Policy Analysis
MS&E 91SI: U.S. National Cybersecurity

Due: December 2nd in class

The final assignment for MS&E 91SI is intended to be an enjoyable, exploratory look at realistic cybersecurity policy decision-making. It consists of two parts: a short written response to a cybersecurity-related legislative proposal and an in-class group presentation and debate on the same topic. You will have a choice between two possible topics that are outlined on the following pages. Unless there is a significant imbalance between the numbers of students who choose each topic, you will be able to write and debate on your preferred issue.

Written Response

Imagine that you are the Legislative Director for a U.S. Senator who must vote for or against the proposed legislation. The Senator has sent you an urgent request for a policy memo and voting recommendation. As a former Silicon Valley executive, the Senator is technology-savvy and understands the text of the legislation, yet does not have the time to analyze the implications of the proposed bill. The Senator is relying on you to provide him with a balanced description of his options and a logical recommendation for action.

Write the Senator a concise 2-page policy memo that describes and weighs the pros and cons of the legislation and concludes with a recommendation for one of three options:

> ***Support the bill.*** If you believe the pros of the legislation outweigh the cons, you may recommend that the Senator vote YES when the bill comes to the floor.
>
> ***Amend the bill (or: conditional support).*** If you believe the bill could be effective if altered but is flawed in its current form, you may suggest that the Senator PROPOSE AN AMENDMENT to the bill, and make his support conditional on the passage of that amendment.
>
> ***Reject the bill.*** If you believe the legislation is fundamentally flawed—the cons outweigh the pros—you may recommend that the Senator vote NO when the bill comes to the floor.

You may assume:

- The Senator is as tech savvy as Keith, Martin or Dan. You will likely not need technical details in your analysis, but you should feel free to include them if you feel the memo would benefit.
- The Senator understands the bill, just not the implications. Include, *at most*, one short paragraph recapping important details of the legislation itself. The vast majority of your memo should be analysis.
- Politics exist, but are not everything. Obviously this scenario leaves out some political realities (e.g. tit-for-tat voting with other Senators), but you should feel free to consider any significant political factors that would weigh into a realistic voting decision (e.g. constituent outcry).

Your memo should:

- Clearly outline the pros and cons of the legislation.

- Take a structured, analytical approach to the problem. For example, consider the following:
    - What are our cybersecurity goals?
    - What actors does the legislation affect?
        - How does it affect them?
        - What other relevant influences and incentives affect them?
    - What technology might be affected by these actors?
        - How might the legislation affect this technology?
    - What other implications (or side effects) might the bill have?
    - Will the legislation bring us closer to our goals? How so?

- Provide a clear voting recommendation. If you propose an amendment, explain what you would amend and how you would amend it. Your analysis should clearly support your recommendation.

In-Class Presentation/Debate

The class will be split into four groups: two for each issue, one of which will argue in support of the legislation and the other which will argue against it. You will receive your groups after expressing a preference for either bill in class on Nov. 22nd.

Each group will have 15 minutes to present, and a short 2 minute rebuttal. After both the pro and con groups for one issue speak, we'll take a brief class poll to decide how our class would vote, along with a short discussion about interesting issues raised, possible amendments, etc.

Your group's presentation may take any form you like: one person may speak or every person may speak; you may use PowerPoint, slides, the whiteboard, or unadulterated dramatic oration—whatever you think will be most effective.

We will provide you with contact information for each member of your group, and you are encouraged to meet outside of class. In addition, groups will have 20 minutes at the beginning of the class period to make any final preparations.

The team with the most convincing argument (regardless of whether the final vote is in favor of their legislative position) will receive a cybersecurity prize. Winners will be selected by a panel of the course staff and celebrity guests.

CASE STUDY 1: Corporate Information Security Accountability Act of 2003 (CISAA)

The bill is sponsored by Rep. Adam Putnam, (R-Fla.), chairman of the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. CISAA would require companies to hire an independent auditor to assess existing information security controls and ensure that they meet basic standards that the SEC has yet to determine. The agency would have 60 days after passage of the bill to come up with specific standards for the audits. Companies would be required "to assess the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems," and "determine the levels of information security appropriate to protect such information and information systems."

(Adapted from Computer World, http://www.computerworld.com/printthis/2003/0,4814,86455,00.html)

More information, including the text of the legislation, is available at: http://msande91si.stanford.edu

CASE STUDY 2: Internet Service Provider Security and Accountability Act of 2004 (ISPSA)

This bill, known popularly as ISPSAA, places requirements on US consumer Internet Service Providers to promptly respond to and block reported attacks originating from their networks. It removes liability on behalf of the service provider when the agreed upon procedures are followed but leaves service providers ignoring ISPAA guidelines potentially open to civil suits. The details of the initiative will be designed and administered by a public-private partnership—specifically, by a combined industry, government, and independent-expert group called the ISP Security Consortium (ISPSC).

More information, including an overview of the legislation, is available at: http://msande91si.stanford.edu