total Units: 3.0**

This course will cover topics in using what would traditionally be called “hacking” techniques for the purpose of securing your own network. It will explore security architectures and methodologies that will enable a good cyber defense as well as the tools and techniques necessary to test your defense before cyber adversaries do it for you. The course will include hands-on experience in conducting the various types of attacks that are launched against enterprise networks every day. The course will explore proven techniques for successful and effective management, empowering managers to immediately apply what they’ve been taught in their workplace. Prerequisites: A degree in Computer Science or Electrical Engineering (or equivalent), Knowledge of TCP/IP, Unix and Windows operating systems.

**Mobile Security and BYOD**

**Total Units: 3.0**

The proportion of mobile devices providing open platform functionality is expected to continue to increase in future. The openness of these platforms offers significant opportunities to all parts of the mobile eco-system by delivering the ability for flexible program and service delivery options that may be installed, removed or refreshed multiple times in line with the user’s needs and requirements. However, with openness comes responsibility and unrestricted access to mobile resources and APIs by applications of unknown or untrusted origin could result in damage to the user, the device, the network or all of these. This course will explore how to build and manage suitable security architectures and network precautions.

**Security Auditing**

**Total Units: 3.0**

This 8-week course provides information technology (IT) professionals an understanding of how security auditing can be successfully integrated as an important component in an
Data Warehousing

**Total Units: 3.0**

This course will introduce you to the major activities involved in data warehousing and its application to a business. The class will concentrate on topics such as: requirements gathering for data warehousing, business constraints, data warehouse technologies and architectures, dimensional model design, entity relationship model design, physical database design for data warehousing, extracting, transforming, and loading strategies, introduction to business intelligence and reporting, expansion and support of a data warehouse. Once the basic principles have been established, the remainder of the class will be built around a group data warehouse project. The project will begin with your group gathering requirements and developing a data warehouse design. Once the design is complete you will build a prototype data warehouse containing the necessary structures within your database and populating them with source data. This will require you to develop the table definitions, extract/transformation/load (ETL) logic, and example report definitions. We intend this class to be a hands-on example of a simple data warehouse implementation. Focus Areas and Skills Obtained After Completion of the Course: Gather Requirements for Data Warehousing, Explain Data Warehouse Technologies and Architecture, Understand the Advantages and Disadvantages of Both Dimensional and ER Modeling for Data Warehousing, Identify Data Sources, Design a Physical Model for Data Warehousing, Comprehend Extract, Transform and Load Strategies, Design and Develop Business reports and Business Considerations for Expanding and Supporting a Data Warehouse.

Cryptography

**Total Units: 3.0**

As the world becomes increasingly dependent on digital communications, computing, and information, the need for robust cyber security becomes ever more paramount. Within this context, cryptography becomes an indispensable component of any cyber security system. The purpose of this course is to equip cyber security professionals with a firm understanding of cryptographic principles and applications and how cryptography can be used to secure, protect, and safeguard the organization’s communications and information. Students will survey the history of cryptography, the evolution of cryptographic algorithms including important symmetric and asymmetric approaches, hashing, authentication and digital signatures, mutual trust, public key infrastructure, key management, user authentication, and cryptographic attacks. Particular focus will be placed on the integration of cryptography within the organization’s IT infrastructure to include IPSec; email, wireless, and data encryption and how to analyze, support, and present the business case for cryptography in the IT enterprise. NOTE: Although cryptography is a mathematically intense discipline, the course will be taught from a managerial perspective. As such, the course is self-contained mathematically and students are not required to have an extensive math background although some college-based coursework is recommended.

Executives Perspectives for Technical Professionals

**Total Units: 3.0**

Executive leadership is fundamentally dealing with human emotions and relationships. Technical and other professionals are challenged in this course to think from an executive leadership position. Being able to assess and lead other people requires balancing existing realities with new visions and moving people to these new visions. Issues addressing executive leadership include: Executive competencies, consulting in executive environments, re-initiating strategic moves, leadership development, succession planning, and enterprise leadership political skills. These topics are explored through lectures, case studies, and in-class discussions with industry executives.

Advanced Risk Analysis and Response Planning

**Total Units 3.0**

This course develops Mastery Level skills to allow the risk practitioner to focus on meeting Threat and Opportunity Uncertainty challenges in rapidly changing project and business environments and on developing competencies needed for the future project and portfolio success. Advance application of Quantitative Risk Analysis, Dual contingency analysis, Advanced Decision Analysis, Risk valuation, and risk data accuracy/precision are covered. Advanced contingency planning with predictive analytics will be included. Key business environments that would leverage these competencies include Information Technology, Cyber Security, Engineering, Manufacturing, Procurement and Financial Services. Focus areas of discussion include: 1. Expose risk practitioners to advanced risk response planning for threat avoidance, mitigation and transferring risk to appropriate stakeholders. Advanced response planning for Exploiting, Enhancing and Sharing Opportunities will be addressed. 2. Critical Decision Analysis incorporating risk will be covered. Key risk management capabilities and trends that affect organizations in the 21st century- cyber security, financial...
uncertainty, global management, entrepreneurship, employee competency risk, team-based management and managing risk threats and opportunities in a competitive and ethical manner will be examined. 3. Develop competency at predicting the likelihood (probability) and consequence (impact) associated with risk events. This includes determining how project outcome can be affected by known and unknown risks. Prioritization and Valuation of multiple risks; determining project risk scores to aid in portfolio analysis, strategic capital allocation and maximizing alignment to business strategies. 4. Expanded Quantitative Analysis including Asymmetrical, Symmetrical and Uniform Probabilistic Distribution scenarios. This will include expanded Monte Carlo simulations to predict risk probability of project completing according to baseline schedule, cost, and likelihood of risk occurrence. Expanded Decision Tree Analysis, annotations and calculations will be mastered. 5. Learn how to develop detailed and proactive risk triggers indicative of pending risk event occurrence. Development of secondary risk, contingency plans and fallback plans will also be included. 6. Practical methodology of Decision Analysis and Alternative Evaluations of multiple options to select course of action with most probable success and crisis avoidance. Use of Monte Carlo analysis and Decision Tree analysis will be covered to address risky decisions key leaders are faced with. Innovation-based risk analysis will be discussed for leading edge technology, cyber and software applications. 7. Current risk certification requirements, corporate application and value proposition for CISSP, PMI-RMP®, etc. will be examined. 8. Threats and Opportunities related to corporate procurement applications will be presented for application in outsourcing, contracts, joint ventures/acquisition activities, etc.

Privacy In The Digital Age

Total Units: 3.0

The reduction of the cost of storing and manipulating information has led organizations to capture increasing amounts of information about individual behavior. New trade-offs have emerged for parties involved with privacy-enhancing or intrusive technologies: individuals want to avoid the misuse of the information they pass along to others, but they also want to share enough information to achieve satisfactory interactions; organizations want to know more about the parties with which they interact, but they do not want to alienate them with policies deemed as intrusive. Is there a “sweet” spot that satisfies the interests of all parties? Is there a combination of technological solutions, economic incentives, and legal safeguards that is acceptable for the individual and beneficial to society? Privacy is a complex and multi-faceted concept. This course combines technical, economic, legal, and policy perspectives to present a holistic view of its role and value in the digital age. It begins by comparing early definitions of privacy to the current information-focused debate. It then focuses on: > Technological aspects of privacy (privacy concerns raised by new IT such as the Internet, wireless communications, and computer matching; tracking techniques and data mining; privacy enhancing technologies and anonymous protocols;) > Economic aspects (economic models of the market for privacy; financial risks caused by privacy violations; the value of customer information; > legal aspects (laissez-faire versus regulated approaches; US versus EU legal safeguards; > managerial implications (the emerging role of Chief Privacy Officers; compulsory directives and self-regulative efforts; > policy aspects (trade-offs between individual privacy rights and societal needs; The course will consist of a combination of readings, assignments, and class discussions. Assignments will include essays and technical projects.

Business and Organization Courses:

Select 9 units of the following:

Financial Principles of the Company

Total Units: 3.0

The course is designed to a) provide incoming program enrollees with little or no finance and accounting experience or background with a solid basic understanding of financial accounting concepts with an emphasis on the managerial applications of financial data, b) prepare those incoming students for the more advanced, discipline specific courses offered later in the program and, c) give the those students a grounding in financial concepts that the student can utilize as they advance to higher and more responsible leadership positions post-graduation. The course is divided into three phases. The first consists of introducing and stressing basic financial concepts, rules, and principles. The second phase consists of leveraging that basic skill set to perform and evaluate analysis in the organization. The last phase will be case study driven and will challenge the student to take the lessons of the first two phases, combine that information with already existing experience and background, and develop a business correction plan for an ailing organization.

Management and Corporate Responsibility

Total Units 1.5

Corporate leaders are expected to maximize returns to shareholders, produce compelling products and services, and create attractive work environments for their employees while at the same time adhering to the laws and expectations of the communities and countries within which they operate. This course will explore real situations in which the objectives of the corporation’s various constituencies -shareholders, employees and communities are in conflict. It will also focus on situations in which societal concerns-environmental and health, for example may be at odds with the immediate interests of important stakeholders. Through vigorous case discussions, dialogues with industry leaders and role-play simulations students will wrestle with these often ambiguous dilemmas, gain insights into
the conflicts, and develop their own approaches and decision-making frameworks for resolving these situations and those they will face during their careers.

Creative Thinking and Leading the Creative Organization

Total Units 1.5
This course is for students who want to improve their ability to develop creative and innovative solutions to business problems and to lead in a way that fosters creativity in others. In a world of rapid technological and product-market change, the ability to constantly refresh existing products through new ideas, to introduce new product or service offerings, and to continuously improve processes and practices is an indispensable element of sustained competitive advantage. Managers who have mastered the skills of creative thinking and can foster those skills in others are therefore in a position to add tremendous value to their firms and, ultimately, to society. This course is designed to help you understand and begin to master those skills. Prerequisite: MBA First-Year Core

Negotiation

Total Units 3.0
Skillful negotiation is an important aspect of management. Designed to improve a student's skills in analyzing and conducting negotiations in a variety of settings. Topics include two-party bargaining, multi-party bargaining, arbitration, and coalition formation. Prerequisite: OB 360.

Leading Change

Total Units 1.5
This course introduces the concepts of how leaders create and manage change. It focuses initially on the role of leaders in articulating a new organizational operating model for their constituents. The course focuses on leader perspectives, behaviors, and skills required to implement organizational change including the leader’s role in articulating the organization’s operating model, the roles of those involved in strategic change; how to effectively challenge current processes, building support regarding a new vision; and enabling others to act. The class approach will include presentations on leadership experiences, case studies of examples of leaders exhibiting specific behaviors, and experiential exercises. Students cannot take this course and OB 525B for credit. NOTE: This course will have a lab fee.

Information Technology and Supply Chain Management

Total Units 1.5
Recent developments and breakthroughs in information technology have radically changed the business world, offering opportunities not only for new products and services also for reengineering supply chains and improving supply chain performance. The course will study how the innovations in information technology affect the ways information flows through the supply chain, which in turns provide opportunities to better coordinate the material and financial flows. The course will review business cases in which companies use supply chain management concepts and emerging technologies to improve business processes as well as creating values. Prerequisites: OMM5700; or OMM5701 and OMM5702

Public Speaking and Presentation Skills for Technical Professionals

Total Units: 3.0
More and more, major corporations require their technical staff to have the skills to communicate to other employees and to be able to deliver compelling and succinct presentations. One of the goals of the MIS and MCSM programs is to produce great analytical thinkers. The goal of this course is to create analytical thinkers who are great communicators and can deliver clear, concise, creative and perhaps even entertaining presentations - within a technical setting. In order to bring out their more expressive side, students will learn how to overcome the fear of public speaking and truly communicate with an audience of any size; study techniques actors learn to perfect their ability to think quickly on their feet, including improvisation and storytelling; and learn the keys to great presentations both graphically and auditorially-including advanced PowerPoint® skills. Students will be assigned and graded on presentations delivered on a myriad of topics culminating in a final presentation in the student’s core area of study, which will be delivered to a panel of business professionals. To put it succinctly: this is the preparation course for your TED talk.

If you have questions, contact us at:
Washington University
School of Engineering & Applied Science
Lopata Hall, CB 1220, 1 Brookings Drive, St. Louis, MO, 63130
Phone: (314) 935-5455, Fax: (314) 935-5449
engineeringgradadmissions@wustl.edu