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

Due: December 7 in class

The final assignment for MS&E 91si is intended to be an enjoyable, exploratory look at realistic cybersecurity policy decision-making. With a team of 3-4 classmates, you will debate the merits of a real piece of proposed cybersecurity legislation, and argue a vote for or against the bill.

Scenario

Imagine that you are group of tech-savvy U.S. Congressmen. The proposed bill is coming to a vote on the floor of the House, and you are making a last-ditch effort to ensure the proper fate of the bill. Meanwhile, an opposing group of Congressmen is preparing a similar effort and plans to debate you on the floor.

One team will argue for the bill, the other against. Both groups can propose amendments to the bill—the team arguing for it can propose amendments that would improve it, the team arguing against it can propose amendments that would make it acceptable.

You may assume:

- The other Congressmen attending your debate are as technical as Keith and Martin. You will not necessarily need technical details in your analysis, but you should feel free to include them if you feel the argument would benefit.

- The other Congressmen attending your debate understand the bill, just not the implications. Include, *at most*, one minute (or one slide) recapping important details of the legislation itself. The vast majority of your argument should be analysis.

- Politics exist, but are not everything. Obviously this scenario leaves out some political realities, but you should feel free to consider any significant political factors that would weigh into a realistic voting decision (e.g. constituent outcry).

Your argument 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 affect or 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?

- 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 Debate Format

Each team will have 15 minutes to present an initial argument, and 10 minutes for rebuttal after the other team has spoken.

After the arguments have been presented, we'll take a class poll to decide how our class (as non-Congressmen) would actually vote on the bill, and discuss the interesting issues raised, possible amendments, etc.

The team with the most convincing argument will also receive a prize. Winners will be selected by the course staff and (possible) celebrity guests.

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 30 minutes at the beginning of the class period to make any final preparations.

Bill: 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