Class Three: Cyber Security

In our third class we are going to cover fundamental concepts and principles of cyber security and their application through case studies.

1. Read the following sections of **Cybersecurity Fundamentals, Study Guide, 3rd Edition**, ISACA, ISBN: 978-1-60420-751-4:

   - 1.13 (Information Security Objectives) through 1.15 (Privacy vs Security)
   - 3.2 (Risk Identification, Standards, Frameworks and Industry Guidance) through 3.2.4 (Compliance Sources)
   - 3.4 (Security Controls) through 3.4.6 (Identity and Access Management)
   - 3.4.11 (Application Security) through 3.4.13 (Database Security)

2. Read the **Interagency Guidelines Establishing Information Security Standards** (for small entities), published by the Board of Governors of the Federal Reserve Bank (file attached in Moodle). As reference material, *see also* the FFIEC Information Security Examination Handbook (2016). This handbook is used by federal financial services examiners to review a security program.

3. Skim the **State Data Breach Notification Law Chart** (file attached in Moodle) that describes state breach notification/unauthorized access laws. Look up California and Iowa in the chart and review in more detail.

4. Read the **Zoom Communications** complaint and settlement (files are attached in Moodle). Be prepared to discuss:
   a. What security controls were missing?
   b. What is meant by (1) "commonly known or reasonably foreseeable attacks," (2) "readily available measures to safeguard," and (3) "systematic process[es]?"
   c. Was Zoom deceptive, and if yes, how (use specific facts set forth in the complaint)?
   d. Was Zoom's security program reasonable?

5. Prepare to discuss security issues presented by the **Perfect Grocery** case study (the file is attached in the first week's reading).

6. Optional Reading**,** Chapter 9 (Cybersecurity & Privacy) by Lujo Bauer in **An Introduction to Privacy For Technology Professionals,** Editor, Travis D. Breaux, ISBN: 9781948771917.