Winter 15

Cybersecurity Foundations:

An Interdisciplinary Introduction

Pedagogy

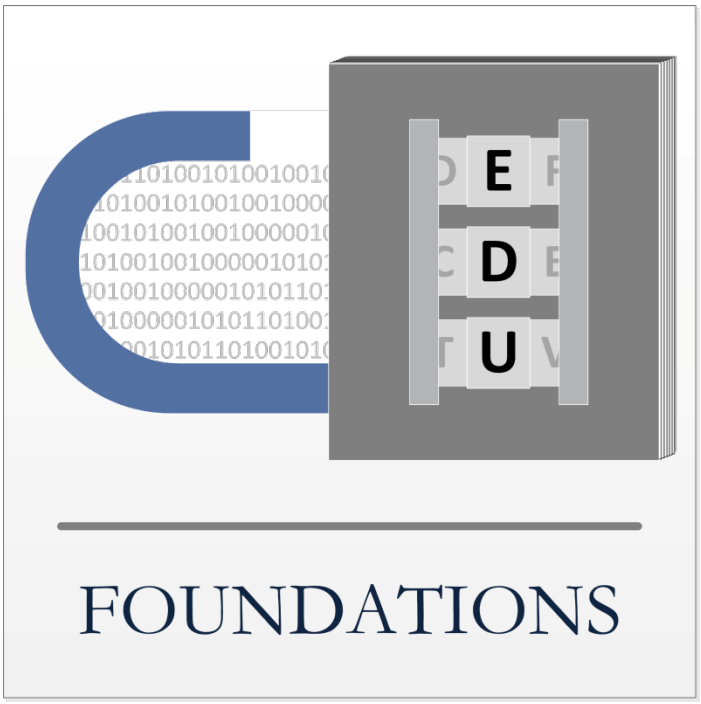

Table of Contents

Executive Summary

The modern world is characterized by increasing levels of technological sophistication, and cybersecurity has emerged as a defining challenge for the global community. In order to confront threats from cyberspace, the world will need leaders and policymakers who possess a proficiency in cybersecurity fundamentals and an understanding of the challenges facing the field.

If these individuals are to craft effective solutions to cybersecurity challenges, they will need more than just an understanding of computer science and engineering. Certainly, a grasp of these topics is important – however, cybersecurity is a truly interdisciplinary field, drawing upon subject areas ranging from risk management to US law and policy.

Our textbook is designed with cybersecurity's interdisciplinary nature in mind. Over the course of seven chapters, students will become familiar with the numerous threads that complete the cybersecurity tapestry. This interdisciplinary approach will encourage students to make connections between seemingly-disparate academic disciplines, and to appreciate the "big picture" of cybersecurity, rather than solely focusing on a narrow aspect of the field. By the end of this course, each student will understand how his or her unique skill set can be applied to cybersecurity, as well as how students with other interests can contribute.

This pedagogy includes a suggested class structure for instructors to follow in teaching this course. This structure is based on a combination of traditional lectures and interactive discussion. The former is useful for teaching such "hard" subjects as quantitative risk assessment or earned value management, while the latter is better suited for instruction on "soft" subjects, such as how different components of the US government interact in the development of cyber-legislation. Regardless of which method teachers choose to utilize, however, they should bear in mind that this course aims to impart two kinds of knowledge to students– "Textbook Fundamentals" and "Cybersecurity Applications." "Textbook Fundamentals" refer to concepts and lessons explicitly explained in the textbook, such as the various steps of the risk management process. "Cybersecurity Applications," on the other hand, may be mentioned or alluded to in the textbook, but require further explanation from the instructor. In so elaborating, we recommend that the instructor draw from this textbook's Academic Package, which includes supplemental readings and case studies that instructors can use to illuminate topics that the textbook does not fully explain.

Ultimately, however, it is important to bear in mind that this pedagogy is not a concrete blueprint – different classes will have different needs, and so it is up to individual instructors to determine the needs of their class, and construct lessons that will serve their students most effectively.

The interdisciplinary approach is not without its challenges – these issues range from a perceived lack of continuity between the different disciplines explored in the class, to difficulties in crafting effective modes of assessments for students with diverse academic

backgrounds. Nonetheless, we believe that achieving an understanding of the cybersecurity field *demands* an interdisciplinary approach. Only by developing an in-depth grasp of cybersecurity's many component parts can the world's future leaders develop the skills needed to craft effective solutions to the most pressing cybersecurity challenges.

I. Introduction: Academia Has a Key Role in Teaching Cybersecurity

As an academic field, cybersecurity is ripe for development and new contributions, having evolved from a relatively obscure concentration into a highly complex and interdisciplinary subject of research, study, and practice.

Cybersecurity's growth as an academic field corresponds with its emergence as a dynamic and growing industry. The United States has long served as a central hub of this industry, producing reams of policy documents, laws, and regulations on cybersecurity-related matters. Scholars trace the root of all cybersecurity theory and practice to the U.S. government's interest in securing critical information and infrastructure at the dawn of the Cold War. At that time, nearly all of the computers in the United States were located in the offices of the federal government, whose primary concern was to protect these newly developed mainframe computers, as well as the limited but sensitive data stored on them.

The world's cyber capabilities have come a long way since the days of mainframes. Today, digital data is stored and transferred far beyond the walls of government offices, and has become the foundation of business and personal transactions around the modern world. Indeed, the basic security of our society depends on the security of digital information, as all businesses, from grocery stores to investment banks, have developed a strong reliance upon IT tools. The public benefit of these new cyber tools has been incalculable, but they are not without their vulnerabilities – vulnerabilities that have, in turn, led to the emergence of revolutionary new threats.

In the cyber age, governments and other institutions confront a threat environment that is markedly different from that of decades past. Equipped with modern technologies, one person with limited resources can damage a huge organization on the other side of the world easily, cheaply, and quickly. For hundreds of years, large superpowers could easily handle small attackers by way of force. This is no longer true in the modern world, where threats can strike over long distances with unprecedented speed and impact.

As businesses and individuals have deepened their dependence upon information technology systems, the U.S. federal government has continued to increase its role in establishing cyber policies, laws, and regulations. While proactive, this approach has raised significant concerns about the appropriate balance between national security and privacy in the cyber realm.

To address this multitude of complex problems, the world will need a cadre of professionals from a wide range of academic and professional backgrounds. Recognizing this need, we believe it is important to begin teaching the fundamentals of cybersecurity as an introductory course to college students. Not every student who takes this course will ultimately concentrate in computer science or other "traditional" cybersecurity-related fields, but we feel that the nature of the modern world demands that every citizen understand the global significance and interdisciplinary application of cybersecurity.

II. Cybersecurity Demands Introductory Instruction

Students might assume that a course titled "Cybersecurity Foundations" is only for engineering and computer science majors. In reality, most cybersecurity problems require solutions that draw from a range of academic disciplines. Many of the issues involved in achieving cybersecurity goals have nothing to do with computer science or engineering, but require skill sets developed in the humanities, in business classes, in political science studies, and in a variety of other academic fields.

Even those who enjoy the computer science and engineering-based approaches to solving cyber problems will need to understand these other aspects of cybersecurity in order to fully appreciate and comprehend the field. Our interdisciplinary cybersecurity course will allow all students to consider perspectives on the topic from multiple vantage points, and to recognize the fundamental importance of the following areas:

A. Risk Management

Risk management is the foundation of all cybersecurity theory and practice. It is critical for future cybersecurity professionals to understand both the qualitative and quantitative aspects of managing risk. Our course walks students through the formalized process of risk management for organizations and introduces newcomers to the complexity of managing both cyber and physical risk.

B. Computer Science and Engineering

Computer science and engineering jargon constitutes a significant portion of industry language in cybersecurity, and computer science and engineering specialists create the technical tools to protect critical information and infrastructure. In order for anyone to truly comprehend the cybersecurity field, they must have a basic understanding of the technical language and skills that engineers and computer scientists use.

C. Law and Policy

The U.S. federal government is the world's leading actor in the field of cybersecurity. It is critical for future cyber professionals to recognize the broad influence of U.S. federal cybersecurity policy and the ways in which the U.S. federal government involves the private sector in its cybersecurity policymaking process.

D. The Private Sector

The private sector plays an increasingly active role in U.S. national cybersecurity law and policy. Moreover, all organizations, even those with no intention of working in coordination with the federal government, must have an understanding of the cybersecurity systems needed to protect their most critical assets and insulate them from legal action in the event of a cyber attack.

E. Management

It is essential for students to understand that management, not technology, dictates the success or failure of most cybersecurity programs and operations. Only with the guidance of skilled managers can organizations carry out effective programs to secure critical information, networks, and systems. Managers play a crucial role in coordinating cybersecurity professionals across disciplines and overseeing the "big picture" in organizations and government.

F. Research and Methods

Many of cybersecurity's most important documents and informational sources are not easily accessible through popular Internet search engines. Therefore, cybersecurity professionals must possess the ability to conduct more advanced and in-depth research, which will, in turn, allow them to access documentation and legislation on cybersecurity topics from each of the three branches of the US government, as well as from other external sources.

III. The Benefits of Teaching Cybersecurity as an Interdisciplinary Topic

Interdisciplinary courses approach a general topic by drawing upon a variety of disciplines and perspectives. We recommend this approach to instructors teaching the fundamentals of cybersecurity. Achieving a true grasp of cybersecurity issues requires one to draw upon knowledge and skills rooted in a range of academic fields. Our course is designed with this reality in mind, as we firmly believe that future cyber professionals must have an understanding of each of the disciplines discussed above in order to create and apply solutions to cybersecurity problems.

Interdisciplinary courses challenge students to actively draw connections between seemingly-disparate course materials, and to understand the "big picture" rather than to specialize immediately in one aspect of the field. Moreover, interdisciplinary courses encourage students to appreciate how their particular skill sets and interests apply to a broader issue. At the end of this class, each student will recognize how their interests and areas of expertise apply to cybersecurity: business majors will learn how cybersecurity policy affects large corporations; history majors will be able to use their skills in analyzing historical documents and trends to examine important cybersecurity statements and policies, and engineers will be able to apply their math and science backgrounds to cybersecurity and risk management tools. At the end of this course, students will also be

able to appreciate the skill sets of others and to understand how these myriad skill sets can be combined to create interdisciplinary solutions to cybersecurity problems.

Teaching cybersecurity in an interdisciplinary manner will give students an accurate introduction to the complexities of the cybersecurity field and provide an opportunity for those with a range of backgrounds, skills, and interests to come together in one classroom to explore this revolutionary topic.

IV. Suggested Cybersecurity Class Structure

Almost all interdisciplinary courses include a mixture of traditional lectures and interactive discussion. Each class will involve a range of students with different skill levels and different levels of both intrinsic and extrinsic motivation. Accordingly, instructors must recognize the diverse academic backgrounds of their students and structure class time in a manner geared towards meeting the specific needs of each class. Some classes will need more time dedicated to covering technical material, while others may need more time to discuss policy-related content. Some classes will need more grounding in the structure of the U.S. federal government, while others may require more of a focus on management strategies. It is advised that all instructors use the class schedule on the syllabus only as a *guide*, and adjust their own course according to the needs of the students.

This course requires a fair amount of "hard-learning" when approaching subjects such as quantitative risk assessment or earned value management. These kinds of subjects require that a portion of class time be devoted to traditional lecturing. However, "softer" subjects, such as the influence of government in creating cybersecurity legislation, or the extent to which private sector companies must leverage resources to protect customer information, requires more discussion-based learning. How professors choose to structure their class time will depend on their professional judgment, as well as consideration of their students' needs and the relative difficulty of the day's course content.

Regardless of whether class time is structured as a discussion, a lecture, or a mix of both styles, each string of classes devoted to a particular chapter should always teach two types of information – "Textbook Fundamentals" and "Cybersecurity Applications".

"Textbook Fundamentals" consist of the lessons and objectives explained in the textbook, such as the risk management process or the federal government's use of the program management framework.

"Cybersecurity Applications" are the topics that may be mentioned in the book, but require further elaboration from the instructor. The instructor may make use of supplemental readings and case studies as a trajectory for Cybersecurity Applications. Examples and suggestions can be found in the Lesson Plan portion of the academic package.

V. Common Issues Unique to Interdisciplinary and Cybersecurity Courses

Although interdisciplinary courses provide a range of benefits to students, covering every topic in equal depth may prove challenging to instructors. Another problem to overcome may be a lack of continuity and connectivity between the disciplines explored in the class. An interdisciplinary cybersecurity course is even more susceptible to this problem because of the wide range of academic fields that it draws upon. In order to prevent this cybersecurity course from appearing to be a randomly configured assortment of lessons, we advise instructors to follow a few recommended processes.

First, all instructors should develop a logical order to the course. This will ensure that students understand the course's progression from lesson to lesson and the reason why certain topics must be covered before others. The course syllabus lists a logical schedule of lessons from the beginning to the end of the course. Instructors may adjust the schedule in consideration of their specific audience.

In addition to developing a logical order for the course, the instructor should always stress the interdisciplinary nature of both the course and cybersecurity as a field. Always consider questions from an interdisciplinary perspective. Instructors should encourage students to explicitly draw connections between the topics covered in the course, and each lesson should relate back to earlier material in discussions, lectures, and assessments. Instructors should also encourage students to relate the content of each individual lesson to the broader topic of cybersecurity as much as possible. In this way, the "big picture" will illuminate more specialized topics at each step in the course, and vice-versa.

Another concern frequently raised by instructors of interdisciplinary courses is that their students will suffer from "disciplinary egocentrism."[1] This is the idea that students will only concentrate on the course content that connects to their respective academic concentrations. Within our cybersecurity course, this means that computer science students will only focus on the computer science section, or that political science majors will focus solely on the law and policy content.

To ensure that students recognize the significance of every topic covered in this interdisciplinary course, it is important for instructors to give assessments and assignments that encourage students to be proficient in all facets of the cybersecurity field. This approach requires that instructors give equal weight to all subjects – a difficult task for educators with deep connections to one discipline.

Assessments can also be a challenge for instructors of interdisciplinary courses. Students from different academic backgrounds will be accustomed to different assessment methods. While many humanities majors may feel more comfortable writing papers, most math students will be used to taking calculation-based exams and completing problem sets. Providing a variety of assessment opportunities and encouraging students to stretch

[1] "Disciplinary egocentrism," http://scholar.lib.vt.edu/theses/available/etd-05092008-110413/unrestricted/Richter_Thesis.pdf

beyond their comfort zones will benefit all involved. In group projects, students from diverse academic backgrounds can work together to share their knowledge and learn from each other's unique problem-solving approaches.

Additionally, educators should promote in-class discussions that draw from a variety of disciplines. For instance, when discussing the role of government in implementing cybersecurity mandates, make sure to consider business perspectives and the technological and management constraints associated with various policies. Promoting interdisciplinary discussions will help students develop their critical reasoning skills and give them a realistic picture the variety of challenges associated with most cybersecurity issues.

The guides and assessments found in the syllabus and in the academic package address some of these pedagogic challenges. And yet, while it is important to ensure that students understand all of the disciplines that comprise cybersecurity, this does not mean that students shouldn't be able to look deeply into the subjects that they enjoy. Students should be challenged to apply what they know to projects and discussions, and to explore areas of particular interest.

VI. Conclusion

Now, more than ever, as threats from cyberspace continue to grow in quantity and sophistication, it is crucial that students possess a basic understanding of cybersecurity issues. It is our hope that this teaching note provides a set of guidelines for those with experience in cybersecurity to teach an introductory cybersecurity course to college-aged students.