











Cybersecurity Law, Standards and Regulations Syllabus (Sample)

-  **Instructor:** Tari Schreider
-  **Phone:** 678.595.2818
-  **Email:** trschreider@gmail.com
-  **Description:** A study of cybersecurity law, standards and regulations from a layman's perspective. This course is essential for students entering the cybersecurity field to understand the legal and regulatory parameters that cybersecurity programs must adhere. This course provides an understanding of US and international cybersecurity law, civil and criminal procedure relating to cybercrime, cyber offense case law, privacy violation defense, and an overview of industry cybersecurity rules and statutes.
-  **Prerequisites:** Prerequisites can be assigned once the course level has been determined.
-  **Required Text:** Building an Effective Cybersecurity Program – Author: Tari Schreider – Publisher: Rothstein Publishing – ISBN: **Print** – 9781944480561, **PDF** – 9781944480585 – **EPUB** – 9781944480578
-  **Duration:** Can be Taught as an 8- or 16-Week Course
-  **Class Length:** One or Two 90-minute Classes Held Weekly
-  **Credits:** 3 Credits
-  **Overview:** In this course, you will study how to comply with legal and regulatory requirements from a Chief Information Security Officer's (CISO) perspective.
- The course is designed to guide students through the intricacies of securing information and assets according to government and industry cybersecurity acts, rules and regulations.

The course includes a review of infamous cybercrimes, an overview of the basic elements of criminal and civil law, legal enforcement mechanisms, an analysis of data breach lawsuits, and doctrines related to duty of care, warn and act.

Students will learn the rules of criminal procedure applicable to cybercrimes as well as the legal aspects of cryptography and digital forensics. Discussions on amendment rights, client privilege and data protection boundaries are used as a background for the students to learn how individual personal rights and privacy may be maintained while protecting an organization.

The course provides strategies of how to defend a company from data breach and shareholder lawsuits. The international perspective of cyberlaw is covered ranging from US foreign policy to the law of the sea and the law of armed conflict.

The course also covers the latest developments in cybersecurity law, cybersecurity treaties and the impact of evolving technology on cyberlaw.



Outcomes:

After completing this course, students should be able to:

- Create a cybersecurity law program applicable to any public or private organization.
- Understand the differences between cybersecurity acts, standards and regulations.
- Understand the four basic elements of criminal law in context of cybersecurity crime.
- Understand the branches of law, jurisdictional boundaries and cybersecurity law enforcement.
- Recommend a legal defense against data breaches or cybercrime civil or criminal proceedings.
- Know which laws apply to international cybercrimes and how the extradition of international cybercriminals occurs.
- Understand how cyber privacy and data protection laws affect the protection of information.
- Know how to protect employee first, fourth and fifth amendment rights while implementing cybersecurity program functionality.
- Understand how international trade pacts and treaties can affect how information is protected.
- Possess a broad understanding of US and international cybersecurity and privacy laws.



Projects:

During the course, students are responsible for the following projects:

▪ Papers:

- **Cybercrime Taxonomy** – Research and create a PowerPoint presentation on examples of bad actor and technology-centric cybercrimes.
- **Cybercrime Case Law** – Develop a position based on caselaw that supports defending against a data breach lawsuit brought by shareholders.
- **Privacy Violation Encounters** – Identify all manner of public privacy monitoring commenting on ways that personal privacy could be violated and callout which laws are meant to protect privacy during everyday encounters.
- **Team Paper** – Team presentations of assigned course project using the cybersecurity law program model.

▪ Case Studies:

- **Data Breach Lawsuit Outcome** – Identify and research a major organization that has experienced a data breach lawsuit detailing their defense and outcomes.
- **Data Privacy Regulatory Compliance** – Select an international public company and create a profile of all the data privacy laws they must comply.
- **Security Standard Compliance Mapping** – Select either the ISO or NIST standards, identify which standards should map to a legal and regulatory statute.
- **Trade Pact Cyberlaw Implications** – Select an international company and a trade pact to report on the impact of the pact on their cybersecurity approach.
- **Tallinn Manual** – Reference the Tallinn Manual in contrast to a recent armed conflict and comment on its applicability.

▪ Labs:

- **Cyber Liability Stress Test** – Identify a company to perform a cyber liability stress test and report the results.
- **Cyber Liability Insurance Policy** – Acquire a sample cyber liability insurance policy and report on the various ways an insurance carrier can void coverage.

- **Cyber Tort Readiness Checklist** – Identify a company to perform a cyber tort readiness checklist and report on results.



Schedule:

The following provides an overview of the 16-week course with associated assignments:

Week	Assignments
1	<p>Topic: Introduction to Cybersecurity Law</p> <p>Readings: As assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ Infamous cybercrimes ○ Cybercrime taxonomy ○ Civil vs criminal offenses <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions ○ Paper – Cybercrime taxonomy
2	<p>Topic: Understanding the Four Basic Elements of Criminal Law</p> <p>Readings: As assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ Branches of law ○ Tort law ○ Cyberlaw enforcement ○ Cyberlaw jurisdiction <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions ○ Lab – Cyber liability stress test
3	<p>Topic: Overview of US Cybersecurity Law</p> <p>Readings: Assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ Overview of US cybersecurity law ○ History of resolving cybersecurity disputes ○ Alternate dispute resolution ○ Data breach lawsuits <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions ○ Case Study – Data breach lawsuit outcome
4	<p>Topic: Legal Doctrine</p> <p>Readings: As assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ Duty of care doctrine ○ Failure to act doctrine ○ Reasonable person doctrine <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions

Week	Assignments
	<ul style="list-style-type: none"> ○ Paper – Cybercrime case law
5	<p>Topic: Procedural Law</p> <p>Readings: Assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ Rules of criminal procedure ○ State computer crime laws ○ False claims act <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions ○ Lab – Cyber liability insurance policy
6	<p>Topic: Data Privacy Law</p> <p>Readings: As assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ Common law of privacy ○ Privacy laws ○ Data breach laws ○ Data breach litigation <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions ○ Case Study – Data privacy regulatory compliance
7	<p>Topic: Personal Liability and Privacy</p> <p>Readings: As assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ Personal liability ○ Directors and officer’s insurance ○ Preemptive liability ○ Whistleblower protections <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions ○ Paper – Privacy violation encounters
8	<p>Topic: Data Encryption Law</p> <p>Readings: As assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ Overview of cryptology ○ Cryptology law ○ State encryption laws ○ International cryptography laws <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions ○ Lab – Cyber tort readiness
9	<p>Topic: Digital Forensics Law</p> <p>Readings: As assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ Preservation orders ○ Digital evidence rules ○ Digital chain of custody ○ Digital evidence spoliation

Week	Assignments
	<ul style="list-style-type: none"> ○ Expert witness testimony <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions ○ Lab – Security stories, SWOT matrix
10	<p>Topic: Acts, Standards and Regulations</p> <p>Readings: As assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ International statutes ○ Domestic statutes ○ Industry statutes <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions ○ Case study – Security standard compliance mapping
11	<p>Topic: Cybersecurity Law Program</p> <p>Readings: As assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ Model and architecture ○ Staffing and roles ○ Policies and procedures ○ Technology <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions ○ Labs – TBD
12	<p>Topic: Cyber Liability Insurance</p> <p>Readings: As assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ Coverage categories ○ Policy restrictions ○ Claim processes <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions ○ Lab – Data breach calculator
13	<p>Topic: Compliance Auditing</p> <p>Readings: As assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ Critical audit matters ○ Internal vs external auditing ○ Auditing standards <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions ○ Lab – Critical audit matter response
14	<p>Topic: Developments in Cybersecurity Law</p> <p>Readings: As assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ Future of cyberlaw ○ Impact of technology on cybersecurity law

Week	Assignments
	<ul style="list-style-type: none"> ○ Future of US cyberlaw <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions ○ Paper – Tallinn Manual
15	<p>Topic: International Cyber and Privacy Law</p> <p>Readings: As assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ US foreign policy on cybersecurity ○ Harmonization of international cyberlaws ○ Cyber treaties and trade pacts ○ Cyberlaw of the sea and space <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions ○ Paper – Trade pact implications on cybersecurity
16	<p>Topic: Team Project Presentations</p> <p>Readings: As assigned in classroom</p> <p>Key Concepts:</p> <ul style="list-style-type: none"> ○ Team presentations of course project using the cybersecurity law program model <p>Assignments:</p> <ul style="list-style-type: none"> ○ Participate in classroom discussions ○ Lab – None



Instructor Notes

The following are important notes for institutions considering incorporating Building an Effective Cybersecurity Program as part of their cybersecurity curriculum:

- The sample syllabus can be used in both an 8-week and 16-week configuration.
- The course can be delivered as a 100-level to Master-level course if required. The emphasis of depth would be applied by the instructor. Labs, case studies and papers can be made more complex to match the course level.
- Papers, case studies and labs are suggestions, many other materials exist within the text to create other projects.
- The total estimated classroom time is 48 hours.
- The total projected study and project time is 48 hours.

 **Support**

Institutions committing to this coursebook would receive the following support:

- Author will guest lecture via Skype on a topic related to the course material for one-hour.
- Author will provide two hours of instructor phone and/or email support during the first semester the course is taught.
- Course delivery materials provided consist of instructor sample syllabus, delivery courseware, activity assignments, and a test bank of 50 questions.