Please answer the questions below as fully and completely as you can. Turn in your written answers in class during the next class meeting. As part of this exercise set, you must read the following.

- Ch. 2.5, A Gift of Fire: Privacy
- Ch. 8.1-8.3, A Gift of Fire: Errors, Failures, and Risks

1. List as many kinds of damages software can cause to consumers/users as you can, and for each write down who you think should be responsible for the losses incurred and why. Be specific in the damages by giving concrete scenarios.

2. Do you think that individual software developers should ever be liable for the damages caused by the software they write? Explain your answer and give specific examples.
3. Look over MITRE’s 25 programming practices related to security (http://cwe.mitre.org/top25/) and the more recent top-10 list specifically for web applications (http://cwe.mitre.org/data/definitions/1026.html). For your project, describe all potential issues that could lead to security problems based on the lists.

4. What other security risks not mentioned in Question 3 do you think are a potential issue for your project? You should consider the technology you are using, including services or applications you depend on in addition to languages you are using, and whether there have been issues in the past with these or what potential vulnerabilities exist along with best practices for their use.
5. According to the article *Should Software Companies be Legally Liable for Security Breaches?*¹

“There’s no doubt that liability would make the software industry take security far more seriously. It would also impose immense costs and slow down the pace of innovation drastically.” As quoted by Bruce Schneier in the article, “Today there are no real consequences for having bad security, or having low-quality software of any kind. Even worse, the marketplace often rewards low quality. More precisely, it rewards additional features and timely release dates, even if they come at the expense of quality.”

Describe what is meant by the claim that liability would impose “immense costs and slow down the pace of innovation drastically” and provide an argument for and an argument against this claim.

¹ [https://techcrunch.com/2015/08/06/should-software-companies-be-legally-liable-for-security-breaches/](https://techcrunch.com/2015/08/06/should-software-companies-be-legally-liable-for-security-breaches/)
5. Listen to the NPR report on “cyber insurance”² and read the requirements to become a Licensed Professional Engineer³. While some efforts to create a licensure program for software engineers have been proposed in the past and continue to this day⁴, there are still effectively no requirements to becoming a professional software engineer/developer. As the cost and frequency of security breaches continues, and as more and more devices become reliant on software, do you think the Professional Engineer model will ever be applied to software engineering? Could you imagine such a requirement being imposed by cyber insurance companies (e.g., to be insured a company must hire only licensed software engineers)? Do you think requiring licensure would improve the situation today with security breaches?

---

² [www.npr.org/2015/03/19/393865187/companies-worried-about-hackers-turn-to-cyber-insurance](http://www.npr.org/2015/03/19/393865187/companies-worried-about-hackers-turn-to-cyber-insurance)
³ [www.nspe.org/resources/licensure/what-pe](http://www.nspe.org/resources/licensure/what-pe)
⁴ [theinstitute.ieee.org/career-and-education/career-guidance/licensing-software-engineers-is-in-the-works](http://theinstitute.ieee.org/career-and-education/career-guidance/licensing-software-engineers-is-in-the-works)