A Flood of New Regulations are Coming: Do you have your Lifeboats Ready?

Governments Need to “Do Something”

- Cyber attacks are in the news all the time: High-profile incidents such as the Colonial Pipeline attack have garnered significant media attention.
- Growing Demand for Government Action: Public concern has led to increasing calls for governments to address the issue of cyber attacks.
- New Legislation and Regulations: Numerous entities are contributing to the development of new cybersecurity policies, including:
  - The White House
  - Congress
  - Federal agencies (e.g., SEC, FTC, FDA, DoT, DoE, CISA)
  - State governments (with at least 36 states involved)
  - International governments (e.g., EU, India, Australia, China, Russia)

The question remains: Are these measures effective? Is there room for improvement?

What Types of Regulations are Being Considered?

One of the most active areas for regulations: Incident Reporting

**Advantages:**
- It helps organizations keep track of incidents, reduce future occurrences, identify potential risks, and incentivize organizations to take preventative/corrective measures.

**Challenges:**
- Under-reporting (or over-reporting) due to confidentiality (privacy vs cybersecurity dilemma) and/or regulatory gaps
- Timing differences in regulations (regulatory fragmentation)
- Unclear definition of incident: why report incidents and what to report?

Our Goal

- Identify the feature categories in new regulations
- Identify overlaps between regulations based on common features
- Analyze the likely effectiveness of new regulations
- Help to improve regulations
- Provide direction to organizations navigating the flood of new cybersecurity regulations and the governments enacting them

We welcome your help with this project!

Please share your thoughts, experiences, and insights with us. Send us a note.

Dr. Angelica Marotta amarotta@mit.edu  Dr. Stuart Madnick smadnick@mit.edu