



# WHY EDUCATION IN THE LAW AND POLICY OF CYBERSECURITY IS A MUST

*Markus Rauschecker, J.D.*

*Cybersecurity Program Manager, University of Maryland Center for Health and Homeland Security  
Adjunct Faculty, University of Maryland Francis King Carey School of Law*

Cybersecurity is no longer within the sole purview of information technologists – its increased prominence has made it an interdisciplinary problem. Solutions require involvement from many stakeholders. Organizational leaders, including CEOs, financial and privacy officers, lawyers, human resources specialists, policymakers, and many others in both the public and private sectors, must all have a basic understanding of cybersecurity issues if the threats to national security, the economy, and privacy are to be mitigated.

Many cybersecurity issues fall within a legal and policy context. Fundamentally, organizations must know how to comply with and implement new cybersecurity laws, regulations, and standards, and to develop plans and policies in order to prepare for, respond to, and recover from a cyber incident. There are countless non-technical issues that must be addressed. For example, how can government and the private sector share cyber threat information? Should a company adopt the NIST Cybersecurity Framework? To what extent can an organization monitor the internet traffic of employees to keep its networks safe? What notification requirements are there for businesses that have suffered a cyber-attack? Can or should a victim “hack back” against an attacker? These and many other questions carry complex legal and policy ramifications that must be considered before any action is taken.

Government and industry are continually searching for qualified professionals to help tackle the most complex legal and policy questions in cybersecurity. Whether it is drafting new laws and regulations, developing plans and policies, or providing legal advice to clients, a grasp of cybersecurity law and policy is critical. At every stage, professionals of all kinds need to not only understand the basic cybersecurity issues which confront them, but must be able to think critically about the consequences of any decision they might make.

Recognizing this demand, new students and current professionals are seeking more opportunities to learn and develop their expertise in cybersecurity. As employers and job applicants can attest, the value of a degree or credential is key to demonstrating competence in the subject matter.

With the presence of government agencies such as the National Security Agency (NSA), U.S. Cyber Command, the National Institute of Standards and Technology (NIST), the National Cybersecurity Center of Excellence, as well as hundreds of private sector firms, the state of Maryland is an epicenter for cybersecurity. The area's high concentration of cybersecurity demand also creates a need for providing multiple degree programs focused on the law and policy of cybersecurity, tailored to both lawyers and non-lawyers.

To that end, individuals pursuing a traditional JD degree can enhance their legal knowledge through cybersecurity law and policy courses as well as specialized topics such as cybercrime and privacy. Individuals who already have a law degree and wish to enhance their understanding of cybersecurity have the option of studying cybersecurity as part of a Master of Laws (LL.M.) degree.

Lawyers are not the only professionals with a need to understand the legal and policy dimensions in cybersecurity. Those currently in the cybersecurity field increasingly face a complex web of federal and state laws and regulations. These individuals do not necessarily require a general law degree for their purposes, but can nevertheless benefit from acquiring legal and regulatory knowledge to help their organizations. New degree programs, such as a Master of Science in Law (M.S.L.), exist for professionals who want to know more about the ways that laws and regulations intersect with their fields of expertise.

Of course, academic instruction alone is not sufficient to adequately prepare cybersecurity professionals for the legal and regulatory challenges they face. Classroom instruction must be paired with real-world opportunities for students to apply the concepts they learn in the classroom.

## Go further with cybersecurity at Maryland Carey Law

Cybersecurity needs professionals with academic and practical experience at the intersections of law, policy, science, and technology.

- **J.D. and Master of Science in Law** for non-lawyers
- **LL.M.** for U.S. and international lawyers


Learn from practicing professionals at the **University of Maryland Center for Health and Homeland Security.**



[www.law.umaryland.edu/cybersecurity](http://www.law.umaryland.edu/cybersecurity)  
[www.mdchhs.com](http://www.mdchhs.com)



Internships allow students to work on plans or policies, think critically about problems that organizations face, and be involved with hands-on projects. A combination of rigorous academic coursework and practical experience will prepare students for whatever aspect of the cybersecurity field they choose to enter.

The cybersecurity problem requires an interdisciplinary approach that includes legal and policy expertise. Current and future cybersecurity professionals must have the educational opportunities to acquire the necessary foundational skills to answer these questions. 

### About the Author:



**Markus Rauschecker, J.D.**, is the Cybersecurity Program Manager for the University of Maryland Center for Health and Homeland Security. He is also an adjunct faculty member at the University of Maryland Francis King Carey School of Law.

