MaCuDE
Management Curriculum for the Digital Era

A PRELIMINARY SURVEY OF BUSINESS SCHOOL CURRICULA IN THE AREAS OF CYBER SECURITY / CYBER PRIVACY

Phase I Report of the MaCuDE project[1]

Management Curriculum for the Digital Era
Undertaken at the Request of Dean Prastacos, Stevens Institute of Technology, Head of the MACUDE Project

Task Force on Cyber Security / Cyber Privacy

Eric K. Clemons
Jessy Syed
Matthew Weiss

The Wharton School, University of Pennsylvania

13 July 2020
Revised 20 November 2020

[1] The MaCuDE project is sponsored by AACSB International and led by Stevens Institute of Technology.

A PRELIMINARY SURVEY OF BUSINESS SCHOOL CURRICULA IN THE AREAS OF CYBER SECURITY / CYBER PRIVACY

ABSTRACT

We were charged with developing proposed additions to both the undergraduate business curriculum and the MBA curriculum that would prepare graduates to deal with the challenges their organizations will face from Cyber Security and Cyber Privacy attacks. Since there is no equivalent to GAAPs in the area of preparing for Cyber attacks, we started **Phase 1** by reviewing the existing curricula in the top business schools and the top computer science departments, both in the US and abroad. We prepared a list of critical topics and created a survey for our MACUDE partners, to see what other faculty members believed should be taught.

In **Phase 2** we plan to prepare a ***Recruiter Survey*** to explore what knowledge employers want their new hires to possess about Cyber Privacy and Cyber Security, now and in the future. We added a subject area to our study during Phase 2, based on recent litigation about Cyber breaches and the effect on share price. The survey explores skills employers expect in entry level employees in each of several areas within the firm, and will be administered to executives in a range of functional areas and in firms across a range of sizes and industry classifications.

Phase 3 will begin with a small pre-test of the Recruiter Survey and will then administer the survey to our full sample population and will analyze and summarize the findings.

INTRODUCTION

The topic of Cyber Security and Cyber Privacy is relatively new to the business school curriculum. Unlike more established disciplines like accounting or finance, there is no generally accepted standard or agreement on what should be covered. Accounting has GAAP. Finance has CAPM and market microstructure. But the field of Cyber Security and Cyber Privacy has only recently gained managerial significance. We therefore started with a clean slate. The first thing we needed to do was to determine what is and is not currently taught in the premier academic institutions globally. Moreover, since the subject is under-represented in business schools, we began by surveying top computer science departments as well as the top business schools. This enabled us to understand what is currently taught, and to identify some gaps based on the topics we have observed covered in technology-focused business conferences. Finally, we created a survey that will allow us to assess the current view of Cyber Privacy and Cyber Security course offerings among our colleagues at business schools in the US and abroad. We assess what is currently taught. And we assess beliefs about what *should* be taught, what *should* be taught in which courses, and what *should* be taught to which groups of students.

Our **Phase One Report** started with a review of the top ten computer science departments in the US and the top two abroad and the top ten business schools in the US and the two two abroad. We surveyed all courses in relevant departments to determine what these schools taught in the areas of Cyber Security and Cyber Privacy. Our Report is divided into four sections. Section 1 lists the schools we reviewed and lists all of the courses we found that covered topics in Cyber Security and Cyber Privacy (CSCP), whether as the subject of the entire course, or as a topic in other courses. Section 2 contains a list of all topics covered. Section 3 summarizes the implications of Sections 1 and 2 and provides a structured list of all topics that we believe should be covered, including but not limited to those topics listed in Section 2. That is, where appropriate we added topics that we believed were newly emerging as significant. Section 4 presents our survey instrument.

All CSCP Task Force members will be given the opportunity to comment on the Survey before it is distributed.

SECTION 1

Section 1 reviews what we learned about CSCP course offerings in some of the top US and international business schools. We surveyed all courses in relevant departments to determine what these schools taught in the areas of Cyber Security and Cyber Privacy.

Schools included in this preliminary report

Computer Science

→ Top 10 US Schools:
Carnegie Mellon University, MIT, Stanford University, University of California Berkeley, University of Illinois Urbana Champaign, Cornell University, University of Washington, Georgia Institute of Technology, Princeton University, University of Michigan Ann Arbor

→ Top 2 International Schools:
University of Oxford (UK), ETH Zurich (Switzerland)

Business - Undergraduate

→ Top 10 US Schools:
University of Pennsylvania, MIT, University of California Berkeley, University of Michigan Ann Arbor, Carnegie Mellon University, University of Texas Austin, University of North Carolina Chapel Hill, University of Virginia, Cornell University, University of Notre Dame

→ Top 2 International Schools:
London School of Economics, University of Oxford

Business - MBA

→ Top 10 US Schools:
University of Pennsylvania*, Stanford University, Northwestern University, University of Chicago, MIT*, Harvard University, University of California Berkeley*, Columbia University, Yale University, New York University
* denotes repeat from business undergrad

→ Top 2 International Schools:
Insead (France/Singapore), London Business School (UK)

Key Takeaways

Computer Science

1. There is no set standard for CS curriculum related to privacy and security. There is a large variation in courses offered even among the nation's top programs.
    a. However, there are visible tiers of programming based on the quantity of privacy and security courses offered, as well as if the courses are dedicated to privacy and security, or if it is included as a subtopic.
        i. Top Tier: Carnegie Mellon, Georgia Institute of Technology
        ii. Middle Tier: MIT, Stanford, University of California Berkeley, Cornell, ETH Zurich
        iii. Bottom Tier: University of Illinois Urbana-Champaign, Washington University, Princeton University, University of Michigan Ann Arbor, University of Oxford
2. Two schools, University of California Berkeley and Georgia Institute of Technology, offer Masters of Cybersecurity
3. Privacy and security are much more likely to be a subtopic in a broader CS course than to have a course dedicated solely to it.
4. Almost every school offered a cryptography course, making it one common denominator in an otherwise varied curriculum.
5. Many schools offered small group seminars and practicums on topics in privacy and security.

Business - Undergraduate

1. There is little to no undergraduate business curriculum that mentions privacy and security.
    a. Top Tier: includes at least one course specifically on the topic(s) of privacy and/or security
        i. University of Pennsylvania, University of Virginia, University of Notre Dame
    b. Middle Tier: privacy and security is a subtopic in at least one course
        i. University of Michigan Ann Arbor, Carnegie Mellon University, Cornell University, London School of Economics
    c. Bottom Tier: there is no mention of privacy and security at all
        i. MIT, University of California Berkeley, University of Texas Austin, University of North Carolina Chapel Hill, University of Oxford
2. Privacy and security is much more likely to be a subtopic in a broader course than to have a course dedicated solely to it.
3. When privacy and security is mentioned, it is most often in a legal or policy context.
4. There was no explicit mention of fiduciary responsibility in any curriculum.

Business - MBA

1. There is little to no MBA curriculum that mentions privacy and security.
    a. Top Tier: includes at least one course specifically on the topic(s) of privacy and/or security
        i. Northwestern University, New York University
    b. Middle Tier: privacy and security is a subtopic in at least one course
        i. University of Pennsylvania, Stanford University, University of Chicago, MIT, Columbia University, Yale University
    c. Bottom Tier: there is no mention of privacy and security at all
        i. Harvard University, University of California Berkeley, Insead, London School of Business
2. Privacy and security is much more likely to be a subtopic in a broader course than to have a course dedicated solely to it.
3. When privacy and security is mentioned, it is most often in the cryptocurrency or law and policy context.
4. There was no explicit mention of fiduciary responsibility in any curriculum.

Research Findings

Key:

- Highlighted courses indicate the main focus of the course is privacy and security
- When privacy and security is a subtopic of a course, it is **bolded**

Computer Science

Carnegie Mellon University

→ Offers a comprehensive list of classes on privacy and security, making it one of the most in-depth CS curriculums on the topic. The school also has the Information Networking Institute, a department that more specifically houses classes on the topic.

https://enr-apps.as.cmu.edu/open/SOC/SOCServlet/search

a. 15316 Software Foundations of Security and Privacy
    i. "Security and privacy issues in computer systems continue to be a pervasive issue in technology and society. Understanding the security and privacy needs of software and being able to rigorously demonstrate that those needs are met, is key to eliminating vulnerabilities that cause these issues. Students who take this course will learn the principles needed to make these assurances about software, and some of the key strategies used to make sure that they are correctly

implemented in practice. Topics include: policy models and mechanisms for confidentiality, integrity, and availability, language-based techniques for detecting and preventing security threats, mechanisms for enforcing privacy guarantees, and the interaction between software and underlying systems that can give rise to practical security threats. Students will also gain experience applying many of these techniques to write code that is secure by construction."

b. 15330 Introduction to Computer Security
   i. Security is becoming one of the core requirements in the design of critical systems. This course will introduce students to the intro-level fundamental knowledge of computer security and applied cryptography. Students will learn the basic concepts in computer security including software vulnerability analysis and defense, networking and wireless security, and applied cryptography. Students will also learn the fundamental methodology for how to design and analyze security critical systems.
   ii. https://www.andrew.cmu.edu/course/18-330/

c. 15356 Introduction to Cryptography
   i. "This course is aimed as an introduction to modern cryptography...We will cover **formal definitions of security**, as well as constructions based on well-established assumptions like factoring."
   ii. http://www.cs.cmu.edu/~goyal/15356/

d. 15441 Networking and the Internet
   i. "... Topics to be covered include: network architecture, routing, congestion/flow/error control, naming and addressing, peer-to-peer and the web, internetworking, and **network security**."

e. 14735 Secure Coding
   i. "...The course covers secure software development tools and processes while focusing on **low-level technical security issues intrinsic to the C and C++ programming languages** and associated libraries. Proficiency in C and C++ are required."

f. 14741 Introduction to Information Security
   i. The growing importance of information systems, and their use to support safety-critical applications, has made information security a central issue for modern systems. The course introduces the technical and policy foundations of information security. The main objective of the course is to enable students to reason about information systems from a security engineering perspective. Topics covered in the course include elementary cryptography; access control; common software vulnerabilities; common network vulnerabilities; digital rights management; policy and export control law; privacy; management and assurance; and special topics in information security.

g. 14809 Introduction to Cyber Intelligence
   i. Cyber intelligence; a phrase often used, but interpreted by government agencies, private companies, and the general public in many different ways. For the purpose of this course, cyber intelligence is the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities to offer courses of action that enhance decision making. Students will explore a different aspect of the definition each week to develop an analytic framework capable of discerning the interdependencies of and external influences on cyber intelligence, as it relates to an organization's environment, data gathering, functional analysis, strategic analysis, and decision maker. The framework will demonstrate how traditional intelligence practices and emerging technologies influence cyber intelligence; empowering students to assess the likelihood of cyber threat actors executing attacks, the impact attacks have on an

organizations business, and the risk threats pose because of an organization's known vulnerabilities.

h. 14821 Special Topics
    i. In this course, students learn about US and international laws they must comply with while working as cyber operations professionals. Learn how to stay on the right side of the law Starting with international law, we cover the formation of the United Nations, plus the Hague and Geneva Conventions. We study sources of US law including the three branches of government, the Constitution, and **relevant case law in privacy**. We address statutory laws that apply generally to computer professionals like the Computer Fraud and Abuse act and other Title 18 crimes, as well as laws specific to military applications like Titles 10 and 50. Woven throughout, we consider ethics and social responsibility, then conclude with specific issues around ethical hacking.

i. 14829 Mobile and IoT Security
    i. For many people, mobile and embedded devices have become an essential part of life and work. As such devices represent many and varied combinations of technologies, they have unique security and privacy issues that potentially impact users, developers, service providers, manufacturers, and regulators. This course will focus on various aspects of security and privacy that are faced by mobile and Internet of Things devices, including aspects of wireless communication and networking, mobile computing, data analytics, security, and privacy. The course will include studies of security and privacy aspects of networking (including telecom, enterprise, personal, etc.), applications, and data analytics as relevant to mobile and embedded/IoT devices. One of the main goals of the course is to improve knowledge and awareness of security issues faced by mobile application developers, embedded system builders, and smart system designers. Material will cover standards, best practices, and research challenges in both deployed and emerging systems. Topics of study include (but are not limited to) telecom protocols and vulnerabilities; mobile/IoT network security; security and privacy in edge computing; mobile application security; and location and activity privacy.
    ii. http://wnss.sv.cmu.edu/teaching/14829/f13/

j. 14850 INSuRE Cybersecurity Research
    i. This course engages students in real-world cybersecurity and information systems security problems of interest to government organizations and industry partners. Students will learn how to apply research techniques, think clearly about problems and constraints, formulate and analyze potential solutions, evaluate solutions through simulation and experimentation, and communicate their results effectively. Working in small groups under the mentorship of technical clients from government and industry, teams of students will formulate, carry out, and present original research on current cybersecurity/information assurance problems of interest. Project topics come from lists supplied by government and industry partners.

k. 95444 Cybersecurity Policy and Governance I
    i. The ability to secure information within a modern enterprise is a growing challenge. Threats to information security are global, persistent, and increasingly sophisticated. Long gone are the days when managers could hope to secure the enterprise through ad hoc means. Effective information security at the enterprise level requires participation, planning, and practice. Fortunately, the information security community has developed a variety of resources, methods, and best practices to help modern enterprises address the challenge. However, employing these tools demands a high degree of commitment, understanding, and skill

attributes that must be sustained through constant awareness and training. An essential part of the information security plan is cyber security policy this includes the written plans for how the enterprise IT assets will be protected. This course provides students with information on the origin of cyber security policy, governance structures for policy creation, selection and implementation of policy, and audit and control functions to ensure compliance and efficacy. Students will be exposed to the national and international policy and legal considerations related to cybersecurity and cyberspace such as privacy, intellectual property, cybercrime, homeland security (i.e., critical infrastructure protection) and cyberwarfare, and the organizations involved in the formulation of such policies. Broader technology issues also are discussed to demonstrate the interdisciplinary influences and concerns that must be addressed in developing or implementing effective national cybersecurity laws and policies.

l. 95743 Cybersecurity Policy and Governance II
    i. Across the board, IT managers in government and industry are concerned with regulatory compliance. This course is designed to introduce students to key Information Security industry and government policies, regulations and standards. The course is structured to familiarize students with base standards, like NIST, and more specific regulatory requirements, and to help students understand how those requirements are met, using frameworks, controls and training. The goal of this course is provide students with an understanding of how to develop an organizations information security policy and procedures to comply with government and industry regulations. This course is an elective for graduate students seeking to work or manage an information security and privacy department.
m. 95452 Introduction to Information Security Management
    i. This course is intended to give students an introduction to a variety of information and cyber security topics. As a survey course, it will cover foundational technical concepts as well as managerial and policy topics. Coverage includes foundations of information security; introductory cryptography; program, data, and operating system security; security of user-web interaction; safeguarding the Internet of Things; cyberwarfare; securing virtual, cloud, and mobile environments; network concepts and network security; incident management and IT auditing processes; security risk management; legal and ethical issues of security and privacy. Students are exposed to common sources of vulnerability information and how to incorporate this information into information security management processes. The purpose of the course lectures, assignments, readings, and examinations are to ensure students have sufficient technical awareness and managerial competence that will enable them to pursue advanced study in information security policy and management. There is no prerequisite for this course, however successful students will have fundamental knowledge of information and computer systems, and a general awareness of security issues in these systems.
n. 95748 Software and Security
    i. This course exposes students with limited exposure to programming and software engineering development foundational concepts to enable further understanding of the challenges of insecure and vulnerable software. Students are exposed to basic programming constructs (such as variables, control structures, data structures, programming syntax) , secure software development process and implementation details as well as the specific principles of enterprise-wide secure system development practices. The course also surveys the types of threats and vulnerabilities inherent in software and the origins of these deficiencies. A brief

overview of secure coding concepts and techniques are provided to students to provide exposure to how software can be made more secure and resilient and how security can be part of overall software development process.

o. 95758 Network and Internet Security
   i. This course emphasizes practical employment of network security. Topics in this course will provide: - A working knowledge of the need to design networks to - properly support an organization, - properly accommodate networking protocols, and - properly secure an organizations cyber assets through its network infrastructure
p. 95818 Privacy Policy, Technology, and Law
   i. This course focuses on policy issues related to privacy from the perspectives of governments, organizations, and individuals. We will begin with a historical and philosophical study of privacy and then explore recent public policy issues. We will examine the privacy protections provided by laws and regulations, as well as the way technology can be used to protect privacy. We will emphasize technology-related privacy concerns and mitigation, for example: social networks, smartphones, behavioral advertising (and tools to prevent targeted advertising and tracking), anonymous communication systems, big data, and drones. This course is part of a three-course series of privacy courses offered as part of the MSIT-Privacy Engineering masters program. Foundations of Privacy (offered in the Fall semester) offers more in depth coverage of technologies and algorithms used to reason about and protect privacy. Engineering Privacy in Software (offered in the Spring semester) focuses on the methods and tools needed to design systems for privacy.
   ii. http://cups.cs.cmu.edu/courses/privpolawtech.html
q. 95862 Current Topics in Privacy Seminar
   i. Note: Previously offered as 08-602. In this seminar course students will discuss recent papers and current public policy issues related to privacy. Privacy professionals from industry, government, and non-profits will deliver several guest lectures each semester.
r. 95884 Network Defenses
   i. Network Defenses will cover the basics of network security through lecture and hands-on interaction with live virtual systems. Topics and labs include network traffic analysis, firewalls, networking, intrusion detection systems, logging and system event management, and network flow. The course will culminate in a group exercise where teams will identify and detect live attacks occurring on a virtual environment. Network Defenses is geared towards students who may be non-technical by nature, but who want to gain hands-on insight into the tools and techniques used in network security and computer security in general. However, no prior hands-on skills are required in order to succeed in this course. Course concepts will be tested via weekly quizzes and a final exam.
s. 17331 Information Security, Privacy, and Policy
   i. As layers upon layers of technology mediate increasingly rich business processes and social interactions, issues of information security and privacy are growing more complex too. This course takes a multi-disciplinary perspective of information security and privacy, looking at technologies as well as business, legal, policy and usability issues. The objective is to prepare students to identify and address critical security and privacy issues involved in the design, development and deployment of information systems. Examples used to introduce concepts covered in the class range from enterprise systems to mobile and pervasive computing as well as social networking.
t. 17731 Foundations of Privacy

i. Privacy is a significant concern in modern society. Individuals share personal information with many different organizations - healthcare, financial and educational institutions, the census bureau, Web services providers and online social networks - often in electronic form. Privacy violations occur when such personal information is inappropriately collected, shared or used. We will study privacy in a few settings where rigorous definitions and enforcement mechanisms are being developed - statistical disclosure limitation (as may be used by the census bureau in releasing statistics), semantics and logical specification of privacy policies that constrain information flow and use (e.g., by privacy regulations such as the HIPAA Privacy Rule and the Gramm-Leach-Bliley Act), principled audit and accountability mechanisms for enforcing privacy policies, anonymous communication protocols - and other settings in which privacy concerns have prompted much research, such as in social networks, location privacy and Web privacy (in particular, online tracking targeted advertising).

MIT

→ Only has 2 classes specifically on the topic of security. It is more common for security to appear as a potential subtopic in a broader course. Privacy does not appear in much of the curriculum.

http://student.mit.edu/catalog/extsearch.cgi

1. 125 Architecting and Engineering Software Systems
    a. "...Also discusses **cyber-security issues** of key management and use of encrypted messaging for distributed ledgers, e.g., blockchain."
1. 6.033 Computer Systems Engineering
    a. "Topics on the engineering of computer software and hardware systems: techniques for controlling complexity; strong modularity using client-server design, operating systems; performance, networks; naming; **security and privacy**; fault-tolerant systems, atomicity and coordination of concurrent activities, and recovery; impact of computer systems on society."
2. 6.829 Computer Networks
    a. "Topics on the engineering and analysis of network protocols and architecture, including architectural principles for designing heterogeneous networks; transport protocols; Internet routing; router design; congestion control and network resource management; wireless networks; **network security**; naming; overlay and peer-to-peer networks."
3. 6.857 Network and Computer Security
    a. "Emphasis on applied cryptography and may include: **basic notion of systems security**, cryptographic hash functions, symmetric cryptography (one-time pad, stream ciphers, block ciphers), cryptanalysis, secret-sharing, authentication codes, public-key cryptography (encryption, digital signatures), public-key attacks, elliptic curve cryptography; pairing functions, fully homomorphic encryption, differential privacy, bitcoin, viruses, electronic voting."
4. 6.858 Computer Systems Security
    a. Design and implementation of secure computer systems. Lectures cover attacks that compromise security as well as techniques for achieving security, based on recent research papers. Topics include operating system security, privilege separation, capabilities, language-based security, cryptographic network protocols, trusted hardware, and security in web applications and mobile phones.
5. 15.565[J] Digital Evolution: Managing Web 3.0
    a. "Introduces Management 3.0 and the range of new Web technologies, applications, and business opportunities and challenges that it supports. Addresses topics such as big data, cloud computing, and **cybersecurity**."
6. 15.561 Information Technology Essentials

    a. "Other topics include hardware and operating systems, software development tools and processes, relational databases, **security and cryptography**, enterprise applications, and electronic commerce."
7. 17.447 Cybersecurity & 17.448 Cybersecurity
    a. Focuses on the complexity of cybersecurity in a changing world. Examines national and international aspects of overall cyber ecology. Explores sources and consequences of cyber threats and different types of damages. Considers impacts for and of various aspects of cybersecurity in diverse geostrategic, political, business and economic contexts. Addresses national and international policy responses as well as formal and informal strategies and mechanisms for responding to cyber insecurity and enhancing conditions of cybersecurity.
8. 6.805[J] Foundations of Information Policy
    a. "Studies the growth of computer and communications technology and the new legal and ethical challenges that reflect tensions between individual rights and societal needs. Topics include computer crime; intellectual property restrictions on software; **encryption, privacy,** and national security; academic freedom and free speech."
9. 24.131 Ethics of Technology
    a. "Introduces the tools of philosophical ethics through application to contemporary issues concerning technology. Takes up current debates on topics such as **privacy** and surveillance, algorithmic bias, the promise and peril of artificial intelligence, automation and the future of work, and threats to democracy in the digital age from the perspective of users, practitioners, and regulatory/governing bodies."

Stanford University
→ Offers a decent number of courses focused on security and privacy compared to other high ranking CS schools. Includes CS courses that incorporate ethics and privacy from more of a policy standpoint as opposed to just CS.

1. CS 1C: Introduction to Computing at Stanford (VPTL 1)
    a. "For those who want to learn more about Stanford's computing environment. Topics include: **computer maintenance and security**, computing resources, **Internet privacy**, and copyright law."
2. CS 142: Web Applications
    a. "Concepts and techniques used in constructing interactive web applications… Issues in **web security** and application scalability."
3. CS 155: Computer and Network Security
    a. Principles of computer systems security. Attack techniques and how to defend against them. Topics include: network attacks and defenses, operating system security, application security (web, apps, databases), malware, privacy, and security for mobile devices.
4. CS 181: Computers, Ethics, and Public Policy
    a. "Ethical and social issues related to the development and use of computer technology… Scenarios in problem areas: **privacy**, reliability and risks of complex systems, and responsibility of professionals for applications and consequences of their work."
5. CS 196: Computer Consulting (VPTL 196)
    a. "Focus is on Macintosh and Windows operating system maintenance, and troubleshooting through hardware and software foundation and concepts. Topics include operating systems, networking, **security**, troubleshooting methodology with emphasis on Stanford's computing environment."
6. CS 203: Cybersecurity: A Legal and Technical Perspective (INTLPOL 251)
    a. This class will use the case method to teach basic computer, network, and information security from technology, law, policy, and business perspectives. Using real world topics, we will study the technical, legal, policy, and business aspects of an incident or issue and

its potential solutions. The case studies will be organized around the following topics: vulnerability disclosure, state sponsored sabotage, corporate and government espionage, credit card theft, theft of embarrassing personal data, phishing and social engineering attacks, denial of service attacks, attacks on weak session management and URLs, security risks and benefits of cloud data storage, wiretapping on the Internet, and digital forensics. Students taking the class will learn about the techniques attackers use, applicable legal prohibitions, rights, and remedies, the policy context, and strategies in law, policy and business for managing risk. Grades will be based on class participation, two reflection papers, and a final exam.

7. CS 208E: Great Ideas in Computer Science
    a. "Great Ideas in Computer Science Covers the intellectual tradition of computer science emphasizing ideas that reflect the most important milestones in the history of the discipline. Topics include programming and problem solving; implementing computation in hardware; algorithmic efficiency; the theoretical limits of computation; **cryptography and security**; computer networks; machine learning; and the philosophy behind artificial intelligence."
8. CS 253: Web Security
    a. Principles of web security. The fundamentals and state-of-the-art in web security. Attacks and countermeasures. Topics include: the browser security model, web app vulnerabilities, injection, denial-of-service, TLS attacks, privacy, fingerprinting, same-origin policy, cross site scripting, authentication, JavaScript security, emerging threats, defense-in-depth, and techniques for writing secure code.
9. CS 255: Introduction to Cryptography
    a. For advanced undergraduates and graduate students. Theory and practice of cryptographic techniques used in computer security. Topics: encryption (symmetric and public key), digital signatures, data integrity, authentication, key management, PKI, zero-knowledge protocols, and real-world applications.
10. CS 349D: Cloud Computing Technology
    a. "This research seminar will cover industry and academic work on cloud computing and survey challenges including programming interfaces, cloud native applications, resource management, pricing, availability and reliability, **privacy and security**."
11. CS 350: Secure Compilation
    a. This course explores the field of secure compilation, which sits at the intersection between security and programming languages. The course covers the following topics: threat models for secure compilers, formal criteria for secure compilers to adhere to, security relevance of secure compilation criteria, security architectures employed to achieve secure compilation, proof techniques for secure compilation with a focus on back translation.
12. CS 356: Topics in Computer and Network Security
    a. Research seminar covering foundational work and current topics in computer and network security. Students will read and discuss published research papers as well as complete an original research project in small groups.

University of California Berkeley
→ Privacy and security are mentioned in a limited number of course offerings, but when they do come up, they are the central focus of the class as opposed to a subtopic. The school also offers a Masters of Cybersecurity.

1. COMPSCI 161 Computer Security
    a. Introduction to computer security. Cryptography, including encryption, authentication, hash functions, cryptographic protocols, and applications. Operating system security, access control. Network security, firewalls, viruses, and worms. Software security,

defensive programming, and language-based security. Case studies from real-world systems.

2. COMPSCI 162 Operating Systems and System Programming
    a. Basic concepts of operating systems and system programming. Utility programs, subsystems, multiple-program systems. Processes, interprocess communication, and synchronization. Memory allocation, segmentation, paging. Loading and linking, libraries. Resource allocation, scheduling, performance evaluation. File systems, storage devices, I/O systems. Protection, **security, and privacy**.
3. COMPSCI 171 Cryptography
    a. Cryptography or cryptology is the science of designing algorithms and protocols for enabling parties to communicate and compute securely in an untrusted environment (e.g. secure communication, digital signature, etc.) Over the last four decades, cryptography has transformed from an ad hoc collection of mysterious tricks into a rigorous science based on firm complexity-theoretic foundations. This modern complexity-theoretic approach to cryptography will be the focus. E.g., in the context of encryption we will begin by giving a precise mathematical definition for what it means to be a secure encryption scheme and then give a construction (realizing this security notion) assuming various computational hardness assumptions (e.g. factoring).
4. COMPSCI 276 Cryptography
    a. Graduate survey of modern topics on theory, foundations, and applications of modern cryptography. One-way functions; pseudorandomness; encryption; authentication; public-key cryptosystems; notions of security. May also cover zero-knowledge proofs, multi-party cryptographic protocols, practical applications, and/or other topics, as time permits.
5. COMPSCI 195 Social Implications of Computer Technology
    a. Topics include electronic community; the changing nature of work; technological risks; the information economy; intellectual property; **privacy**; artificial intelligence and the sense of self; pornography and censorship; professional ethics.
6. COMPSCI 261 Security in Computer Systems
    a. Graduate survey of modern topics in computer security, including protection, access control, distributed access security, firewalls, secure coding practices, safe languages, mobile code, and case studies from real-world systems. May also cover cryptographic protocols, privacy and anonymity, and/or other topics as time permits.
7. COMPSCI 261N Internet and Network Security
    a. Develops a thorough grounding in Internet and network security suitable for those interested in conducting research in the area or those more broadly interested in security or networking. Potential topics include denial-of-service; capabilities; network intrusion detection/prevention; worms; forensics; scanning; traffic analysis; legal issues; web attacks; anonymity; wireless and networked devices; honeypots; botnets; scams; underground economy; attacker infrastructure; research pitfalls.
8. **Berkeley does offer a Masters of Cybersecurity**
    a. https://cybersecurity.berkeley.edu
        i. UC Berkeley School of Information's (I School) Master of Information and Cybersecurity (MICS) is an accredited online program that prepares students with the cybersecurity skills needed to assume leadership positions in private-sector technology companies as well as government and military organizations.
        ii. Curriculum:
            1. Beyond the Code: Cybersecurity in Context
            2. Network Security
            3. Software Security
            4. Cryptography for Cyber and Network Security
            5. Operating System Security
            6. Managing Cyber Risk

7. Government, National Security, and the Fifth Domain
8. Usable Privacy and Security
9. Privacy Engineering

University of Illinois Urbana Champaign
→ Very few courses on the topics of privacy and security. Only 2 courses focus on the topics, and they come up as subtopics in only 4 other courses.

1. CS 210 Ethical & Professional Issues
    a. Ethics for the computing profession. Ethical decision-making; licensing; intellectual property, freedom of information, and **privacy**.
2. CS 461 Computer Security
    a. Fundamental principles of computer and communications security and information assurance: ethics, privacy, notions of threat, vulnerabilities, and risk in systems, information warfare, malicious software, data secrecy and integrity issues, network security, trusted computing, mandatory and discretionary access controls, certification and accreditation of systems against security standards. Security mechanisms: authentication, auditing, intrusion detection, access control, cryptography, security protocols, key distribution.
3. CS 563 Advanced Computer Security
    a. Current research trends in computer and network security. Privacy, tamper-resistance, unwanted traffic, monitoring and surveillance, and critical infrastructure protection. Subtopics will vary depending upon current research trends.
4. IS 206 Introduction to Database Concepts & Applications
    a. "Introduction to database technology concepts and architecture. Explore data types and reading/writing database layout descriptions. Discussion of database ethics and **privacy** concerns…"
    b. Not technically in CS school, but CS prereqs needed
5. IS 584 Advanced Topics in Ethics & Privacy
    a. Variety of newly developed and advanced topics courses within the field of ethics and **privacy**, intended to augment the existing Information Sciences curricula.
    b. Not technically in CS school, but CS prereqs needed
6. CS 425 Distributed Systems
    a. Protocols, specification techniques, global states and their determination, reliable broadcast, transactions and commitment, **security**, and real-time systems.

Cornell University
→ Offers a good list of courses focused specifically on privacy and security, but many are taught at Cornell Tech in New York City, with only some offered via online learning for students in Ithaca.

1. CS 4830 - Introduction to Cryptography
    a. Introductory course in cryptography. Topics include one-way functions, encryption, digital signatures, pseudo-random number generation, zero-knowledge and basic protocols. Emphasizes fundamental notions and constructions with proofs or security based on precise definitions and assumptions.
2. CS 5430 - System Security
    a. Discusses security and survivability for computers and communications networks. Includes discussions of policy issues (e.g., the national debates on cryptography policy) as well as discussions of the technical alternatives for implementing the properties that comprise "trustworthiness" in a computing system. Covers mechanisms for authorization and authentication as well as cryptographic protocols.
3. CS 6113 - Language-Based Security
    a. An exploration of methods for using programming languages and language semantics to enforce security. We will read recent papers on a variety of topics, including language-based authorization, enforcement of both confidentiality and integrity using type systems

for controlling information flow, quantitative security measures, secure distributed computing, and methods for incorporating and checking uses of cryptography.

4. CS 6431 - Security and Privacy Technologies
    a. A survey of modern security and privacy technologies. Topics include exploitation techniques, Web and mobile security, uses and misuses of cryptography in secure systems, attacking and defending secure network protocols, data privacy and anonymity, censorship resistance, electronic payments.
    b. Offered at Cornell Tech in New York City. Offered via distance learning for students in Ithaca.
5. CS 7493 - Computer Security Seminar
    a. This is a graduate seminar primarily aimed at Ph.D. students. Students will read, present, and discuss recent and classic papers in the computer security area. Outside speakers will also be invited to present current research.
6. CS 5831 - Security Protocols and Privacy
    a. This course covers advanced security and privacy protocols. Topics include basic key-exchange protocols, Internet Security Protocols (e.g., SSL/TLS), Oblivious RAM, Secure Two-party Computation, Voting protocols, and methods for data sanitization (i.e., how to ensure that publicly released data does not violate individuals' privacy).
    b. Offered at Cornell Tech in New York City.
7. CS 5435 - Security and Privacy Concepts in the Wild
    a. This course will impart a technical and social understanding of how and why security and privacy matter, how to think adversarially, how (and how not) to design systems and products. Less attention will be paid to specific skills such as hacking, writing secure code, and security administration. Topics will include user authentication, cryptography, malware, behavioral economics in security, human factors in security, privacy and anonymity, side channels, decoys and deception, and adversarial modeling. We will explore these concepts by studying real-world systems and attacks, including Bitcoin, Stuxnet, retailer breaches, implantable medical devices, and health apps, and considering issues to come in personal genomics, virtual worlds, and autonomous vehicles.
    b. T. Ristenpart.
    c. Offered at Cornell Tech in New York City.
8. CS 5436 - Privacy in the Digital Age
    a. This course introduces students to privacy technologies and surveys the current state of digital privacy from multiple perspectives, including technology, law, policy, ethics, economics, and surveillance.
    b. V. Shmatikov.
    c. Enrollment limited to: Cornell Tech students. Offered at Cornell Tech in New York City

University of Washington
→ Very few courses on the topics of privacy and security, half of which list it as the focus of the class, the other half have it as a subtopic. Comparable showing to University of Illinois Urbana-Champaign.

1. CSE 491 Data Science and Society Seminar (1)
    a. "Current topics related to the societal implications of data science. Topic selection will vary from quarter to quarter and **may include data privacy and security**, data anonymization, hypothesis-testing on a shared database, impact of data science-based decisions on society."
2. CSE 564 Computer Security and Privacy (4)
    a. Examines the fundamentals of computer security including: human factors; attack detection, measurements, and models; cryptography and communications security; system design and implementation; and side channels.
3. CSE 154 Web Programming (5) QSR

    a. Covers languages, tools, and techniques for developing interactive and dynamic web pages. Topics include page styling, design, and layout; client and server side scripting; **web security**; and interacting with data sources such as databases.
4. CSE 461 Introduction to Computer-Communication Networks (4)
    a. Computer network architectures, protocol layers, network programming. Transmission media, encoding systems, switching, multiple access arbitration. Network routing, congestion control, flow control. Transport protocols, real-time, multicast, **network security**.
5. CSE 484 Computer Security (4)
    a. Foundations of modern computer security, including software security, operating system security, network security, applied cryptography, human factors, authentication, anonymity, and web security.
6. CSE 526 Cryptography (4)
    a. Introduction to the theoretical foundation of cryptography, teaching the design and application of selected important cryptographic objects, and the mathematical frameworks and methodologies of modern cryptography for formalizing security goals and developing provably secure solutions.

Georgia Institute of Technology
→ Within their College of Computing, they have a School of Cybersecurity and Privacy. Offers one of the most comprehensive listings of privacy and security courses. Has a large amount of courses dedicated specifically to the topics as opposed to them being subtopics in other classes. The school also offers a Master of Science in Cybersecurity. Comparable to Carnegie Mellon.

1. CS 4235. Introduction to Information Security.
    a. Terms/concepts, threats, controls; problem definition; comprehensive information security model; security for operating systems, databases, network/distributed systems; administering security; legal/ethical/policy issues.
2. CS 4237. Computer and Network Security.
    a. Fundamental concepts and principles of computer security, operating system and database security, secret key and public key cryptographic algorithms, hash functions, authentication, firewalls and intrusion detection systems, IPSec ad VPN, and wireless security.
3. CS 4725. Information Security Strategies and Policies.
    a. Information security vulnerabilities and risks; legal, cost, privacy, and technology constraints; derivation of strategies; technical and procedural means of achieving desired results.
4. CS 4726. Privacy, Technology, Policy, and Law.
    a. This course takes a multi-disciplinary approach to privacy, a topic of great interest in the technology, policy, ethics, law, and business realms.
5. CS 6035. Introduction to Information Security.
    a. A broad spectrum of information security: threats, basic cryptography, software vulnerabilities, programming for malice, operating system protections, network security, privacy, data mining, computer crime.
6. CS 6238. Secure Computer Systems.
    a. Design principles of secure systems, authentication, access control and authorization, discretionary and mandatory security policies, secure kernel design, and secure databases.
7. CS 6262. Network Security.
    a. Design principles of secure network protocols and systems, authentication, integrity, confidentiality, privacy, information hiding, digital watermarking, access control, firewall, intrusion detection, and case studies.
8. CS 6263. Intro to Cyber-Physical Systems Security.

    a. This course provides an introduction to security issues relating to various cyber-physical systems including industrial control systems and those considered critical infrastructure systems.
9. CS 6265. Information Security Laboratory.
    a. This course covers advanced techniques for writing exploits, taught through an intense, hands-on security laboratory, following a cyberspace war game called Capture-The-Flag
10. CS 6266. Information Security Practicum.
    a. Capstone independent study placing each student in a commercial, industrial, academic, or government setting where they must solve real-world security problems.
11. CS 6402. Databases and Information Security.
    a. Fundamentals of designing and using databases: conceptual data models to database-specific models, SQL, storage structures. Security-related topics include privacy, access control, backup, recovery, SQL injection.
12. CS 6727. Cyber Security Practicum.
    a. Capstone independent study project placing each student in a commercial, academic or government setting where he or she identifies a major cyber security problem, and explores and evaluates a solution that addresses it with realistic assumptions about the organizational context. The chose problem must be approved by course instructor.
13. CS 7292. Reliability and Security in Computer Architecture.
    a. Hardware support for process isolation, virtualization, debugging, and protection from side-channel attacks. Faults and failures, error tolerance, error rate budgeting, lifetime reliability of devices.
14. CS 8803. Special Topics.
    a. Empirical security research seeks to understand how computer security concerns manifest in practice. For example, what strategies and techniques do attackers actually use, and how do they profit from their actions? How do users behave in different security contexts, and why do they behave in those (often insecure) ways? Gaining this understanding is vital for driving improvements in real-world security. This seminar-style course will cover both classic and recent empirical security studies across a wide range of security topics, including Internet security, underground ecosystems, usable security, and online privacy. You will analyze, critique, and discuss these works. Beyond broadening your knowledge of real-world computer security, you will gain a deeper understanding of sound and rigorous measurement methodologies for applying to your own work.
15. **In their College of Computing, they have a School of Cybersecurity and Privacy where they offer a Master of Science in Cybersecurity**
    a. http://www.catalog.gatech.edu/colleges/computing/cybersecurity-privacy/
    b. http://www.catalog.gatech.edu/programs/cybersecurity-ms/

Princeton University
→ Very few courses on security and privacy, with no courses specifically on the topics. More often, the topics are mentioned as potential subtopics in other courses. Comparable to University of Illinois Urbana-Champaign and University of Washington.
https://www.cs.princeton.edu/courses/catalog

1. COS109 - Computers in Our World
    a. "...This course is a broad introduction to computing technology for humanities and social science students. Topics will be drawn from current issues and events, and will include discussion of how computers work, what programming is and why it is hard, how the Internet and the Web work, **security and privacy**."
2. CS318 - Operating Systems
    a. "A study of the design and analysis of operating systems. Topics include: processes, mutual exclusion, synchronization, semaphores, monitors, deadlock prevention and

detection, memory management, virtual memory, processor scheduling, disk management, file systems, **security**, protection, distributed systems."

3. COS432 - Information Security
    a. Security issues in computing, communications, and electronic commerce. Goals and vulnerabilities; legal and ethical issues; basic cryptology; private and authenticated communication; electronic commerce; software security; viruses and other malicious code; operating system protection; trusted systems design; network security; firewalls; policy, administration and procedures; auditing; physical security; disaster recovery; reliability; content protection; privacy.
4. CS433 - Cryptography
    a. An introduction to modern cryptography with an emphasis on fundamental ideas. The course will survey both the basic information and complexity-theoretic concepts as well as their (often surprising and counter-intuitive) applications. Among the topics covered will be private key and public key encryption schemes, digital signatures, pseudorandom generators and functions, chosen ciphertext security; and time permitting, some advanced topics such as zero knowledge proofs, secret sharing, private information retrieval, and quantum cryptography.
5. COS461 - Computer Networks
    a. "This course studies computer networks and the applications and services that run on them. The course covers concepts in networking including: packet switching; Internet routing and business relationships; IPv4 and IPv6 addressing; the domain name system (DNS), router, switch, and middlebox design; **network security**; content distribution networks; wireless networks; and networked applications such as streaming video."
6. ELE 574 - Security and Privacy in Computing and Communications
    a. As our society transitions towards an information-driven paradigm, concerns about security and privacy of computing and communication have come to a forefront. This course exposes students to foundational principles and mechanisms that enable security and privacy in computing and communications. In addition, we study the interdisciplinary dimension of security and privacy by exploring its intersections with machine learning, information theory, computer architecture and formal methods.
    b. Not technically a CS class, but tailored towards it
    c. https://registrar.princeton.edu/course-offerings/course-details?term=1212&courseid=012709

University of Michigan Ann Arbor
→ Very few courses are dedicated to the topics of privacy and security, but the two are mentioned as subtopics in a larger number of courses than the closest competitors of University of Illinois Urbana-Champaign, University of Washington, and Princeton University.

1. EECS 388. Introduction to Computer Security
    a. This course introduces the principles and practices of computer security as applied to software, host systems, and networks. It covers the foundations of building, using and managing secure systems. Topics include standard cryptographic functions and protocols, threats and defenses for real-world systems, incident response and computer forensics.
2. EECS 485. Web Systems
    a. Concepts surrounding web systems, applications, and internet scale distributed systems. Topics covered include client/server protocols, **security**, information retrieval and search engines, scalable data processing, and fault tolerant systems.
3. EECS 547 (SI 652). Electronic Commerce
    a. Introduction to the design and analysis of automated commerce systems, from both a technological and social perspective. Infrastructure supporting search for commerce opportunities, negotiating terms of trade and executing transactions. Issues of **security, privacy,** incentives and strategy

4. EECS 582. Advanced Operating Systems
    a. Course discusses advanced topics and research issues in operating systems. Topics will be drawn from a variety of operating systems areas such as distributed systems and languages, networking, **security and protection**, real-time systems, modeling and analysis, etc.
5. EECS 588. Computer and Network Security
    a. Survey of advanced topics and research issues in computer and network security. Topics will be drawn from a variety of areas such as mandatory and discretionary security policies, secure storage, security kernels, trust management, preventing software vulnerabilities, applied cryptography, network security.
6. EECS 589. Advanced Computer Networks
    a. Advanced topics and research issues in computer networks. Topics include routing protocols, multicast delivery, congestion control, quality of service support, **network security**, pricing and accounting and wireless access and mobile networking.
7. EECS 691. Mobile Computing
    a. In-depth study of research issues in mobile and pervasive computing systems. Topics include location and context awareness, mobile data access, resource management, consistency protocols, mobile and ad hoc networking, networked sensors, **security and privacy**.

University of Oxford
→ Not much information on specific curriculum is available, but computer security is listed as a topic of study in the later years of the CS degree.
http://www.cs.ox.ac.uk/admissions/undergraduate/index.html
http://www.ox.ac.uk/admissions/undergraduate/courses-listing/computer-science

1. Computer security is a topic option in Year 3
2. Advanced security is a topic option in Year 4

ETH Zurich
→ Offers a good amount of courses related to privacy and security. These courses tend to be centered on the topics as opposed to subtopics.
http://www.vvz.ethz.ch/Vorlesungsverzeichnis/sucheLehrangebotPre.view?lang=en

1. 252-0408-00L Cryptographic Protocols
    a. The course presents a selection of hot research topics in cryptography. The choice of topics varies and may include provable security, interactive proofs, zero-knowledge protocols, secret sharing, secure multi-party computation, e-voting, etc.
    b. http://www.vvz.ethz.ch/Vorlesungsverzeichnis/lerneinheit.view?lerneinheitId=136623&semkez=2020S&ansicht=KATALOGDATEN&lang=en
2. 263-4660-00L Applied Cryptography
    a. This course will introduce the basic primitives of cryptography, using rigorous syntax and game-based security definitions. The course will show how these primitives can be combined to build cryptographic protocols and systems.
    b. http://www.vvz.ethz.ch/Vorlesungsverzeichnis/lerneinheit.view?lerneinheitId=138979&semkez=2020S&ansicht=KATALOGDATEN&lang=en
3. 263-2925-00L Program Analysis for System Security and Reliability
    a. Security issues in modern systems (blockchains, datacenters, AI) result in billions of losses due to hacks. This course introduces the security issues in modern systems and state-of-the-art automated techniques for building secure and reliable systems. The course has a practical focus and covers systems built by successful ETH spin-offs.
    b. http://www.vvz.ethz.ch/Vorlesungsverzeichnis/lerneinheit.view?lerneinheitId=136822&semkez=2020S&ansicht=KATALOGDATEN&lang=en
4. 263-4600-00L Formal Methods for Information Security

a. The course focuses on formal methods for the modelling and analysis of security protocols for critical systems, ranging from authentication protocols for network security to electronic voting protocols and online banking.
b. http://www.vvz.ethz.ch/Vorlesungsverzeichnis/lerneinheit.view?lerneinheitId=135980&semkez=2020S&ansicht=KATALOGDATEN&lang=en

5. 851-0740-00L Big Data, Law, and Policy
   a. This course introduces students to societal perspectives on the big data revolution. Discussing important contributions from machine learning and data science, the course explores their legal, economic, ethical, and political implications in the past, present, and future
   b. http://www.vvz.ethz.ch/Vorlesungsverzeichnis/lerneinheit.view?lerneinheitId=135928&semkez=2020S&ansicht=KATALOGDATEN&lang=en
6. 252-0211-00L Information Security
   a. This course provides an introduction to Information Security. The focus is on fundamental concepts and models, basic cryptography, protocols and system security, and privacy and data protection. While the emphasis is on foundations, case studies will be given that examine different realizations of these ideas in practice
   b. http://www.vvz.ethz.ch/Vorlesungsverzeichnis/lerneinheit.view?lerneinheitId=135137&semkez=2020S&ansicht=KATALOGDATEN&lang=en
7. 263-4651-00L Current Topics in Cryptography
   a. In this seminar course, students present and discuss a variety of recent research papers in Cryptography.
   b. http://www.vvz.ethz.ch/Vorlesungsverzeichnis/lerneinheit.view?lerneinheitId=139038&semkez=2020S&ansicht=KATALOGDATEN&lang=en

Business - Undergraduate
University of Pennsylvania
→ Offers one class focused on the topic of cybersecurity, from a legal perspective. Does mention it as a subtopic in a few other courses.
https://catalog.upenn.edu/courses/

1. BEPP 261 Risk Analysis and Environmental Management
   a. This course will introduce students to concepts in risk governance. We will delve into the three pillars of risk analysis: risk assessment, risk management, and risk communication. The course will spend time on risk financing, including insurance markets. There will be particular emphasis on climate risk management, including both physical impact risk and transition risk, although the course will also discuss **several other examples, including** management of environmental risks, terrorism, and **cyber-security**, among other examples. The course will cover how people perceive risks and the impact this has on risk management. We will explore public policy surrounding risk management and how the public and private sector can successfully work together to build resilience, particularly to changing risks.
   b. Also Offered As: BEPP 261, BEPP 761, BEPP 961, ESE 567, OIDD 261
2. LGST 222 / OIDD 222 Internet Law, Privacy, and Cybersecurity
   a. This course looks at how courts, legislatures, and regulators confront the major issues of the internet world. Billions of people are now active on social media, and firms such as Google, Facebook, Amazon, and Alibaba are among the worlds most valuable and influential. The legal interfaces between the physical world and the digital world are therefore increasingly important. In particular, exploitation of personal information online by governments, digital platforms, and bad actors is becoming a constant source of major controversies. The material in the course ranges from the foundations of cyberlaw, developed during the e-commerce bubble of the 1990s, to current leading-edge questions around the power and responsibility of digital intermediaries; data protection in the U.S.

and Europe; cybercrime;blockchain; and network neutrality. No pre-existing legal or technical knowledge is required.

3. LGST 242 Big Data, Big Responsibilities: The Law and Ethics of Business Analytics
    a. Significant technologies always have unintended consequences, and their effects are never neutral. A World of ubiquitous data, subject to ever more sophisticated collection, aggregation, and analysis, creates massive opportunities for both financial gain and social good. It also **creates dangers in areas such as privacy, security,** discrimination, exploitation, and inequality, as well as simple hubris about the effectiveness of management by algorithm. Firms that anticipate the risks of these new practices will be best positioned to avoid missteps. This course introduces students to the legal, policy, and ethical dimensions of big data, predictive analytics, and related techniques. It then examines responses-both private and governmental-that may be employed to address these concerns.

MIT
→ No courses mention privacy and security.

1. No specific classes in Sloan

University of California Berkeley
→ No courses mention privacy and security.
http://guide.berkeley.edu/courses/ugba/

1. No specific classes in Haas

University of Michigan Ann Arbor
→ Privacy and security is a subtopic in 2 listed classes, but almost nonexistent in curriculum.
https://michiganross.umich.edu/course-catalog

1. TO 426: Mobile Innovation Development
    a. Mobile platforms have emerged as the preferred vehicle for delivering business innovation to consumers. BBA students specifically those with interests in entrepreneurship or career interests in mobile businesses, need to understand the unique requirements of mobile businesses to successfully design, develop, deploy and manage business innovations. This course is designed to help students conceptualizing, designing, developing, delivering and managing technology solutions by taking them through the application (app) development process covering the full spectrum from identifying customer needs to prototyping/simulating a mobile innovation solution. Students will learn business issues related to mobile businesses including business and revenue models, customer engagement through gamification and personalization, **security and privacy challenges**, role of big data and mobile analytics, and integration of emerging technology directions such as wearables, smart devices, loT, location based features and Social Media Integration. The course will seek to organize students in project groups with a combination of business, design and technology expertise. Project groups will then conceptualize, design and prototype/simulate a mobile business innovation throughout the course.
    b. https://michiganross.umich.edu/courses/mobile-innovation-development-10703
2. Business Information Systems
    a. In keeping with AACSB guidelines, this course focuses on information technologies as they influence the structure and processes of organizations and economies, and as they influence the roles and techniques of management. We will address such questions as: How do information systems influence organizational competitiveness? Why are technology infrastructures so important to modern organizations? What is the role of the Internet and networking technology in organizations? How do information systems enable organizational processes? How do organizations develop, acquire and implement

information systems? **What ethical, criminal and security issues do organizations face when using information systems?**

b. https://michiganross.umich.edu/courses/business-information-systems-9144

Carnegie Mellon University
→ Privacy is mentioned in one class on e-commerce, but essentially non existent in curriculum.
http://coursecatalog.web.cmu.edu/schools-colleges/tepper/undergraduatebusinessadministrationprogram/#coursestext

1. 70-366 Intellectual Property and E-Commerce
    a. The course is intended to instruct students on the creation of the Internet and the World Wide Web, including the creation of the Domain Naming System. The course will provide an understanding of how the WWW "Web" operates (from its creation to the present), how the laws of various countries interact with the Web; **how issues of privacy are addressed and the role of private parties and government in monitoring privacy**. The course will examine how intellectual property is created and protected; who owns the property; and the role of ownership of the intellectual property interacts with antitrust laws. The course examines how contracts are formed and administered on the Web by entities created to minimize taxes and personal liability risks for the owners/shareholders of those entities.

University of Texas Austin
→ No courses mention privacy and security.
https://www.mccombs.utexas.edu/Departments

1. No specific classes in McCombs

University of North Carolina Chapel Hill
→ No courses mention privacy and security.
https://catalog.unc.edu/courses/busi/

1. No specific classes in Kenan-Flagler

University of Virginia
→ Offers a specific course on cybersecurity from a manager's perspective, but otherwise privacy and security are not found in business undergraduate curriculum.
http://records.ureg.virginia.edu/content.php?catoid=47&navoid=3428

1. COMM 4240 - Electronic Commerce and Web Analytics
    a. This course provides an overview of the concepts, technologies, and tools necessary for designing and implementing information systems that support electronic commerce and online analytics initiatives; including web development, web and social media analytics, online marketing tactics, Internet fraud detection, **online security**, and emerging Web 2.0 technologies.
2. COMM 4263 - Intro to Cybersecurity
    a. This course provides a manager's view of cybersecurity and privacy that contains an overview of methods for managing and mitigating cybersecurity risk in organizations. Further, this course includes an emphasis on applying analytics to understand cybersecurity threats. The course will also explore the role of privacy in society.

Cornell University
→ Privacy is mentioned in one class on e-commerce, but essentially non existent in curriculum. Comparable to Carnegie Mellon.
http://courses.cornell.edu/preview_program.php?catoid=36&poid=17641
http://courses.cornell.edu/preview_program.php?catoid=36&poid=17512

1. HADM 4890 - The Law of the Internet and E-Commerce

a. The computer industry and the Internet have fundamentally changed the world in swift, dramatic fashion. The emergence of global digital networks and digital technologies offer to nearly anyone the ability to access, store, mine, manipulate, and transmit vast amounts of information. At the same time, this revolution in the use of information raises new and often complex legal disputes in areas such as copyright, trademark, privacy, speech, contract formation, jurisdiction, **information security**, etc. Moreover, the rapidly growing maze of laws directed at the Internet is another thorny obstacle for persons and companies doing business on the web. The purpose of this course is to acquaint students with the **legal topics and principles applicable to the Internet**, and to help students identify and understand the rapid developments of the law of the Internet by exploring specific problems.

University of Notre Dame
→ Offers 2 specific classes dedicated to privacy and security, which is the most robust showing among the undergraduate business programs.
https://mendoza.nd.edu/undergraduate/

1. ITAO 40510: Ethics of Data Analytics
    a. Data-informed decision making has created new opportunities, but also expands the set of possible risks to organizations. One of these risks comes from grappling with the "should we?" question with regard to data and analytics, and **associated privacy concerns**. In this course, we will explore several frameworks to address the issues related to the proper roles of public law, government regulation, and ethics in performing and managing analytics activities. The course will cover applicable theory and guidelines, and also make use of case studies. Upon completion, the student should be comfortable adapting one of these ethical frameworks for use in alignment with their organizational mission.
2. ITAO 30640: Privacy & Security
    a. In today's digital age, people and organizations produce and deal with unprecedented amounts of data. Thus, issues concerning information privacy and security have taken on critical importance. Information privacy and security are fundamentally about data protection. Information privacy refers to decisions around what information should be protected, from whom, why, and issues related to the ownership of information; whereas information security refers to the tactics and technologies to ensure data protection. In this course, we will address questions such as: How should organizations manage privacy and security issues? What are the various privacy and security threats that organizations and individuals face? What are the current advancements in privacy and security technologies and government regulations? We will learn about economics of privacy, biases and heuristics in privacy decisions, privacy ethics, social engineering, and public policy and regulations. Also, we will gain an understanding of security threats and gain insight into managerial best practices for managing information security. This course will involve a number of assignments along with interactive in-class exercises aimed at enhancing your privacy and security decisions.
3. MGTI 40670. Internet Security and Privacy
    a. According to FBI crime statistics, 85 percent of all companies with networked computer systems suffered measurable losses in 2001. Many in the computer-security industry believe that the other 15 percent were either unaware of their losses, or they were unwilling to reveal such potentially damaging information. The purpose of this course is to exam- ine computer security and privacy to better assess related risks.

London School of Economics
→ Has one course that includes security and privacy as a subtopic, but otherwise not present in the curriculum.

1. Management and Innovation of e-business IS3167

a. https://london.ac.uk/courses/management-and-innovation-e-business-is3167
b. It combines transaction cost economics with a decade's experience of e-business development to discuss e-business trends and strategies. Focussing on management information systems, it considers how the organisational, managerial, technological and theoretical aspects of e-business can be combined to produce innovation in business models, processes and products.
c. Topics covered include: **Security and privacy aspects of e-business**, E-business environment - economic, ethical, legal and security issues.

University of Oxford
→ No courses mention privacy and security.
http://www.ox.ac.uk/admissions/undergraduate/courses-listing/economics-and-management
https://www.sbs.ox.ac.uk/programmes/bahons-economics-and-management

1. No specific classes

Business - MBA
University of Pennsylvania
→ Offers only one course (also offered as an undergraduate course) that has cybersecurity as just one example of overall risk. No mention of privacy and security in any curriculum beyond this.

1. BEPP761 / OIDD761 - RISK ANALY & ENV MGMT
    a. This course will introduce students to concepts in risk governance. We will delve into the three pillars of risk analysis: risk assessment, risk management, and risk communication. The course will spend time on risk financing, including insurance markets. There will be particular emphasis on climate risk management, including both physical impact risk and transition risk, although the course will also discuss **several other examples**, including management of environmental risks, terrorism, and **cyber-security**, among other examples. The course will cover how people perceive risks and the impact this has on risk management. We will explore public policy surrounding risk management and how the public and private sector can successfully work together to build resilience, particularly to changing risks.

Stanford University
→ Only 2 courses mention privacy and security; very non intensive coverage.
https://exploredegrees.stanford.edu/graduateschoolofbusiness/#courseinventory

1. MGTECON 515. Cryptocurrency.
    a. This class will provide an overview of the rapidly evolving area of distributed ledger and blockchain technologies, with a focus on economic and strategic issues. We will cover key components of the architecture that affect the products derived from cryptocurrency. We then consider tokens as a store of value and exchange, analyzing models of cryptocurrency pricing and as a vehicle for raising of capital. Next, we consider use cases including payments, micropayments, asset registries, and smart contracts. We then analyze barriers to entry in cryptocurrencies, as well as how the new products they enable affect industry structure in both the financial sector and the economy and society as a whole. For example, how might decentralized systems like the blockchain impact the sharing economy? The government? We consider the governance of these decentralized systems and how decentralization affects the potential for the management and success of platforms. We discuss the potential for national digital currencies and the end of cash. Finally, **we consider consumer protection, privacy, security**, regulation, and the power of governments and regulators over borderless, decentralized systems. Students will benefit from guest lectures by industry and thought leaders.
    b. GSBGEN 578. Is the Internet Broken?

i. This interdisciplinary course examines the promise, peril, and possible future of the Internet and the impact of the World Wide Web on our lives. We will explore the most pressing contemporary issues facing the Internet, including **debates on privacy**, antitrust, freedom of speech, access, neutrality, and regulation. We will also unpack the claim that "decentralization," as it has grown with new technologies such as blockchain and crypto assets, captures the original vision of the Internet. A key question we will address is: What should be the roles of markets, governments, and different stakeholders in shaping the Internet? Students will have the opportunity to reflect on their own motivations and roles as digital consumers, potential innovators, and future leaders in this process.

Northwestern University
→ One of the few MBA programs to offer a course specifically focusing on cybersecurity.
https://www4.kellogg.northwestern.edu/coursecatalogschedule/

1. Information Privacy (BLAW-984-5)
    a. On May 25, 2018 the General Data Protection Regulation (GDPR) goes into effect. US Companies and lawmakers are wildly unprepared, relying on outdated enforcement mechanisms and vows of companies who flout data protection. Global issues of surveillance and propaganda are daily news. Widespread use of AI in decision-making, revenge porn and deep fakes are commonplace. States react quickly, passing legislation which mimics GDPR and lights a fire under technology companies to lobby for Federal legislation to provide a preemption cover. How did we get here? **This course will examine the tension between opposing approaches to privacy**; how these laws came into being and some of their disparate, intended and unintended consequences. We will have a guest speaker from a Silicon Valley technology company who will discuss how these laws are put into practice in building the technology of tomorrow. By the end of the class you will understand the contours of data privacy in Europe and the US and the factors that have gone into the recent surge of interest in US consumer privacy. You will also have a greater understanding of how companies struggle with the technology they create; its impact on privacy and how they manage it.
2. Technology in the Age of Analytics (KMCI-930-5)
    a. Information technology is inextricably linked with the generation and management of data for use in analytics. The course provides an overview of enterprise and cloud technology building blocks and how they enable data analytics. We also discuss today's typical technology infrastructures for data analytics and where the technology seems to be headed. Finally, we talk about the benefits and costs of different ways to organize a data analytics function as well as **privacy and security considerations around data.** The overall goal is to develop an understanding for how information technology decisions affect the performance of Data Analytics in organizations.

University of Chicago
→ Even without access to course description, it can be assumed that it is unlikely privacy and security are the focus of either course listed.
https://intranet.chicagobooth.edu/pub/coursesearch/coursesearch

1. Cryptocurrency and Blockchain: Markets, Models and Opportunities
2. Technology Strategy

**No descriptions of the courses were found on any school webpages or in course catalogs

MIT
→ One course mentions privacy and security as a subtopic; very non intensive coverage.

1. 15.561 Information Technology Essentials

a. Examines technology concepts and trends underlying current and future uses of information technology (IT) in business. Emphasis on networks and distributed computing, including the web. Other topics include hardware and operating systems, software development tools and processes, relational databases, **security and cryptography**, enterprise applications, and electronic commerce. Exposure to web, database, and graphical user interface (GUI) tools. Primarily for Sloan master's students with limited IT background.

Harvard University
→ No courses mention privacy and security.
https://www.hbs.edu/coursecatalog/

1. No specific courses

University of California Berkeley
→ No courses mention privacy and security.
https://mba.haas.berkeley.edu/academics/curriculum
http://guide.berkeley.edu/courses/mba/
https://courses.haas.berkeley.edu/Schedule/Schedule?strParams=Fall:2018:%

1. No specific courses
2. **Has "technology" as an optional area of interest for MBAs**
    a. https://haas.berkeley.edu/mba/academics/course-planning/areas-of-emphasis/technology/

Columbia University
→ One course mentions privacy and security as a subtopic; very non intensive coverage.
https://www8.gsb.columbia.edu/programs/mba/academics/core-curriculum
https://www8.gsb.columbia.edu/courses/mba

1. B8462-001: An Introduction to Blockchain and Cryptocurrencies
    a. This course will introduce fundamental concepts and a high-level overview of the burgeoning blockchain and cryptocurrency space. The course will begin by providing a background in fundamental concepts in Computer Science such as in **cryptography**, distributed systems, and data structures. It will then move on to an in-depth overview of blockchain, the history of Bitcoin and the proliferation of new consensus models, ICOs, smart contracts, and more. Industry guest speakers will share their perspectives.
    b. https://www8.gsb.columbia.edu/courses/mba/2019/fall/b8462-001

Yale University
→ The only mention of privacy and security is specifically courses related to secure transactions.
https://som.yale.edu/elective-core-courses

1. MGMT667: Secured Transactions
    a. This course will provide an in-depth examination of the basic structure and purposes of **secured credit transactions** under Article 9 of the Uniform Commercial Code. Discussions will focus on the essential elements of secured financing (including the **creation and enforcement of security interests** in various types of tangible and intangible property) as well as the longstanding debate over the essential utility and fairness of contractual security devices and the secured creditor's priority. We will also consider the treatment of security interests in bankruptcy proceedings; securitizations as an alternative to traditional methods of secured lending; consignments; bailments; letters of credit; and a variety of other commercial law concepts. Prior courses in commercial transactions, corporate finance, and bankruptcy, although helpful, are not required. Relevant commercial concepts will be explained as they arise. Students should expect a lively discussion of a number of important issues of current and enduring significance in the study of commercial law.

2. MGMT 673: History and Theory of Secured Transactions
    a. This seminar is designed as a one-credit "add-on" to the basic three-credit course on Secured Transactions. The seminar will provide an in-depth examination of the history and **theory of the law of secured credit transactions**, including the development, enactment, and reform of Article 9 of the Uniform Commercial Code. Discussions of the history of the subject will **focus on the origins of the law of security interests** in various types of tangible and intangible personal property, focusing on the development of security devices in England and the United States. Discussions of the theory of the subject will focus on various scholarly writings analyzing why security interests exist, their function, their utility, various problems that arise from having them, and possible reform. Two chapters of the course book used in the basic three-credit course are devoted to the history and theory of security devices, and we will focus on the materials in these chapters. Students should expect a lively discussion of the history and theory of secured transactions from a number of different perspectives. Enrollment in the basic three-credit Secured Transactions course concurrent with enrollment in the seminar, or a prior course in secured transactions under Article 9, is required.

New York University
→ The most robust privacy and security MBA curriculum out of the schools surveyed. It includes two courses dedicated to the subject, as well as multiple other courses that list it as a subtopic.
https://www.stern.nyu.edu/programs-admissions/full-time-mba/academics/course-index
https://www.stern.nyu.edu/portal-partners/registrar/course-information/course-descriptions-prerequisites

1. Cybersecurity & Privacy
    a. As the frequency, size and consequences of breaches of customer personal information and corporate intellectual property have grown exponentially, the protection of information held by companies has become a critical business issue for managers, executives and Boards of Directors. Students in this course will develop a fundamental understanding of business, technical, legal and ethical issues and challenges related to cybersecurity and privacy. They will learn how business managers cope with these challenges across different industries by developing robust Information Security and Privacy Management Programs to maintain confidentiality, integrity and availability of the information, networks, computing systems and applications managed by the organization. Upon completing this course, students will be prepared to consider the cybersecurity and privacy risks inherent in a wide range of business decisions and have incisive conversations with cybersecurity and privacy experts about these risks and how they can be mitigated. Examples of topics to be addressed in this course include: (1) The roles of the Board of Directors, executives and business managers in cybersecurity and privacy protection; (2) Strategies to prevent intrusions and theft of data, and to detect intrusions if they do occur; (3) How to conduct risk-based management â to assess and prioritize cybersecurity and privacy risks; (4) How to prepare for a data breach, and necessary actions following a breach, with a focus on critical business decisions that senior corporate management will face; (5) Unique privacy management requirements for marketers, for the financial industry and for the healthcare industry, as well as workplace privacy issues across industries; (6) The realities of cyberespionage; and (7) Lessons from the business and technical mistakes of companies whose security deficiencies left them vulnerable to data breaches with consequential negative impact on their customers, corporate reputation and financial position.
2. Managing Climate, Cyber, Geopolitical, and Financial Risk
    a. Businesses and governments now face a growing and immediate array of nonfinancial risks, including climate-related, **cyber** and operational, and geopolitical risks. Precisely because these critical risks are hard to measure and analyze, firms are putting new resources â people and moneyâ to work to anticipate, manage and mitigate them. To

address cybersecurity risks, for example, JP Morgan alone has 3000 employees and spends $600 million annually. Firms are only starting to grapple with existential climate-related risks. And startups are mushrooming to provide assessments to businesses. This course will study these risks alongside financial risks. It will outline frameworks for measuring, assessing and analyzing them, and for actions needed to meet them. We will examine case studies of climate, **cyber and geopolitical risks**, including from current events. Finally, we will study whether and how the information in financial markets can both inform the assessment of these risks and potentially provide tools to transfer, insure against or hedge them.

3. INFO-GB.2332 Managing a High Tech Company: The CEO perspective
    a. We are living in an era where 'technology' companies are totally changing our lifestyle and it is obvious that artificial intelligence will push this trend further. Each and every industry will be disrupted by technology so understanding this mass transformation is crucial. **Students will study how 'management' is executed in high tech companies** and examine the differences from managing a traditional company. This course will cover mega trends in technology sector and will study a number of real word business cases. Examples of topics in this course include: (1) How to manage innovation (2) Critical success factors in tech companies (3) Technology's role in platform business (two sided business, content platform business) (4) Culture & Talent management in tech industry (5) Tech M&As. On top of U.S tech companies, Asian tech companies will also be discussed due to their advanced implementation of technology (such as Baidu, Tencent, Alibaba in China and Kakao, Naver in South Korea) Also, the lecturer will share his experience as CEO of Kakao a technology company that services Kakao Talk, a mobile messenger that has 95%+ market share and is valued at around $10B in South Korea.
4. Computer & Ntwrk Security
    a. As enterprises become increasingly reliant on electronic media and communication the protection of data and electronic infrastructure becomes critically important Incidents of security failures in commercial and noncommercial environments are increasing in number and severity Hence it is essential that enterprises continually develop and refine security strategies that reflect the changing uses of information technology This course introduces basic concepts of computer and network security with an emphasis on the threats and countermeasures relevant to Internet and Web services Students are prepared to evaluate the security needs of organizations and to develop strategies to address these needs The requirements and design of security technologies are reviewed and case studies are presented
5. Data Governance
    a. How much is your data worth What are the probabilities of risk How much should you spend to protect your data from theft fraud abuse and regulatory fines Who is using your data inside your company with business partners outsourcers offshore why and when What policies do you need How do you govern them These are key questions that every business executive needs to answer today because data is the raw material of economic growth and Data Governance is a strategic imperative There are a lot of myths about Governance It is not a technology not something new not very hard to do but hard to do very well Effective Data Governance is a culture of organizational behavior that mitigates risk It is as much about self control as it is about quality control the rule of law and the architecture of regulation It is the process of balancing appropriate access to information to maximize value creation with control and discipline to manage risk How an organization strikes that balance impacts employees customers business partners citizens political institutions and global networks Governing data well is a critical challenge for businesses today Course Content We will begin by exploring the threats to data including **Security Privacy** Offshoring Regulations Semantics Fraud and Operational Risks We

will then look at methods for assessing the value and inherent liabilities of data from both business and IT perspectives We will explore Operational Risk looking at Basel II definitions and Insurance Professional Liability examples And we will look at different kinds of IT access controls such as Firewalls Roll Based Access Control Identity Management Encryption and Anonymity Course Objectives Understanding Data Governance models Assessing Data Value and Risk Managing regulatory requirements policy and obligations Evaluating data standards and Master Data Management Modeling business processes and controls Measuring and reporting results Creating consistency and good data governance

Insead
→ No courses mention privacy and security.
https://www.insead.edu/master-programmes/mba/core-courses
https://www.insead.edu/master-programmes/mba/academics/elective-courses

1. No specific courses

London Business School
→ No courses mention privacy and security.
https://www.london.edu/masters-degrees/mba/programme-content/core-courses
https://www.london.edu/masters-degrees/mba/programme-content/electives

1. No specific courses

SECTION 2
Review of Existing Cyber Security and Cyber Privacy Course Offerings

Section 2 reviews a complete list of all topics currently covered in computer science curricula, undergraduate business curricula, and MBA Curricula. Where we observed gaps that we found surprising we noted those.

Key Concepts Already Taught

→ Computer Science

1. Security and privacy foundations in software
2. Including security: described in a few courses as "architectural principles for designing networks"
    a. Operating system security
    b. Firewalls
3. Software vulnerability analysis and defense
    a. This is meant to focus specifically on identifying vulnerabilities in existing software
4. Networking and wireless security
5. Cryptography
    a. With varying, but comprehensive subtopics
6. Secure coding: developing software in a way that protects against accidental security vulnerabilities
7. Information security
    a. With varying, but comprehensive subtopics
8. Cybersecurity policy: company policies regarding cybersecurity including incentives, punishments, and standards of security
9. Legal and ethical issues related to security and privacy
10. The Internet of Things
    a. Portrayed similarly to secure cloud computing in that we need to develop specific security protocols for the expanding internet of things
    b. Appropriate to cover because often smart devices create trojan horse entry points
11. Cyberwarfare and cyberthreats
12. Securing virtual / cloud computing environments
13. Big data
    a. Although not described this way in course listings, often it was referenced in the context of data protection
14. Language-based security
    a. "An exploration of methods for using programming languages and language semantics to enforce security."
15. Anonymity
    a. It was listed as a common subtopic in privacy courses since it relates to providing users privacy.
16. Authorization and authentication
    a. This is a separate topic because every app and every pieces of software can determine its own levels of authorization and authentication
17. Mobile security
18. Intrusion detection
    a. This is its own topic because active intrusion monitoring and active countermeasures are often third-party services
19. Viruses and malicious code
20. Vulnerabilities created by supporting legitimate remote access

→ Business: Undergraduate

1. Cyberlaw
2. Cybersecurity risks and threats
    a. Cybercrime
3. E-commerce privacy and security considerations
4. The internet (how it works, how it can be used, etc.)
5. Data protection
    a. Legal, policy, and ethical dimensions of big data
    b. Exploitation of personal information
    c. Data ownership
6. Information systems
    a. With varying, and non-comprehensive, subtopics
    b. Includes managerial methods for managing information security
7. Role of private parties and governments in monitoring privacy
8. Legal topics applicable to the Internet
9. Integration of emerging technology directions such as wearables
10. Why / how technology infrastructures are important to modern organizations
11. Software and Privacy Risk management

→ Business: MBA

1. Risk management
2. Cryptocurrency and blockchain
    a. Often touches on cryptography
3. Decentralized systems
4. The internet
    a. Regulation, access, privacy, etc.
5. Data privacy laws
6. Cloud technology / data analytics
    a. Privacy and security of big data
7. Networks
8. Secured transactions
    a. Creation, enforcement, laws
9. Legal and ethical issues and challenges of privacy and security
10. Confidentiality
11. Role of executives in cybersecurity and privacy protection
12. Effective data governance
    a. Ways to protect data from intrusions and threat
    b. How to prepare for a data breach, necessary actions following a breach
13. Cyber threats / cyberespionage
14. Computer and network security
15. Threats and countermeasures against data breaches
16. IT access controls
    a. Firewalls, access controls, identity management, etc.

<u>What We Believe Needs to be Taught, but is Not Currently Offered</u>

→ Computer Science

1. Human error
2. Error tolerance
3. Disaster recovery
4. Protection from side-channel attacks
5. Lifetime reliability of devices
6. Data sovereignty and data residency

    a. Who owns data, and what country has control over data, when it is moved about in the cloud? Whose regulations apply?

→ Business: Undergraduate

1. Smart devices and their implications
2. Internet of Things
3. Fiduciary responsibility
4. Survivability (including physical survivability)
5. Controlled interfaces
6. Personnel security
7. Human error
8. Error tolerance
9. Legal responsibilities of corporations
10. Legal responsibilities / fiduciary responsibilities of officers and board members

→ Business: MBA

1. Survivability (including physical survivability)
2. Controlled interfaces
3. Personnel security
4. Human error
5. Error tolerance
6. Smart devices and their implications
7. Internet of Things
8. Fiduciary responsibility
9. Legal responsibilities of corporations
10. Legal responsibilities / fiduciary responsibilities of officers and board members
11. Data sovereignty and data residency
    a. Who owns data, and what country has control over data, when it is moved about in the cloud? Whose regulations apply?

SECTION 3
Summary List of Topics that Could be Covered in Cybersecurity Course Offerings

Section 3 Presents summaries of CSCP topics that could potentially be covered in computer science curricula and in undergraduate and MBA business curricula.

Key Concepts That Could Be Taught
→ Computer Science

1. Type of Threat — Denial of service, theft of IP, theft of personnel information, theft of customer ID information, destruction of local information (RansomWare), phishing and other forms of exploiting human weakness
2. Mechanism of Attack — masquerade as legitimate user, exploit local vulnerability, exploit operating system vulnerability, exploit other software vulnerability, "eavesdropping", planting of malware
3. Mechanism of defense — encryption, operating system software defense, threat monitoring systems, firewalls, networking security, cloud security
4. Local policy and human defenses, including authentication and multiple-level authentication
5. Legal issues, including national policy obligations, fiduciary responsibility, data residence and data sovereignty
6. Other topics, including cyberwarfare

Key Concepts That Could Be Taught
→ Undergraduate and MBA Business

1. Type of Threat — Denial of service, theft of IP, theft of personnel information, theft of customer ID information, destruction of local information (RansomWare), phishing and other forms of exploiting human weakness
2. Mechanism of Attack — masquerade as legitimate user, exploit local vulnerability, exploit operating system vulnerability, exploit other software vulnerability, "eavesdropping", planting of malware
3. Need for Defense — Business value of stolen IP, business liability for loss of customer data, cost of business interruption due to denial of service attack, cost of ransomware, implications for share price, personal implications for senior officers and board members due to fiduciary responsibility for oversight of critical operations
4. Mechanism of defense — encryption, operating system software defense, threat monitoring systems, firewalls, networking security, cloud security
5. Local policy and human defenses, including authentication and multiple-level authentication, with a stronger emphasis on policy and on employees' compliance with policy
6. Legal issues, including national policy obligations, fiduciary responsibility, data residence and data sovereignty
7. Legal issues associated with vulnerabilities the company creates for its customers through incomplete security in its smart devices built for the internet of things
8. Other topics, including cyberwarfare

SECTION 4
Curriculum Survey of Potential Cyber Security and Cyber Privacy Course Offerings: What *Is* Taught, What *Should be* Taught, and *to Which* Students

Section 4 provides the text of our survey instrument.

Topic 1: **Type of Threat**
→ Denial of service, theft of IP, theft of personnel information, theft of customer ID information, destruction of local information (RansomWare), phishing and other forms of exploiting human weakness

1. Should "Type of Threat" be taught to business students?
    a. Yes
    b. No
    c. Unsure
2. If "Type of Threat" is currently part of the curriculum, where is it taught?
    a. Core undergraduate management course
    b. Core graduate management course
    c. Core undergraduate information systems course
    d. Core graduate information systems course
    e. Core undergraduate legal studies course
    f. Core graduate legal studies course
    g. Elective undergraduate information systems course
    h. Elective graduate information systems course
    i. Other (please specify)
    j. This topic is not currently included in the curriculum
3. Where should "Type of Threat" ideally be taught?
    a. Core undergraduate management course
    b. Core graduate management course
    c. Core undergraduate information systems course
    d. Core graduate information systems course
    e. Core undergraduate legal studies course
    f. Core graduate legal studies course
    g. Elective undergraduate information systems course
    h. Elective graduate information systems course
    i. Other (please specify)
    j. This topic does not need to be taught to business students at this time

Topic 2: **Mechanism of Attack**
→ Masquerading as legitimate user, exploiting local vulnerability, exploiting operating system vulnerability, exploiting other software vulnerability, "eavesdropping"/wiretapping, planting of malware, hacking into cloud vendor

4. Should "Mechanism of Attack" be taught to business students?
    a. Yes
    b. No
    c. Unsure
5. If "Mechanism of Attack" is currently part of the curriculum, where is it taught?
    a. Core undergraduate management course
    b. Core graduate management course
    c. Core undergraduate information systems course
    d. Core graduate information systems course
    e. Core undergraduate legal studies course
    f. Core graduate legal studies course
    g. Elective undergraduate information systems course

h. Elective graduate information systems course
i. Other (please specify)
j. This topic is not currently included in the curriculum

6. Where should "Mechanism of Attack" ideally be taught?
    a. Core undergraduate management course
    b. Core graduate management course
    c. Core undergraduate information systems course
    d. Core graduate information systems course
    e. Core undergraduate legal studies course
    f. Core graduate legal studies course
    g. Elective undergraduate information systems course
    h. Elective graduate information systems course
    i. Other (please specify)
    j. This topic does not need to be taught to business students at this time

Topic 3: **Need for Defense**

→ Business value of stolen IP, business liability for loss of customer data, cost of business interruption due to denial of service attack, cost of ransomware payments, implications for share price, personal implications for senior officers and board members due to fiduciary responsibility for oversight of critical operations

7. Should "Need for Defense" be taught to business students?
    a. Yes
    b. No
    c. Unsure
8. If "Need for Defense" is currently part of the curriculum, where is it taught?
    a. Core undergraduate management course
    b. Core graduate management course
    c. Core undergraduate information systems course
    d. Core graduate information systems course
    e. Core undergraduate legal studies course
    f. Core graduate legal studies course
    g. Elective undergraduate information systems course
    h. Elective graduate information systems course
    i. Other (please specify)
    j. This topic is not currently included in the curriculum
9. Where should "Need for Defense" ideally be taught?
    a. Core undergraduate management course
    b. Core graduate management course
    c. Core undergraduate information systems course
    d. Core graduate information systems course
    e. Core undergraduate legal studies course
    f. Core graduate legal studies course
    g. Elective undergraduate information systems course
    h. Elective graduate information systems course
    i. Other (please specify)
    j. This topic does not need to be taught to business students at this time

Topic 4: **Mechanism of Defense**

→ Encryption, operating system software defenses, active real-time threat monitoring systems, passive after-the-fact threat monitoring, firewalls, networking security, cloud security

10. Should "Mechanism of Defense" be taught to business students?
    a. Yes

b. No
c. Unsure

11. If "Mechanism of Defense" is currently part of the curriculum, where is it taught?
    a. Core undergraduate management course
    b. Core graduate management course
    c. Core undergraduate information systems course
    d. Core graduate information systems course
    e. Core undergraduate legal studies course
    f. Core graduate legal studies course
    g. Elective undergraduate information systems course
    h. Elective graduate information systems course
    i. Other (please specify)
    j. This topic is not currently included in the curriculum
12. Where should "Mechanism of Defense" ideally be taught?
    a. Core undergraduate management course
    b. Core graduate management course
    c. Core undergraduate information systems course
    d. Core graduate information systems course
    e. Core undergraduate legal studies course
    f. Core graduate legal studies course
    g. Elective undergraduate information systems course
    h. Elective graduate information systems course
    i. Other (please specify)
    j. This topic does not need to be taught to business students at this time

Topic 5: **Local Policy and Human Defenses**

→ Authentication and multiple-level authentication, with a stronger emphasis on policy and on employees' compliance with policy, standards for allowable devices, standards for allowable software, standards for permitting modes of remote connection, standards for virus detection

13. Should "Local Policy and Human Defenses" be taught to business students?
    a. Yes
    b. No
    c. Unsure
14. If "Local Policy and Human Defenses" is currently part of the curriculum, where is it taught?
    a. Core undergraduate management course
    b. Core graduate management course
    c. Core undergraduate information systems course
    d. Core graduate information systems course
    e. Core undergraduate legal studies course
    f. Core graduate legal studies course
    g. Elective undergraduate information systems course
    h. Elective graduate information systems course
    i. Other (please specify)
    j. This topic is not currently included in the curriculum
15. Where should "Local Policy and Human Defenses" ideally be taught?
    a. Core undergraduate management course
    b. Core graduate management course
    c. Core undergraduate information systems course
    d. Core graduate information systems course
    e. Core undergraduate legal studies course
    f. Core graduate legal studies course
    g. Elective undergraduate information systems course

h. Elective graduate information systems course
i. Other (please specify)
j. This topic does not need to be taught to business students at this time

Topic 6: **Legal Issues**

→ National policy obligations, obligations for multinational corporations, obligations imposed by the GDPR (General Data Protection Regulation) in the EU, fiduciary responsibility, data residence and data sovereignty, role of search warrants and Mutual Legal Assistance Treaties, establishing jurisdiction for data in the cloud, and recent efforts in some jurisdictions to criminalize online activities like operating a website that permits hate speech

16. Should "Legal Issues" be taught to business students?
    a. Yes
    b. No
    c. Unsure
17. If "Legal Issues" is currently part of the curriculum, where is it taught?
    a. Core undergraduate management course
    b. Core graduate management course
    c. Core undergraduate information systems course
    d. Core graduate information systems course
    e. Core undergraduate legal studies course
    f. Core graduate legal studies course
    g. Elective undergraduate information systems course
    h. Elective graduate information systems course
    i. Other (please specify)
    j. This topic is not currently included in the curriculum
18. Where should "Legal Issues" ideally be taught?
    a. Core undergraduate management course
    b. Core graduate management course
    c. Core undergraduate information systems course
    d. Core graduate information systems course
    e. Core undergraduate legal studies course
    f. Core graduate legal studies course
    g. Elective undergraduate information systems course
    h. Elective graduate information systems course
    i. Other (please specify)
    j. This topic does not need to be taught to business students at this time

Topic 7: **Internet of Things Legal Issues**

→ Responsibility for vulnerabilities the company creates for its customers through incomplete security in its smart devices built for the internet of things, privacy regulations recording, analyzing, and using voice data captured through smart devices

19. Should "Internet of Things Legal Issues" be taught to business students?
    a. Yes
    b. No
    c. Unsure
20. If "Legal Issues" is currently part of the curriculum, where is it taught?
    a. Core undergraduate management course
    b. Core graduate management course
    c. Core undergraduate information systems course
    d. Core graduate information systems course
    e. Core undergraduate legal studies course
    f. Core graduate legal studies course

g. Elective undergraduate information systems course
h. Elective graduate information systems course
i. Other (please specify)
j. This topic is not currently included in the curriculum

21. Where should “Legal Issues” ideally be taught?
    a. Core undergraduate management course
    b. Core graduate management course
    c. Core undergraduate information systems course
    d. Core graduate information systems course
    e. Core undergraduate legal studies course
    f. Core graduate legal studies course
    g. Elective undergraduate information systems course
    h. Elective graduate information systems course
    i. Other (please specify)
    j. This topic does not need to be taught to business students at this time

SECTION 5
Employer Survey of Potential Cyber Security and Cyber Privacy Areas of Competence:

What Should Students be Taught, to Prepare for Entry-Level Positions in a Range of Functional Areas and a Range of Businesses

We assume that employers will increasingly require future hires to possess a range of skills in the areas of Cyber Security and Cyber Privacy. Moreover, we assume that the sets of skills required will differ across different job descriptions and different functional areas. We consider entry level positions in the following areas:

- General management
- Strategy
- eCommerce and customer-focused applications development
- Internal information systems
- Legal / Compliance
- Public relations / Shareholder relations
- Marketing

First, general questions about your company:

1. Size / Number of Employees
    a. Xxx // <<we will need to divide into reasonable brackets>>
    b. Xxx
    c. Xxx
    d. Xxx
    e. Xxx
    f. Xxx

2. Size / Annual Revenue
    a. Xxx // <<we will need to divide into reasonable brackets>>
    b. Xxx
    c. Xxx
    d. Xxx
    e. Xxx
    f. Xxx

3. Recruiting / Average number of MBA students hired annually
    a. Xxx // <<we will need to divide into reasonable brackets>>
    b. Xxx
    c. Xxx
    d. Xxx

4. Recruiting / Average number of undergraduate business students hired annually
    a. Xxx // <<we will need to divide into reasonable brackets>>
    b. Xxx
    c. Xxx
    d. Xxx

5. Industry / Sector [Check all that apply] // <<is this the right list of sectors?>>
    a. Travel (air, rail) // <<or should we just ask for industry codes?>>
    b. Hospitality (hotels, restaurants, resorts, cruise ships)
    c. Transportation, shipping, warehousing

d. Retail banking / credit cards / insurance
e. Commercial banking / investment management / wealth management
f. Retailing
g. Manufacturing / fast moving consumer products
h. Manufacturing / consumer durables
i. Manufacturing / commercial durables
j. Energy
k. Chemicals
l. Software development
m. Other professional services
n. Web services
o. Health care
p. Education
q. Other services

Topic 1: **Type of Threat**
→ Denial of service, theft of IP, theft of personnel information, theft of customer ID information, destruction of local information (RansomWare), phishing and other forms of exploiting human weakness

22. Should "Type of Threat" be taught to business students?
    a. Yes
    b. Yes / To some students pursuing some careers
    c. No
    d. Unsure
23. If you answered "yes" or "yes to some" to the previous question, which functional areas within your firm would require this awareness? Check all that apply:
    - General management
    - Strategy
    - eCommerce and customer-focused applications development
    - Internal information systems
    - Legal / Compliance
    - Public relations / Shareholder relations
    - Marketing

Topic 2: **Mechanism of Attack**
→ Masquerading as legitimate user, exploiting local vulnerability, exploiting operating system vulnerability, exploiting other software vulnerability, "eavesdropping"/wiretapping, planting of malware, hacking into cloud vendor

24. Should "Mechanism of Attack" be taught to business students?
    a. Yes
    b. Yes / To some students pursuing some careers
    c. No
    d. Unsure
25. If you answered "yes" or "yes to some" to the previous question, which functional areas within your firm would require this education? Check all that apply:
    - General management
    - Strategy
    - eCommerce and customer-focused applications development
    - Internal information systems
    - Legal / Compliance
    - Public relations / Shareholder relations
    - Marketing

Topic 3: **Need for Defense**

→ Business value of stolen IP, business liability for loss of customer data, cost of business interruption due to denial of service attack, cost of ransomware payments, implications for share price, personal implications for senior officers and board members due to fiduciary responsibility for oversight of critical operations

26. Should "Need for Defense" be taught to business students?
    a. Yes
    b. Yes / To some students pursuing some careers
    c. No
    d. Unsure
27. If you answered "yes" or "yes to some" to the previous question, which functional areas within your firm would require this education? Check all that apply:
    - General management
    - Strategy
    - eCommerce and customer-focused applications development
    - Internal information systems
    - Legal / Compliance
    - Public relations / Shareholder relations
    - Marketing

Topic 4: **Mechanism of Defense**

→ Encryption, operating system software defenses, active real-time threat monitoring systems, passive after-the-fact threat monitoring, firewalls, networking security, cloud security

28. Should "Mechanism of Defense" be taught to business students?
    a. Yes
    b. Yes / To some students pursuing some careers
    c. No
    d. Unsure
29. If you answered "yes" or "yes to some" to the previous question, which functional areas within your firm would require this education? Check all that apply:
    - General management
    - Strategy
    - eCommerce and customer-focused applications development
    - Internal information systems
    - Legal / Compliance
    - Public relations / Shareholder relations
    - Marketing

Topic 5: **Local Policy and Human Defenses**

→ Authentication and multiple-level authentication, with a stronger emphasis on policy and on employees' compliance with policy, standards for allowable devices, standards for allowable software, standards for permitting modes of remote connection, standards for virus detection

30. Should "Local Policy and Human Defenses" be taught to business students?
    a. Yes
    b. Yes / To some students pursuing some careers
    c. No
    d. Unsure

31. If you answered "yes" or "yes to some" to the previous question, which functional areas within your firm would require this education? Check all that apply:
    - General management
    - Strategy
    - eCommerce and customer-focused applications development
    - Internal information systems
    - Legal / Compliance
    - Public relations / Shareholder relations
    - Marketing

Topic 6: **Legal Issues**

→ National policy obligations, obligations for multinational corporations, obligations imposed by the GDPR (General Data Protection Regulation) in the EU, fiduciary responsibility, data residence and data sovereignty, role of search warrants and Mutual Legal Assistance Treaties, establishing jurisdiction for data in the cloud, and recent efforts in some jurisdictions to criminalize online activities like operating a website that permits hate speech

32. Should "Legal Issues" be taught to business students?
    a. Yes
    b. Yes / To some students pursuing some careers
    c. No
    d. Unsure
33. If you answered "yes" or "yes to some" to the previous question, which functional areas within your firm would require this education? Check all that apply:
    - General management
    - Strategy
    - eCommerce and customer-focused applications development
    - Internal information systems
    - Legal / Compliance
    - Public relations / Shareholder relations
    - Marketing

Topic 7: **Internet of Things Legal Issues**

→ Responsibility for vulnerabilities the company creates for its customers through incomplete security in its smart devices built for the internet of things, privacy regulations recording, analyzing, and using voice data captured through smart devices

34. Should "Internet of Things Legal Issues" be taught to business students?
    a. Yes
    b. Yes / To some students pursuing some careers
    c. No
    d. Unsure
2. If you answered "yes" or "yes to some" to the previous question, which functional areas within your firm would require this education? Check all that apply:
    - General management
    - Strategy
    - eCommerce and customer-focused applications development
    - Internal information systems
    - Legal / Compliance
    - Public relations / Shareholder relations
    - Marketing

Topic 8: **Fiduciary Responsibility Legal Issues**

→ Fiduciary responsibility and legal liability for harm caused by security breaches, including harm to users from the firm's failure to maintain adequate protection of confidential data, harm to shareholders from loss of value due to the firm's failure to maintain adequate protection of confidential data, penalties from failure to report breaches in a timely fashion, and personal financial and criminal penalties to the firm's officers as a result of the firm's failure to maintain adequate protection of confidential data.

35. Should "Fiduciary Responsibility Legal Issues" be taught to business students?
    a. Yes
    b. Yes / To some students pursuing some careers
    c. No
    d. Unsure
3. If you answered "yes" or "yes to some" to the previous question, which functional areas within your firm would require this education? Check all that apply:
    - General management
    - Strategy
    - eCommerce and customer-focused applications development
    - Internal information systems
    - Legal / Compliance
    - Public relations / Shareholder relations
    - Marketing