DECISION DOCUMENT - CYBER 9/12, GEORGETOWN STIA STINGERS

Issue: SEAFARER Cargo Management Software Cyber-Attack.

Recommendation: Engage in inter-agency, international, and public-private collaboration to mitigate the immediate threat and prevent the further distribution and impact of the malware.

Policy Alternatives & Analysis:

1. Objective: Lead the mitigation effort via diplomatic means; U.S. government central coordinating agent to share threat information and ongoing mitigations efforts with allies and affected partners.
   Lead & Action: Department of State will lead diplomatic efforts to *bring allies and other partners together* to create a strategic multilateral dialogue to discern the nature of the threat and identify the threat actor. The Office of the Director of National Intelligence (ODNI) will *coordinate intelligence sharing* and vulnerability management with Five Eye partners to rapidly respond to the threat.
   Risk: Potential risk of loss of classified intelligence sources and methods. Diplomacy takes time to execute and domestic political environments can hamper the efficiency of this multi-lateral approach.
   Benefit: A U.S. led comprehensive and holistic policy serves to build an international political platform that contributes to building the international system's cyber resilience.

2. Objective: Immediately work to erode the potential ramifications and avoid escalation of the attack.

   Lead & Action: Deny international ships using BOLH software docking and connection to external networks. *Release an Executive Order* requiring all U.S. flagged vessels using BOLH to 1) implement paper manifest backups, 2) immediately patch or switch software, or if unable 3) stop shipping routes altogether. International flagged ships attempting to dock in the U.S. must also comply.

   Risk: Imposes high economic costs at a domestic and international level since it significantly slows or halts international trading routes. Its unilateral nature could foster diplomatic friction. Benefit: Lowers the threat of importing containers with unknown contents which can put US national security at risk and create bottleneck at ports. The U.S. has the economic heft to lead the international response to confront the threat.

3. Objective: Institute a central coordinating authority for inter-agency collaboration and public-private

   partnership to immediately develop a patch and execute a comprehensive mitigation procedure.

Lead & Action: Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) will lead *coordination between government agencies and private partners* to rapidly develop and deploy a patch for the Windows vulnerability and conduct back-end forensics analysis.
Risk: Potentially time consuming to coordinate which risks more attacks in the interim.
Benefit: Leverage public and private technical know-how to develop a patch. Rapid creation of patch limits economic and political impact of the attack. Forensic analysis enables attribution.

4. Objective: Attribution of attackers for prosecution to deter potential attacks by other actors.
   Lead & Action: The White House and Department of Justice jointly spearheads a public information campaign to "name and shame" the attackers to underscore the *U.S.'s determination to maintain a rules- based international system* that imposes legal costs on actions outside that order.
   Risk: Prosecution must meet high evidentiary thresholds. Sources and methods may be jeopardized in a public trial. Potential diplomatic friction due to public and unilateral nature of the action.
   Benefit: The policy builds a legal and diplomatic framework for the emergence, acceptance, and internalization of norms for the scope of actions that constitute legal behavior in cyberspace.

Justification of Recommended Policy Response:

- Erodes the possibility of long-term exploitation.
- Immediately mitigates economic impact through coordinated use of paper and backup records.
- Provides a comprehensive and holistic approach that provides flexibility as the situation evolves.