

# CYBERSECURITY POLICY AND RISK MANAGEMENT (CPRM)

<https://online.unh.edu/cprm>

## Overview

### Degree Offered: M.S.

*This program is offered online.*

The demand for master's-level cybersecurity and risk management professionals is on the rise in the U.S. and globally. Guided by full-time faculty, practicing experts and senior executives, the CPRM degree fosters the strategic thinking, policy development and risk management skills that will set you apart in the high-demand cybersecurity field. Our highly interdisciplinary program is designed for students and working professionals with a variety of backgrounds – business, healthcare, IT, finance, homeland security, law and more – so you do not need an undergraduate degree in a technical field to be successful.

## Programs

- [Cybersecurity Policy and Risk Management \(M.S.\)](#)

## Courses

### Cybersecurity Policy and Risk Management (CPRM)

#### CPRM 810 - Foundations of Cybersecurity Policy

**Credits: 3**

Examine the societal and organizational impacts of cybersecurity policy in our interconnected world that is increasingly dependent on advanced technologies and systems for communications and control. Explore the components of information systems and control systems and review the history and development of cybersecurity. Gain an appreciation of policy as one tool for managing risk, and start to consider the challenges of cybersecurity policy-making.

#### CPRM 820 - Policy Development and Communication

**Credits: 3**

Discover the fundamental concepts and practices for developing and drafting organizational policy, including related documents to support implementation. Explore how to communicate policies to internal and external audiences (in both written and oral communications). Learn how to incorporate organizational priorities and mandates into managerial policies. Case studies are primarily based in security studies, but other professional fields are welcomed.

#### CPRM 830 - Security Measures I

**Credits: 3**

This course introduces common technological and organizational measures for cybersecurity, with a focus on protection concepts. Students assess the organizational impacts of security measures, and explore how best practices, standards, and organizational policy can help manage such measures. Topics include identity management, authentication, access control, data and system security and availability, encryption, integrity mechanisms, system maintenance, and continuity of operations. Note that we do not focus on how to technically implement these security systems. Prereq: CPRM 810.

#### CPRM 840 - Cybersecurity Standards, Regulations, and Laws

**Credits: 3**

We survey laws, regulations, and standards for cybersecurity in the United States, including "soft law" and self-regulation. Topics include the pros and cons of regulatory solutions and market solutions; the different approach to data protection regulation in the European Union; and cybersecurity concerns and regulatory authorities in various U.S. industries and sectors. Students become familiar with key standards bodies involved in cybersecurity, and explore organizational processes for remaining current with industry best practices.

#### CPRM 850 - Security Measures II

**Credits: 3**

This course continues surveying common technological and organizational measures for cybersecurity, with a focus on detection and organizational relationships. Topics include auditing and log records; monitoring and testing for threat detection; vulnerability scans; and the security of external services (e.g., cloud providers) and supply chains. We do not focus on how to technically implement these measures. Students assess organizational impacts and explore how best practices and standards can help manage such measures. Pre- or Co-req: CPRM 830.

#### CPRM 860 - Incident Response and Investigation

**Credits: 3**

This course fosters cybersecurity incident response and investigative knowledge, from both the organizational and system perspective. Material includes laws, standards, codes of behavior and best practices for incident response, including the management of relationships (e.g., regulators, clients, vendors). Case studies are presented and discussed in light of organizational resource limitations, legal mandates, and jurisdictional boundaries. Prereq: CPRM 830. Pre- or Co-req: CPRM 850.

#### CPRM 870 - Cybersecurity Risk Management

**Credits: 3**

This course establishes foundations for addressing cybersecurity as a risk management concept and process, and as a component of overall risk management within an organization. Students will become familiar with theories of risk and methods of risk management, as well as frameworks/models for applying these theories and methods to cybersecurity. Prereq: CPRM 840 and CPRM 860.

#### CPRM 879 - Research Methods

**Credits: 3**

This course helps students understand and apply research methods and planning processes for accomplishing a graduate-level thesis. Students will survey a variety of research approaches and select those most applicable to each student's research project. Within those approaches, students will explore planning and management skills as well as academic components (e.g., literature review, critical analyses) in preparation for applying these skills and knowledge in a Capstone: Thesis Option course.

**Equivalent(s):** EDUC 882

**CPRM 880 - Cybersecurity Metrics and Evaluation**

**Credits:** 3

This course provides an overview of analytical techniques for the documentation and evaluation of cybersecurity metrics, and the incorporation of such assessments in organizational risk management. Students will become familiar with methods for cybersecurity evaluation and the translational impacts to function and mission success of an organization (business, public administration, homeland security, etc.); as well as processes for security measurements, comparisons, and reassessments for purposes of risk management. Pre- or Co-req: CPRM 870.

**CPRM 890 - Organizations, Change Management, and Leadership**

**Credits:** 3

This course examines both private and public institutions as systems whose effectiveness depends on how an organization adapts to opportunities, threats, and demands (external and internal). Students explore the design and leadership of ethical and socially responsible organizations. In course examples and exercises, students will apply this knowledge to their respective research interests (e.g., cybersecurity, analytics, criminal justice, public health, etc.).

**CPRM 895 - Independent Study**

**Credits:** 3

This course allows students to complete a graduate-level course in Cybersecurity Policy and Risk Management program via independent study if they were unable to take the course when it was offered. This course can substitute for a required course.

**Repeat Rule:** May be repeated for a maximum of 6 credits.

**CPRM 898 - Capstone: Non-Thesis Option**

**Credits:** 3

This capstone integrates all disciplines and competencies that have been learned in this degree program, plus the student's past experiences, areas of specialization, and professional goals, into a single work-based project, internship experience, or other appropriate activity. In consultation with an advisor, each student develops a project plan, establishes goals and objectives; collects and analyzes information; and prepares and delivers a final project agreed upon by the student and advisor. Prereq: CPRM 720 / CPRM 820 and CPRM 880. Pre- or Co-req: CPRM 790 / CPRM 890.

**CPRM 899 - Capstone: Thesis Option**

**Credits:** 3

Students synthesize, evaluate, and integrate past experiences, new research, and the cross-disciplinary knowledge constructed during this degree program to create a publishable quality, graduate-level thesis. In continuation with an advisor, each student develops a project plan; establishes goals and objectives; collects and analyzes information; and prepares and delivers a final product agreed upon by the student and advisor. Prereq: CPRM 720 / CPRM 820, CPRM 870 & (CPRM 879 or EDUC 882). Pre- or Co-req: CPRM 790 / CPRM 890.

**Repeat Rule:** May be repeated for a maximum of 6 credits.

## Faculty

[https://online.unh.edu/program/ms/cybersecurity-policy-risk-management#collapse\\_314](https://online.unh.edu/program/ms/cybersecurity-policy-risk-management#collapse_314)